FÖRSVARSMAKTEN

Reglemente
Säkerhetstjänst

2021

Reglemente Säkerhetstjänst

R SÄK 2021

REGLEMENTE

Bilder på omslaget: *Ingrid Ärfström/HRC Service Grafisk produktion*
Grafisk bearbetning: *Kim Hakkarainen, Must.*
Produktionsid: *200915-021*
Produktionsformat: Word, A4
Publikationsområde: FMPUBL MUST, 882
Förrådsbeteckning: M7739-353149
Tryck:

VIDAR-handling: **FM2019-26528:3**

Beslut om fastställande av reglemente säkerhetstjänst 2021

Reglemente säkerhetstjänst (R SÄK 2021) fastställs att gälla från och med 2021-01-01.

Publikationens registrerade M-nr är: M7739-353149.

Följande upphävs 2021-01-01:

- Handbok för Försvarsmaktens säkerhetstjänst, Hotbedömning (H Säk Hot), 2006 års utgåva (M7745-734022).
- Handbok för Försvarsmaktens säkerhetstjänst, Grunder (H SÄK Grunder), 2013 års utgåva (M7745-734011).
- Handbok Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (Handbok SUA) (M7739-352025).
- Instruktion avseende kunskapskrav säkerhetstjänst (FM2013-489:1).
- Instruktion avseende säkerhetsprövning (2013-06-18 HKV 10 730:58639).
- Kommentarer till Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd (FM2019-11683:1).
- Direktiv om utformning av sekretessmarkering i Försvarsmakten (2009-06-26 10 812:60437).
- Utformning av sekretessmarkering och säkerhetsskyddsklasser i Försvarsmakten (FM2019-14769:1 och FM2019-14769:2).
- Försvarsmaktens metod för säkerhetsskyddsanalys (FM2020-1146:1).

Publikationen tillgängliggörs genom publicering på intranätet emilia, IS UNDSÄK och www.forsvarsmakten.se. Publikationen distribueras och lagerhålls av FMCL/FBF.

Detta beslut är fattat av generalmajor Lena Hallin. Samråd har skett med FM CIO. I den slutliga handläggningen har som föredragande deltagit informationssäkerhetsspecialist Kim Hakkarainen och avdelningsdirektör Zenobia Rosander.

Lena Hallin
Försvarsmaktens säkerhetsskyddschef

Kim Hakkarainen Zenobia Rosander

Ändringar

Nr	Mom	Omfattning av förändringar i stort	Datum föredragning Beslut av	VIDAR - handling nr
0		Ursprunglig fastställelse	2020-11-25 FM säkerhets-skyddschef	FM2019-26528:3

Mom avser nummer i den rättade versionen.

Ändringar i texten framgår av ändringsmarkör. I de fall rad eller stycke har utgått markeras det med en blankrad och ändringsmarkör.

KOM IHÅG!
Om du läser denna publikation i pappersform – *kontrollera att du har den senaste utgåvan*. Fastställd och gällande utgåva finns alltid publicerad på Försvarsmaktens intranät.

Avvikelserapportering, förslag och behov att förtydliga, ändringar etc. sänds till must-sakk-saks@mil.se. Ange i e-posten att det fråga om R SÄK 2021. Inkommande avvikelser följs upp och återkopplas till berörda.

Förord

Detta reglemente innehåller bestämmelser om den militära säkerhetstjänstens genomförande samt förklaringar av skydd för Försvarsmaktens säkerhetsintressen. Den militära säkerhetstjänstens uppgift är att skydda de säkerhetsintressen som rör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen. Reglementet ska inte förväxlas med reglementen för verksamhetssäkerhet.

I och med den nya säkerhetsskyddslagen, som trädde i kraft den 1 april 2019, har det skett väsentliga förändringar inom alla områden som reglementet beskriver. Exempel på sådana förändringar är säkerhetsskyddsplanering (kapitel 2) och att den fysiska säkerheten ska förebygga skadlig inverkan (kapitel 5). Ett tredje exempel är säkerhetsskyddad upphandling som inte längre benämns SUA, eftersom säkerhetsskyddslagens krav på säkerhetsskyddsavtal gäller från säkerhetsskyddsklass konfidentiell.

Målgruppen för reglementet är säkerhetschefer, signalskyddschefer, it-säkerhetschefer och it-säkerhetsansvariga, personal vid säkerhetsfunktioner på central och regional nivå samt personal vid säkerhetsfunktioner på organisationsenheter inklusive krigsförband.

Reglementet ska följas i fred och under höjd beredskap, inklusive krig.

Reglementet beskriver i alla delar inte *hur* något ska genomföras. Detta kan beskrivas i handböcker (t.ex. hur samtal för säkerhetsprövning kan genomföras), lokala instruktioner eller rutinbeskrivningar som publiceras på emilia. Produktionschefen får besluta reglementen, instruktioner, manualer och handböcker som också beskriver hur något ska genomföras.[1] FM CIO beslutar handböcker för it-verksamhet och informationshantering. Dessa omfattar även tillämpningen av bestämmelser om it-säkerhet respektive informationssäkerhet. FM CIO beslutar även metoder och direktiv för it-verksamhet (inklusive it-säkerhet) och informationshantering (inklusive informationssäkerhet).[2]

Reglementet gäller endast i Försvarsmakten men kan även i tillämpliga delar användas av de myndigheter som Försvarsmakten utövar tillsyn över. Särskilt relevant är de vägledande förklaringarna till Försvarsmaktens föreskrifter om säkerhetsskydd.

Innehållet i denna publikation omfattas inte av sekretess.

[1] 9 kap. 8 § 2 FM ArbO.
[2] 8 kap. 39 § 3 och 4 FM ArbO.

Läsanvisning

Reglementet innehåller bestämmelser för hur militär säkerhetstjänst ska genomföras i Försvarsmakten avseende säkerhetsskyddsplanering (kapitel 2), informationssäkerhet (kapitel 3 och 4), fysisk säkerhet (kapitel 5), personalsäkerhet (kapitel 6), utbildning och övning (kapitel 7), säkerhetsskyddad upphandling (kapitel 8), kontroll och tillsyn (kapitel 9), säkerhetsrapportering (kapitel 10) samt incidenter och avvikelser (kapitel 11). Kapitel delas in i avsnitt. Beslut om avvikelse och undantag från bestämmelser beskrivs i avsnitt 1.10.

Till skillnad från handböcker innehåller reglementet bindande bestämmelser i form av *moment* om ledning och genomförande av, eller förhållningssätt för, militär säkerhetstjänst inom Försvarsmakten. Ett moment numreras löpande per kapitel och texten är kursiverad. För att kunna hänvisa till delar inom ett moment kan krav inom ett moment vara numrerat. Alla moment är även samlade i bilaga 1.

I kapitel 4 om informationssäkerhet i och kring informationssystem beskrivs inte Försvarsmaktens interna bestämmelser om it-säkerhet. Bestämmelserna är framtagna före den nya säkerhetsskyddslagen men gäller i tillämpliga delar. Kapitel 4 kommer att ses över vid ett senare tillfälle.

I reglementet förekommer förkortningar, dessa är:

- *FM ArbO* avser Försvarsmaktens interna bestämmelser (FIB 2020:1) med arbetsordning för Försvarsmakten (FM ArbO). Ändrad genom FIB 2020:3.
- *OSL* avser offentlighets- och sekretesslagen (2009:400).
- *OSF* avser offentlighets- och sekretessförordningen (2009:641).
- *Must* avser den militära underrättelse- och säkerhetstjänsten i Högkvarteret.
- *HKV LEDS JUR* avser den juridiska avdelningen vid ledningsstaben i Högkvarteret.

I övrigt förklaras förkortningar första gången de nämns eller i begreppsförklaringen på sidan 336 om de inte är definierade i den löpande texten.

Med *enhet i Högkvarteret* avses i detta reglemente ledningsstaben, produktionsledningen, insatsledningen respektive militära underrättelse- och säkerhetstjänsten.[3]

Med *säkerhetsprövningssektionen* avses säkerhetsprövningssektionen vid Must.

I reglementet förklaras *författningskrav* inom den militära säkerhetstjänstens område, främst bestämmelser om säkerhetsskydd (bild 0.1). Författningskrav återges kursiverade i citatrutor. Även utdrag ur regeringens regleringsbrev återges i citatrutor. Citatrutorna måste läsas eftersom innehållet inte återges i text utanför rutorna. I källförteckningen framgår vilka författningar som omnämns i reglementet.

[3] De enheter som ska ha en säkerhetschef enligt 1 kap. 8 § Försvarsmaktens interna bestämmelser om säkerhetsskydd.

REGLEMENTE

För bestämmelser i lag har *vägledande förklaringar* hämtats från propositioner. Den förklarande texten återges direkt under respektive ruta. Hänvisning till propositionstext finns som fotnot. Sådana förklaringar kan innehålla begrepp som avviker från begrepp som används i Försvarsmakten.

Vägledande förklaringar under rutor med författningstext från Försvarsmaktens föreskrifter om säkerhetsskydd är hämtade från *Kommentarer till Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd* (FM2019-11683:1). Vissa justeringar har dock gjorts.

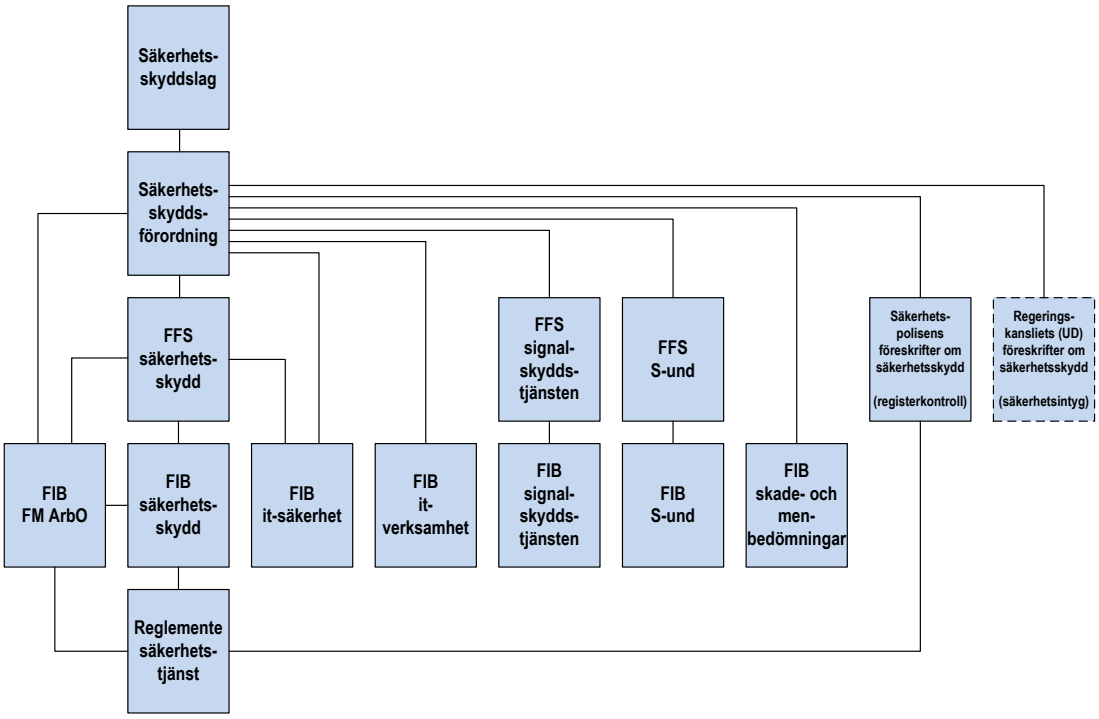


Bild 0.1. Struktur för styrdokument med bestämmelser om säkerhetsskydd som gäller i Försvarsmakten. Streckad ruta avser författning som ännu inte är beslutad. Kim Hakkarainen/Försvarsmakten

Innehåll

1. Militär säkerhetstjänst

1.1. Grunder

Försvarsmakten ska enligt regeringen särskilt leda och bedriva militär säkerhetstjänst samt leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information.[4]

> *”Den militära säkerhetstjänstens uppgift är att skydda de säkerhetsintressen som berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen.”*
>
> Ur riktlinjer för den militära säkerhetstjänsten i regleringsbrevet för Försvarsmakten

Regeringens riktlinjer för den militära säkerhetstjänsten finns i regleringsbrevet för Försvarsmakten.[5] Begrepp och beskrivningar i riktlinjerna har inte reviderats efter den nya säkerhetsskyddslagen. I Doktrintillägg underrättelse- och säkerhetstjänst 2019 (DTLG UNDSÄK 19) beskrivs militär säkerhetstjänst ytterligare och sätts i ett sammanhang med militär underrättelsetjänst. Den militära säkerhetstjänsten består av *säkerhetsunderrättelsetjänst*, *säkerhetsskyddstjänst* och *signalskyddstjänst*.[6] [7] Dessa beskrivs i doktrintillägget.

Försvarsmaktens inriktning av underrättelse- och säkerhetstjänsten (FM INRI US) som beslutas av överbefälhavaren, utgör en årlig inriktning för chefen för Must.[8] [9] Chefen för Must inriktar militär säkerhetstjänst inom ramen för FM INRI US.

Det är chefen för Must som leder militär säkerhetstjänst.[10] Chefen för Must får besluta militära säkerhetstjänstens direktiv.[11]

Chefen för Must är *Försvarsmaktens säkerhetsskyddschef*[12] som kontrollerar att Försvarsmaktens verksamhet bedrivs i enlighet med vad som föreskrivs i säkerhetsskyddslagen och säkerhetsskyddsförordningen.[13] Försvarsmaktens säkerhetsskyddschef är direkt underställd överbefälhavaren och ska stödja Försvarsmaktens ledningsgrupp (FML) i strategiska frågor rörande säkerhetsskydd.[14] [15] Chefen för Must utser ersättare för Försvarsmaktens säkerhetsskyddschef och vid behov biträdande

[4] 3 b § andra och tredje punkterna förordningen (2007:1266) med instruktion för Försvarsmakten.
[5] Bilaga 4 till Regleringsbrev för budgetåret 2020 avseende Försvarsmakten, 2019-12-19.
[6] Bilaga 4 till Regleringsbrev för budgetåret 2020 avseende Försvarsmakten, 2019-12-19.
[7] 11 kap. 1 § första stycket andra meningen FM ArbO.
[8] 4 kap. 2 § andra stycket FM ArbO.
[9] 6 kap. 1 § 2 FM ArbO.
[10] 11 kap. 1 § första stycket första meningen FM ArbO.
[11] 11 kap. 12 § 1 FM ArbO.
[12] 11 kap. 19 § första stycket FM ArbO.
[13] 2 kap. 2 § säkerhetsskyddsförordningen.
[14] 3 kap. 11 § FM ArbO.
[15] 11 kap. 20 § 2 FM ArbO.

säkerhetsskyddschef.[16] Ställföreträdande chefen för Must ersätter chefen för Must som Försvarsmaktens säkerhetsskyddschef. Chefen för säkerhetskontoret vid Must är Försvarsmaktens biträdande säkerhetsskyddschef.

Uppgifter och bemyndiganden för Försvarsmaktens säkerhetsskyddschef finns i 11 kap. FM ArbO och Försvarsmaktens interna bestämmelser om säkerhetsskydd. Försvarsmaktens säkerhetsskyddschef får inom Högkvarteret besluta direktiv om åtgärder rörande säkerhetsskydd.[17]

Chefen för Must är *Försvarsmaktens signalskyddschef*[18] och lyder under Försvarsmaktens säkerhetsskyddschef avseende signalskyddstjänsten. Chefen för Must utser ersättare för Försvarsmaktens signalskyddschef och vid behov biträdande signalskyddschef.[19] Ställföreträdande chefen för Must ersätter chefen för Must som Försvarsmaktens signalskyddschef. Chefen för säkerhetskontoret vid Must är Försvarsmaktens biträdande signalskyddschef.

Försvarsmaktens säkerhetsskyddschef och Försvarsmaktens signalskyddschef stöds av Musts säkerhetskontor.

Regional säkerhetstjänst leds av insatschefen i Högkvarteret och omfattar signalskyddstjänst, säkerhetsskyddstjänst och säkerhetsunderrättelsetjänst.[20] Uppgiften innebär att samordna militära och civila resurser för militär verksamhet enligt bl.a. direktiv från Försvarsmaktens säkerhetsskyddschef.[21] I samband med operationer leder och samordnar insatschefen signalskyddstjänst, säkerhetsskyddstjänst och säkerhetsunderrättelsetjänst.[22]

Chef för en militärregion leder regional säkerhetstjänst inom egen militärregion.[23]

Vid varje organisationsenhet ska det finnas en *säkerhetschef* som, direkt underställd chefen för organisationsenheten, leder och samordnar säkerhetsskyddsarbetet vid organisationsenheten.[24] En säkerhetschef ska även leda och samordna det skydd som ska finnas för sekretessklassificerade uppgifter.[25] Befattningen säkerhetschef ska inte förväxlas med säkerhetsskyddschef. Försvarsmakten har endast en säkerhetsskyddschef.

Vid varje organisationsenhet och krigsförband ska det finnas en *signalskyddschef*.[26]

---

[16] 11 kap. 19 § tredje stycket FM ArbO.
[17] 11 kap. 20 § 7 FM ArbO.
[18] 11 kap. 6 a § första stycket FM ArbO.
[19] 11 kap. 6 a § andra stycket FM ArbO.
[20] 10 kap. 4 § första stycket FM ArbO.
[21] 10 kap. 4 § andra stycket FM ArbO.
[22] 10 kap. 4 § tredje stycket FM ArbO.
[23] 15 kap. 1 § första stycket FM ArbO.
[24] 1 kap. 8 § första stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd.
[25] 1 kap. 5 § Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
[26] 14 § Försvarsmaktens interna bestämmelser om signalskyddstjänsten.

Vid varje organisationsenhet ska det finnas en *it-säkerhetschef* som leder och samordnar it-säkerhetsarbetet direkt under säkerhetschefen.[27] Det kan även finnas *biträdande it-säkerhetschefer* på andra platser än den där enheten huvudsakligen är lokaliserad.[28] Flera organisationsenheter kan också ha samma it-säkerhetschef. Det kan dock vara olämpligt med hänsyn till behov och verksamheternas komplexitet.

För en övning, ett projekt eller verksamhet kan det finnas ett behov av att utse en säkerhetschef, signalskyddschef eller en it-säkerhetschef. Ett sådant behov kan t.ex. identifieras i en särskild säkerhetsskyddsanalys. Om sådana chefer utses ska säkerhetsorganisation och lydnadsförhållanden regleras särskilt.[29]

Militär säkerhetstjänst bedrivs på lokal, regional och central nivå. *Försvarsmaktens säkerhetsorganisation* är i detta reglemente ett samlingsnamn för den militära säkerhetstjänstens organisation, inklusive befattningar, oavsett nivå.

Avseende säkerhetstjänst inom Högkvarteret lyder chefen för ledningsstaben, produktionschefen, insatschefen, chefen för Must, chefen för specialförbanden, chefen för internrevisionen, chefen för säkerhetsinspektionen, försvarsinspektören för hälsa och miljö och flygsäkerhetsinspektören under chefen för Högkvarteret.[30]

> *”I Högkvarteret ska det även finnas en säkerhetschef vid ledningsstaben, produktionsledningen, insatsledningen respektive militära underrättelse- och säkerhetstjänsten som leder och samordnar*
>
> *1. Högkvarterets säkerhetsskyddsarbete vid respektive enhet, och*
>
> *2. det säkerhetsskyddsarbete som ska bedrivas i den verksamhet som respektive enhet ansvarar för.”*
>
> 1 kap. 8 § tredje stycket
> Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Bestämmelsen hindrar inte att det även finns andra säkerhetschefer i Högkvarteret.

Vägledande förklaring till punkten 1: Säkerhetsskyddsarbetet inom organisationsenheten Högkvarteret leds och samordnas av Högkvarterets säkerhetschef. Säkerhetschef vid de angivna enheterna i Högkvarteret ska leda och samordna Högkvarterets interna säkerhetsskyddsarbete vid respektive enhet. Gränsdragningsfrågor om det interna säkerhetsskyddet vid Högkvarteret kan regleras i t.ex. Högkvarterets arbetsordning. Det kan t.ex. handla om i vilken utsträckning utbildning och säkerhetsprövning ska genomföras av säkerhetssektionen vid HKV STAB.

[27] 1 kap. 8 § första stycket Försvarsmaktens interna bestämmelser om it-säkerhet.
[28] 1 kap. 8 § andra stycket Försvarsmaktens interna bestämmelser om it-säkerhet.
[29] 3 kap. 13 § FM ArbO.
[30] 3 kap. 5 § FM ArbO.

Att det ska finnas säkerhetschefer vid de angivna enheterna i Högkvarteret innebär inte att bestämmelser om en säkerhetsskyddsåtgärd som en organisationsenhet ska vidta, även ska vidtas av enheterna. Ett exempel är att varje organisationsenhet ska föra förteckning över nycklar, kort och koder. Endast av den anledningen att det ska finnas en säkerhetschef vid enheterna innebär inte att enheterna ska föra en sådan förteckning. Enheterna är således inte likställda med organisationsenheter vad gäller säkerhetsskydd.

Vägledande förklaring till punkten 2: Säkerhetschef vid de angivna enheterna i Högkvarteret ska även leda och samordna säkerhetsskyddsarbete *i den verksamhet som respektive enhet ansvarar för*. Det säkerhetsskyddsarbetet ligger utanför vad Högkvarterets säkerhetschef ska leda och samordna.

Ett exempel är att chefen för ledningsstaben ska leda och samordna Försvarsmaktens arbete med forskning och utveckling.[31] Säkerhetschefen vid ledningsstaben ska därför leda och samordna säkerhetsskyddsarbetet i frågor som rör Försvarsmaktens arbete med forskning och utveckling.

Ett annat exempel är att säkerhetsskyddsanalys och säkerhetsskyddsplan ska tas fram vid enheterna.[32] Ett tredje exempel är att FM CIO vid ledningsstaben, produktionschefen och chefen för Must ska kontrollera att en leverantör följer ett ingånget säkerhetsskyddsavtal som någon av dessa har tecknat. Resultat av dessa kontroller ska årligen redovisas för Försvarsmaktens säkerhetsskyddschef.[33]

1.2. Skydd för Försvarsmaktens säkerhetsintressen

Försvarsmaktens säkerhetsintressen omfattar eller kan hänföras till *personal*, *materiel*, *information*, *anläggningar* och *verksamhet*.[34]

Säkerhetskänslig verksamhet är verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktigande internationellt åtagande om säkerhetsskydd.[35]

Det finns verksamhet i Försvarsmakten som uppenbart är säkerhetskänslig, men all verksamhet utgör inte säkerhetskänslig verksamhet. Det finns också verksamheter som stöder säkerhetskänslig verksamhet, men som i sig inte utgör säkerhetskänslig verksamhet. I kapitel 2 beskrivs metod för säkerhetsskyddsplanering där den säkerhetskänsliga verksamheten identifieras. Enligt metoden bryts den analyserade verksamheten ner i *funktioner*, *system* och *anläggningar*. Dessa har i sin tur beroenden till säkerhetsintressena (t.ex. behöver en logistikfunktion bemannas av personal).

Den verksamhet i Försvarsmakten som inte är säkerhetskänslig ska också skyddas, men inte med säkerhetsskydd. Skyddet för sådan verksamhet benämns i detta regle-

[31] 8 kap. 4 § 5 FM ArbO.
[32] 2 kap. 2 § andra stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd.
[33] 8 kap. 40 a §, 9 kap. 6 a § och 11 kap. 16 § FM ArbO.
[34] Bilaga 4 till Regleringsbrev för budgetåret 2020 avseende Försvarsmakten, 2019-12-19.
[35] 1 kap. 1 § första stycket säkerhetsskyddslagen.

mente som *verksamhetsskydd* (bild 1.1). Verksamhetsskydd ska inte förväxlas med verksamhetssäkerhet, som leds av säkerhetsinspektionen, och som lutar sig mot andra regelverk. Begreppet verksamhetsskydd är inte definierat i någon författning, men är vanligt förekommande hos andra myndigheter.

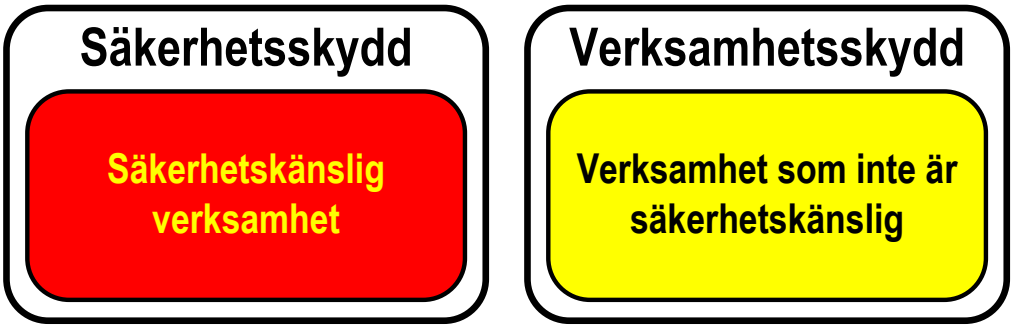


Bild 1.1. Säkerhetsskydd och verksamhetsskydd.

Grunden är att endast säkerhetskänslig verksamhet ska ges ett säkerhetsskydd (bild 1.1).[36] Vissa åtgärder som förknippas med säkerhetsskydd kan även användas för verksamhetsskydd. Ett exempel är att säkerhetsskåp även kan används för förvaring av stöldbegärlig materiel som inte är av någon betydelse för Sveriges säkerhet. Ett annat exempel är att it-säkerhetskomponenter och signalskydd också kan användas för att skydda informationssystem och uppgifter som inte omfattas av krav på säkerhetsskydd. Det är inte förbjudet att använda sådana komponenter och krypton som skyddsåtgärder i verksamhetsskyddet. Om sådana skyddsåtgärder används i verksamhetsskyddet innebär det inte att man ger det ett säkerhetsskydd.

Vissa säkerhetsskyddsåtgärder är exklusiva för säkerhetsskyddet och får inte användas som skyddsåtgärder i verksamhetsskyddet. Ett exempel är placering i säkerhetsklass av befattningar och registerkontroll av personer. Ett annat exempel är säkerhetsskyddsklassificering av uppgifter som inte är säkerhetsskyddsklassificerade.

1.3. Regler för skydd av Försvarsmaktens säkerhetsintressen

Skydd för Försvarsmaktens säkerhetsintressen regleras i flera lagar, bl.a.:

- Offentlighets- och sekretesslagen.
- Säkerhetsskyddslagen.
- Skyddslagen.
- Lagen om skydd för geografisk information.
- Brottsbalken.

Eftersom Försvarsmaktens huvudsakliga uppgifter utgör säkerhetskänslig verksamhet är säkerhetsskyddslagen av stor betydelse för skyddet av Försvarsmaktens säker-

[36] 1 kap. 2 § första stycket säkerhetsskyddslagen.

hetsintressen. I avsnitt 1.7 beskrivs säkerhetsskydd. Kapitel 2-10 i detta reglemente tar i huvudsak upp säkerhetsskydd.

Det finns också bestämmelser i annan lagstiftning som indirekt skyddar säkerhetsintressena. Några exempel är bestämmelser om totalförsvar i miljöbalken och plan- och bygglagen. Försvarsmakten ska lämna uppgifter i skriftlig form till länsstyrelserna om områden som myndigheten bedömer vara av riksintresse för totalförsvarets anläggningar enligt 3 kap. 9 § miljöbalken.[37]

För viss upphandling gäller lagen om upphandling på försvars- och säkerhetsområdet (LUFS). LUFS gäller bl.a. för upphandling av militär utrustning, inklusive alla delar, komponenter och delar av komponenter, byggentreprenader och tjänster särskilt avsedda för militära syften eller byggentreprenader och tjänster av känslig karaktär.[38]

Tillstånd till kamerabevakning krävs inte vid bevakning av vissa skyddsobjekt, enligt kamerabevakningslagen. Det krävs enligt nämnda lag inte heller tillstånd när Försvarsmakten bedriver bevakning från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning.[39]

1.3.1. SAMSÄK

Bestämmelser i lagar både möjliggör och begränsar den militära säkerhetstjänstens verksamhet. Bestämmelser och riktlinjer som är frekvent förekommande inom den militära säkerhetstjänstens verksamhetsområde finns förtecknade i *Sammanställning över bestämmelser och riktlinjer för säkerhetstjänsten* (SAMSÄK). SAMSÄK ges ut årligen och publiceras på Försvarsmaktens myndighetswebb på internet och säkerhetstjänstens samarbetsyta på emilia.[40]

1.4. Legalitet, objektivitet och proportionalitet

”En myndighet får endast vidta åtgärder som har stöd i rättsordningen.

I sin verksamhet ska myndigheten vara saklig och opartisk.

Myndigheten får ingripa i ett enskilt intresse endast om åtgärden kan antas leda till det avsedda resultatet. Åtgärden får aldrig vara mer långtgående än vad som behövs och får vidtas endast om det avsedda resultatet står i rimligt förhållande till de olägenheter som kan antas uppstå för den som åtgärden riktas mot.”

5 § förvaltningslagen (2019:900)

Vägledande förklaring: Även i militär säkerhetstjänst gäller bestämmelserna i förvaltningslagen om legalitet, objektivitet och proportionalitet. 5 § förvaltningslagen

[37] 2 § 12 förordningen (1998:896) om hushållning med mark och vattenområden.
[38] 1 kap. 2 § 1 och 4 lagen om upphandling på försvars- och säkerhetsområdet.
[39] 9 § 2 och 3 kamerabevakningslagen.
[40] Vid fastställandet av detta reglemente gällde ”Sammanställning över bestämmelser och riktlinjer för säkerhetstjänsten (SAMSÄK) 2020” (FM2019-27553:1).

gäller i all verksamhet som en myndighet bedriver, dvs. vid såväl handläggning av och beslutsfattande i enskilda ärenden som s.k. faktiskt handlande. Bestämmelsens första stycke uttrycker *legalitetsprincipen* och innebär att det måste finnas någon form av normmässig förankring för all typ av verksamhet som en myndighet bedriver.[41] Faktiskt handlande innebär att man utför uppgifter som inte är ärenden.

Bestämmelsens andra stycke uttrycker *objektivitetsprincipen* och innebär ett förbud för myndigheterna att låta sig vägledas av andra intressen än dem som de är satta att tillgodose, eller att grunda sina avgöranden på hänsyn till andra omständigheter än sådana som enligt tillämpliga författningar får beaktas vid prövningen av ett ärende. Detta inbegriper även ett krav på respekt för allas likhet inför lagen. En myndighet får alltså inte låta sig påverkas av omständigheter som t.ex. en sökandes etniska bakgrund eller politiska åsikter, om de är ovidkommande. Diskriminering och andra former av obefogad särbehandling är ytterligare exempel på åtgärder som strider mot bestämmelsen.[42]

Bestämmelsens tredje stycke uttrycker den allmänna *proportionalitetsprincip* som har utvecklats genom Högsta förvaltningsdomstolens praxis och innebär ett skydd för enskilda intressen mot en ensidig prioritering av det allmännas önskemål vid myndigheternas agerande. Bestämmelsen ska inte tolkas alltför vidsträckt. Avsikten är t.ex. inte att ställa något krav på myndigheterna att i detalj väga en från allmän synpunkt angelägen åtgärd mot varje tänkbart motstående enskilt intresse. Bestämmelsen tar inte heller sikte på balansen mellan motstridiga allmänna intressen.[43]

Ett exempel är att säkerhetsskyddsåtgärder kan vara kostsamma, effektivitetshämmande och integritetskränkande. Det är viktigt att åtgärderna är proportionerliga och att säkerhetsskyddet inte görs mer omfattande än vad som krävs.

Kravet på rimlighet innebär att det inte får föreligga ett klart missförhållande mellan det allmänna intresset av ett visst ingripande och den belastning som detta medför för den enskilde. Innan myndigheten väger olika intressen mot varandra, måste den ha tagit ställning till om åtgärden uppfyller principens krav på lämplighet och nödvändighet. Det krävs alltså att myndigheten först prövar om den tilltänkta åtgärden kan antas leda till det avsedda resultatet. Myndigheten måste också konstatera att åtgärden är det minst ingripande av de alternativ som finns för att uppnå samma resultat. Bestämmelsen avser inte att hindra myndigheterna från att vidta åtgärder utan avser att säkerställa att de åtgärder som vidtas är proportionella.[44]

1.5. Personuppgiftsbehandling

Den 25 maj 2018 började EU:s dataskyddsförordning att gälla. Försvarsmakten kommer dock, genom en övergångsbestämmelse till lagen (2018:218) med komplet-

[41] Prop. 2016/17:180 s. 289.
[42] Prop. 2016/17:180 s. 290.
[43] Prop. 2016/17:180 s. 290.
[44] Prop. 2016/17:180 s. 290.

terande bestämmelser till EU:s dataskyddsförordning, att i en övergångsperiod fortsatt tillämpa personuppgiftslagen (1998:204).

För personuppgiftsbehandling inom ramen för Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst gäller:

- Lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (PUL UNDSÄK).
- Förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (PUF UNDSÄK).

Must personuppgiftsombud har bl.a. till uppgift att självständigt se till att personuppgifter behandlas på ett lagligt och korrekt sätt. Must personuppgiftsombud är ombud för all behandling i Försvarsmakten som görs med stöd av PUL UNDSÄK.

1.6. Säkerhetsunderrättelsetjänst

”Säkerhetsunderrättelsetjänstens uppgift är att klarlägga och analysera den säkerhetshotande verksamhetens mål, medel och metoder.”

Ur riktlinjer för den militära säkerhetstjänsten i regleringsbrevet för Försvarsmakten

Vägledande förklaring: Säkerhetsunderrättelsetjänst genomförs i stort under liknande arbetsformer som underrättelsetjänst. Skillnaden mellan underrättelse- och säkerhetsunderrättelsetjänst är att den senare primärt tillgodoser underrättelsebehov avseende säkerhetshot mot Försvarsmakten och dess säkerhetsintressen, medan den förstnämnda besvarar övriga underrättelsebehov.

”Försvarsunderrättelseverksamhet skall bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetsarbete. Försvarsunderrättelseverksamheten får endast avse utländska förhållanden.”

1 § första stycket lagen (2000:130) om försvarsunderrättelseverksamhet

Vägledande förklaring: Försvarsunderrättelseverksamhet ska enligt 2 § lagen om försvarsunderrättelseverksamhet fullgöras genom inhämtning, bearbetning och analys av information. Underrättelser rapporteras till berörda myndigheter. I försvarsunderrättelseverksamhet används teknisk och personbaserad inhämtning och samarbete i underrättelsefrågor genomförs med andra länder och internationella organisationer.[45]

[45] 2-3 §§ lagen (2000:130) om försvarsunderrättelseverksamhet.

Försvarsmakten är en av de myndigheter som särskilt ska bedriva försvarsunderrättelseverksamhet.[46] [47] Chefen för Must är bemyndigad att samarbeta med andra myndigheter samt andra länder och internationella organisationer i enlighet med 3 § lagen om försvarsunderrättelseverksamhet.[48]

I Försvarsmakten är det endast Must som bedriver försvarsunderrättelseverksamhet enligt lagen om försvarsunderrättelseverksamhet. I Försvarsmaktens säkerhetsorganisation är det endast säkerhetsunderrättelseavdelningen vid Must som bedriver försvarsunderrättelseverksamhet.

Säkerhetsunderrättelsetjänst beskrivs ytterligare i doktrintillägg underrättelse- och säkerhetstjänst (DTLG UNDSÄK 19). Metoder för säkerhetsunderrättelsetjänst beskrivs inte i detta reglemente.

1.6.1. Hotbedömning

Detta avsnitt behandlar vad som gäller generellt för hotbedömning. Hotbedömning inom ramen för säkerhetsskyddsanalys beskrivs i avsnitt 2.5.5.

En av säkerhetsunderrättelsetjänstens uppgifter är att bedöma hot. Hotbedömning genomförs inte endast av säkerhetsunderrättelsetjänsten, utan behöver göras i nära samverkan med verksamhetsansvariga så att hotbilden blir relevant och anpassad.

Med *hotbild* avses en uppsättning hot som bedöms föreligga mot ett visst skyddsvärde. I avsnitt 2.1 beskrivs indelning av skyddsvärde i säkerhetsskyddsvärde och verksamhetsskyddsvärde.

Med *hot* avses en möjlig oönskad händelse med negativ konsekvens för verksamheten. En sådan verksamhet kan avse säkerhetskänslig verksamhet eller en verksamhet som inte är säkerhetskänslig.

I avsnitt 2.5.5 beskrivs hotbild inom ramen för säkerhetsskyddsplanering. Det som står där är även relevant för hotbilder utanför säkerhetsskyddsplanering.

1.6.2. Hotnivåer

Hotnivån är en samlad bedömning av en eller flera aktörers intention, kapacitet och tillfälle att, i tid och rum, direkt eller indirekt, angripa eller på annat sätt medvetet påverka ett eller flera skyddsvärden. Det viktigaste för en hotbedömning är att mottagaren förstår vad som bedömts och vad detta får för konsekvenser för mottagarens verksamhet. De kunskapsluckor som identifieras under framtagning av en hotbedömning kan arbetas om till underrättelsebehov, vilka kan utgöra grund för egen kompletterande inhämtning alternativt hemställan om information till närmast högre nivå inom Försvarsmaktens säkerhetsorganisation.

[46] 3 b § 1 förordningen (2007:1266) med instruktion för Försvarsmakten.
[47] 2 § förordningen (2000:131) om försvarsunderrättelseverksamheten.
[48] 11 kap. 13 § 2 FM ArbO.

REGLEMENTE

Moment 1:1 *Följande hotnivåer för säkerhetshotande verksamhet ska användas.*

Tabell 1.1. Hotnivåer.

Hotnivå		Betydelse	Färg vid presentation
5	MYCKET HÖGT HOT	Dimensionerande hotaktör har hög intention, kapacitet och tillfälle att agera mot aktuella skyddsvärden. Incidenter inträffar med hög frekvens eller med stor komplexitet. Det kontextuella sammanhanget är ogynnsamt och har stor och sannolikt verksamhetshotande inverkan.	Röd
4	HÖGT HOT	Dimensionerande hotaktör har hög intention, kapacitet och tillfälle att agera mot aktuella skyddsvärden. Incidenter har inträffat vid ett flertal tillfällen i närtid. Det kontextuella sammanhanget är ogynnsamt och har stor men inte verksamhetshotande inverkan.	Orange
3	FÖRHÖJT HOT	Dimensionerande hotaktör har hög intention, kapacitet och tillfälle att agera mot aktuella skyddsvärden. Enstaka incidenter har inträffat. Det kontextuella sammanhanget är ogynnsamt och har stor men inte verksamhetshotande inverkan.	Gul
2	LÅGT HOT	Dimensionerande hotaktör har begränsad intention, kapacitet och tillfälle att agera mot aktuella skyddsvärden. Enstaka incidenter har inträffat, men inte i närtid. Det kontextuella sammanhanget är ogynnsamt men har låg inverkan.	Grön
1	INGET IDENTIFIERAT HOT	Ingen tillgänglig information som tyder på att dimensionerande hotaktör har intention, kapacitet och tillfälle att agera mot aktuella skyddsvärden. Inga incidenter har inträffat. Det kontextuella sammanhanget är inte ogynnsamt.	Vit

1.6.3. Hotkomponenterna intention, kapacitet och tillfälle

Moment 1:2 *I en hotbedömning av säkerhetshot ska hotkomponenterna intention, kapacitet och tillfälle analyseras.*

Vägledande förklaring: Med *intention* avses en aktörs dolda, uttalade eller påvisade vilja att i direkt, indirekt eller i överförd bemärkelse negativt påverka ett specifikt skyddsvärde genom bruk av ett visst offensivt eller defensivt modus operandi.

Kapacitet är ett mått på en aktörs resurser och förutsättningar för att direkt eller indirekt påverka ett specifikt skyddsvärde genom bruk av ett visst offensivt eller defensivt modus operandi.

Tillfälle är en aktörs möjlighet i tid och rum att i direkt, indirekt eller i överförd bemärkelse påverka ett specifikt skyddsvärde genom bruk av ett visst offensivt eller defensivt modus operandi.

Att bedöma dessa tre komponenter räcker normalt för en generell beskrivning av ett hot. För en mer precis och nyanserad analys kan hotkomponenterna i sin tur brytas ner i delkriterier. Dessa beskrivs inte i detta reglemente.

1.6.4. Uttryckssätt vid bedömningar

Moment 1:3 *Följande konfidensgrader ska användas för att uttrycka säkerheten i en hotbedömningen avseende säkerhetshot.*

Tabell 1.2. Konfidensgradernas betydelse. [49]

Konfidensgrad	Betydelse
Bekräftat	Bekräftad information är att betrakta som fakta. Ska inte användas som prognos eller bedömning.
Sannolikt	Avsevärt fler och tyngre faktorer talar till stöd för bedömningen än emot.
Troligen	Fler eller tyngre faktorer talar till stöd för bedömningen än emot.
Möjligen	Endast få och eller svaga faktorer talar till stöd för bedömningen.
Tveksamt	I det närmaste inga faktorer talar till stöd för bedömningen, men det går inte att utesluta.

[49] Försvarsmaktens underrättelsereglemente 2010 (FM UndR 2010), bilaga 1, s. 95.

Konfidensgraderna används även vid andra bedömningar, t.ex. bedömning av händelser som har säkerhetsrapporterats.

Den militära säkerhetstjänsten använder samma konfidensgrader som den militära underrättelsetjänsten. Varje bedömning uttrycker ett ställningstagande. Verbet *bedöms* uttrycker en osäkerhet (men inte graden av osäkerhet) och ska därför inte användas. I syfte att säkerställa att avsändaren och mottagaren har samma uppfattning om kvaliteten på en underrättelse ska bedömningen ges en konfidensgrad och en giltighetstid.

Tabell 1.3. Konfidensgrader med ställningstagande och exempel.

Konfidens-grad	Betydelse	Ställnings-tagande i procent	Exempel
Bekräftat	Bekräftad information är att betrakta som fakta. Ska inte användas som prognos eller bedömning.	> 95 %	Låset vid objekt A är uppbrutet … Individ A befann sig…
Sannolikt	Avsevärt fler och tyngre faktorer talar till stöd för bedömningen än emot.	75-95 %	Aktören X har sannolikt kapacitet att … JAS 39 jaktradar är sannolikt ett prioriterat underrättelsebehov för aktören Y.
Troligen	Fler eller tyngre faktorer talar till stöd för bedömningen än emot.	40-75 %	Organisationen X kommer troligen att med personbaserad inhämtning försöka…
Möjligen	Endast få och eller svaga faktorer talar till stöd för bedömningen.	5-40 %	Aktören Z kommer möjligen att genomföra sabotage riktat mot skyddsvärden av typen Y de närmsta två veckorna…
Tveksamt	I det närmaste inga faktorer talar till stöd för bedömningen, men det går inte att utesluta.	0-5 %	Det är tveksamt om staten X kommer att bedriva subversion mot Försvarsmakten i samband med verksamheten Y…

1.6.5. Kategorier av säkerhetshotande verksamhet

Säkerhetshot och säkerhetshotande verksamhet delas in i följande kategorier:

- Främmande underrättelseverksamhet.
- Kriminalitet.
- Terrorism.
- Sabotage.
- Subversion.

Ett hot eller en verksamhet kan delas in i en eller fler av kategorierna. Kategorierna beskrivs i avsnitten 1.6.5.1-1.6.5.5.

1.6.5.1 Främmande underrättelseverksamhet

Aktörer bedriver, precis som Försvarsmakten, underrättelseverksamhet som stöd för deras beslutfattande. Aktörer kan vara såväl stater som privata aktörer. Syftet med underrättelseverksamhet riktat mot Försvarsmakten och våra skyddsvärden kan t.ex. vara krigsförberedelser, inhämtning av underlag för teknikutveckling eller förberedelser för kriminell verksamhet.

1.6.5.2 Kriminalitet

Kriminalitet som riktas mot Försvarsmakten kan få olika konsekvenser beroende på dess omfattning och vad den riktas mot. Förluster av materiel genom kriminella handlingar får en varierande grad av ekonomiska konsekvenser för Försvarsmakten.

1.6.5.3 Terrorism

”För terroristbrott döms den som begår en gärning som anges i 3 §, om gärningen allvarligt kan skada en stat eller en mellanstatlig organisation och avsikten med gärningen är att

1. injaga allvarlig fruktan hos en befolkning eller en befolkningsgrupp,

2. otillbörligen tvinga offentliga organ eller en mellanstatlig organisation att vidta eller att avstå från att vidta en åtgärd, eller

3. allvarligt destabilisera eller förstöra grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturer i en stat eller i en mellanstatlig organisation.”

2 § första stycket lagen (2003:148) om straff för terroristbrott

Vägledande förklaring: Med terrorism avses i detta reglemente gärningar som räknas upp i 3 § lagen om straff för terroristbrott som uppfyller villkoren för terroristbrott i 2 § första stycket samma lag. *Exempel* på gärningar är mord, dråp, människorov, grov skadegörelse, allmänfarlig ödeläggelse, sabotage, spridande av gift eller smitta, vapenbrott och viss smuggling.

En bedömning om intentionen hos en viss grupp eller syftet bakom en viss gärning är avgörande för att kunna bedöma om ett visst hot faller in under kategorin terrorism. Modus operandi är i sammanhanget av underordnad betydelse. Våldsbrott som inte är terrorism kan fortfarande utgöra ett säkerhetshot, men klassificeras i så fall som kriminalitet.

1.6.5.4 Sabotage

Bestämmelser om straff för *sabotage* finns i 13 kap. 4 § brottsbalken. Sabotage föreligger bl.a. när någon förstör eller skadar egendom som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning eller förvaltning eller för upprätthållande av allmän ordning och säkerhet i riket. Bestämmelsen omfattar även skadegörelse eller annan åtgärd som allvarligt stör eller hindrar den allmänna samfärdseln eller användningen av telegraf, telefon, radio eller dylikt allmänt hjälpmedel eller av anläggning för allmänhetens förseende med vatten, ljus, värme och kraft.[50]

1.6.5.5 Subversion

Subversion är verksamhet som genom spridande av vilseledande eller oriktig information, ofta kompletterat med annan för ändamålet anpassat agerande, syftar till att påverka en specifik målgrupps lägesuppfattning, lojalitet eller förtroende för sin ledning. Kännetecknande för subversion är att syftet är dolt eller att den bakomliggande aktören hålls dold.

Subversion är associerat med, men inte identiskt med påverkansoperationer. Påverkansoperationer[51] är ett vidare begrepp och syftar till att påverka beslut, uppfattningar och beteenden hos en målgrupp.

1.7. Säkerhetsskydd

1.7.1. Vad ska säkerhetsskyddet skydda mot?

> *”Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.”*
>
> 1 kap. 2 § första stycket säkerhetsskyddslagen

Vägledande förklaring: Säkerhetsskyddslagen ska skydda mot i första hand antagonistiska hot, exempelvis spionerі, sabotage och terroristbrott. Skyddet mot terroristbrott avser endast brott enligt 2 § lagen (2003:148) om straff för terroristbrott som kan hota säkerhetskänslig verksamhet. Paragrafen tar även sikte på skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Därmed avses att sådana uppgifter inte bara ska skyddas mot brott. Det kan t.ex. innebära att handlingar ska förvaras på ett

[50] SOU 2015:25 s. 142.
[51] Nomenklatur operationer (NOMEN OP), FM2018-2732:2, 2018-12-14, bilaga 5, s. 13.

betryggande sätt och att spridningen av uppgifter i handlingarna så långt det är möjligt ska begränsas till personer som behöver dem för sin tjänsteutövning. [52]

Spioneribrottet i 19 kap. 5 § brottsbalken beskrivs i avsnitt 1.1 i Handbok Försvarsmaktens säkerhetstjänst Menbedömning (H SÄK Men).

Se avsnitt 1.6.5.4 om brottet *sabotage*.

Med *andra brott* avses brott som kan ge konsekvenser för Sveriges säkerhet, även om detta inte varit brottets primära syfte. Det kan t.ex. röra sig om stöld, dataintrång, olaga intrång eller skadegörelse. Ett exempel är stöld av datorer i ett luftövervakningssystem kan medföra begränsningar i skyddet av Sveriges territorium trots att detta inte var avsikten med stölden.[53]

Säkerhetsskyddsklassificerade uppgifter i en myndighet är uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).[54] Säkerhetsskyddsklassificering beskrivs i avsnitt 3.1.3.

1.7.2. Säkerhetskänslig verksamhet

> *”Denna lag gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet).”*
>
> 1 kap. 1 § första stycket säkerhetsskyddslagen

Vägledande förklaring: Med ”till någon del” avses att det inte krävs att hela verksamheten är säkerhetskänslig för att säkerhetsskyddslagen ska gälla. Säkerhetsskyddslagstiftningen gäller endast för de delar av verksamheten som är säkerhetskänsliga.

Verksamheter som är säkerhetskänsliga karaktäriseras av att de har betydelse för Sveriges säkerhet ur ett nationellt perspektiv. Bild 1.2 visar schematiskt säkerhetskänslig verksamhet och annan verksamhet. Det är de mest skyddsvärda verksamheterna i samhället (pyramidens topp) som ska skyddas med ett säkerhetsskydd.

Även andra verksamheter och andra uppgifter kan behöva ett skydd, men ett sådant skydd är inte ett säkerhetsskydd. Det är därför olämpligt att använda centrala begrepp såsom säkerhetsskydd, säkerhetskänslig verksamhet och säkerhetsskyddsklassificerad uppgift så att de får en annan betydelse än hur de är definierade i säkerhetsskyddslagen. I Försvarsmakten ger vi sådana andra verksamheter och andra uppgifter ett verksamhetsskydd (avsnitt 2.4).

---

[52] Prop. 2017/18:89 s. 134.
[53] Prop. 2017/18:89 s. 50.
[54] 1 kap. 2 § andra stycket säkerhetsskyddslagen.

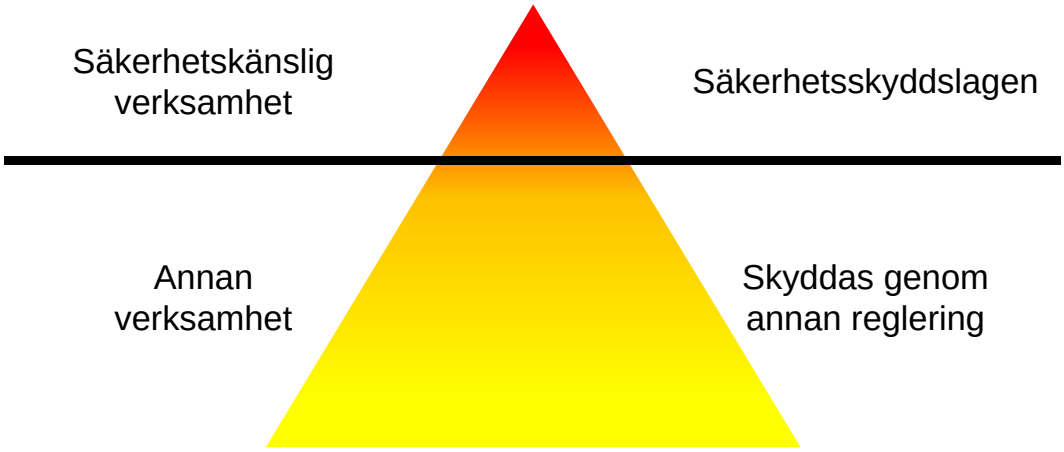


Bild 1.2. Säkerhetsskyddslagen ska skydda Sveriges mest skyddsvärda verksamheter. Bilden ska inte uppfattas som att andra lagar inte gäller för säkerhetskänslig verksamhet.

1.7.3. Sveriges säkerhet

Sveriges säkerhet tar sikte på förhållanden av grundläggande betydelse för Sverige. Det innebär att säkerhetsskyddslagens krav på säkerhetsskydd på samma sätt som tidigare gäller för såväl militär som civil verksamhet. Vilka verksamheter som är av betydelse för att upprätthålla Sveriges säkerhet måste bedömas i ljuset av samhällsutvecklingen. Vad som behöver skyddas för att förebygga hot mot Sveriges säkerhet kan därför i viss utsträckning förändras över tid. Tidigare var uttrycket starkt förknippat med Försvarsmaktens verksamhet, eftersom det främsta hotet mot rikets säkerhet ansågs vara ett militärt angrepp. I dag är samhället och hotbilden mer komplex och föränderlig, vilket i sin tur har fört med sig att uppgifter som rör förhållanden inom andra samhällssektorer också kan vara av betydelse för den nationella säkerheten. Det kan exempelvis gälla uppgifter om viktig civil infrastruktur såsom flygplatser, energianläggningar och förmedlingsstationer för telekommunikation.[55]

Alla delar i en verksamhet som har betydelse för Sveriges säkerhet omfattas av 1 kap. 1 § säkerhetsskyddslagen. Det kan t.ex. röra sig om uppgifter som är säkerhetsskyddsklassificerade med hänsyn till Sveriges säkerhet och som kan finnas i informationssystem eller fysiska handlingar. Det kan också röra sig om personal, fastigheter och andra anläggningar samt informationssystem som inte i första hand behöver skyddas för att de innehåller säkerhetsskyddsklassificerade uppgifter utan för att de är vitala för förmågan att upprätthålla kritiska samhällsfunktioner, t.ex. för Sveriges demokratiska statsskick, rättsväsende eller brottsbekämpande förmåga.[56]

Utgångspunkten för bedömning om en verksamhet är av betydelse för Sveriges säkerhet bör även fortsättningsvis vara uppdelningen i Sveriges yttre och inre säkerhet. En verksamhetsutövare måste därför inledningsvis fråga sig om verksamheten till någon del ryms inom dessa områden. Sveriges *yttre säkerhet* kan delas in i territoriell suveränitet och politisk självständighet. En viktig beståndsdel är den nationella för-

[55] Prop. 2017/18:89 s. 133.
[56] Prop. 2017/18:89 s. 134.

svarsförmågan av Sveriges territorium där Försvarsmakten har huvudansvaret. I den uppgiften ligger att kunna försvara Sverige och främja svensk säkerhet, upptäcka och avvisa kränkningar av det svenska territoriet samt värna om Sveriges suveräna rättigheter och nationella intressen inom Försvarsmaktens verksamhet i sin helhet. Utöver Försvarsmakten finns andra verksamheter, t.ex. inom försvarsindustrin, som är viktiga för det militära försvarets förmåga att utföra sitt uppdrag. Det rör sig exempelvis om verksamheter som bedriver forskning, utveckling och produktion av försvarsmateriel. Sveriges oberoende och handlingsfrihet, politisk självständighet, handlar om att upprätthålla förmågan att förebygga och avvärja brott enligt framför allt spionerilagstiftningen i 19 kap. brottsbalken. Säkerhetspolisen har huvudansvaret för denna uppgift.[57]

Sveriges *inre säkerhet* rör påverkan på förmågan att upprätthålla och säkerställa Sveriges statsidé avseende funktion, handlingsfrihet och oberoende. Säkerhetsskyddet för Sveriges inre säkerhet handlar till stor del om att skydda särskilt kritiska anläggningar, funktioner och informationssystem för Sveriges demokratiska statsskick, rättsväsende eller brottsbekämpande förmåga.[58]

Även så kallad samhällsviktig verksamhet kan bedömas röra Sveriges säkerhet. Verksamheter som både nationellt och internationellt definieras som samhällsviktiga finns ofta inom sektorerna energiförsörjning, livsmedelsförsörjning, elektroniska kommunikationer, vattenförsörjning, transporter och finansiella tjänster. Avgörande för om sådan verksamhet kan anses röra Sveriges säkerhet bör vara om en antagonistisk handling (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra skadekonsekvenser på nationell nivå. Sådana skadekonsekvenser kan t.ex. vara störningar i eller bortfall av leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet ur ett nationellt perspektiv.[59]

En verksamhet kan anses vara av betydelse för Sveriges säkerhet om säkerhetsskyddsklassificerade uppgifter hanteras i verksamheten.[60] Ett exempel är när säkerhetsskyddsklassificerade uppgifter genereras i ett företags verksamhet, utan att det är fråga om en upphandling med säkerhetsskyddsavtal. Ett annat exempel är när en myndighet hanterar en annan myndighets säkerhetsskyddsklassificerade handlingar.

Att begreppet *rikets säkerhet* har bytts ut mot *Sveriges säkerhet* i säkerhetsskyddslagen innebär inte en utökning av lagens tillämpningsområde, utan är en modernisering av språket. Utökningen av tillämpningsområdet finns i andra delar, bl.a. att genom att säkerhetsskyddsåtgärderna även ska förebygga skadlig inverkan.

[57] Prop. 2017/18:89 s. 44.
[58] Prop. 2017/18:89 s. 44.
[59] Prop. 2017/18:89 s. 44.
[60] Prop. 2017/18:89 s. 45.

1.7.4. Internationella åtaganden om säkerhetsskydd

> *”Denna lag gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet).”*
>
> 1 kap. 1 § första stycket säkerhetsskyddslagen

Vägledande förklaring: Med ”som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd” avses uppgifter som är säkerhetskänsliga för andra stater och mellanfolkliga organisationer och som Sverige genom säkerhetsskyddsöverenskommelser har åtagit sig att skydda.[61] Genom sådana överenskommelser förbinder sig även den andra staten eller mellanfolkliga organisationen att ge svenska säkerhetsskyddsklassificerade uppgifter ett säkerhetsskydd.

Överenskommelserna möjliggör att på ett säkert sätt, ömsesidigt utbyta säkerhetsskyddsklassificerade uppgifter mellan två eller flera parter. Överenskommelserna innehåller vanligen en översättningstabell för ländernas eller organisationernas säkerhetsskyddsklasser. De innehåller normalt även bestämmelser om hur information ska överföras mellan avtalsparterna och hur den ska skyddas. Huvudprincipen i överenskommelserna är att parternas ordinarie säkerhetsskyddslagstiftningar i största möjligaste mån ska tillämpas även på den andra partens information. En viktig del av överenskommelsen är vilka åtgärder som parterna ska vidta om säkerhetsskyddsklassificerade uppgifter som härrör från den andra parten förloras eller röjs.

Sverige har i dag ett 35-tal överenskommelser med stater och vissa mellanfolkliga organisationer, bl.a. EU och Nato. Överenskommelser om säkerhetsskydd som är generella, dvs. de omfattar både civil och militär verksamhet, benämns *generella säkerhetsskyddsavtal* (GSA). Överenskommelsen om säkerhetsskydd mellan de nordiska länderna är ett exempel på en sådan generell överenskommelse. Flera säkerhetsskyddsavtal avser dock verksamhet inom försvars- och säkerhetsområdet, däribland forsknings- och materielfrågor.

En förteckning över internationella säkerhetsskyddsåtaganden i form av säkerhetsskyddsavtal mellan Sverige och andra länder samt mellanfolkliga organisationer finns i *Sammanställning över bestämmelser och riktlinjer för säkerhetstjänsten* (SAMSÄK) (avsnitt 1.3.1).

1.7.5. Internationell samverkan om säkerhetsintyg

> *”I lagen finns också bestämmelser om internationell samverkan i övrigt på säkerhetsskyddsområdet.”*
>
> 1 kap. 1 § andra stycket säkerhetsskyddslagen

[61] Prop. 2017/18:89 s. 134.

Vägledande förklaring: Härmed avses framförallt bestämmelserna om säkerhetsintyg för internationella ändamål.

1.7.6. Företräde för vissa bestämmelser i internationellt samarbete

> *”Om det i en överenskommelse som avses i 10 kap. 1 eller 2 §§ regeringsformen som rör ett visst internationellt samarbete förekommer bestämmelser om säkerhetsskydd som avviker från denna författning ska bestämmelserna i avtalet ha företräde.”*
>
> 11 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: I vissa fall förekommer det att säkerhetsskyddsbestämmelser tas in i internationella avtal eller i säkerhetsskyddsavtal mellan två eller flera länder eller mellanfolkliga organisationer. Det är viktigt att Sverige lever upp till de bestämmelser som har avtalats med andra länder och mellanfolkliga organisationer och därför ska säkerhetsskyddsbestämmelser i sådana avtal äga företräde framför bestämmelserna i Försvarsmaktens föreskrifter om säkerhetsskydd. Avvikelserna kan utgöras av såväl minskade som ökade krav på säkerhetsskydd för vissa uppgifter, handlingar eller verksamheter.

Av 10 kap. 1 § regeringsformen (RF) framgår att det är regeringen som ingår överenskommelser med andra stater och mellanfolkliga organisationer. En mellanfolklig organisation är t.ex. Förenta nationerna (FN) och Europeiska unionen (EU). Regeringen har med stöd av 10 kap. 1 § RF ingått ett antal generella säkerhetsskyddsavtal (GSA) med andra länder och mellanfolkliga organisationer. Regeringen får dessutom enligt 10 kap. 2 § RF ge en förvaltningsmyndighet (t.ex. Försvarsmakten eller Försvarets materielverk) i uppdrag att ingå en internationell överenskommelse i en fråga där överenskommelsen inte kräver riksdagens eller Utrikesnämndens medverkan. Ett sådant bemyndigande har t.ex. Försvarsmakten när myndigheten förhandlar och ingår en överenskommelse om en övning med ett annat land, eller ingår en överenskommelse med anledning av en internationell militär insats (t.ex. MINUSMA).

1.7.7. Säkerhetsskyddsplanering

> *”Den som bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska dokumenteras.*
>
> *Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.”*
>
> 2 kap. 1 § första och andra styckena säkerhetsskyddslagen

”Myndighetens säkerhetsskyddsplanering ska innehålla en säkerhetsskyddsanalys och en säkerhetsskyddsplan. Myndigheten ska vartannat år och vid behov utvärdera säkerhetsskyddsplaneringen, inklusive analysen och planen.”

2 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Säkerhetsskyddsplanering är ett samlingsnamn för den process som mynnar ut i konkreta säkerhetsskyddsåtgärder.

Behov av att utvärdera säkerhetsskyddsplaneringen trots att en utvärdering nyligen har gjorts kan t.ex. uppstå i samband med större organisationsförändringar, förändrad verksamhet (som väsentligt påverkar den säkerhetskänsliga verksamheten) eller vid en förändrad hotbild.

Säkerhetsskyddsanalysen ska vara konsekvensdriven och inriktad på skyddsvärden som har betydelse för Sveriges säkerhet.[62] Fokus ska vara på antagonistiska hot som spioneri, sabotage och terrorism samt andra brott som kan hota verksamheten. Andra brott kan t.ex. vara olovlig underrättelseverksamhet och obehörig befattning med hemlig uppgift. Lagen syftar även till att skydda säkerhetskänslig verksamhet mot andra brott som kan ge konsekvenser för Sveriges säkerhet, även om detta inte varit brottets primära syfte, t.ex. dataintrång, skadegörelse, m.m. Ett exempel är en stöld av datorer i ett luftövervakningssystem vilket kan medföra begränsningar i skyddet av Sveriges territorium trots att det inte var avsikten med stölden.[63]

1.7.8. Säkerhetsskyddsåtgärder

I säkerhetsskyddslagen föreskrivs tre säkerhetsskyddsåtgärder: informationssäkerhet, fysisk säkerhet och personalsäkerhet. De tre säkerhetsskyddsåtgärderna samverkar och utgör ett sammanhållet system för skydd av säkerhetskänslig verksamhet.

1.7.8.1 Informationssäkerhet

”Informationssäkerhet ska

1. förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och

2. förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.”

2 kap. 2 § säkerhetsskyddslagen

Vägledande förklaring: *Första punkten* tar sikte på skyddet av säkerhetsskyddsklassificerade uppgifter. Om ett informationssystem ska hantera säkerhetsskyddsklassificerade uppgifter ska informationssystemets säkerhetsfunktioner anpassas för att förebygga att sådana uppgifter obehörigen röjs, ändras, görs otillgängliga eller

[62] Prop. 2017/18:89 s. 56.
[63] Prop. 2017/18:89 s. 50.

förstörs. Förekommer uppgifter som har delats in i olika säkerhetsskyddsklasser enligt 2 kap. 5 § säkerhetsskyddslagen ska systemet vara inrättat med säkerhetsfunktioner som svarar upp mot den högsta skyddsnivån.

Andra punkten tar framför allt sikte på skyddsåtgärder för att tillgodose behov av tillgänglighet och riktighet i fråga om uppgifter och informationssystem som inte utgör eller innehåller säkerhetsskyddsklassificerade uppgifter, men som har avgörande betydelse för t.ex. styrning, reglering och övervakning av för Sverige viktiga samhällsfunktioner inom t.ex. el- och vattenförsörjning, digital infrastruktur och sådana sammanställningar av uppgifter, t.ex. folkbokföringsregistret, som är av grundläggande betydelse för ett fungerande samhälle. Med uppgifter och informationssystem avses i detta sammanhang såväl uppgifter som de tekniska system som används för att i olika avseenden elektroniskt behandla uppgifter.[64]

Avsnitt 3 i detta reglemente beskriver Försvarsmaktens modell för informationsklassificering inklusive säkerhetsskyddsklassificering samt regler för hantering av säkerhetsskyddsklassificerade handlingar och lagringsmedier i Försvarsmakten. I avsnitt 4 beskrivs regler för informationssäkerhet i och kring informationssystem.

> *”Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll ska uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.”*
>
> 3 kap. 5 § andra stycket säkerhetsskyddsförordningen

Se även avsnitt 4.8.9 om skydd mot obehörig avlyssning.

Enligt regeringen syftar säkerhetsskyddstjänst och signalskyddstjänst till att förebygga, förhindra och motverka den säkerhetshotande verksamheten.[65]

Begreppet signalskyddstjänst innefattar *kryptografiska funktioner som är avsedda för att skydda säkerhetskänslig verksamhet*.[66] Bestämmelser om signalskyddstjänst finns i:

- Försvarsmaktens föreskrifter (FFS 2019:9) om signalskyddstjänsten.
- Försvarsmaktens interna bestämmelser (FIB 2008:3) om signalskyddstjänsten.

Signalskyddstjänst beskrivs i Handbok totalförsvarets signalskyddstjänst, grundläggande regler för signalskyddstjänsten (H TST Grunder).

Chefen för Must leder och samordnar totalförsvarets signalskyddstjänst, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information och förhandlar internationella signalskyddsöverenskommelser. Chefen

[64] Prop. 2017/18:89 s. 138.
[65] Bilaga 4 till Regleringsbrev för budgetåret 2020 avseende Försvarsmakten, 2019-12-19.
[66] 1 kap. 2 § Försvarsmaktens föreskrifter om signalskyddstjänsten.

för Must stöder produktionschefen vid utveckling, anskaffning, vidmakthållande och avveckling av säkra kryptografiska funktioner.[67]

Av 2 kap. 2 § säkerhetsskyddslagen (2018:585) och 3 kap. 5 § andra stycket säkerhetsskyddsförordningen (2018:658) följer att kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet utgör en del av säkerhetsskyddsåtgärden informationssäkerhet. Chef för organisationsenhet har ett ansvar för säkerhetsskyddet vid organisationsenheten och måste därför se till att signalskyddstjänst samordnas med annat säkerhetsskyddsarbete.

1.7.8.2 Fysisk säkerhet

> *”Fysisk säkerhet ska*
>
> *1. förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs, och*
>
> *2. förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt som avses i 1.”*
>
> 2 kap. 3 § säkerhetsskyddslagen

Vägledande förklaring: I *första punkten* har det tydliggjorts att fysisk säkerhet inte enbart innebär att förebygga att obehöriga får tillträde till platser utan att åtgärden också kan avse byggnader och anläggningar av olika slag samt objekt, t.ex. fordon. Även delar av t.ex. en anläggning innefattas.

I *andra punkten* har vidare tydliggjorts att åtgärden kan avse också ett skydd mot sådan skadlig inverkan som kan orsakas utan ett obehörigt tillträde. Det skulle t.ex. kunna röra sig om att en kabel för samhällsviktig elektronisk kommunikation skyddas genom ett robust hölje eller larm eller åtgärder för att skydda ett objekt mot obemannade farkoster, t.ex. drönare.[68] Se även avsnitt 1.8 om skyddsobjekt enligt skyddslagen.

Fysisk säkerhet beskrivs i kapitel 5.

1.7.8.3 Personalsäkerhet

Personalsäkerhet ska förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller delta i en verksamhet som av annan anledning är säkerhetskänslig, samt säkerställa att de som deltar i säkerhetskänslig verksamhet har en tillräcklig kunskap om säkerhetsskydd.[69]

---

[67] 11 kap. 6 § FM ArbO.
[68] Prop. 2017/18:89 s. 138-139.
[69] 2 kap. 4 § säkerhetsskyddslagen.

Personalsäkerhet kan vara aktuell vid olika slag av verksamheter, dels vid deltagande i verksamheter där tillgång ges till säkerhetsskyddsklassificerade uppgifter, dels i verksamheter som av annan anledning är säkerhetskänsliga, t.ex. deltagande i verksamhet vid ett skyddsobjekt.

Säkerhetsprövning beskrivs i kapitel 6. Utbildning och övning beskrivs i kapitel 7.

1.7.9. Säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar (S-und)

> *”För särskilda underrättelseuppgifter och särskilda underrättelsehandlingar gäller även Försvarsmaktens föreskrifter om säkerhetsskydd för särskilda underrättelseuppgifter och särskilda underrättelsehandlingar.”*
>
> 1 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen är en upplysning om att särskilda underrättelseuppgifter och särskilda underrättelsehandlingar även omfattas av ett regelverk om särskilt säkerhetsskydd. Regelverket består av:

- Försvarsmaktens föreskrifter om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar.
- Försvarsmaktens interna bestämmelser om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar.

Innehållet i regelverket omfattas av sekretess enligt 15 kap. 2 § OSL.

1.8. Skyddsobjekt enligt skyddslagen

För att ge vissa byggnader, andra anläggningar och områden samt militära fartyg och luftfartyg samt vissa fordon och fordonstransporter ett förstärkt skydd kan dessa beslutas vara skyddsobjekt enligt skyddslagen. Skyddsändamålen är sabotage, terroristbrott, spionerі samt röjande i andra fall av hemliga uppgifter som rör totalförsvaret samt grovt rån. Även allmänheten ska genom skyddslagen skyddas mot skada som kan uppkomma till följd av militär verksamhet. Det förstärkta skyddet består av:

- Förbud för obehörigas tillträde, inklusive tillträde med hjälp av obemannad farkost. Det kan särskilt beslutas om förbud att göra avbildningar (t.ex. fotografera eller rita av) eller beskrivningar eller förbud mot att bada, dyka, ankra eller fiska.
- Bevakning av skyddsobjekt får utföras av skyddsvakt eller polisman. Polisman har de befogenheter som framgår av polislagen. För skyddsvakt gäller de särskilda befogenheter som framgår av skyddslagen. Skyddsvakt har befogenhet att, under vissa förutsättningar, bl.a. undersöka fordon, fartyg och luftfartyg samt genomföra kroppsvisitation, gripa personer och ta föremål i beslag.

Förbudet för obehörigt tillträde med obemannad farkost gäller oavsett om dessa fjärrstyrs i realtid eller om färden sker genom förprogrammering eller användning av

artificiell intelligens. Således omfattas även en autonom farkost. Det spelar vidare ingen roll om farkosten agerar i luften, på land eller i vatten.[70]

Bestämmelser om skyddsobjekt finns i skyddslagen och skyddsförordningen. I Försvarsmaktens skyddsföreskrifter finns bestämmelser om bl.a. utbildning och utrustning av skyddsvakter beträffande Försvarsmaktens personal. Bestämmelser i Försvarsmaktens skyddsföreskrifter om utformningen av skyltar gäller även skyddsobjekt som beslutas av länsstyrelserna.

Handbok Bevakning (H Bev) beskriver olika metoder och synsätt för att lösa bevakningstjänsten.

Försvarsmaktens tillämpning av skyddslagens bestämmelser om beslag beskrivs i beslutet Tillämpning av skyddslagens fotoförbud m.m.[71]

1.9. Skydd för geografisk information

Lagen om skydd för geografisk information ska skydda uppgifter av betydelse för totalförsvaret som omfattas av försvarssekretess.[72] Uttrycket totalförsvar täcker in skyddsvärda intressen avseende såväl militära anläggningar som civila samhällsviktiga anläggningar. Lagen begränsar rätten till sjömätning, fotografering eller liknande registrering från luftfartyg och spridning av en sammanställning av geografisk information. *Geografisk information* avser lägesbestämd information om förhållanden på och under markytan samt på och under sjö- och havsbottnen.[73]

1.9.1. Sjömätning

Betydande delar av den svenska kusten har en unik geografi i form av skärgårdar med stora djup och avsevärda bottentopografiska variationer samt områden med stora mängder av grund. Detta har historiskt utnyttjats som en naturlig del i försvaret av landet och som basområden för egna stridskrafter. Dessa geografiska förhållanden fyller även i dag en viktig funktion för det militära försvaret.[74]

Sjömätning är, med vissa undantag, tillståndspliktig.[75] Försvarsmakten prövar frågor om tillstånd.[76] Tillstånd ska ges om sjömätningen inte kan antas medföra skada för totalförsvaret.[75]

1.9.2. Fotografering eller liknande registrering från luftfartyg

Det är tillåtet att utan tillstånd fotografera eller genomföra liknande registrering (t.ex. laserskanning) från luftfartyg. När det råder höjd beredskap, eller under annan tid som regeringen beslutar med hänsyn till Sveriges försvarsberedskap, får dock foto-

[70] Prop. 2018/19:127 s. 71.
[71] FM2015-12123:1.
[72] Prop. 2015/16:63 s. 19.
[73] 2 § 1 lagen om skydd för geografisk information.
[74] Prop. 2015/16:63 s. 23.
[75] 3 § lagen om skydd för geografisk information.
[76] 2 § förordningen om skydd för geografisk information.

grafering eller liknande registrering från luftfartyg inte utföras utan tillstånd inom eller av restriktionsområden för luftfart.[77] Vilka restriktionsområden som finns framgår i förordningen (2005:801) om restriktioner för luftfart inom vissa områden.

1.9.3. Spridning av geografisk information över sjöterritoriet

Med undantag av insjöar, vattendrag och kanaler är det förbjudet att utan tillstånd sprida en sammanställning av geografisk information om förhållanden i ett visst vattenområde eller en viss sträcka av ett vattenområde som avser Sveriges sjöterritorium.[78]

Frågor om tillstånd till spridning av sammanställningar av geografisk information över sjöterritoriet prövas av Sjöfartsverket.[79] Tillstånd ska ges om spridningen inte kan antas medföra skada för totalförsvaret.[80] Försvarsmakten ska lämna Sjöfartsverket upplysningar som behövs för att verket ska kunna bedöma om spridningen kan antas medföra skada för totalförsvaret. Försvarsmakten ska samråda med Säkerhetspolisen innan uppgifterna lämnas.[81]

Tillstånd till spridning behövs inte om den geografiska informationen har framställts endast med hjälp av fjärranalys från satellit.[82]

1.9.4. Spridning av geografisk information över markterritoriet

Det är förbjudet att utan tillstånd sprida en sammanställning av geografisk information om informationen har inhämtats från luftfartyg genom fotografering eller liknande registrering.[83]

Frågor om tillstånd till spridning av sammanställningar av geografisk information över markterritoriet prövas av Lantmäteriet.[84] Tillstånd ska ges om spridningen inte kan antas medföra skada för totalförsvaret.[85] Försvarsmakten ska lämna Lantmäteriet upplysningar som behövs för att Lantmäteriet ska kunna bedöma om spridningen kan antas medföra skada för totalförsvaret.

Försvarsmakten ska lämna upplysningar om såväl skyddsobjekt som Försvarsmakten har beslutat om, som skyddsobjekt som länsstyrelserna har beslutat om. Länsstyrelserna ska lämna upplysningar till Försvarsmakten om beslut för skyddsobjekt för vilka det råder avbildningsförbud (7 § andra och tredje styckena skyddslagen) som avser objektets utsida, samt vilka uppgifter om skyddsobjektet som har legat till grund för beslutet.[86] Syftet är att Försvarsmakten ska kunna uttala sig om vilka av de

[77] 6 § lagen om skydd för geografisk information.
[78] 9 § första stycket 1 lagen om skydd för geografisk information.
[79] 6 § andra stycket 1 förordningen om skydd för geografisk information.
[80] 9 § tredje stycket lagen om skydd för geografisk information.
[81] 7 § första stycket förordningen om skydd för geografisk information.
[82] 10 § lagen om skydd för geografisk information.
[83] 9 § första stycket 2 lagen om skydd för geografisk information.
[84] 6 § andra stycket 2 förordningen om skydd för geografisk information.
[85] 9 § tredje stycket lagen om skydd för geografisk information.
[86] 5 § andra stycket skyddsförordningen.

civila skyddsobjekten med avbildningsförbud som innehåller uppgifter som omfattas av sekretess enligt 15 kap. 2 § OSL.[87] Försvarsmakten ska samråda med Säkerhetspolisen innan uppgifterna lämnas till Lantmäteriet.[88]

Tillstånd till spridning behövs inte om den geografiska informationen har framställts endast med hjälp av fjärranalys från satellit.[89]

Lantmäteriet har meddelat föreskrifter (LMFS 2016:1) om spridningstillstånd för sammanställningar av landgeografisk information som bl.a. innehåller bestämmelser om undantag från krav på spridningstillstånd.

1.10. Avvikelse eller undantag från bestämmelser

1.10.1. Grunder

Säkerhetsskyddsarbetet måste bedrivas så att det är möjligt att vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.[90] Militär säkerhetstjänst i övrigt måste bedrivas så att det är möjligt att vidta de åtgärder som framgår av momenten i detta reglemente.

Med hänsyn till att det kan finnas olika oförutsedda situationer som kan medföra att det inte är möjligt att följa en bestämmelse, är det rimligt att det finns en möjlighet att medge avvikelse eller undantag.

- Ett beslut om *avvikelse* får fattas av den som i en författning eller ett reglemente har getts ett uttryckligt bemyndigande att under vissa givna förutsättningar kunna besluta att en viss bestämmelse inte behöver följas.
- Ett beslut om *undantag* avser ett beslut om att en viss bestämmelse för ett visst sammanhang inte behöver följas.

Ett exempel på beslut om avvikelse är den möjlighet som chef för organisationsenhet har att, under förutsättning att motsvarande skydd kan upprätthållas, fatta beslut som avviker från krav på förvaringsutrymmen för säkerhetsskyddsklassificerade handlingar eller lagringsmedier (avsnitt 5.3.8).

I en situation där en bestämmelse inte kan följas och möjligheterna att följa bestämmelsen är uttömda, bör stödet för avvikelse först undersökas. Om man finner att det saknas stöd för avvikelse måste stödet för undantag undersökas.

För att kunna medge avvikelse eller undantag från författning eller reglemente måste det finnas stöd i författningen respektive reglementet. Saknas stöd i författningen eller reglementet får avvikelse eller undantag inte medges. Den som beslutar en av-

[87] SOU 2013:51 s. 213-215.
[88] 7 § första stycket förordningen om skydd för geografisk information.
[89] 10 § lagen om skydd för geografisk information.
[90] 2 kap. 1 § andra stycket säkerhetsskyddslagen.

vikelse eller ett undantag måste vara bemyndigad att fatta ett sådant beslut. Ett undantag får heller inte strida mot en bestämmelse i en överordnad författning. Om ett undantag medges måste risken för Sveriges säkerhet vara acceptabel för den som beslutar.

KOM IHÅG!
Det juridiskt möjliga är inte alltid lämpligt ur säkerhetsskyddssynpunkt.

Beslut om avvikelse från bestämmelser i nationell verksamhet beskrivs i avsnitt 1.10.2.

Beslut om avvikelse från bestämmelser i internationell verksamhet beskrivs i avsnitt 1.10.3.

Beslut om undantag från bestämmelser i detta reglemente beskrivs i avsnitt 1.10.4.

Beslut om undantag från bestämmelser i författningar beskrivs i avsnitt 1.10.5.

Moment 1:4 *I en begäran om undantag från en bestämmelse i författning eller reglemente ska det i begäran anges:*

a) Vilken bestämmelse som undantaget rör.

b) Vad anledningen är till varför bestämmelsen inte går att följa.

c) En bedömning av konsekvenser för verksamheten om ett undantag inte medges.

d) En bedömning av sårbarheter till följd av att bestämmelsen inte kan följas.

e) En bedömning om risken för Sveriges säkerhet är acceptabel.

f) När bestämmelsen bedöms vara uppfylld, eller om den inte går att uppfylla.

Vägledande förklaring: Med författning avses t.ex. säkerhetsskyddsförordningen, Försvarsmaktens föreskrifter om säkerhetsskydd och Försvarsmaktens interna bestämmelser (FIB 2020:4) om säkerhetsskydd. Utrymmet att besluta om undantag från bestämmelser i säkerhetsskyddsförordningen är begränsad till bl.a. vissa skyddsåtgärder i informationssystem (avsnitt 4.9 och 4.10).

1.10.2. Avvikelse från bestämmelser i nationell verksamhet

”Insatschefen får inom en uppkommen nationell militär insats, i fråga om verksamhet som syftar till hävdande av Sveriges suveränitet och territoriella integritet, fatta beslut som avviker från Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd samt denna författning, om det är oundgängligen nödvändigt för verksamheten.”

1 kap. 9 § första stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Bestämmelsen avser bl.a. situationer där IKFN-förordningen[91] tillämpas. Avgränsningen innebär att övningsverksamhet inte omfattas.

”Ett sådant beslut ska dokumenteras och, om möjligt, föregås av samråd med Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer. Har sådant samråd inte skett ska Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, snarast underrättas om beslutet.”

1 kap. 9 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 1:5 *Samråd och underrättelse enligt 1 kap. 9 § andra stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd ska ske med säkerhetsskyddsavdelningen vid Must.*

Moment 1:6 *Insatschefen får, i fråga om verksamhet som syftar till hävdande av Sveriges suveränitet och territoriella integritet, fatta beslut som avviker från moment i detta reglemente, om det är oundgängligen nödvändigt för verksamheten.*

Ett sådant beslut ska dokumenteras och, om möjligt, föregås av samråd med säkerhetsskyddsavdelningen vid Must. Har sådant samråd inte skett ska säkerhetsskyddsavdelningen vid Must snarast underrättas om beslutet.

1.10.3. Avvikelse från bestämmelser i internationell verksamhet

”Om det i en överenskommelse som avses i 10 kap. 1 eller 2 §§ regeringsformen som rör ett visst internationellt samarbete förekommer bestämmelser om säkerhetsskydd som avviker från denna författning ska bestämmelserna i avtalet ha företräde.”

11 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

[91] Förordning om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet, m.m. (IKFN-förordning).

”Om det i ett avtal för visst internationellt samarbete förekommer bestämmelser om säkerhetsskydd som avviker från bestämmelserna i denna författning ska bestämmelserna i avtalet ha företräde.”

1 kap. 4 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 1:7 *Om det i ett avtal för visst internationellt samarbete förekommer bestämmelser om säkerhetsskydd som avviker från bestämmelserna i detta reglemente ska bestämmelserna i avtalet ha företräde.*

Vägledande förklaring: I vissa fall förekommer det att säkerhetsskyddsbestämmelser tas in i internationella avtal eller i säkerhetsskyddsavtal mellan två eller flera länder eller mellanfolkliga organisationer. Det är viktigt att Sverige lever upp till de bestämmelser som har avtalats med andra länder och mellanfolkliga organisationer och därför ska säkerhetsskyddsbestämmelser i sådana avtal äga företräde framför bestämmelserna i Försvarsmaktens föreskrifter om säkerhetsskydd, Försvarsmaktens interna bestämmelser om säkerhetsskydd och detta reglemente. Avvikelserna kan utgöras av såväl minskade som ökade krav på säkerhetsskydd för vissa säkerhetsskyddsklassificerade uppgifter och handlingar eller säkerhetskänsliga verksamheter.

Av 10 kap. 1 § regeringsformen (RF) framgår att det är regeringen som ingår överenskommelser med andra stater och mellanfolkliga organisationer. En mellanfolklig organisation är t.ex. Förenta nationerna (FN) och Europeiska unionen (EU). Regeringen får dessutom enligt 10 kap. 2 § RF ge en förvaltningsmyndighet (t.ex. Försvarsmakten eller Försvarets materielverk) i uppdrag att ingå en internationell överenskommelse i en fråga där överenskommelsen inte kräver riksdagens eller Utrikesnämndens medverkan. Ett sådant bemyndigande har t.ex. Försvarsmakten när myndigheten förhandlar och ingår en överenskommelse om en övning med ett annat land, eller ingår en överenskommelse med anledning av en internationell militär insats (t.ex. ISAF eller MINUSMA).

Företrädet får inte medföra att bestämmelser i andra ovanliggande författningar i t.ex. OSL, säkerhetsskyddslagen och säkerhetsskyddsförordningen inte följs. Ett beslut om avvikelse får därför endast omfatta bestämmelserna i Försvarsmaktens föreskrifter om säkerhetsskydd, Försvarsmaktens interna bestämmelser om säkerhetsskydd och detta reglemente.

”Chefen för en kontingent i en internationell militär insats får, i fråga om verksamhet utanför Sverige, fatta beslut som avviker från Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd samt denna författning, om det är oundgängligen nödvändigt för verksamheten.

Ett sådant beslut ska dokumenteras och, om möjligt, föregås av samråd med Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer. Har sådant samråd inte skett ska Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, snarast underrättas om beslutet.”

1 kap. 11 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Anledningen till att en kontingentschef har rätten att besluta om avvikelse är att den ordinarie processen med beslut om undantag med beredning inom Högkvarteret, inte bedöms vara lämplig för internationella militära insatser i utlandet. Undantag från bestämmelser i författningar beskrivs i avsnitt 1.10.2.

Av ordalydelsen ”oundgängligen nödvändigt” följer att föreskriftens första stycke ska användas restriktivt. Avsikten är inte att en avvikelse ska tillämpas över tiden istället för att vidta de åtgärder som säkerställer att författningarna följs.

Moment 1:8 *Chefen för en kontingent i en internationell militär insats får, i fråga om verksamhet utanför Sverige, fatta beslut som avviker från moment i detta reglemente, om det är oundgängligen nödvändigt för verksamheten.*

Ett sådant beslut ska dokumenteras och, om möjligt, föregås av samråd med säkerhetsskyddsavdelningen vid Must. Har sådant samråd inte skett ska säkerhetsskyddsavdelningen vid Must snarast underrättas om beslutet.

Vägledande förklaring: Momentet innebär att det är kontingentschefen som beslutar om avvikelse istället för Försvarsmaktens säkerhetsskyddschef. Någon beredning enligt moment 1:9 behövs inte inför att kontingentschefen beslutar i ärendet. I kontingentschefens beslut måste det framgå vilket moment som avvikelsen rör, motivet för avvikelsen och om samråd har ägt rum.

1.10.4. Undantag från bestämmelser i detta reglemente

Moment 1:9 *Säkerhetsskyddsavdelningen vid Must bereder ärenden om undantag från moment i detta reglemente.*

Moment 1:10 *Försvarsmaktens säkerhetsskyddschef, eller den som säkerhetsskyddschefen bestämmer, beslutar i ärenden om undantag från moment i detta reglemente.*

1.10.5. Undantag från bestämmelser i författningar

I bilaga 2 på sidan 371 finns en sammanställning av vem som leder beredningar samt vem som beslutar i ärenden om undantag från bestämmelser i författningar.

”Försvarsmakten får medge undantag från föreskrifterna i denna författning.

Överbefälhavaren, eller den han eller hon bestämmer, fattar beslut i ärenden om undantag.”

12 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

Motsvarande gäller bl.a. i Försvarsmaktens interna bestämmelser om säkerhetsskydd.[92]

Vägledande förklaring: Det är överbefälhavaren som beslutar författningen, då är det även naturligt att det är överbefälhavaren eller den han eller hon bestämmer som beslutar i ärenden om sådana undantag. Således kan ingen annan person besluta om undantag från en bestämmelse i författningen utan att först ha blivit bemyndigad av överbefälhavaren.

”Chefen för militära underrättelse- och säkerhetstjänsten leder beredningen av ärenden om undantag från

1. Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd, förutom i fråga om ärenden som bereds enligt 8 kap. 35 §, och

2. Försvarsmaktens föreskrifter (FFS 2019:9) om signalskyddstjänsten, och

3. övriga föreskrifter rörande säkerhetsskydd.”

11 kap. 5 § andra stycket FM ArbO

Vägledande förklaring: Enligt 8 kap. 35 § leder FM CIO beredningen av Försvarsmaktens ärenden om undantag från Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd avseende it-säkerhet och Försvarsmaktens interna bestämmelser (FIB 2017:8) om it-säkerhet. Innebörden är att undantagsberedningar för Försvarsmaktens informationssystem leds av CIO. Chefen för Must leder undantagsberedningar i ärenden från andra myndigheter.[93] I avsnitt 4.10 beskrivs undantag från bestämmelser om it-säkerhet i Försvarsmakten.

Med övriga föreskrifter rörande säkerhetsskydd avses t.ex. föreskrifter om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar (S-und) (avsnitt 1.7.9).

Ärenden om undantag från Försvarsmaktens föreskrifter om säkerhetsskydd bereds tillsammans med juridiska avdelningen vid ledningsstaben i Högkvarteret. Innan en hemställan om undantag skickas in bör samverkan genomföras med den som leder beredningen av undantaget.

[92] 9 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd.
[93] 11 kap. 5 § andra stycket 1 FM ArbO.

”Chefen för militära underrättelse- och säkerhetstjänsten leder beredningen av ärenden om undantag enligt 3 kap. 6 § säkerhetskyddsförordningen (2018:658).”

11 kap. 5 § första stycket FM ArbO

Vägledande förklaring: I 3 kap. 6 § säkerhetsskyddsförordningen finns bestämmelser om undantag från krav i:

- 3 kap. 4 § första stycket säkerhetsskyddsförordningen om skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på ett informationssystem som ska användas i säkerhetskänslig verksamhet, skyddsåtgärder för obehörig avlyssning av, åtkomst till och nyttjande av systemet, samt spårbarhet för händelser som är av betydelse för säkerheten i systemet.[94] Skyddsåtgärderna beskrivs i avsnitt 4.8.1.

- 3 kap. 5 § andra stycket säkerhetsskyddsförordningen att säkerhetsskyddsklassificerade uppgifter ska skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten, när uppgifterna kommuniceras utanför verksamhetsutövarens kontroll.[95]

”Överbefälhavaren beslutar

24. i ärenden om undantag enligt 3 kap. 6 § första stycket säkerhetskyddsförordningen (2018:658).”

6 kap. 1 § 24 FM ArbO

Vägledande förklaring: ÖB beslutar om undantag på krav på skyddsåtgärder som anges i 3 kap. 4 § första stycket säkerhetsskyddsförordningen. Skyddsåtgärderna beskrivs i avsnitt 4.8.1.

”Chefen för militära underrättelse- och säkerhetstjänsten beslutar i ärenden om undantag enligt 3 kap. 6 § andra stycket säkerhetskyddsförordningen (2018:658).”

11 kap. 12 § 8 FM ArbO

Bemyndigandet får inte delegeras.[96] Ett sådant undantag får endast beslutas om det finns särskilda skäl.[97]

[94] 3 kap. 4 § första stycket säkerhetsskyddsförordningen.
[95] 3 kap. 5 § andra stycket säkerhetsskyddsförordningen.
[96] 11 kap. 12 § andra stycket FM ArbO.
[97] 4 kap. 6 § andra stycket säkerhetsskyddsförordningen.

Vägledande förklaring: Chefen för Must beslutar om undantag från krav på 3 kap. 5 § andra stycket säkerhetsskyddsförordningen att säkerhetsskyddsklassificerade uppgifter ska skyddas med hjälp av kryptografiska funktioner.

”Försvarsmaktens säkerhetsskyddschef leder beredningen av ärenden om undantag från Försvarsmaktens interna bestämmelser (FIB 2008:3) om signalskyddstjänsten och övriga interna bestämmelser inom säkerhetsskydd.”

11 kap. 23 § tredje stycket FM ArbO

Vägledande förklaring: Med övriga interna bestämmelser om säkerhetsskydd avses t.ex.:

- Försvarsmaktens interna bestämmelser om säkerhetsskydd.
- Försvarsmaktens interna bestämmelser om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar (S-und) (avsnitt 1.7.9).

Ärenden om undantag bereds tillsammans med juridiska avdelningen vid ledningsstaben i Högkvarteret. Innan en hemställan om undantag skickas in bör samverkan genomföras med den som leder beredningen av undantaget.

2. Analys och planering

2.1. Grunder

Säkerhetsskyddsplanering ska innehålla en säkerhetsskyddsanalys och en säkerhetsskyddsplan, och mynnar ut i konkreta säkerhetsskyddsåtgärder.[98] Syftet med säkerhetsskyddsplaneringen är att omhänderta de skyddsvärden som är av betydelse för Sveriges säkerhet. Dessa skyddsvärden benämns *säkerhetsskyddsvärden*.

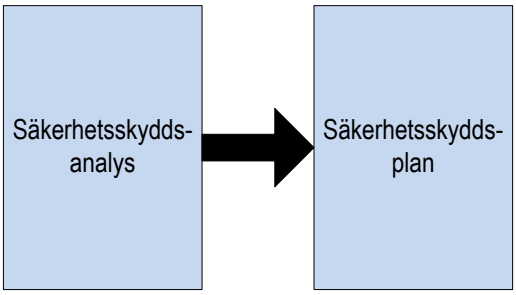


Bild 2.1. Säkerhetsskyddsanalys och säkerhetsskyddsplan.

Verksamhetsskyddsplanering ska genomföras för att omhänderta skyddsvärden som inte ska ges ett säkerhetsskydd. Verksamhetsskyddsplaneringen består av en verksamhetsskyddsanalys och verksamhetsskyddsplan som mynnar ut i konkreta skyddsåtgärder. Skyddsvärden, som omhändertas vid en verksamhetsskyddsplanering, benämns *verksamhetsskyddsvärden*. Verksamhetsskyddsplanering ska inte förväxlas med verksamhetssäkerhet, som leds av Säkerhetsinspektionen, och som lutar sig mot andra regelverk.

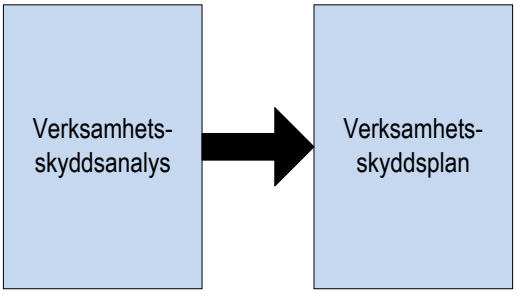


Bild 2.2. Verksamhetsskyddsanalys och verksamhetsskyddsplan.

Avsnitt 2.2-2.4 ger en bakgrund till säkerhetsskyddsplanering samt hur den ska genomföras i en verksamhet och hur resultatet av olika säkerhetsskyddsåtgärder kontrolleras och utvärderas. Kontroll av säkerhetsskyddet behandlas även i kapitel 9.

Avsnitt 2.5 förklarar och beskriver den metod som används för att genomföra en säkerhetsskyddsanalys. Där beskrivs även hur metoden kan användas för att genomföra en verksamhetsskyddsanalys.

[98] 2 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd.

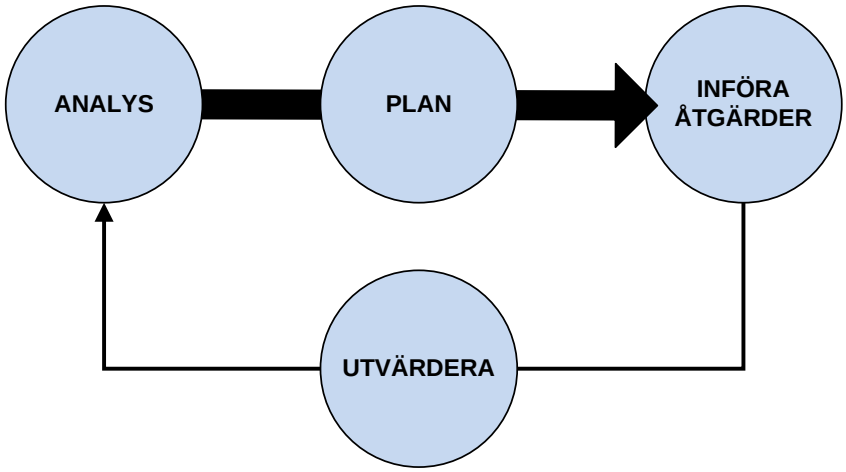


Bild 2.3. Planeringen mynnar ut i konkreta åtgärder, som behöver utvärderas för att förbättra skyddet.

Säkerhetsskyddsanalys och säkerhetsskyddsplan ska inte förväxlas med *särskild säkerhetsskyddsbedömning* (SSB) som finns för informationssystem (avsnitt 4.2.1) och säkerhetsskyddad upphandling (avsnitt 8.6).

2.2. Säkerhetsskyddsplanering

2.2.1. Säkerhetsskyddsanalys

> *”Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionageri, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.”*
>
> 1 kap. 2 § första stycket säkerhetsskyddslagen

> *”Den som bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska dokumenteras.”*
>
> 2 kap. 1 § första stycket säkerhetsskyddslagen

> *”Säkerhetsskyddsanalysen innebär att säkerhetsskyddsklassificerade uppgifter och vad som i övrigt behöver ett säkerhetsskydd ska identifieras. Vilka delar av verksamheten som är skyddsvärda med hänsyn till Sveriges säkerhet samt vilka hot och sårbarheter som finns kopplade till detta skyddsvärde ska också identifieras. Säkerhetsskyddsanalysen ska även innehålla en bedömning av vilka säkerhetsskyddsåtgärder som är nödvändiga. Analysen ska hållas uppdaterad.”*
>
> 2 kap. 1 § andra stycket säkerhetsskyddsförordningen

Vägledande förklaring: Säkerhetsskyddsanalysen ska identifiera vilken säkerhetskänslig verksamhet som Försvarsmakten bedriver och vilka säkerhetsskyddsvärden i den säkerhetskänsliga verksamheten som ska ges ett säkerhetsskydd. Behovet av säkerhetsskydd avgörs av vilka hot, säkerhetsskyddsvärden och sårbarheter som finns i verksamheten.

Säkerhetsskyddsanalysen är grunden för ett väl anpassat säkerhetsskydd, för att identifiera säkerhetsskyddsvärden, hot och sårbarheter i en säkerhetskänslig verksamhet och vilka negativa konsekvenser ett angrepp kan medföra. Det är bedömningarna i säkerhetsskyddsanalysen som motiverar de säkerhetsskyddsåtgärder som vidtas.[99] Detta innebär att säkerhetsskyddsanalysarbetet måste vara konsekvensdrivet och inriktat mot säkerhetskänslig verksamhet.

2.2.2. Säkerhetsskyddsplan

”Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.

Så långt det är möjligt ska säkerhetsskyddsåtgärderna utformas så att de inte medför någon skada eller annan olägenhet för andra allmänna eller enskilda intressen.”

2 kap. 1 § andra och fjärde styckena säkerhetsskyddslagen

Vägledande förklaring: Med andra allmänna och enskilda intressen avses bl.a. skyddet för den personliga integriteten. Lagen inskränker inte allmänhetens möjligheter att enligt offentlighetsprincipen ta del av allmänna handlingar.[100]

”Med säkerhetsskyddsanalysen som grund ska myndigheten upprätta en säkerhetsskyddsplan. Av planen ska framgå vilka säkerhetsskyddsåtgärder som ska vidtas, vem som har ansvaret och när respektive åtgärd ska vara genomförd. Behov av resurser, ansvarsfördelning, organisation, utbildning, övning samt rutiner och bestämmelser ska särskilt framgå.”

2 kap. 4 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Säkerhetsskyddsåtgärder kan vara kostsamma, effektivitetshämmande och integritetskränkande. Det är viktigt att åtgärderna är proportionerliga och att säkerhetsskyddet inte görs mer omfattande än vad som krävs. I utformningen av säkerhetsskyddsåtgärder ska aktuella hot och sårbarheter beaktas och vägas in.

[99] Prop. 2017/18:89 s. 56.
[100] Prop. 2017/18:89 s. 137.

Säkerhetsskyddsåtgärder ska skydda mot alla typer av brott som på något sätt kan hota Sveriges säkerhet:[101]

- I första hand ska åtgärderna skydda mot *spionerі*, *sabotage* och *terroristbrott*.[102]
- Åtgärderna ska även skydda säkerhetskänslig verksamhet mot *andra brott* som kan ge konsekvenser för Sveriges säkerhet, även om detta inte varit brottets primära syfte. Sådana brott kan vara stöld, dataintrång, olaga intrång eller skadegörelse. Ett exempel är en stöld av datorer i ett luftövervakningssystem kan medföra begränsningar i skyddet av Sveriges territorium trots att detta inte var avsikten med stölden.[103]

Säkerhetsskyddsklassificerade uppgifter ska inte bara skyddas mot brott. Säkerhetsskyddsåtgärder kan bl.a. bestå av att handlingar förvaras på ett betryggande sätt och att spridningen av uppgifter i handlingarna så långt det är möjligt begränsas till personer som behöver dem för sin tjänsteutövning.[104]

”Säkerhetsskyddsplanen ska även beskriva vilka åtgärder som behöver vidtas inför, under eller efter sådana avbrott och störningar i myndighetens säkerhetskänsliga verksamhet som kan medföra mer än ringa skada.”

2 kap. 4 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Trots att säkerhetsskyddslagen främst är avsedd att ge ett skydd mot antagonistiska hot, så påverkas den säkerhetskänsliga verksamheten även av avbrott och störningar som inte är aktörsdrivna. Exempel är olyckshändelser eller naturkatastrofer. Sådana händelser kan särskilt påverka tillgängligheten till verksamheten eller säkerhetsskyddsvärdet. Bestämmelsen innebär att säkerhetsskyddsplanen även ska innehålla en kontinuitetsplan som tar hänsyn till sådana störningar, om den potentiella skadan är mer än ringa.

2.3. Genomförande av säkerhetsskyddsplanering i Försvarsmakten

2.3.1. Inledning

Försvarsmaktens verksamhet bedrivs på många olika platser i och utanför Sverige. Det är därför inte tillräckligt att säkerhetsskyddsplanering endast sker centralt för myndigheten, eller att det endast finns en säkerhetsskyddsanalys och -plan som omhändertar alla myndighetens säkerhetsskyddsvärden. I Försvarsmakten genomförs säkerhetsskyddsplanering därför inom hela organisationen och nära den säkerhetskänsliga verksamheten.

[101] Prop. 2017/18:89 s. 50.
[102] Prop. 2017/18:89 s. 50.
[103] Prop. 2017/18:89 s. 50.
[104] Prop. 2017/18:89 s. 134.

Chefer för organisationsenheter och enheter i Högkvarteret är verksamhetsansvariga för den verksamhet som bedrivs vid organisationsenheten och enheten. Det är den verksamhetsansvarige som ansvarar för att säkerhetsskyddsplanering genomförs, dvs. att säkerhetsskyddsanalysen och säkerhetsskyddsplanen tas fram, dokumenteras och hålls uppdaterad, samt att de åtgärder som beslutas i säkerhetsskyddsplanen verkligen vidtas.[105]

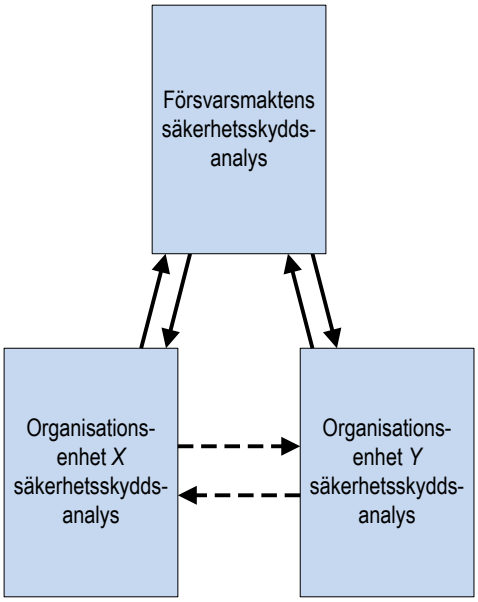


Bild 2.4. Försvarsmaktens myndighetsövergripande säkerhetsskyddsanalys har beroenden till organisationsenheternas analyser. I vissa fall finns beroenden mellan organisationsenheternas analyser (streckad pil).

Moment 2:1 *Försvarsmaktens metod för säkerhetsskyddsanalys ska användas vid genomförande av säkerhetsskyddsanalys i Försvarsmakten.*

Vägledande förklaring: Försvarsmaktens metod för genomförande av säkerhetsskyddsanalys finns i avsnitt 2.5. När *ska* anges i avsnitt 2.5 är det krav som ingår i metoden enligt moment 2:1.

Myndighetens, organisationsenheternas och i Högkvarteret enheternas säkerhetsskyddsplanering är inte isolerade företeelser. Tvärtom är det av största vikt att Försvarsmaktens olika säkerhetsskyddsvärden identifieras och värderas utifrån flera olika verksamhetsansvarigas säkerhetsskyddsanalyser. På så sätt blir det möjligt för Försvarsmakten att få en överblick över myndighetens säkerhetsskyddsvärden som ger underlag för prioriteringar av säkerhetsskyddsåtgärder på central och lokal nivå. Säkerhetsskyddsplaner måste vidare vara förankrade i Försvarsmaktens övriga verksamhetsplanering. Säkerhetsskyddsplaner ger ingångsvärden till verksamhetsplaneringen. Säkerhetsskyddsplanen bör därför tas fram koordinerad med övrig verksam-

[105] 2 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd.

hetsplanering. På så sätt finns en långsiktighet och en välgrundad förståelse för behovet av säkerhetsskyddsåtgärder, som blir en integrerad del av verksamheten.

Säkerhetsskyddsåtgärder är ofta kostsamma och rör inte sällan fortifikatoriska eller infrastrukturella åtgärder som tar lång tid att genomföra. Om säkerhetsskyddsplanering koordineras med övrig infrastrukturplanering kan åtgärderna effektiviseras både ur kostnads- och tidsbesparingsperspektiv.

Säkerhetsskyddsplanen ska innefatta de säkerhetsskyddsåtgärder som ska vidtas för de säkerhetsskyddsvärden som den verksamhetsansvarige själv ansvarar för. Planen ska även omfatta sådana säkerhetsskyddsvärden som den verksamhetsansvarige inte ansvarar för, men är beroende av. Det kan innebära att:

- Den verksamhetsansvarige ska samverka med den som ansvarar för det aktuella säkerhetsskyddsvärdet för att göra denne medveten om hur den verksamhetsansvarige värderat säkerhetsskyddsvärdet.
- Flera verksamhetsansvariga med samma säkerhetsskyddsvärde samverkar avseende både bedömning av säkerhetsskyddsvärdet och vilka säkerhetsskyddsåtgärder som ska vidtas. De kritiska beroenden som har identifierats i säkerhetsskyddsanalysen fungerar som ett underlag för säkerhetsskyddsplanen.

2.3.2. Försvarsmaktens säkerhetsskyddsplanering

”Överbefälhavaren beslutar Försvarsmaktens säkerhetsskyddsanalys enligt 2 kap. 1 § säkerhetsskyddsförordningen liksom Försvarsmaktens säkerhetsskyddsplan enligt 2 kap. 4 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.”

6 kap. 1 § 25 FM ArbO

Vägledande förklaring: Överbefälhavaren är som myndighetens chef ytterst ansvarig för säkerhetsskyddet i Försvarsmakten och ska därför besluta myndighetens säkerhetsskyddsanalys och säkerhetsskyddsplan.

”Försvarsmaktens säkerhetsskyddschef ska leda och samordna säkerhetsskyddsarbetet vid myndigheten. I uppgiften ingår att utarbeta Försvarsmaktens säkerhetsskyddsplanering enligt vad som föreskrivs i 2 kap. 1-4 §§ Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.”

11 kap. 20 § 1 FM ArbO

Vägledande förklaring: Försvarsmakten bedriver säkerhetskänslig verksamhet. Försvarsmakten ska därför enligt säkerhetsskyddslagen ha en säkerhetsskyddsanalys och säkerhetsskyddsplan på myndighetsnivå.

Överbefälhavaren leder myndigheten Försvarsmakten, och är därmed verksamhetsansvarig för all verksamhet som bedrivs i Försvarsmakten. Cheferna för organisat-

ionsenheterna är dock verksamhetsansvariga för verksamheterna vid respektive organisationsenhet. På samma sätt är chefer för krigsförband verksamhetsansvariga för verksamheten vid förbandet.

Överbefälhavaren har i FM ArbO pekat ut Försvarsmaktens säkerhetsskyddschef som ansvarig för att utarbeta Försvarsmaktens säkerhetsskyddsplanering.[106] Att Försvarsmaktens säkerhetsskyddschef ska leda och samordna säkerhetsskyddsarbetet[107] i Försvarsmakten innebär att säkerhetsskyddschefen ska planera och följa upp att säkerhetsskyddsplanering genomförs i myndigheten och att denna planering är aktuell. Säkerhetsskyddsplanering är inte endast en angelägenhet för den militära säkerhetstjänsten, utan kräver samverkan med de verksamheter som planeringen rör.

”Innan myndighetens säkerhetsskyddsanalys och säkerhetsskyddsplan beslutas ska myndighetens ledning orienteras.”

2 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med myndighetens ledning avses i detta reglemente Försvarsmaktens ledningsgrupp (FML).[108]

2.3.3. Organisationsenheternas och krigsförbandens säkerhetsskyddsplanering

”Vid varje organisationsenhet och krigsförband ska det göras en säkerhetsskyddsanalys och säkerhetsskyddsplan för den egna enheten respektive krigsförbandet.”

2 kap. 2 § första stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Säkerhetsskyddsplanering ska genomföras vid varje organisationsenhet med utgångspunkt i Försvarsmaktens säkerhetsskyddsplanering. Med detta avses att det ska finnas en röd tråd mellan den myndighetsövergripande säkerhetsskyddsplaneringen och den lokala eller regionala säkerhetsskyddsplaneringen. Detta är naturligt eftersom de säkerhetsskyddsvärden som identifierats och värderats i den myndighetsövergripande säkerhetsskyddsanalysen, finns ute på förband, skolor och centra. Många säkerhetsskyddsvärden är dessutom gemensamma för flera organisationsenheter, och en säkerhetsskyddsplanering som är koordinerad mellan dessa organisationsenheter ger bättre förutsättningar för att ge säkerhetsskyddsvärdena ett likvärdigt skydd oavsett var i verksamheten de finns.

[106] 11 kap. 20 § 1 FM ArbO.
[107] 11 kap. 20 § 1 FM ArbO.
[108] 1 kap. 5 § FM ArbO.

”I Högkvarteret ska det även göras en säkerhetsskyddsanalys och säkerhetsskyddsplan vid ledningsstaben, produktionsledningen, insatsledningen respektive militära underrättelse- och säkerhetstjänsten.”

2 kap. 2 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Utöver säkerhetsskyddsanalys och säkerhetsskyddsplan för organisationsenheten Högkvarteret ska vissa enheter i Högkvarteret göra sådana analyser och planer. Vägledning för vad enheternas säkerhetsskyddsanalyser och säkerhetsskyddsplaner omfattar framgår på sidan 14, i de vägledande förklaringarna till punkterna 1 och 2 i 1 kap. 8 § tredje stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd.

”Säkerhetsskyddsanalysen och säkerhetsskyddsplanen beslutas av chefen för organisationsenheten respektive krigsförbandschefen. I Högkvarteret beslutar chefen för ledningsstaben, produktionsledningen, insatsledningen och militära underrättelse- och säkerhetstjänsten i Högkvarteret respektive enhets säkerhetsskyddsanalys och säkerhetsskyddsplan.”

2 kap. 2 § tredje stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 2:2 *Innan chefen för organisationsenheten eller en enhet i Högkvarteret beslutar en säkerhetsskyddsanalys eller en säkerhetsskyddsplan ska organisationsenhetens eller enhetens ledningsgrupp, eller motsvarande, orienteras.*

Vägledande förklaring: Om inte säkerhetschefen är den som genomför orienteringen, är det nödvändigt att denna deltar vid orienteringen.

Observera!
Om en säkerhetsskyddsanalys eller säkerhetsskyddsplan omfattar säkerhetskänslig verksamhet som inte alla i ledningsgruppen ska få insyn i, måste orienteringen anpassas.

Moment 2:3 *Alla säkerhetsskyddsanalyser, säkerhetsskyddsplaner, särskilda säkerhetsskyddsanalyser och särskilda säkerhetsskyddsplaner ska delges säkerhetskontoret vid Must.*

2.3.3.1 Organisationsenhetens fysiska säkerhetsskyddsåtgärder

Moment 2:4 *Organisationsenhetens, samt enheternas i Högkvarteret, säkerhetsskyddsplanering ska identifiera behovet av fysiska säkerhetsskyddsåtgärder. Säkerhetsskyddsplaneringen ska minst innehålla:*

a) *Identifiering av platser där säkerhetsskyddsklassificerade handlingar, lagringsmedier och säkerhetskänslig materiel förvaras. Hur förvaringen ska utformas med hänsyn till platsernas belägenhet, möjligheterna att upptäcka intrång och den tid det tar för en särskilt avdelad styrka att försvåra intrång i förvaringsutrymmena.*

b) *Identifiering av platser där det i övrigt bedrivs säkerhetskänslig verksamhet och hur den fysiska säkerheten ska utformas vid dessa platser, för att förebygga skadlig inverkan på verksamheten.*

c) *Identifiering av utrymmen som ska användas för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell eller högre.*

d) *Rutiner som ska följas eller andra fysiska säkerhetsskyddsåtgärder som ska vidtas vid förhöjd beredskap eller förändrad hotbild.*

Vägledande förklaring: I säkerhetsskyddsplaneringen identifieras behovet av fysiska säkerhetsskyddsåtgärder för att förebygga såväl obehörigas tillträde som skadlig inverkan.

Exempel på rutiner eller andra säkerhetsskyddsåtgärder i punkt d) är skärpt bevakning av administrativa zoner, att förvaring av säkerhetsskyddsklassificerade handlingar och lagringsmedier endast får ske i en administrativ zon eller säkerhetszon eller att inga ytterligare skyddsåtgärder behövs.

2.3.4. Särskild säkerhetsskyddsplanering

Utöver säkerhetsskyddsanalyser och säkerhetsskyddsplaner, som omhändertar den löpande och långsiktiga verksamheten, kan det finnas behov av säkerhetsskyddsplanering för specifika verksamheter som är avgränsade i tid och rum. Sådan säkerhetsskyddsplanering benämns i Försvarsmakten som särskild säkerhetsskyddsanalys (SSSA) och särskild säkerhetsskyddsplan (SSSP).

Försvarsmaktens metod för säkerhetsskyddsanalys används även för särskild säkerhetsskyddsanalys.

> *”Om behovet av säkerhetsskydd för en övning, ett projekt eller en verksamhet inte har utretts i en säkerhetsskyddsanalys, ska en särskild säkerhetsskyddsplanering genomföras.”*
>
> 2 kap. 3 § första stycket
> Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: I en sådan övning, projekt eller verksamhet kan säkerhetsskyddsvärden exponeras utanför det ordinarie säkerhetsskyddet, t.ex. när:

- Säkerhetsskyddsåtgärderna för den tänkta övningen, projektet eller verksamheten inte har omhändertagits i säkerhetsskyddsplaneringen.
- Den tänkta övningen, projektet eller verksamheten ska genomföras på en plats som inte har omhändertagits i säkerhetsskyddsplaneringen.

Exempel där särskild säkerhetsskyddsplanering behövs kan vara tidsbegränsade materielprojekt, övningar, högnivåbesök, vissa transporter och inför övervägande om utkontraktering (outsourcing) av säkerhetsskyddsvärden.

Syftet med den särskilda säkerhetsskyddsplaneringen är att:

- identifiera och värdera de specifika säkerhetsskyddsvärden som exponeras utanför det ordinarie säkerhetsskyddet,
- identifiera och värdera eventuella specifika hot,
- identifiera och värdera specifika sårbarheter,
- identifiera hur säkerhetsskyddsvärdena är exponerade samt
- identifiera vilka säkerhetsskyddsåtgärder som ska vidtas.

För en övning, ett projekt eller verksamhet kan det finnas ett behov av att utse en säkerhetschef, signalskyddschef eller en it-säkerhetschef. Ett sådant behov kan identifieras i en särskild säkerhetsskyddsanalys. Om sådana chefer utses ska säkerhetsorganisation och lydnadsförhållanden regleras särskilt.[109]

Om den särskilda säkerhetsskyddsplaneringen rör utkontraktering av säkerhetsskyddsvärden gäller ytterligare bestämmelser, se kapitel 8 om säkerhetsskyddad upphandling.

”Den särskilda säkerhetsskyddsanalysen och den särskilda säkerhetsskyddsplanen beslutas av den chef som ansvarar för övningen, projektet eller verksamheten.”

2 kap. 3 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 2:5 *En särskild säkerhetsskyddsanalys ska samordnas med Försvarsmaktens säkerhetsskyddsanalys samt med övriga relevanta säkerhetsskyddsanalyser.*

[109] 3 kap. 13 § FM ArbO.

Vägledande förklaring:

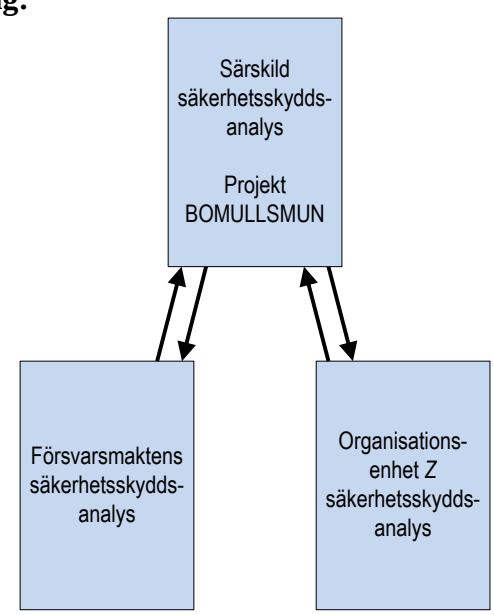


Bild 2.5. Exempel på relationer mellan en särskild säkerhetsskyddsanalys för ett projekt, Försvarsmaktens myndighetsövergripande säkerhetsskyddsanalys och en organisationsenhets säkerhetsskyddsanalys.

Den särskilda säkerhetsskyddsplanen ska innefatta de säkerhetsskyddsåtgärder som ska vidtas så att de exponerade säkerhetsskyddsvärdena för den tänkta övningen, projektet eller verksamheten ges ett säkerhetsskydd.

2.3.5. Kommunikation av säkerhetsskyddsplaneringen

Observera!
De som är berörda måste få ta del av analyser och planer.

Relevanta delar ur säkerhetsskyddsanalyser och säkerhetsskyddsplaner måste delges de som är berörda av analyserna och planerna. Även särskilda säkerhetsskyddsanalyser och säkerhetsskyddsplaner måste delges till de som är berörda av dem.

Organisationsenheternas säkerhetsskyddsanalyser och säkerhetsskyddsplaner bör vanligtvis delges den militärregionstab som organisationsenheten hör till. Se även moment 2:3.

2.3.6. Utvärdering

”Myndigheten ska vartannat år och vid behov utvärdera säkerhetsskyddsplaneringen, inklusive analysen och planen.”

2 kap. 2 § andra meningen Försvarsmaktens föreskrifter om säkerhetsskydd

Moment 2:6 *Organisationsenhet samt enhet i Högkvarteret ska vartannat år och vid behov utvärdera säkerhetsskyddsplaneringen. Utvärderingen ska dokumenteras.*

Vägledande förklaring: Det är viktigt att utvärdera vidtagna säkerhetsskyddsåtgärder, så att de förväntade effekterna av att åtgärda brister ger ett bättre säkerhetsskydd. Om inte ett förbättrat säkerhetsskydd uppnås, måste säkerhetsskyddsplaneringen revideras.

Behov av att utvärdera säkerhetsskyddsplaneringen kan t.ex. uppstå i samband med

- större organisationsförändringar,
- förändrad verksamhet (som väsentligt påverkar den säkerhetskänsliga verksamheten),
- att verksamhet utkontrakteras,
- att hot har identifierats som inte tidigare har beaktats,
- att den tekniska utvecklingen har medfört nya sårbarheter som kräver säkerhetsskyddsåtgärder som inte är införda, eller
- förändringar i lagstiftning eller regelverk som påverkar säkerhetsskyddsplaneringen.

Vid en utvärdering bör man undersöka om ovanstående punkter har aktualiserats sedan föregående utvärdering.

Om en utvärdering visar att det finns ett behov av att uppdatera säkerhetsskyddsplaneringen får uppdateringen göras från det steg i analysmetoden som uppdateringsbehovet finns i. Ett exempel är att det normalt räcker med att uppdatera säkerhetsskyddsplaneringen från analysmetodens steg 6 (avsnitt 2.5.6) och framåt, om en kritisk sårbarhet har identifierats i utvärderingen.

Om en utvärdering visar att det finns ett behov av att ta fram en ny säkerhetsskyddplanering måste analysmetodens samtliga steg (avsnitt 2.5) gås igenom.

2.4. Verksamhetsskyddsplanering

Det finns skyddsvärden som måste ges ett skydd i verksamheten, även om de inte omfattas av säkerhetsskyddslagstiftningen (verksamhetsskydd). Sådana verksamhetsskyddsvärden ska inte ges ett säkerhetsskydd. Det kan t.ex. röra sig om:

- Att skydda stöldbegärlig materiel med höga ekonomiska värden mot stöld (t.ex. motorfordon, snöskotrar, datorer och specialverktyg).
- Att skydda materiel för en specifik förmåga som samtidigt är svårersättlig (t.ex. ballistiska kroppsskydd och CBRN-materiel).
- Att skydda allmänfarlig materiel (t.ex. vapen och ammunition) mot stöld så att den inte kan användas för att skada allmänheten.
- Att skydda sekretessklassificerade uppgifter (uppgifter som omfattas av sekretess enligt OSL men som inte är säkerhetsskyddsklassificerade) mot röjande.

Att säkerställa tillgänglighet, riktighet och konfidentialitet i informationssystem som inte ska ges ett säkerhetsskydd. Sådana verksamhetsskyddsvärden kan omfattas av annan lagstiftning än säkerhetsskyddslagstiftningen med krav på hantering, förvaring och skydd, som kan likna de säkerhetsskyddskrav som gäller för säkerhetsskyddsvärden som omfattas av säkerhetsskyddslagstiftningen.

Dessa olika krav och behov kan samordnas, för att nå vinster i tid, ekonomi, m.m.

Exempel
På förbandet X finns en verkstad med dyra specialverktyg som behöver skyddas mot stöld. Förbandet har även behov av att anskaffa säkerhetsskåp för förvaring av säkerhetsskyddsklassificerade handlingar. Sådana skåp är även lämpliga som skydd mot stöld av specialverktygen. Förbandet samordnar anskaffningen av säkerhetsskåpen.

Analysmetoden i avsnitt 2.5 kan med fördel användas för att identifiera de verksamhetsskyddsvärden som ska ges ett verksamhetsskydd och vilka skyddsåtgärder som ska skydda verksamhetsskyddsvärdena.

Det finns inget hinder mot att en säkerhetsskyddsplan och en verksamhetsskyddsplan slås ihop i ett och samma dokument. Det ska då tydligt framgå vilka åtgärder som ska vidtas med stöd av säkerhetsskyddslagen (för att ge säkerhetsskyddsvärden ett säkerhetsskydd), och vilka andra åtgärder som ska vidtas för att skydda verksamhetsskyddsvärdena.

Om man i arbetet med verksamhetskyddsanalysen identifierar säkerhetsskyddsvärden ska de föras över till arbetet med säkerhetsskyddsanalys.

2.5. Analysmetod

I detta avsnitt förklaras de steg som ingår i analysmetoden. Metoden ska enligt moment 2:1 användas när man tar fram en säkerhetsskyddsanalys. När *ska* anges i detta avsnitt är det krav som ingår i metoden enligt moment 2:1 (sidan 49).

Säkerhetsskyddsanalysen genomförs av verksamheten, med stöd av säkerhetsorganisationen. Det är viktigt att analysen sker i lagarbete med dem som har relevant kompetens, dvs. har kännedom om verksamheten lokalt och dess relation till Försvarsmaktens verksamhet i stort.

Metoden kan även med fördel användas vid framtagning av en verksamhetsskyddsanalys. Stegen i metoden är identiska för såväl säkerhetsskyddsanalysen som verksamhetsskyddsanalysen, förutom steg 2 och 3 där alternativ 2 ska tillämpas för verksamhetsskyddsanalysen (bild 2.7).

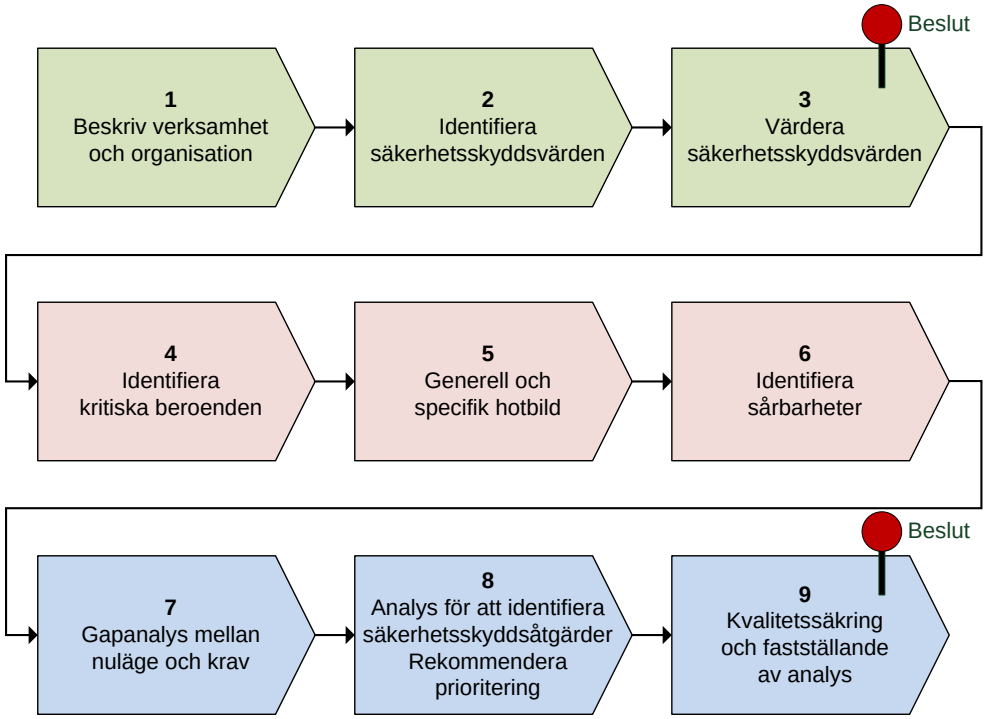


Bild 2.6. Säkerhetsskyddsanalysmetodens nio steg.

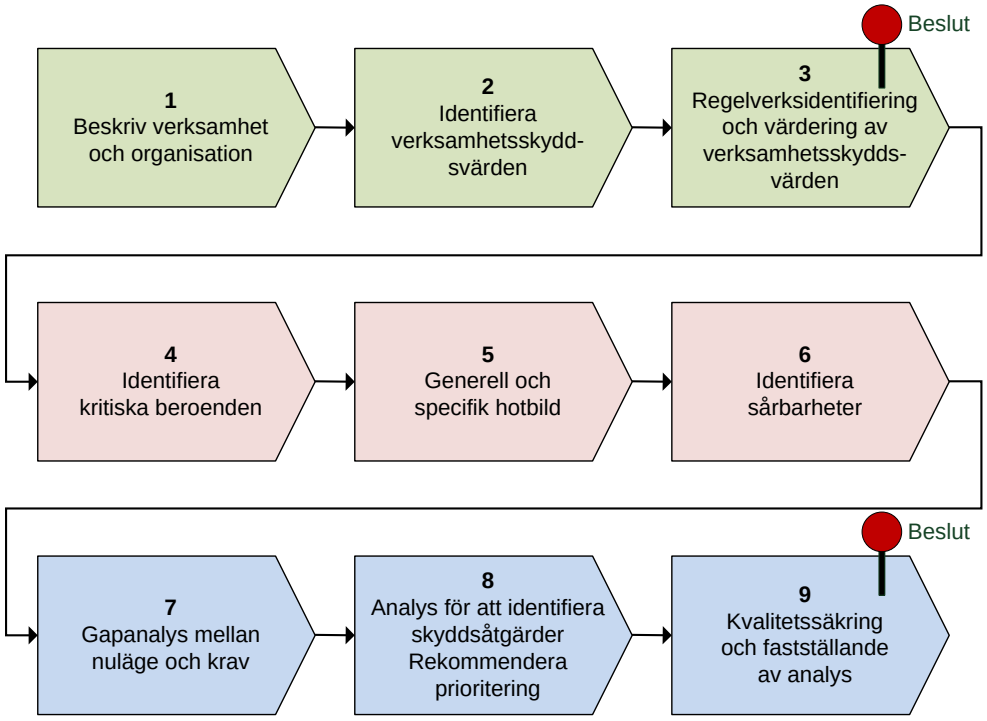


Bild 2.7. Motsvarande metod för verksamhetskyddsanalys. Steg 2 och 3 skiljer sig från bild 2.6.

2.5.1. Steg 1 – Verksamhetsbeskrivning

> *”En säkerhetsskyddsanalys ska innehålla en beskrivning av myndighetens verksamhet och organisation samt dess skyddsvärden (verksamhetsbeskrivning).”*
>
> 2 kap. 3 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

I avsnitt 1.7.2 beskrivs säkerhetskänslig verksamhet.

Vägledande förklaring: Verksamhetsbeskrivningen ska urskilja vilka delar av verksamheten som utgör säkerhetskänslig verksamhet, och som därmed ska ges ett säkerhetsskydd, och vilka delar som utgör verksamhet som ska ges ett verksamhetsskydd. I avsnitt 1.2 beskrivs skillnaden mellan säkerhetsskydd och verksamhetsskydd.

Inled med att göra en övergripande beskrivning av verksamheten som svarar på frågorna: vilka uppgifter ska lösas och vilka verksamheter genomförs?

Försvarsmaktens uppgifter framgår främst av förordningen (2007:1266) med instruktion för Försvarsmakten. Dessa uppgifter är stående uppgifter, som gäller över tid. Försvarsmakten får även uppgifter i det årliga regleringsbrevet, samt i särskilda regeringsbeslut.

Försvarsmaktens huvuduppgifter är bl.a. att:

- Upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp. Grunden för detta ska vara förmågan till väpnad strid.
- Försvara Sverige, främja svensk säkerhet och upptäcka och avvisa kränkningar av det svenska territoriet.
- Kunna värna Sveriges suveräna rättigheter och svenska intressen samt kunna förebygga och hantera konflikter och krig såväl nationellt som internationellt.
- Vid höjd beredskap kunna krigsorganisera, mobilisera och använda alla krigsförband för att möta ett militärt hot mot Sverige och svenska intressen. Krigsförbanden ska kunna krigsorganiseras även om höjd beredskap inte råder.

Ytterst handlar det om att identifiera sin säkerhetskänsliga verksamhet och härleda denna till Försvarsmaktens huvuduppgifter för att hävda Sveriges yttre säkerhet (Sveriges försvarsförmåga, politiska oberoende och territoriella suveränitet).

Det är lämpligt att utgå från Försvarsmaktens styrdokument. Försvarsmaktens verksamhetsplan (FMVP) och det årliga verksamhetsuppdraget (VU) innehåller uppgifter som hänför sig till både säkerhetskänslig verksamhet och till övrig verksamhet som Försvarsmaktens ska utföra. Även grundoperationsplanen (GROP) och den stående ordern för operationer nationellt (SOFO NAT) innehåller uppgifter som enheter ska utföra.

På regional och lokal nivå kan det vara tillräckligt att utgå från förbandets verksamhetsorder, eftersom denna i sin tur har utgått från ovanstående styrdokument.

Därefter ska en identifiering ske av de kärnuppgifter eller kärnförmågor som har betydelse för Sveriges säkerhet, det vill säga sammanfattar den säkerhetskänsliga verksamheten. Kärnuppgifter eller kärnförmågor som inte är av säkerhetskänslig karaktär men ändå måste ges ett skydd omhändertas i verksamhetsskyddsplaneringen.

Exempel

Verksamhet vid försvarsgren marinen.

- *Värna Sveriges territoriella integritet på och under ytan, samt i övergången mellan land och vatten med militära medel.*
- *Utveckla och fördjupa marinens förmåga till kvalificerad väpnad strid.*
- *Utbilda rekryter*
- *Genomföra statsceremoniell verksamhet*
- *Stöd till civila samhället*

Säkerhetskänslig verksamhet:

Värna Sveriges territoriella integritet, samt utveckla och fördjupa marinens förmåga till kvalificerad väpnad strid. Denna verksamhet härleds till Försvarsmaktens huvuduppgift att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp, samt att försvara Sverige, främja svensk säkerhet och upptäcka och avvisa kränkningar av det svenska territoriet.

Kärnuppgifter och -förmågor:

- *Stridsledning marin och koordinering med övriga delar i Försvarsmakten, t.ex. andra försvarsgrenar.*
- *Övervakning (för lägesbild, tidig förvarning, samt stödfunktion för Kustbevakningen och internationell samverkan).*
- *Verka med sjöstridskrafter (ytstrid, amfibiestrid, undervattensstrid, minkrig och säkra Sveriges transportvägar till Sverige samt kritiska införselhamnar).*

Exempel

Verksamhet vid organisationsenhet X:

- *Utveckla och vidmakthålla krigsförband i enlighet med beslutad krigförbandsspecifikation.*
- *Upprätthålla anbefalld beredskap och genomföra verksamhet enligt Grundoperationsplan (GROP) för organisationsenhetens krigsförband.*
- *Bemanna svensk kontingent.*
- *Utbilda två enheter i subarktisk miljö.*
- *Delta i statsceremoniell verksamhet*

Säkerhetskänslig verksamhet:

Utveckla och vidmakthålla krigsförband och upprätthålla anbefalld beredskap. Denna verksamhet härleds till Försvarsmaktens huvuduppgift att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp.

Kärnuppgifter och -förmågor:

- *Krigsplanläggning och beredskapsplanläggning samt mobiliseringsplanläggning*
- *Genomför förbandsutbildning*
- *Genomför verksamhet enligt GROP*

2.5.1.1 Verksamhetsbeskrivning (verksamhetsskydd)

Verksamhetsbeskrivningen i verksamhetsskyddsanalysen görs på samma sätt som i säkerhetsskyddsanalysen, dvs. man utgår från de uppgifter verksamheten har utöver den säkerhetskänsliga verksamheten.

2.5.2. Steg 2 – Identifiera säkerhetsskyddsvärden

Med utgångspunkt i verksamhetsbeskrivningen ska de säkerhetsskyddsvärden som finns i den säkerhetskänsliga verksamheten identifieras och brytas ner i:

- funktioner,
- system och
- anläggningar.

Kategorierna funktioner, system och anläggningar används för att identifiera specifika säkerhetsskyddsvärden (inklusive säkerhetsskyddsklassificerade uppgifter). Beroende på vilken nivå, dvs. var i organisationshierarkin, säkerhetsskyddsanalysen genomförs blir detaljeringsgraden olika.

Begreppet *funktion* definieras som ett särskilt arbetsområde eller kompetens som krävs för lösande av uppgifter. Begreppet omfattar inte bara personal, utan även arbetssätt (modus), doktrin, teknik, organisation, m.m.[110]

Funktioner kan t.ex. vara:

- Logistikfunktion
- Driftfunktion
- Ledningsfunktion
- Säkerhetsfunktion

[110] Försvarsplan 2019, Bilaga 5 Nomen Op, FM2018-2732:2, s. 3.

System kan t.ex. vara:

- Informationssystem (se definition på sidan 151)
- Kommunikationssystem
- Sensorsystem
- Vapensystem och -plattformar

Anläggningar kan t.ex. vara:

- Ledningsplatser
- Stridsledningscentraler
- Förråd
- Driftcentraler

På myndighetsnivå kan det vara lämpligt att bryta ner säkerhetsskyddsvärdena i t.ex.:

- Logistikfunktion
- Informationssystem på strategisk nivå
- Vapensystem och -plattformar

I säkerhetsskyddsanalysen för en organisationsenhet bryts säkerhetsskyddsvärdena ner ytterligare, t.ex.:

- Olika applikationer eller funktioner i ett informationssystem.
- Ett vapensystem bryts ner i specifika komponenter och informationstyper.
- Olika anläggningar inom organisationsenheten.

Samma säkerhetsskyddsvärde kan behöva delas upp i både funktioner, system och anläggningar.

Exempel
Säkerhetsskyddsvärdet Försvarsmaktens sensorkedja behövs för den säkerhetskänsliga verksamheten övervakning och lägesbild. Sensorkedjan kan huvudsakligen sorteras in under funktion samtidigt som vissa radaranläggningar sorteras in under anläggningar och vissa informationssystem i sensorkedjan sorteras in under system.

Bild 2.8 visar hur en sådan sortering kan göras på ett tydligt sätt. I detta steg är det viktigare att säkerhetsskyddsvärdena identifieras och inkluderas – än hur de kategoriseras.

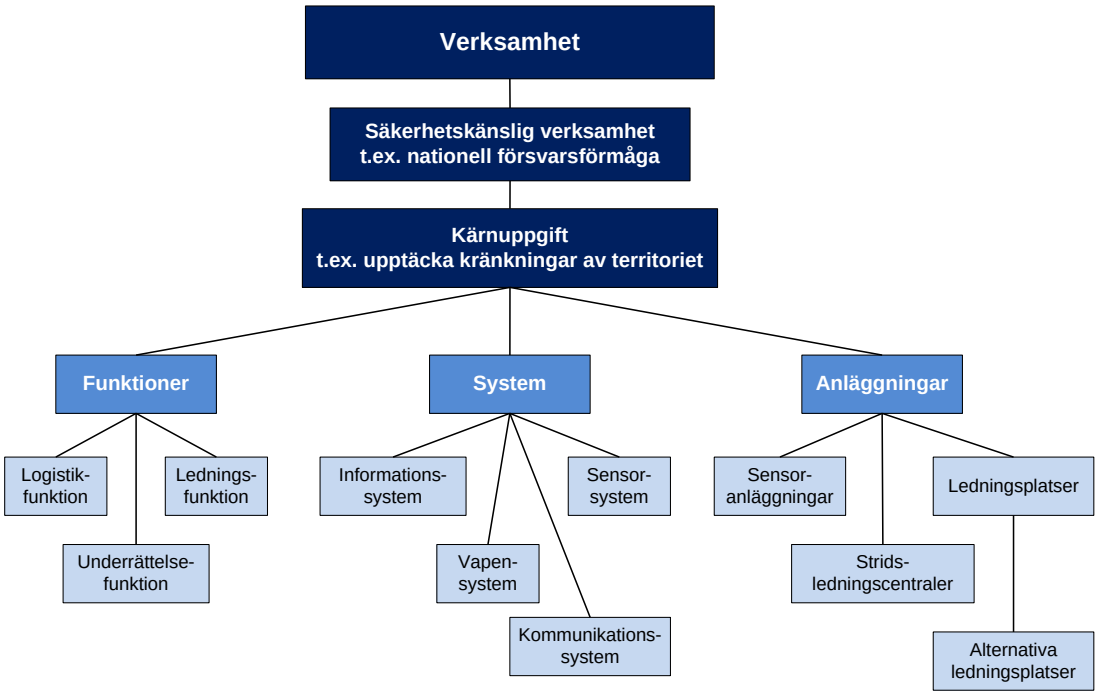


Bild 2.8. Exempel på struktur för att identifiera säkerhetsskyddsvärden.
Kim Hakkarainen/Försvarsmakten

Identifieringen av säkerhetsskyddsvärden ska inte bara omfatta sådana värden som den verksamhetsansvarige (t.ex. chef för en organisationsenhet) själv ansvarar för. Det är minst lika viktigt att identifiera sådana säkerhetsskyddsvärden som verksamheten är beroende av, men som den verksamhetsansvarige själv inte ansvarar för.

Ett exempel på ett sådant säkerhetsskyddsvärde är Försvarsmaktens informationssystem som hanteras och drifthålls centralt.

Vissa säkerhetsskyddsvärden som Försvarsmakten är beroende av omhändertas av andra än Försvarsmakten. Några exempel är teleoperatörer, eldistributörer, statliga myndigheter och internationella partners.

Vissa säkerhetsskyddsvärden förekommer hos flera verksamhetsansvariga i Försvarsmakten, så att flera ansvarar för värdena. Två exempel är stridsflygsystemet och krigsplanläggning.

2.5.2.1 Särskilt om identifiering av säkerhetsskyddsklassificerade uppgifter och informationssystem

Även säkerhetsskyddsklassificerade uppgifter ska identifieras i säkerhetsskyddsanalysen. Avsikten inte att göra en allomfattande informationsvärdering av alla uppgifter, utan att identifiera de informationstyper eller informationsmängder som utgör säkerhetsskyddsklassificerade uppgifter.

Exempel på informationstyper är:

- Uppgifter om sårbarheter i informationssystem,
- Ett vapensystems förmåga,
- Fysiska säkerhetsskyddsåtgärder vid en hemlig anläggning,
- Uppgifter om ett kommunikationssystems funktion, uppsättning m.m.

Enligt 2 kap. 2 § säkerhetsskyddslagen ska informationssäkerhet förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, samt förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. Se avsnitt 1.7.8.1 om informationssäkerhet.

Säkerhetsskyddsanalysen ska därför också identifiera:

- Vilka *uppgifter* som inte är säkerhetsskyddsklassificerade men som behövs för den säkerhetskänsliga verksamheten.
- Vilka *informationssystem* som inte är avsedda för säkerhetsskyddsklassificerade uppgifter, men som behövs för den säkerhetskänsliga verksamheten.

Exempel
System X är inte avsett för säkerhetsskyddsklassificerade uppgifter. Systemet behövs för att Försvarsmakten ska kunna genomföra insatser under höjd beredskap. System X är därmed ett informationssystem som måste skyddas mot skadlig inverkan så att systemet är tillgängligt och informationen är riktig.

2.5.2.2 Identifiera verksamhetsskyddsvärden (verksamhetsskydd)

Med utgångspunkt i verksamhetsbeskrivningen för den verksamhet som inte utgör säkerhetskänslig verksamhet, bryts verksamheten ner i funktioner, system och anläggningar, på samma sätt som i säkerhetsskyddsanalysen.

2.5.3. Steg 3 – Värdera säkerhetsskyddsvärden

Värderingen av ett säkerhetsskyddsvärde ska delas in i en av följande konsekvensnivåer.

Konsekvensnivå 5 Synnerligen allvarlig skada för Sveriges säkerhet.

Konsekvensnivå 4 Allvarlig skada för Sveriges säkerhet.

Konsekvensnivå 3 Inte obetydlig skada för Sveriges säkerhet.

Konsekvensnivå 2 Ringa skada för Sveriges säkerhet.

Konsekvensnivå 1 Inte mätbar eller inte relevant konsekvens för Sveriges säkerhet.

Värderingen är en förutsättning för att kunna få ett prioriteringsunderlag för den fortsatta säkerhetsskyddsplaneringen. Värderingen ska vara konsekvensdriven, dvs. vad blir konsekvensen för Sveriges säkerhet om säkerhetsskyddsvärdet förloras? Värderingen av säkerhetsskyddsvärdet ska inte vara beroende av vilken typ av påverkan som sker på säkerhetsskyddsvärdet, dvs. om det är främmande underrättelseverksamhet eller kriminalitet, eller om en brand förstör säkerhetsskyddsvärdet. Det tas istället upp i säkerhetsskyddsplanen vid bedömningen av vilken säkerhetsskyddsåtgärd som ska vidtas för att säkerställa tillgången till säkerhetsskyddsvärdet.

Med att förlora avses t.ex.:

- Att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs.
- Skadlig inverkan på uppgifter som inte är säkerhetsskyddsklassificerade och informationssystem som behövs för en säkerhetskänslig verksamhet.
  Skadlig inverkan på områden, byggnader, anläggningar och objekt (t.ex. fordon och luftfarkost) där säkerhetskänslig verksamhet bedrivs.
- Att nyckelpersoner inte är tillgängliga för att delta i en säkerhetskänslig verksamhet.

Värderingen av ett säkerhetsskyddsvärde kan ändras i händelse av höjd beredskap eller krig. Ett exempel är drivmedelsförsörjningen, som sannolikt värderas högre i krig än i fred, p.g.a. osäkerheter kring leveransmöjligheter från utlandet m.m. Analysen av säkerhetsskyddsvärdet ska därför även innefatta en bedömning av huruvida säkerhetsskyddsvärdet värderas olika under fred, höjd beredskap och krig.

Värderingen och motivet för värderingen av ett säkerhetsskyddsvärde ska dokumenteras. En väl dokumenterad värdering ger goda förutsättningar för att öka förståelsen för de rekommendationer och prioriteringar som säkerhetsskyddsanalysen ska utmynna i.

2.5.3.1 Konsekvensnivå 5: Synnerligen allvarlig skada för Sveriges säkerhet

Med synnerlig allvarlig skada avses att Sveriges nationella försvarsförmåga eller förmåga att bevara Sveriges politiska oberoende och handlingsfrihet sätts ur spel.

Exempel på säkerhetsskyddsvärden som bedöms som konsekvensnivå 5 är:
- Synnerligen kritiska anläggningar, funktioner och militärgeografi som avgörande kan påverka Sveriges yttre säkerhet på systemnivå över lång tid.
- Strategiska vapensystem, t.ex. JAS och ubåtssystem med strategisk beväpning, som är avgörande för Sveriges förmåga att försvara sitt territorium.
- Ett fungerande ledningssystem som kan koordinera Sveriges försvarsförmåga.

Nyckelord för värdering: systemnivå (försvarsgrenar), helt utslagen försvarsförmåga på nationell nivå, centrala grundförutsättningar för försvarsförmågan inkl. lednings-

system, påverkar hela Sverige, och säkerhetsskyddsvärden som tar decennier att återställa efter en skada.

2.5.3.2 Konsekvensnivå 4: Allvarlig skada för Sveriges säkerhet

Med allvarlig skada avses att Sveriges nationella försvarsförmåga eller förmågan att upprätthålla Sveriges handlingsfrihet och oberoende reduceras i kritiska delar.

Exempel på säkerhetsskyddsvärden som bedöms som konsekvensnivå 4 är:
- Informationssystem som innehåller aggregerad information med kvalificerat hemliga uppgifter.
- Kritiska noder i ledningsstödsystemet som har viss, om än starkt begränsad redundans.
- Ledningsplatser, vapendepåer för strategisk verkan och klareringsverkstäder med viss, om än starkt begränsad, redundans.
- Specifika specialförbandsförmågor, samt kritisk bemanning på nyckelbefattningar.

Nyckelord för värdering: kritiska systemdelar, utslagen regional försvarsförmåga, hela försvarsgrenar kraftigt reducerade eller utslagna, väsentliga delar av ledningssystem är ur funktion och säkerhetsskyddsvärden som tar minst flera år att återställa efter en skada.

2.5.3.3 Konsekvensnivå 3: Inte obetydlig skada för Sveriges säkerhet

Med inte obetydlig skada avses konkret negativ påverkan på Sveriges nationella försvarsförmåga eller förmåga att upprätthålla Sveriges handlingsfrihet eller oberoende som inte reducerar förmågan i kritiska delar.

Exempel på säkerhetsskyddsvärden som bedöms som konsekvensnivå 3 är:
- Vapensystem som ger tydliga operativa fördelar tillsammans med andra vapensystem.
- Informationssystem som innehåller aggregerad information i säkerhetsskyddsklassen hemlig.
- Informationssystem vars tillgänglighet har betydelse för Sveriges nationella försvarsförmåga (även om de inte behandlar säkerhetsskyddsklassificerade uppgifter).
- Stridsfordonsgarage med kritisk mängd stridsfordon.

Nyckelord för värdering: viktig funktion, konkret säkerhetsskyddsvärde, ger Sverige tydliga försvarsfördelar och säkerhetsskyddsvärden som kan ta månader att återställa efter en skada.

2.5.3.4 Konsekvensnivå 2: Ringa skada för Sveriges säkerhet

Med ringa skada avses möjlig negativ påverkan på Sveriges nationella försvarsförmåga eller förmåga att upprätthålla handlingsfrihet eller oberoende, som vare sig går att påvisa eller utesluta. Ofta handlar sådan påverkan om indirekta konsekvenser.

Exempel på säkerhetsskyddsvärden på konsekvensnivå 2:
- Tankning av drivmedel (vissa fysiska tankställen), samt informationssystem kopplat till detta.
- Logistik avseende mat och vatten, t.ex. till ett arméförband.

Nyckelord för värdering: stödjande funktion till andra säkerhetsskyddsvärden, säkerhetsskyddsvärden som kan återställas inom några veckor efter en skada.

2.5.3.5 Konsekvensnivå 1: Inte mätbar eller inte relevant konsekvens för Sveriges säkerhet

Med inte mätbar eller inte relevant avses att skada för Sveriges säkerhet inte kan påvisas eller att verksamheten inte är säkerhetskänslig.

Konsekvensnivå 1 medför att det värderade skyddsvärdet inte är ett säkerhetsskyddsvärde. Sådana skyddsvärden kan istället utgöra verksamhetsskyddsvärden och omhändertas i verksamhetskyddsplaneringen (avsnitt 2.4).

2.5.3.6 Dokumentation av värderingen av säkerhetsskyddsvärden

Värderingen av säkerhetsskyddsvärdena åskådliggörs tydligast i en tabell, se nedan.

Tabell 2.1. Exempel på värdering av säkerhetsskyddsvärden.

Säkerhetsskyddsvärde	Konsekvensnivå	Motiv för värdering
Vapensystem X	3	Ett system med ett konkret säkerhetsskyddsvärde, det finns en begränsad mängd utlokaliserad på x platser
Ledningsfunktion	4	Funktionen är av stor vikt för organisationsenheten, för att leda verksamheten i alla konfliktnivåer.

2.5.3.7 Värdering av informationssystem och kommunikationssystem

Informationssystem och kommunikationssystem värderas utifrån aspekterna konfidentialitet, riktighet och tillgänglighet.

Ett *elektroniskt kommunikationsnät* är ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.[111]

[111] 1 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Med konfidentialitet avses att endast den som är behörig kan ta del av eller på annat sätt hantera information.

När ett informationssystem värderas måste förekomsten av säkerhetsskyddsklassificerade uppgifter identifieras och vilka säkerhetsskyddsklasser uppgifterna är placerade i. Säkerhetsskyddsklassificering beskrivs i avsnitt 3.1.3.

Även aggregering av uppgifter ska beaktas. Med aggregerade uppgifter menas:

- Uppgifter som efter sammanställning har bearbetats så att man av sammanställningen kan utvinna annan och mer säkerhetsskyddsvärd information än från uppgifterna i sig.
- Uppgifter som i den sammanställda formen visar på beroenden mellan olika verksamheter, unika sårbarheter eller annat som inte hade kunnat utvinnas av uppgifterna var för sig.

Med *riktighet* avses att information inte förändras på ett icke önskvärt sätt, vare sig det sker obehörigen, av misstag eller på grund av funktionsstörning.

Med *tillgänglighet* avses att uppgifter, informationssystem eller kommunikationssystem är tillgängliga när de behövs. Det kan ibland finnas anledning att specificera inom vilken tidsrymd uppgiften, informationssystemet eller kommunikationssystemet behöver finnas tillgängligt. I många fall är ett kortsiktigt bortfall i tillgänglighet acceptabelt, men inte en längre periods otillgänglighet. Det kan dock variera stort mellan olika informationssystem och verksamheter hur långt ett avbrott kan vara acceptabelt för Sveriges säkerhet.

Den konsekvensnivå som fått högst värdering (konfidentialitet, riktighet eller tillgänglighet) är också den dimensionerande och bestämmer vilket skydd som verksamheten eller informationssystemet ska ges.

Eftersom värderingen kan skilja sig åt mellan kriterierna konfidentialitet, riktighet och tillgänglighet, kommer variationerna bli tydliga om de förs in i en tabell, se exempel i tabell 2.2.

Tabell 2.2. Exempel på tabell över aspekterna konfidentialitet, riktighet och tillgänglighet.

Informations-system X	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
Fred	4	3	3	
Höjd beredskap	4	4	4-5*	*beroende på krisens art
Krig	3*	5	5	*bedömd 4, dag 1-2 i krig

2.5.3.8 Regelverksidentifiering och värdering av verksamhetsskyddsvärden (verksamhetsskydd)

När analysmetoden används för verksamhetsskyddsanalysen, ersätts värderingssteget för säkerhetsskyddsvärden av ett steg för regelverksidentifiering samt värdering. I detta steg identifieras vilka författningskrav, andra krav i interna styrdokument, krav i överenskommelser och avtal som berör skyddet av verksamhetsskyddsvärdena. Regelverksidentifieringen syftar alltså till att identifiera vilka bestämmelser som ur verksamhetsskyddssynpunkt gäller för de identifierade verksamhetsskyddsvärdena. Vidare görs en värdering av verksamhetsskyddsvärdena, dvs. vad konsekvensen blir för verksamheten om verksamhetsskyddsvärdet förloras.

Ett exempel på verksamhetsskyddsvärden i Försvarsmakten som är särskilt reglerade är *handeldvapen* och *ammunition*. Förordningen (1996:31) om statliga myndigheters skjutvapen m.m. innehåller bestämmelser om hantering, förvaring och transport av skjutvapen och ammunition samt handgranater, truppminor, spräng- och tändmedel samt pansarskott. Syftet med förordningen är att begränsa förluster av materielen, att motverka att den kommer till användning vid brott samt att förebygga annat missbruk och olyckshändelser.[112] Försvarsmaktens föreskrifter (FFS 2007:1) om hantering, förvaring och transport av skjutvapen och ammunition, samt Försvarsmaktens interna bestämmelser (FIB 2013:5) om hantering, förvaring och transport av skjutvapen och ammunition innehåller ytterligare bestämmelser i anslutning till förordningen.

Ett annat exempel på verksamhetsskyddsvärden i Försvarsmakten är *sekretessklassificerade uppgifter*, dvs. uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (OSL) men som inte rör säkerhetskänslig verksamhet och som därmed inte ska ges ett säkerhetsskydd enligt säkerhetsskyddslagstiftningen. Det kan handla om hälsouppgifter (21 kap. 1 § OSL), kommersiell sekretess (bl.a. 31 kap. 16 § OSL), eller sekretess om säkerhets- eller bevakningsåtgärd (18 kap. 8 § OSL). Den sistnämnda sekretessbestämmelsen kan i vissa fall röra säkerhetskänslig verksamhet och omfattas då av säkerhetsskyddslagens bestämmelser; uppgifterna ska i sådana fall identifieras i säkerhetsskyddsanalysen. Bestämmelser om hantering och skydd av sekretessklassificerade uppgifter finns i Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

De identifierade regelverken är sedan ingångsvärde för gapanalysen i steg 7 (avsnitt 2.5.7.1) där man kontrollerar om regelverken faktiskt följs.

Värderingen av verksamhetsskyddsvärden delas in i fyra konsekvensnivåer:

Hög (H) – stor påverkan på verksamheten eller andra

Med stor påverkan menas att det kan få stora konsekvenser för enheten eller andra.

[112] 1 § förordningen om statliga myndigheters skjutvapen m.m.

Nyckelord för värdering: Påverkan på verksamhetsskyddsvärdet renderar i påverkan på hela verksamheten, det rör stora ekonomiska värden, verksamhetsskyddsvärdet påverkas under en längre tid.

Medel (M) – medelstor påverkan på verksamheten eller andra

Med medelstor påverkan menas att det kan få konsekvenser för verksamheten eller andra.

Nyckelord för värdering: Påverkan på verksamhetsskyddsvärdet sker under en överskådlig tid, ekonomiska värden står på spel, påverkar del av verksamheten.

Låg (L) – liten påverkan på verksamheten eller andra

Med liten påverkan menas att det kan bli få små konsekvenser för enheten eller andra om verksamhetsskyddsvärdet påverkas.

Nyckelord för värdering: Påverkan på verksamhetsskyddsvärdet sker under en kort tidsperiod, det påverkar en liten del av verksamheten.

Ingen (-) – inte mätbart eller relevant

Med konsekvensnivå Ingen avses att påverkan på verksamhetsskyddsvärdena inte kan påvisas.

Tabell 2.4. Exempel på identifiering av gällande bestämmelser eller reglering för verksamhetsskyddsvärden och värdera verksamhetsskyddsvärdet.

Verksamhets-skyddsvärde	Konsekvensnivå	Motiv för värdering	Gällande reglering
Mängdammunition 5,56	Medel (M)	Ett system med ett konkret verksamhetsskyddsvärde, det finns en begränsad mängd utlokaliserad på x platser	Förordningen (1996:31) om statliga myndigheters skjutvapen FFS (2007:1) och FIB (2013:5) om hantering, förvaring och transport av skjutvapen och ammunition
Termiska kikarsikten	Medel (M)	Stöldbegärlig materiel Ekonomiska värden står på spel	Avtal med annan stat om hantering och skydd av materielen

2.5.3.9 Beslutspunkt 1 – Fastställande av identifierade och värderade säkerhetsskyddsvärden

Moment 2:7 *De identifierade och värderade säkerhetsskyddsvärdena ska godkännas av verksamhetsansvarig chef innan säkerhetsskyddsanalysen fortsätter.*

Vägledande förklaring: Beslutet syftar till att den verksamhetsansvarige chefen ska känna till vilka säkerhetsskyddsvärden som kommit fram, och ska ges möjlighet att påverka identifieringen och värderingen av säkerhetsskyddsvärdena.

2.5.4. Steg 4 – Kritiska beroenden

Den verksamhetsansvarige ska se till att alla säkerhetsskyddsvärden som hör till den säkerhetskänsliga verksamheten identifieras. Detta avser både säkerhetsskyddsvärden som den verksamhetsansvarige själv ansvarar för, och säkerhetsskyddsvärden som den verksamhetsansvarige själv inte ansvarar för (avsnitt 2.5.2).

De mest kritiska beroendena ska identifieras i det här steget, för att tydliggöra vilka beroenden som ska prioriteras i säkerhetsskyddsplanen. Avsikten är inte att göra komplicerade beroendeanalyser i många steg, utan det är tillräckligt att identifiera ett första beroendeled. De kritiska beroendena kan finnas:

- Inom Försvarsmakten (interna beroenden), till exempel till ett annat förband, en annan funktion (logistikstöd eller liknande).
- Utanför Försvarsmakten (externa beroenden), t.ex. till en leverantör av elektroniska kommunikationer eller till en kommun.

Tabell 2.5. Exempel på identifiering av säkerhetsskyddsvärdenas kritiska beroendeförhållanden till andra verksamhetsansvariga.

Säkerhetsskydds-värde	Interna beroenden	Externa beroenden	Beroenden till utländska parter
El och telekom	Organisationsenhet X och Y	Myndighet X och företag X samt Y	
Informationssystem Q	Organisationsenhet E	Myndighet X och företag X	Betaland

För att det identifierade beroendeförhållandet ska bli tydligt och omhändertaget i den fortsatta säkerhetsskyddsanalysen och den efterföljande säkerhetsskyddsplanen, så krävs det även att dessa beroendeförhållanden beskrivs och motiveras kortfattat i förhållande till respektive säkerhetsskyddsvärde.

2.5.5. Steg 5 – Hotbild

> *”Myndigheten ska beakta Försvarsmaktens dimensionerande hotbeskrivning och ta fram en hotbild som är relevant, anpassad och aktuell i förhållande till den säkerhetskänsliga verksamheten som myndigheten bedriver.”*
>
> 2 kap. 3 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Försvarsmaktens dimensionerande hotbeskrivning utgörs av rapporten *Säkerhetsunderrättelseårsbedömande* (SÅB). SÅB ges ut årligen, normalt i maj, av säkerhetsunderrättelseavdelningen vid Must.

Den verksamhetsansvarige ska, med utgångspunkt i den av Försvarsmakten tillhandahållna dimensionerande hotbeskrivningen, ta fram en hotbild för den egna säkerhetskänsliga verksamheten som är relevant, anpassad och aktuell i förhållande till den säkerhetskänsliga verksamheten som bedrivs. Hotbedömning och framtagande av hotbild inom ramen för militär säkerhetstjänst i allmänhet beskrivs i avsnitten 1.6.1-1.6.5.

Hotbilden ska vara relevant och anpassad, d.v.s. beskriva hur den egna verksamheten påverkas av de beskrivna hoten. En förutsättning för att kunna göra en relevant hotbedömning är att den egna verksamheten och dess skyddsvärden först beskrivs. Om verksamheten ändras måste hotbilden ses över.

Hotbilden kan vid behov kompletteras med aktualiserade specifika hot som kräver kompletterande säkerhetsskyddsåtgärder tillfälligt eller permanent. Den specifika hotbilden för den aktuella verksamheten ska därför innehålla uppgifter om vilken säkerhetskänslig verksamhet och vilka säkerhetsskyddsvärden den är anpassad för, vilken giltighetstid bedömningen har samt vilka eventuella avgränsningar (t.ex. geografiska eller tematiska) som är gjorda.

Om den verksamhetsansvarige inte kan ta fram underlag för en relevant hotbild måste hemställan om information göras till närmast högre nivå i Försvarsmaktens säkerhetsorganisation.

2.5.6. Steg 6 – Sårbarheter

Med sårbarhet avses i detta reglemente en brist i skyddet av ett säkerhetsskyddsvärde som kan utnyttjas av en antagonist. I säkerhetsskyddsanalyser delas sårbarheter in i *kritiska sårbarheter* och *sårbarheter som inte är kritiska*.

Sårbarheter i en verksamhet kan uppstå t.ex. på grund av organisationens utformning, den teknik som används, brister i den fysiska säkerheten och på informationssäkerhetsområdet. Personer som deltar i säkerhetskänslig verksamhet kan vara sårbara ur säkerhetshänseende (kapitel 6).

En sårbarhet i informationssystem kan utgöras av beroenden mellan olika system som var för sig inte har värderats högt enligt konsekvensnivåskalan (avsnitt 2.5.3),

men som tillsammans är mycket skyddsvärda, eller att systemen var för sig inte är sårbara men hopkopplingen gör dem sårbara.

Det är viktigt att sårbarheterna relaterar till den dimensionerande hotbeskrivningen och den framtagna hotbilden. Ett tecken på sårbarhet är om säkerhetsskyddet inte klarar av att hantera det dimensionerande hotet.

Sårbarhetsanalyser som redan har gjorts i verksamheten av andra anledningar (t.ex. verksamhetssäkerhet, verksamhetsskydd m.m.) kan användas som underlag för identifieringen av kritiska sårbarheter.

Tips!
En annan källa till att identifiera de kritiska sårbarheterna är protokoll från den senaste kontrollen av verksamheten.

2.5.6.1 Kritiska sårbarheter

Kritiska sårbarheter är brister i säkerhetsskyddet, för ett säkerhetsskyddsvärde, där bristerna kan utnyttjas av en antagonist och effekten av ett sådant utnyttjande kan medföra allvarliga konsekvenser för säkerhetsskyddsvärden i konsekvensnivå 4 eller 5. Kritiska sårbarheter ska vara av den karaktären att de måste omhändertas.

Uppgifterna i denna del av säkerhetsskyddsanalysen är ofta de mest skyddsvärda uppgifterna, eftersom de kritiska sårbarheterna i verksamheten pekas ut där. För att begränsa spridningen av uppgifterna kan sårbarheterna beskrivas mer utförligt i en bilaga med mer restriktiv delgivning. Det blir då tydligt exakt vilka sårbarheter som behöver omhändertas i säkerhetsskyddsplanen, samtidigt som säkerhetsskyddsanalysen kan delges till en större krets.

2.5.6.2 Sårbarheter som inte är kritiska

Sårbarheter som inte är kritiska är brister i säkerhetsskyddet, för ett säkerhetsskyddsvärde, där bristerna kan utnyttjas av en antagonist och effekten av ett sådant utnyttjande kan medföra konsekvenser men som inte är allvarliga för en säkerhetskänslig verksamhet. Dessa sårbarheter måste också omhändertas i säkerhetsskyddsplaneringen.

2.5.6.3 Dokumentationen av sårbarheter

Sårbarheterna kan lämpligen föras in i en tabell, enligt exemplet i tabell 2.6.

Tabell 2.6. Exempel på dokumentation av sårbarheter.

Sårbarhet	Beskrivning	Kommentar
Hög personal-omsättning	På grund av hög personalomsättning har inte personalen nödvändig utbildning i säkerhetsskydd.	Saknas lärare och utbildare vid förbandet.

Sårbarhet	Beskrivning	Kommentar
Exponering av vapensystem Q vid övning	Säkerhetsskyddsvärdet kommer att exponeras vid övningen, som är öppen och tillgänglig för allmänheten.	Omhändertas inom ramen för en SSSP (fysisk säkerhet, utbildning, fotoförbud).

2.5.6.4 Sårbarheter (verksamhetsskydd)

De identifierade sårbarheterna kan röra operativa frågor eller andra områden som inte direkt härrör till den säkerhetskänsliga verksamheten, eller som härrör till den säkerhetskänsliga verksamheten men som inte kan omhändertas genom säkerhetsskyddsåtgärder (eller där det krävs ytterligare åtgärder utöver säkerhetsskyddsåtgärder). Ett exempel är ett visst verktyg som är centralt för att kunna reparera en stridsvagnsmotor. Om det bara finns ett fåtal av dessa verktyg och reservmateriel saknas utgör detta en kritisk sårbarhet ur ett operativt perspektiv, dvs. om verktygen tar slut kan stridsvagnar inte repareras och stridsvagnarna bli då oanvändbara. En sådan sårbarhet åtgärdas genom att anskaffa flera verktyg, inte genom en säkerhetsskyddsåtgärd. Däremot kan säkerhetsskyddsåtgärder behöva vidtas för att skydda de befintliga verktygen till dess att fler verktyg anskaffats.

2.5.7. Steg 7 – Gapanalys för att identifiera krav som inte följs

Försvarsmaktens verksamhet är i väldigt hög utsträckning regelstyrd, och verksamhetsansvariga på alla nivåer är skyldiga att känna till och följa författningskrav och andra krav i interna styrdokument. Gapanalysens syfte är att identifiera vilka författningskrav, andra krav i interna styrdokument, krav i överenskommelser och avtal som vid analystillfället (nuläge) inte uppfylls, samt att ge en indikation varför dessa inte följs. Detta kommer att ge ingångsvärden till den fortsatta säkerhetsskyddsplaneringen, eftersom åtgärder måste vidtas så att verksamhetsägaren följer kraven.

Det regelverk som gapanalysen ska utgå från är säkerhetsskyddslagstiftningen och de föreskrifter och bestämmelser som finns inom Försvarsmakten kring säkerhetsskydd. Det rör sig alltså främst om:

- Säkerhetsskyddslagen
- Säkerhetsskyddsförordningen
- Försvarsmaktens föreskrifter om säkerhetsskydd
- Försvarsmaktens föreskrifter om signalskyddstjänsten
- Försvarsmaktens föreskrifter om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar
- Försvarsmaktens interna bestämmelser om säkerhetsskydd
- Försvarsmaktens interna bestämmelser om it-säkerhet
- Försvarsmaktens interna bestämmelser om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar
- Försvarsmaktens interna bestämmelser om signalskyddstjänsten

REGLEMENTE

- Reglemente säkerhetstjänst
- Enskilda beslut om säkerhetsskydd
- Organisationsenhetens lokala instruktioner

En förteckning över bestämmelser och riktlinjer för säkerhetstjänsten (SAMSÄK) ges ut årligen av säkerhetsaskyddsavdelningen vid Must, och kan tjäna som stöd i vilka regelverk som gäller.

Liksom vid identifieringen av kritiska sårbarheter är det viktigt att vid gapanalysen använda protokoll från kontroller eller tillsyn. I protokollen anges vilka brister som har identifierats tillsammans med hänvisning till vilket krav som inte följs.

Tabell 2.7. Exempel på tabell med gapanalys mellan nuläge och lagkrav eller krav i annat regelverk.

Lag-/regelverkskrav	Säkerhetsskyddsvärde	Anledning
3 kap. 3 § FFS säkerhetsskydd	Materiel som innehåller säkerhetsskyddsklassificerade uppgifter	Utbildningsstatus på personal, dvs. handhavandefel
3 kap. 20 § FFS säkerhetsskydd	Säkerhetsskyddsklassificerade handlingar eller lagringsmedia	Aktualitet av tillstånd för medförande av handling och lagringsmedia är inte fullgod hos alla anställda
6 kap. 6-7 §§ FFS säkerhetsskydd	Personalsäkerhet	Brister kring uppföljning av säkerhetsprövning

2.5.7.1 Gapanalys för att identifiera krav som inte följs (verksamhetsskydd)

I verksamhetsskyddsanalysen ska en gapanalys också göras, för att kontrollera om regelverken faktiskt följs. Den identifiering av gällande regelverk som gjordes i steg tre i verksamhetsskyddsanalysen (avsnitt 2.5.3.8 ovan) utgör ingångsvärde för gapanalysen.

Tabell 2.8. Exempel på tabell med gapanalys mellan nuläge och lagkrav eller krav i annat regelverk.

Lag-/regelverkskrav	Verksamhets-skyddsvärde	Anledning
Förordningen om statliga myndigheters skjutvapen	Mängdammunition 5,56	Brist på förråd för förvaring av mängdammunition
Avtal med annan stat om hantering och skydd av materielen	Termiska kikarsikten	Samförvaring i strid mot bestämmelse i avtalet

2.5.8. Steg 8 – Analys för att identifiera säkerhetsskyddsåtgärder och rekommendera prioritering

De identifierade och värderade säkerhetsskyddsvärdena, den dimensionerande hotbeskrivningen, de kritiska beroendena och sårbarheterna, samt gapanalysen till gällande bestämmelser, utgör ingångsvärdena till själva analysen. I detta steg ska dessa ingångsvärden vägas samman för att identifiera vilka säkerhetsskyddsvärden som har behov av vilken typ av säkerhetsskyddsåtgärder (informationssäkerhet, fysisk säkerhet och personalsäkerhet) eller om säkerhetsskyddad upphandling är aktuell.

Analysen ska tydligt påvisa var säkerhetsskyddsvärdena finns i verksamheten. Analysen ska dessutom tydligt påvisa var de allvarligaste bristerna i säkerhetsskyddet bedöms finnas, samt vilka av dessa delar som har störst behov av planerade säkerhetsskyddsåtgärder. Om den kritiska sårbarheten för ett visst säkerhetsskyddsvärt informationssystem utgörs av outbildad personal, bör det framgå att säkerhetsskyddsåtgärder i form av utbildningsinsatser bör genomföras. Om hotbilden och den kritiska sårbarheten utgörs av främmande underrättelseverksamhet mot exponering av ett säkerhetsskyddsvärde vid en övning, kan säkerhetsskyddsåtgärder inom området fysiskt skydd vara mer lämpliga. Om gapanalysen visar att flera krav i Försvarsmaktens interna bestämmelser om säkerhetsskydd inte uppfylls, är det en tydlig indikation om vilka säkerhetsskyddsåtgärder som måste vidtas.

Prioritering bör i huvudsak göras utifrån säkerhetsskyddsvärdenas betydelse, dvs. säkerhetsskyddsklass för säkerhetsskyddsklassificerade uppgifter samt den skada som kan uppstå för Sveriges säkerhet om den säkerhetskänsliga verksamheten påverkas av en antagonistisk handling. Samtidigt måste hoten mot säkerhetsskyddsvärdena och de kritiska sårbarheterna beaktas vid prioriteringen av åtgärder, samt regelverkskrav.

Tabellen nedan kan användas för att presentera prioriteringen på ett enkelt sätt.

Tabell 2.9. Exempel på presentation av prioritering.

Prioritering	Säkerhetsskyddsvärde som omhändertas	Hot som omhändertas	Sårbarhet som omhändertas	Säkerhetsskyddsåtgärd
2	Personal	Främmande und	Saknar utbildning i säkerhetsskydd	Utbilda personal, starta regelbundna orienteringar om hotbilden

Prioritering	Säkerhetsskyddsvärde som omhändertas	Hot som omhändertas	Sårbarhet som omhändertas	Säkerhetsskyddsåtgärd
1	Informationssystem Q	Främmande und	Saknas fysiskt skydd vid kopplingen mellan system Q och X	Nytt kablage mellan systemen skapar skydd samt en uppgradering i system X
3	Vapensystem Q (övning)	Främmande und	Exponering av vapensystemets förmåga och effekt vid övning	Vapensystem Q ska endast användas under övningen på tider när mörkret fallit.

Verksamhetsskyddanalysen ska på motsvarande sätt påvisa var verksamhetsskyddsvärdena finns, var de allvarligaste bristerna i verksamhetsskyddet bedöms finnas, och vilka delar som har störst behov av verksamhetsskyddsåtgärder.

2.5.9. Steg 9 – Beslut av säkerhetsskyddsanalys

Säkerhetsskyddsanalysen ska ge tydliga och konkreta ingångsvärden till den fortsatta säkerhetsskyddsplaneringen. Samtidigt måste analysen ge handlingsutrymme till beslutande chefer och de som ansvarar för säkerhetsskyddsplanen att kunna ta hänsyn till operativa, ekonomiska och praktiska aspekter i val och fortsatt prioritering av säkerhetsskyddsåtgärder. Det är därför viktigt att analysen och de slutsatser och rekommendationer som följer av analysen, beslutas av den verksamhetsansvarige.

Hänsyn till operativa, ekonomiska och praktiska aspekter innebär inte att den verksamhetsansvarige inte behöver följa författningskrav om säkerhetsskydd.

2.5.10. Dokumentation av säkerhetsskyddsanalysen

Moment 2:8 *Säkerhetsskyddsanalysen ska dokumenteras enligt följande disposition.*

1. *Sammanfattning.*
2. *Inledning*

   2.1. Syfte och omfattning
3. *Verksamhetsbeskrivning*
4. *Identifierade och värderade säkerhetsskyddsvärden*

   4.1. Funktioner

   4.2. System

4.3. Anläggningar

5. *Kritiska beroenden*
6. *Hotbild mot verksamheten*
7. *Sårbarheter*
8. *Gapanalys till gällande bestämmelser*
9. *Analys*
10. *Slutsatser, förslag på generella säkerhetsskyddsåtgärder och rekommenderad prioritering*

Vägledande förklaring: Under punkten *4. Identifierade och värderade säkerhetsskyddsvärden* samlas säkerhetsskyddsvärdena under rubrikerna *Funktioner, System, Anläggningar*. Dessa rubriker delas i sin tur in i underrubriker som tydliggör vilken funktion, vilken typ av system eller typ av anläggningar som beskrivs. Varje säkerhetsskyddsvärde beskrivs översiktligt och en förklaring ges till värderingen av säkerhetsskyddsvärdet. Efter varje säkerhetsskyddsvärde beskrivs vilka typer av säkerhetsskyddsklassificerade uppgifter som rör säkerhetsskyddsvärdet.

Exempel
4.3 Anläggningar

4.3.1 Fast ledningsplats (stabsbyggnad X) (3)

Stabsbyggnad X är organisationsenhetens ledningsplats i fred och utgör krigsförbandets ledningsplats i krig. Byggnaden värderas till 3 eftersom den utgör en viktig funktion för den territoriella ledningen av enheter i krig.

Säkerhetsskyddsklassificerade uppgifter om fast ledningsplats: säkerhetsskydd (och brister i säkerhetsskydd) för anläggningen, vilka kommunikations- och informationssystem som används i anläggningen.

Under punkten *9. Analys* i säkerhetsskyddsanalysen utförs själva analysen av de ingångsvärden som inhämtats och presenterats i punkterna 2-8. Punkten *9. Analys* måste därför utformas så att det är tydligt hur analysen har genomförts, vilka resonemang som ligger till grund för olika värderingar, och varför en viss prioritering rekommenderas under punkten 10.

Tips!
Dokumentmall för säkerhetsskyddsanalys finns i handlingen *200609 HKV MUST SÄKERHETSSKYDDSANALYS* i IS UNDSÄK.

2.6. Säkerhetsskyddsplan

I avsnitt 2.2.2 beskrivs grunderna för säkerhetsskyddsplan.

I en säkerhetsskyddsplan utvecklas de säkerhetsskyddsåtgärder som har identifierats i säkerhetsskyddsanalysen. För varje identifierat säkerhetsskyddsvärde anges vilka säkerhetsskyddsåtgärder som behövs. Säkerhetsskyddsplanen är en direkt fortsättning av säkerhetsskyddsanalysen och syftar till att reglera hur säkerhetsskyddsvärdena ska skyddas mot säkerhetshoten.

Enligt 2 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd ska en säkerhetsskyddsplan innehålla:

- För varje identifierat säkerhetsskyddsvärde vilka *säkerhetsskyddsåtgärder* som behöver vidtas.
- För varje säkerhetsskyddsåtgärd *vem* som är ansvarig för att åtgärden vidtas och *när* den ska vara genomförd.
- Behov av *resurser*, *ansvarsfördelning*, *organisation*, *utbildning*, *övning* samt *rutiner* och *bestämmelser* för den säkerhetskänsliga verksamhet som säkerhetsskyddsanalysen avser.
- Vilka åtgärder som behöver vidtas inför, under eller efter avbrott och störningar i den säkerhetskänsliga verksamheten som analysen avser och som kan medföra mer än ringa skada för Sveriges säkerhet (*kontinuitetsplanering*).

I de fall något hot eller sårbarhet inte kan omhändertas eller någon säkerhetsskyddsåtgärd inte kan vidtas ska det särskilt framgå i säkerhetsskyddsplanen. Det finns emellertid omständigheter som gör att risker ibland måste accepteras, utan att frångå regelverk. Sådana omständigheter måste också framgå av planen. I säkerhetsskyddsplanen ska riskhanteringsbesluten omsättas i konkreta åtgärder. Avseende vissa informationssystem och it-tjänster finns det bestämmelser om kontinuitetsplanering i Försvarsmaktens interna bestämmelser om it-verksamhet.

Moment 2:9 *Om en säkerhetsskyddsåtgärd inte kan vidtas ska följande anges för åtgärden.*

a) Skäl för att åtgärden inte kan vidtas.

b) En bedömning av konsekvensen för säkerhetsskyddet och den säkerhetskänsliga verksamheten.

c) Om något rättsligt krav eller moment i reglemente inte kan följas.

Moment 2:10 *Om en säkerhetsskyddsåtgärd inte kan vidtas får verksamhetsansvarig chef fatta beslut om att säkerhetsskyddsåtgärden inte ska vidtas. Ett sådant beslut får endast fattas under förutsättning att rättsliga krav eller moment i detta reglemente följs. Beslutet ska dokumenteras.*

3. Informationssäkerhet

3.1. Informationsklassificering

3.1.1. Försvarsmaktens modell för informationsklassificering

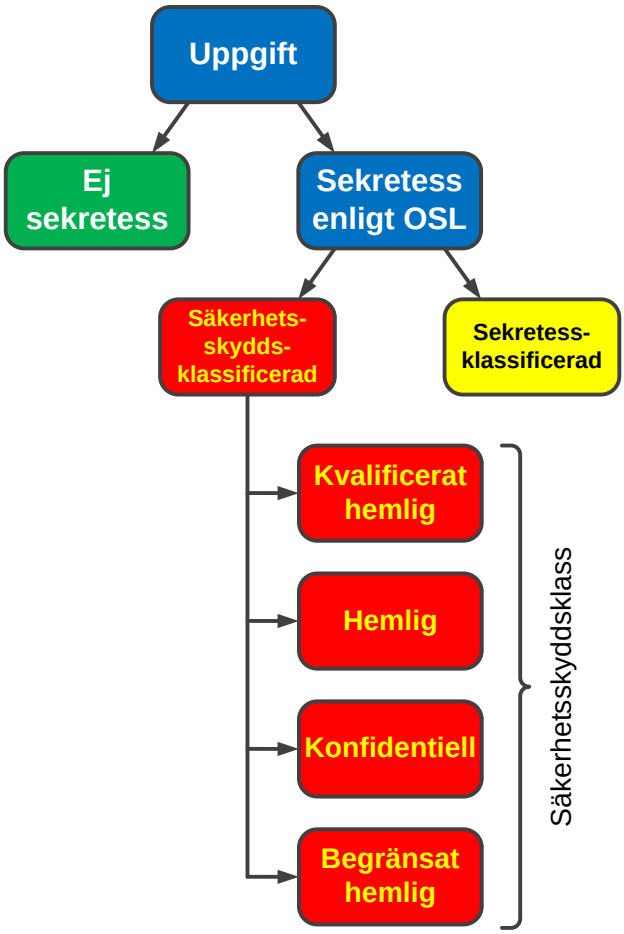


Bild 3.1. Försvarsmaktens modell för informationsklassificering.

Modellen (bild 3.1) utgår från en bedömning om en uppgift omfattas av sekretess eller inte. I offentlighets- och sekretesslagen (OSL) finns bestämmelser om när en uppgift omfattas av sekretess. En uppgift som omfattas av sekretess kan antingen vara *säkerhetsskyddsklassificerad* eller *sekretessklassificerad*. En säkerhetsskydds-klassificerad uppgift placeras i en *säkerhetsskyddsklass*.

Modellen för informationsklassificering tar endast upp konfidentialitetsaspekten utifrån sekretess enligt OSL. I Försvarsmakten finns ingen motsvarande gemensam modell för aspekterna tillgänglighet och riktighet.

Sekretessbestämmelsen 15 kap. 2 § OSL (försvarssekretessen) kommer alltid röra säkerhetskänslig verksamhet. Uppgifter som omfattas av den sekretessen kommer alltid vara säkerhetsskyddsklassificerade (A i bild 3.2).

Det finns sekretessbestämmelser i OSL som beroende på sammanhanget *kan* röra säkerhetskänslig verksamhet, t.ex. 15 kap. 1 § OSL (utrikessekretessen) och 18 kap. 8 § OSL (säkerhets- och bevakningssekretessen). Endast i det fall en uppgift som omfattas av sekretessen rör säkerhetskänslig verksamhet är uppgiften säkerhetsskyddsklassificerad (B i bild 3.2).

Merparten av sekretessbestämmelserna i OSL kommer sannolikt aldrig röra säkerhetskänslig verksamhet så att uppgifterna är säkerhetsskyddsklassificerade. Uppgifter som omfattas av sådan sekretess, t.ex. 19 kap. 3 § OSL (upphandlingssekretess) eller 39 kap. 3 § (sekretess för adresser, telefonnummer m.m. i personaladministrativ verksamhet), är alltid sekretessklassificerade (C i bild 3.2).

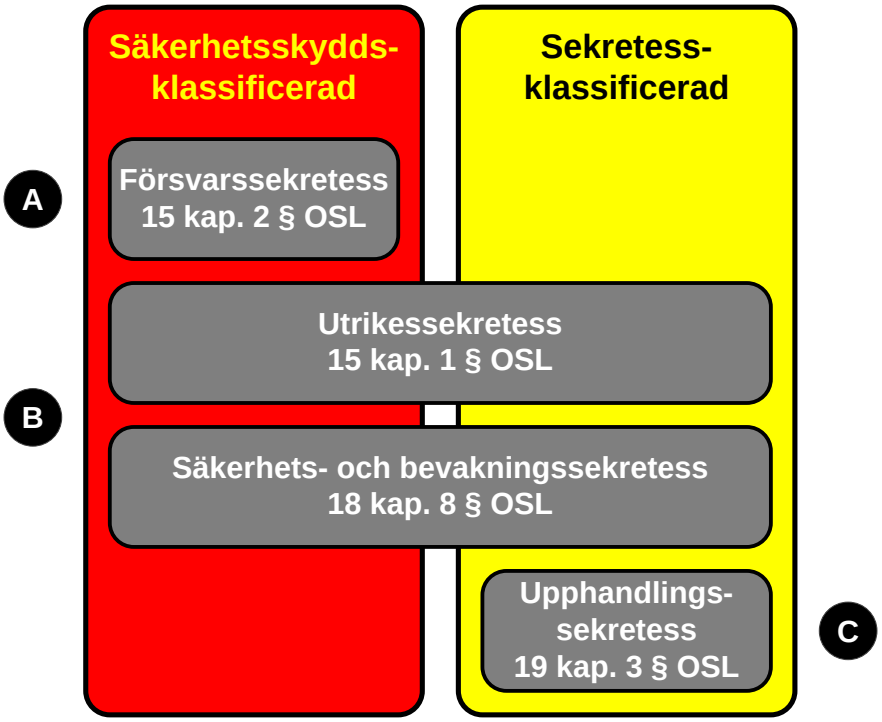


Bild 3.2. Hur fyra sekretessbestämmelser i OSL förhåller sig till säkerhetsskyddsklassificerade uppgifter respektive sekretessklassificerade uppgifter i Försvarsmaktens informationsklassificeringsmodell.

Säkerhetsskyddsklassificering beskrivs i avsnitt 3.1.3.

3.1.2. Begrepp och förkortningar

Om begrepp för informationsklassificering behöver förkortas bör förkortningar i tabell 3.1 användas. Andra myndigheter kan använda andra förkortningar.

Tabell 3.1. Förkortningar för informationsklassificering.

Begrepp	För-kortning
Ej sekretess	ES
Sekretessklassificerad	SK
Säkerhetsskyddsklassificerad	SSK

Säkerhetsskyddsklass	För-kortning
Kvalificerat hemlig	KH
Hemlig	H
Konfidentiell	K
Begränsat hemlig	BH

Mellan 2004 och 2019 delades säkerhetsskyddet i Försvarsmakten in i fyra *informationssäkerhetsklasser*.[113] En uppgift placerades då i en informationssäkerhetsklass efter vilket men som kunde uppstå om uppgifterna röjdes. I säkerhetsskyddslagen finns numera en indelning i säkerhetsskyddsklasser. De äldre informationssäkerhetsklasserna motsvaras av de nya säkerhetsskyddsklasserna. Tabell 3.1 nedan visar hur informationssäkerhetsklasser och säkerhetsskyddsklasser ska översättas. Säkerhetsskyddsklasserna beskrivs i avsnitt 3.1.3.

Tabell 3.2. Översättning mellan informationssäkerhetsklasser och säkerhetsskyddsklasser.

Informationssäkerhetsklass	Säkerhetsskyddsklass
HEMLIG/TOP SECRET	Kvalificerat hemlig
HEMLIG/SECRET	Hemlig
HEMLIG/CONFIDENTIAL	Konfidentiell
HEMLIG/RESTRICTED	Begränsat hemlig

Begreppet *utrikesklassificerad uppgift* användes i Försvarsmakten från 2010 till 2019 för uppgifter som var placerade i någon av nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED eller motsvarande och som var sekretessbelagda enligt 15 kap. 1 § OSL men som *inte* rörde rikets säkerhet. Enligt säkerhetsskyddslagen är numera sådana uppgifter säkerhetsskyddsklassificerade. Begreppet utrikesklassificerad uppgift ska därför inte längre användas. Säkerhetsskyddsklassificering i internationellt samarbete beskrivs i avsnitten 3.1.3.3-3.1.3.6.

[113] 1 kap. 4 § Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd.

Observera!
Begreppet *utrikesklassificerad* ska inte längre användas eftersom den typen av uppgifter numera ingår i *säkerhetsskyddsklassificerade* uppgifter.

Begreppet utrikes*klassificerad* ska inte förväxlas med utrikes*sekretess*.

När den nya säkerhetsskyddslagen trädde i kraft den 1 april 2019 upphörde bestämmelserna om skydd för utrikesklassificerade uppgifter i Försvarsmaktens interna bestämmelser (FIB 2015:1) om skydd för utrikes- och sekretessklassificerade uppgifter att gälla. Istället ska bestämmelser om skydd för säkerhetsskyddsklassificerade uppgifter följas.

Med *sekretessklassificerad uppgift* avses uppgifter som omfattas av sekretess enligt OSL, men som inte är säkerhetsskyddsklassificerade uppgifter. Skyddet för sekretessklassificerade uppgifter beskrivs f.n. inte i detta reglemente. Bestämmelser om skyddet för sådana uppgifter finns i Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter. Reglementet kommer att uppdateras efter att de interna bestämmelserna har reviderats. Skyddsåtgärderna förklaras i Handbok för Försvarsmaktens säkerhetstjänst, Informationssäkerhet (H SÄK Infosäk).

Observera!
Begreppet *sekretessklassificerad* ska inte förväxlas med *säkerhetsskyddsklassificerad*.

3.1.3. Säkerhetsskyddsklassificering

”Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.”

1 kap. 2 § andra stycket säkerhetsskyddslagen

Vägledande förklaring: Det förutsätts att uppgiften till sin natur är sådan att den kan hänföras till en bestämmelse om sekretess, med hänsyn till antingen Sveriges säkerhet eller Sveriges förbindelser med någon annan stat eller mellanfolklig organisation.[114]

Observera!
För att en uppgift ska vara säkerhetsskyddsklassificerad måste uppgiften omfattas av sekretess enligt OSL. Villkor för t.ex. försvarssekretessen måste vara uppfyllda.

[114] Prop. 2017/18:89 s. 135.

Att en uppgift vid ett tillfälle har bedömts vara säkerhetsskyddsklassificerad ska inte vara avgörande vid en senare prövning enligt OSL om utlämnande av uppgifter.[115]

3.1.3.1 Stöd i sekretessbedömning vid säkerhetsskyddsklassificering

Den sekretessbestämmelse som främst avser uppgifter om förberedelser för försvaret av Sverige är sekretessen i 15 kap. 2 § OSL (den s.k. försvarssekretessen). Uppgifter som omfattas av försvarssekretess är alltid säkerhetsskyddsklassificerade uppgifter.

Uppgifter som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande är säkerhetsskyddsklassificerade uppgifter. Uppgifterna omfattas normalt av sekretess enligt 15 kap. 1 § OSL (den s.k. utrikessekretessen).[116] I ett internationellt samarbete kan det också finnas andra uppgifter som *inte* ska skyddas enligt ett internationellt säkerhetsskyddsåtagande, men där det finns något annat intresse som ska skyddas. Även i sådana fall kan uppgifterna omfattas av sekretess enligt 15 kap. 1 § OSL, men är då *inte* säkerhetsskyddsklassificerade.

I 18 kap. OSL finns bestämmelser bl.a. till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. Beroende på omständigheterna i det enskilda fallet kan uppgifter som omfattas av sekretess enligt bestämmelserna i 18 kap. OSL anses röra säkerhetskänslig verksamhet och vara säkerhetsskyddsklassificerade uppgifter.[117] Exempel på sekretessbestämmelser i 18 kap. OSL som skulle kunna komma ifråga är:

- 18 kap. 1 § om förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel m.m.
- 18 kap. 2 § underrättelseverksamhet.
- 18 kap. 3 § myndigheter som biträder åklagarmyndigheter m.fl.
- 18 kap. 5 § kvalificerade skyddsidentiteter.
- 18 kap. 8 § säkerhets- och bevakningsåtgärder.
- 18 kap. 9 § chiffer och kod.
- 18 kap. 12 § upplysning som kan användas i syfte att åstadkomma kärnsprängning eller spridning av kärnvapen.
- 18 kap. 13 § risk- och sårbarhetsanalyser.

Tabell 3.3 sammanfattar när uppgift som omfattas av sekretess enligt några sekretessbestämmelser är säkerhetsskyddsklassificerade.

Tips!
Försvarssekretessen (15 kap. 2 § OSL), utrikessekretessen (15 kap. 1 § OSL) och säkerhets- och bevakningssekretessen (18 kap. 8 § OSL) beskrivs på sidorna 22, 26 och 30 i Handbok för Försvarsmaktens säkerhetstjänst, Sekretessbedömning Del A (H SÄK Sekrbed A).

[115] Prop. 2017/18:89 s. 140.
[116] Prop. 2017/18:89 s. 52.
[117] SOU 2015:25 s. 147.

Tabell 3.3. Förhållande mellan några sekretessbestämmelser och säkerhetsskyddsklassificerade uppgifter.

Sekretess enligt OSL	Säkerhetsskyddsklassificerade uppgifter
15 kap. 2 §	Alltid
15 kap. 1 §	Ja, om ett röjande av uppgiften kan medföra skada för Sveriges säkerhet. Ja, om uppgiften ska skyddas enligt ett internationellt säkerhetsskyddsåtagande. Nej, om ett röjande av uppgiften inte kan medföra skada för Sveriges säkerhet och uppgiften inte ska skyddas enligt ett internationellt säkerhetsskyddsåtagande.
18 kap.	Ja, om ett röjande av uppgiften kan medföra skada för Sveriges säkerhet. Nej, om ett röjande av uppgiften inte kan medföra skada för Sveriges säkerhet.

3.1.3.2 Skada för Sveriges säkerhet

”Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen i säkerhetsskyddsklasser ska göras enligt följande:

1.kvalificerat hemlig vid en synnerligen allvarlig skada,

2.hemlig vid en allvarlig skada,

3.konfidentiell vid en inte obetydlig skada, eller

4.begränsat hemlig vid endast ringa skada.”

2 kap. 5 § första stycket säkerhetsskyddslagen

Vägledande förklaring: Klassificering ska ske efter en bedömning av vilken skada för Sveriges säkerhet som ett röjande av uppgiften skulle medföra. Bedömningen görs endast för att fastställa korrekt skyddsnivå. Till säkerhetsskyddsklasserna kopplas specifika åtgärder för att skydda uppgifterna. Bestämmelsen är teknikneutral. Klassificeringen ska alltså ske av uppgifter i såväl fysisk som digital form.[118]

Med säkerhetsskyddsklasserna i säkerhetsskyddslagen får Sverige ett nationellt system för indelning av säkerhetsskydd för uppgifter i fyra nivåer. Indelningen i fyra säkerhetsskyddsklasser kan jämföras med indelningen av säkerhetsskyddsklassifice-

[118] Prop. 2017/18:89 s. 140.

rade uppgifter i EU, Nato och andra länder. Säkerhetsskyddsklasserna ersätter informationssäkerhetsklasserna som Försvarsmakten införde 2004.

Tabell 3.4 ger stöd i bedömning i vilken säkerhetsskyddsklass en säkerhetsskyddsklassificerad uppgift placeras i, med avseende på den skada för Sveriges säkerhet som ett röjande av uppgiften kan medföra. Med nationell förmåga avses t.ex. den nationella försvarsförmågan.

Tabell 3.4. Beskrivning av konsekvenser vid röjande av säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskyddsklass	Beskrivning av konsekvenser som ett röjande kan medföra
Kvalificerat hemlig **Förkortning: KH**	Synnerligen allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa.
Hemlig **Förkortning: H**	Allvarliga negativa konsekvenser, av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funktioner. Svårt att återställa.
Konfidentiell **Förkortning: K**	Påtagliga negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott.
Begränsat hemlig **Förkortning: BH**	Ringa negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning.

3.1.3.3 Internationellt åtagande om säkerhetsskydd

”Säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd ska på motsvarande sätt delas in i säkerhetsskyddsklass, om de inte redan har klassificerats av en annan stat eller en mellanfolklig organisation. Indelningen i säkerhetsskyddsklass ska i sådant fall göras utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation.”

2 kap. 5 § andra stycket säkerhetsskyddslagen

Vägledande förklaring: Internationellt åtagande om säkerhetsskydd avser överenskommelser om säkerhetsskydd som Sverige har ingått med andra stater och mellanfolkliga organisationer (avsnitt 1.7.4). Sveriges säkerhetsskyddsavtal med andra stater och mellanfolkliga organisationer innehåller vanligen en översättningstabell för ländernas eller organisationernas säkerhetsskyddsklasser. Säkerhetsskyddsavtalen

innehåller bestämmelser som innebär att den part som tar emot säkerhetsskyddsklassificerade uppgifter ska placera uppgifterna i den säkerhetsskyddsklass som motsvarar den avsändande partens säkerhetsskyddsklass.

Om de säkerhetsskyddsklassificerade uppgifterna har klassificerats av en annan stat eller mellanfolklig organisation ska klassificeringen godtas.[119] En inkommande handling från en annan stat eller mellanfolklig organisation som redan är märkt med en motsvarighet till en svensk säkerhetsskyddsklass, ska märkas med den säkerhetsskyddsklass som motsvarar den utländska märkningen.

Exempel
En handling inkommer till Högkvarteret från Huvudstaben för Finlands försvarsmakt. Handlingen är märkt med beteckningen Begränsad Tillgång. *Danmark, Finland, Island, Norge och Sverige har ingått ett generellt säkerhetsskyddsavtal (SÖ 2013:17). Enligt avtalet motsvarar* Begränsad Tillgång *den lägsta nivån av ländernas säkerhetsskyddsklasser. Högkvarteret märker därför handlingen med säkerhetsskyddsklassen* Begränsat hemlig.

Tabell 3.5 visar andra staters och mellanfolkliga organisationers motsvarigheter till säkerhetsskyddsklasserna i säkerhetsskyddslagen. Tabellen är en sammanställning av information från säkerhetsskyddsavtal som Sverige har ingått och andra källor. Vilka säkerhetsskyddsavtal som Sverige har ingått framgår i SAMSÄK (avsnitt 1.3.1).

Andra stater och mellanfolkliga organisationer kan ha klassificeringar av uppgifter som *inte* är säkerhetsskyddsklassificerade i den andra staten eller organisationen (UNCLASSIFIED eller motsvarande beskrivs i avsnitt 3.1.4). Sådana klassificeringar ingår inte i internationella åtaganden om säkerhetsskydd och anges därför inte i tabell 3.5.

Tabell 3.5. Andra staters och mellanfolkliga organisationers motsvarigheter till Sveriges säkerhetsskyddsklasser.

Sverige	Kvalificerat hemlig	Hemlig	Konfidentiell	Begränsat hemlig
Belgien	Très Secret	Secret	Confidentiel	[120]
	Zeer geheim	Geheim	Vertrouwelijk	
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Cypern	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης

[119] Prop. 2017/18:89 s. 140.
[120] Motsvarighet till säkerhetsskyddsklass begränsat hemlig saknas.

REGLEMENTE

Sverige	Kvalificerat hemlig	Hemlig	Konfidentiell	Begränsat hemlig
Danmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
ESA	ESA TOP SECRET	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	Eura - Top Secret	Eura - Secret	Eura - Confidential	Eura - Restricted
Finland	Erittäin Salainen	Salainen	Luottamuksellinen	Käyttö Rajoitettu
	Ytterst hemlig	Hemlig	Konfidentiell	Begränsad tillgång
Frankrike	Très Secret Défense	Secret Défense	Confidentiel Défense	[121]
Grekland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Irland	Top Secret	Secret	Confidential	Restricted
Island	Algjort Leyndarmal	Leyndarmal	Trunadarmal	Takmarkadur Adgangur
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Kanada	Top Secret	Secret	Confidential	[122]
	Très Secret	Secret	Confidentiel	
Korea	[123]	군사 II급 비밀 /SECRET	군사 II급 비밀 /CONFIDENTIAL	군사대외비 /DAE WOI BI

[121] Motsvarighet till säkerhetsskyddsklass begränsat hemlig saknas.
[122] Motsvarighet till säkerhetsskyddsklass begränsat hemlig saknas.
[123] Motsvarighet till säkerhetsskyddsklass kvalificerat hemlig ingår inte i säkerhetsskyddsavtal med Korea (SÖ 2009:24). Information i övrigt saknas.

Sverige	Kvalificerat hemlig	Hemlig	Konfidentiell	Begränsat hemlig
Kroatien	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
	Top Secret	Secret	Confidential	Restricted
Nato	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Nederländerna	STG Zeer geheim	STG Geheim	STG Confidentieel	DEP Vertrouwelijk
Norge	Strengt Hemmelig	Hemmelig	Konfidensielt	Begrenset
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Rumänien	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Schweiz	[124]	GEHEIM	VERTRAULICH	[125]
		SECRET	CONFIDENTIEL	
		SEGRETO	CONFIDENZIALE	
Singapore	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Slovakien	Prísne tajné	Tajné	Dôverné	Vyhradené

[124] Motsvarighet till säkerhetsskyddsklass kvalificerat hemlig ingår inte i säkerhetsskyddsavtal med Schweiz (SÖ 2004:25). Information i övrigt saknas.
[125] Motsvarighet till säkerhetsskyddsklass begränsat hemlig saknas.

Sverige	Kvalificerat hemlig	Hemlig	Konfidentiell	Begränsat hemlig
Slovenien	Strogo tajno	Tajno	Zaupno	Interno
Spanien	Secreto	Reservado	Confidencial	Difusión Limitada
Storbritannien och Nordirland	UK TOP SECRET	UK SECRET		UK OFFICIAL - SENSITIVE
Sydafrika	Top Secret	Secret	Confidential	Restricted
Tjeckien	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Tyskland	Streng geheim	Geheim	VS – Vertraulich	VS - Nur für den Dienstgebrauch
Ungern	Szigorúan titkos	Titkos	Bizalmas	Korlátozott terjesztésű
USA	Top Secret	Secret	Confidential	[126]
Österrike	Streng Geheim	Geheim	Vertraulich	Eingeschränkt

I vissa internationella samarbeten upprättar Försvarsmakten handlingar som innehåller uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande. I sådana fall placeras uppgifterna i säkerhetsskyddsklass utifrån den skada ett röjande kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation. Det regelverk (Memorandum of Understanding, Technical Arrangement etc.) som är tillämpligt i det aktuella samarbetet kan utgöra ett stöd vid bedömningen.[127]

Säkerhetsskyddsklassificerade uppgifter som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande omfattas i regel av sekretess enligt 15 kap. 1 § OSL (den s.k. utrikessekretessen).

Observera!
Att det finns ett säkerhetsskyddsavtal med en annan stat eller mellanfolklig organisation betyder inte att alla säkerhetsskyddsklassificerade uppgifter får lämnas till den andra staten eller organisationen. För att uppgifterna ska få lämnas måste villkor i 8 kap. 3 § OSL vara uppfyllda.

[126] Motsvarighet till säkerhetsskyddsklass begränsat hemlig saknas.
[127] Prop. 2017/18:89 s. 140.

3.1.3.4 Ändra säkerhetsskyddsklassificering i det internationella samarbetet

I överenskommelser om säkerhetsskydd som Sverige har ingått med andra stater och mellanfolkliga organisationer, framgår vanligtvis att säkerhetsskyddsklassificerade uppgifter som har klassificerats av en annan stat eller mellanfolklig organisation inte får ändras utan skriftligt tillstånd från ursprungsparten.

Om det finns behov av att ändra säkerhetsskyddsklass på en säkerhetsskyddsklassificerad handling som har inkommit från en annan stat eller mellanfolklig organisation, måste det avtal som gäller för samarbetet undersökas om Sverige får ändra märkningen eller om det först krävs ett skriftligt tillstånd från ursprungsparten.

3.1.3.5 Kvalificerat hemlig i det internationella samarbetet

I det internationella samarbetet kan det förekomma säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemlig där ett röjande av uppgifterna inte medför en synnerligen allvarlig skada för *Sveriges säkerhet*.

Det kan t.ex. handla om en handling som inkommer från en annan stat och som är märkt TOP SECRET, men där ett röjande av uppgifterna medför en mindre skada för Sveriges säkerhet. Eftersom handlingen redan har klassificerats av en annan stat ska den placeras i säkerhetsskyddsklass kvalificerat hemlig.[128] [129]

Frågan om utlämning av allmänna handlingar som är av *synnerlig betydelse för rikets säkerhet* ska enligt 1 § OSF i vissa fall prövas av en annan myndighet.[130] Se även moment 3:3 i avsnitt 3.4.1 om märkning.

3.1.3.6 Internationellt samarbete där åtagande om säkerhetsskydd saknas

Om Försvarsmakten deltar i internationellt samarbete med andra stater och mellanfolkliga organisationer får inte avsaknaden av säkerhetsskyddsavtal försämra skyddet för den andra statens eller organisationens handlingar. Bestämmelser för hantering av säkerhetsskyddsklassificerade handlingar tillämpas även för sådana handlingar.

Förenta nationerna (FN) har ingen klassificeringsmodell som motsvarar säkerhetsskyddsklasser enligt säkerhetsskyddslagen.[131] Handlingar från FN-organ som är märkta med beteckningarna *strictly confidential* eller *confidential* kan omfattas av sekretess enligt 15 kap. 1 § OSL men placeras inte i säkerhetsskyddsklass.

3.1.4. Handlingar från utlandet som är märkta UNCLASSIFIED eller LIMITE

Handlingar från andra stater och mellanfolkliga organisationer kan vara försedda med beteckningar som anger att handlingen innehåller uppgifter som omfattas av sekretess enligt den andra statens eller mellanfolkliga organisationens regler men som inte ska ges ett särskilt skydd. Exempel på sådana beteckningar är NATO UN-

[128] 2 kap. 5 § andra stycket säkerhetsskyddslagen.
[129] Prop. 2017/18:89 s. 140.
[130] 1 § OSF.
[131] Generalsekreterarens bulletin ”Information sensitivity, classification and handling” (ST/SGB/2007/6).

CLASSIFIED, LIMITE, som förekommer i EU, och Controlled Unclassified Information (CUI), som förekommer i USA.

En handling som är märkt LIMITE lämnas ut internt inom Europeiska rådet, bland dess medlemmar, inom Europeiska kommissionen och vissa andra EU-institutioner och EU-organ. Sådana handlingar får överlämnas till alla tjänstemän vid medlemsstaternas nationella förvaltningar och Europeiska kommissionen.[132]

En handling som inkommer till Försvarsmakten från en annan stat eller en mellanfolklig organisation och som är märkt UNCLASSIFIED eller motsvarande *kan* innehålla uppgifter som omfattas av sekretess enligt OSL. Sådana handlingar innehåller normalt inte säkerhetsskyddsklassificerade uppgifter.

Om ett röjande av uppgifterna i handlingen skulle störa Sveriges mellanfolkliga förbindelser eller på annat sätt skadar Sverige medför detta att handlingen bör sekretessmarkeras med en hänvisning till 15 kap. 1 § OSL. En sådan handling är i Försvarsmakten *sekretessklassificerad*. En handling som är märkt UNCLASSIFIED eller motsvarande är således inte att likställa med att den är offentlig.

En handling från en annan stat eller en mellanfolklig organisation och som är märkt UNCLASSIFIED eller motsvarande kan även innehålla uppgifter som omfattas av andra sekretessbestämmelser i OSL, t.ex. sekretess för uppgifter om enskilds personliga eller ekonomiska förhållanden. Vid sekretessprövning av en handling som inkommer från en annan stat eller mellanfolklig organisation är det därför nödvändigt att inte enbart undersöka om ett röjande av uppgifterna stör Sveriges mellanfolkliga förbindelser.

[132] Europeiska unionens råd, informerande not 5847/06 Hantering av LIMITE-markerade handlingar.

3.2. Informationssäkerhet i säkerhetsskyddet exklusive it-säkerhet

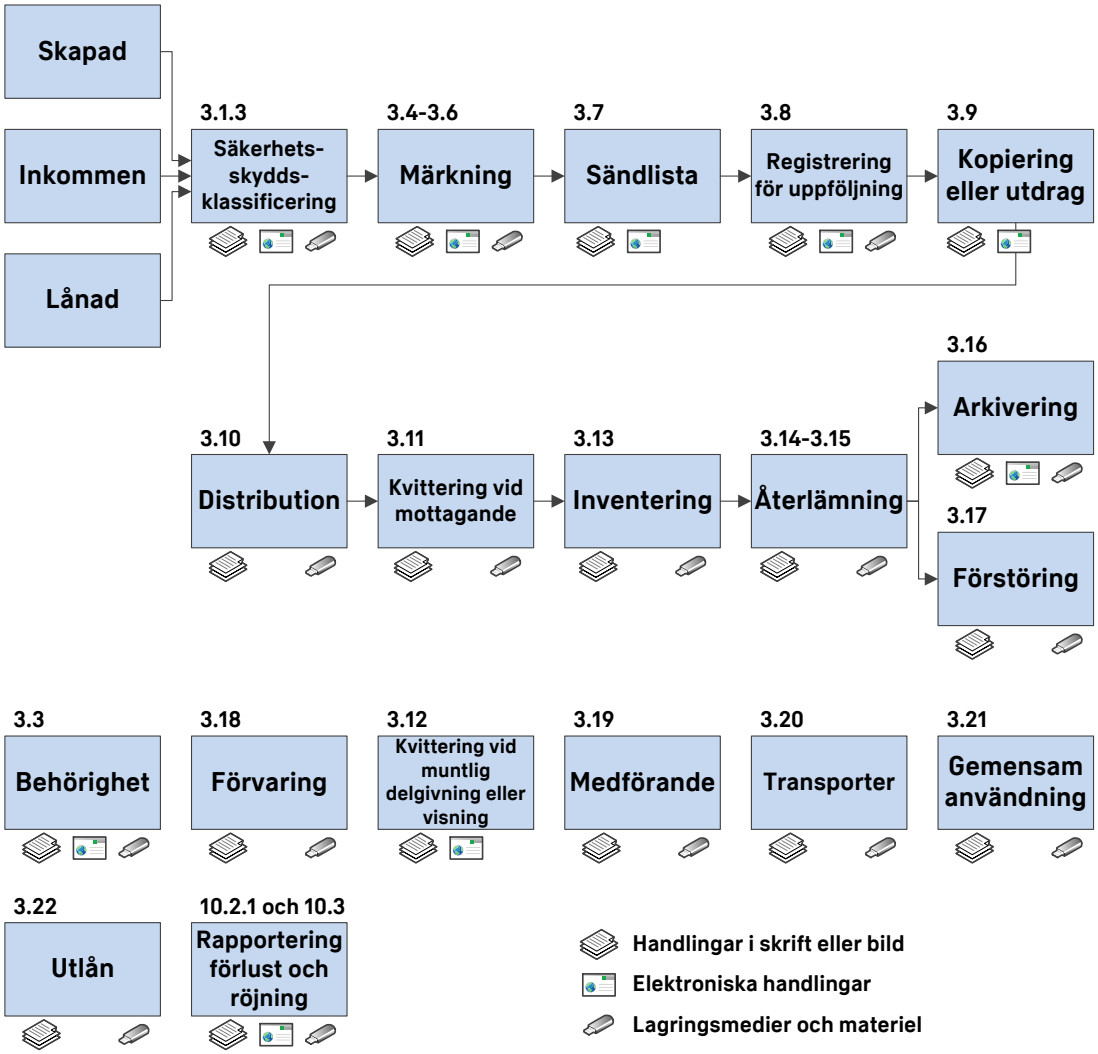


Bild 3.3. Översikt över åtgärder för hantering av säkerhetsskyddsklassificerade handlingar, tryckta skrifter, lagringsmedier och materiel. Siffrorna visar i vilket avsnitt åtgärden beskrivs i reglementet. Kim Hakkarainen/Försvarsmakten

Bild 3.3 visar livscykeln, t.ex. från det att ett exemplar av en handling har skapats till dess att den har förstörts.

3.2.1. Handlingar

Enligt 2 kap. 3 § tryckfrihetsförordningen är en *handling* en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt.

En *säkerhetsskyddsklassificerad handling* är en handling som innehåller en säkerhetsskyddsklassificerad uppgift.[133]

> *”Om inget annat anges, avses med säkerhetsskyddsklassificerad handling även säkerhetsskyddsklassificerad elektronisk handling.*
>
> *Med begreppet säkerhetsskyddsklassificerad handling avses både allmänna och icke allmänna handlingar.”*
>
> 3 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Elektroniska handlingar är inte begränsade till dokument som utgör en direkt motsvarighet till pappersdokument (t.ex. en PDF-fil). Elektroniska handlingar avser även skärmbilder där uppgifter presenteras (t.ex. rapportgenerering från poster i en databas). Även e-post och andra upptagningar i informationssystem, t.ex. nätverksdata och chat, utgör elektroniska handlingar.

3.2.2. Lagringsmedier

Ett *lagringsmedium* är ett permanent minnesmedium som används för att kunna lagra och läsa uppgifter.[134] Ett permanent minnesmedium är ”icke-flyktigt”, dvs. det behöver inte vara anslutet till ström för att behålla lagrade data. Exempel på permanent minnesmedium är lagringsmedier såsom t.ex. hårddiskar med roterande magnetiska skivor, SSD-diskar, CD, DVD, Blu-ray, backupband, USB-minnen och aktiva kort. En dators arbetsminne (RAM) är normalt flyktigt, dvs. tappar sitt innehåll kort tid efter att strömmen slås av, och ingår inte i definitionen av lagringsmedium. Ett lagringsmedium behöver inte vara digitalt utan även analoga lagringsmedium, som t.ex. analoga ljudband, ingår i definitionen.

3.2.3. Materiel

> *”Materiel som innehåller säkerhetsskyddsklassificerade uppgifter ska ges ett säkerhetsskydd som motsvarar vad som gäller för säkerhetsskyddsklassificerade lagringsmedier.”*
>
> 3 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med materiel menas här utrustning som utan att vara ett informationssystem, eller innehålla ett lagringsmedium, innehåller säkerhetsskyddsklassificerade uppgifter. Det kan t.ex. röra sig om teknisk utrustning vars konstruktion, konfiguration eller inställningar är säkerhetsskyddsklassificerade uppgifter.

---

[133] 1 kap. 4 § säkerhetsskyddsförordningen.
[134] 1 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd.

3.2.4. Tryckta skrifter

”En tryckt skrift som innehåller säkerhetsskyddsklassificerade uppgifter ska ges det säkerhetsskydd som gäller för en säkerhetsskyddsklassificerad allmän handling.”

3 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Handlingar som ingår i en myndighets bibliotek är undantagna från att vara allmänna handlingar, enligt det så kallade biblioteksundantaget i 2 kap. 14 § första stycket 3 tryckfrihetsförordningen.

Bestämmelsen innebär att bokpublikationer och andra tryckta skrifter som innehåller säkerhetsskyddsklassificerade uppgifter ska ges samma säkerhetsskydd som allmänna handlingar som innehåller sådana uppgifter, t.ex. registrering av exemplar, kvittering vid mottagande, inventering och dokumenterad förstöring.

Exempel på tryckta skrifter som omfattas av bestämmelsen är materielbokpublikationer, reglementen, manualer och handböcker som innehåller säkerhetsskyddsklassificerade uppgifter. Ett annat exempel är kartor och sjökort som innehåller säkerhetsskyddsklassificerade uppgifter.

3.2.5. Lån av handlingar

”En myndighet som lånar en säkerhetsskyddsklassificerad handling från en annan myndighet ska ge handlingen det säkerhetsskydd som gäller för en säkerhetsskyddsklassificerad allmän handling.”

3 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: När en myndighet lånar en allmän handling från en annan myndighet, kan handlingen komma att anses inte vara en allmän handling hos den inlånande myndigheten. Exempel på en situation som avses är när en myndighet i ett ärende lånar en handling, eller en akt med handlingar, från en annan myndighet för att kunna bedöma en fråga i ärendet. Efter handläggning hos myndigheten återlämnas den lånade handlingen eller akten till den utlånande myndigheten. Ett annat exempel är när den lånande myndigheten behöver få tillgång till information som finns i en handling, utan att det är fråga om ett ärende.

Bestämmelsen innebär att en inlånad säkerhetsskyddsklassificerad handling ska ges samma säkerhetsskydd som om handlingen var en allmän handling. Om handlingen är placerad i säkerhetsskyddsklass konfidentiell eller högre omfattar det bl.a. registrering ur säkerhetsskyddssynpunkt för att möjliggöra uppföljning av innehav, kvittering vid mottagande och inventering. Ett sådant register kan därför behöva göra skillnad på lånade handlingar och andra handlingar.

Bestämmelsen är inte avsedd att tillämpas på s.k. *delningar* där syftet är att skicka ett utkast för att inhämta synpunkter, enligt undantaget i 2 kap. 12 § andra stycket tryckfrihetsförordningen.

Bestämmelsen gäller oavsett om den inlånande handlingen är en allmän handling eller inte, hos den utlånande myndigheten.

I avsnitt 3.22 beskrivs utlåning av säkerhetsskyddsklassificerade handlingar och lagringsmedier.

3.3. Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter

Med behörighet att ta del av en uppgift avses rätt att få ta del av uppgiften först efter att vissa villkor har uppfyllts. Villkoren kan skilja sig åt för olika typer av uppgifter.

> *”Behörig att ta del av säkerhetsskyddsklassificerade uppgifter eller i övrigt delta i säkerhetskänslig verksamhet är, om inte något annat följer av bestämmelser i lag, endast den som*
>
> *1. har bedömts pålitlig från säkerhetssynpunkt,*
>
> *2. har tillräckliga kunskaper om säkerhetsskydd, och*
>
> *3. behöver uppgifterna eller annan tillgång till verksamheten för att kunna utföra sitt arbete eller på annat sätt delta i den säkerhetskänsliga verksamheten.”*
>
> 2 kap. 3 § säkerhetsskyddsförordningen

Vägledande förklaring: Detta är den grundläggande bestämmelsen om behörighet att ta del av säkerhetsskyddsklassificerade uppgifter. Ett exempel på ett undantag är om det av en bestämmelse i lag framgår att det finns en uppgifts- eller informationsskyldighet mellan myndigheter, t.ex. vid tillsyn eller brottsutredning. I sådana fall är personer som ska ta del av de säkerhetsskyddsklassificerade uppgifterna behöriga att ta del av dem utan att villkoren är uppfyllda. Märk väl att uppgifterna i dessa fall fortfarande är säkerhetsskyddsklassificerade.

I avsnitt 7.2.2 beskrivs utbildning för att vara behörig att ta del av säkerhetsskyddsklassificerade uppgifter.

3.3.1. Upplysning och sekretessbevis

> *”En verksamhetsutövare ska upplysa den som tillåts ta del av säkerhetsskyddsklassificerade uppgifter om räckvidden och innebörden av den sekretess och tystnadsplikt som följer av offentlighets- och sekretesslagen (2009:400) respektive 5 kap. 2 § säkerhetsskyddslagen (2018:585).*”
>
> 2 kap. 4 § säkerhetsskyddsförordningen

Vägledande förklaring: Med *räckvidden för sekretessen* avses t.ex. att sekretessen gäller inom myndigheten och mellan myndigheter samt att sekretessen gäller efter avslutad anställning, uppdrag eller motsvarande. Räckvidd för sekretessbestämmelser i OSL bestäms normalt genom att det i bestämmelserna preciseras att sekretessen för de angivna uppgifterna bara gäller i viss typ av verksamhet eller i viss typ av ärende eller hos en viss myndighet. Sekretessbestämmelserna i 15 kap. 1 och 2 §§ OSL, utrikes- och försvarssekretesserna, gäller i all offentlig verksamhet.

Med *innebörden av sekretessen* avses de fall där en viss sekretessbestämmelse ska tillämpas för ett visst förhållande, t.ex. i vilka fall uppgifter i verksamheten är sekretessbelagda enligt 15 kap. 2 § OSL.

Med *tystnadsplikt* avses förbud att röja en uppgift som omfattas av sekretess enligt OSL. Tystnadsplikten i OSL är en begränsning av offentliga funktionärers rätt till yttrandefrihet. Rätten att meddela och offentliggöra uppgifter gäller för alla, även för offentliga funktionärer. Rätten gäller dock inte alltid, bl.a. är det inte tillåtet att meddela eller offentliggöra uppgifter om uppgiftslämnaren på det sättet gör sig skyldig till vissa allvarliga brott mot Sveriges säkerhet, till exempel spionerі, grovt spionerі eller grov obehörig befattning med hemlig uppgift eller försök, förberedelse eller stämpling till sådant brott.[135] Det är heller inte tillåtet att med avsikt lämna ut en allmän handling som innehåller sekretessbelagda uppgifter för publicering. I de fall tystnadsplikt anges särskilt i OSL är det heller inte tillåtet att bryta mot tystnadsplikten.[136]

I det allmännas verksamhet gäller OSL. För annan verksamhet finns det i 5 kap. 2 § säkerhetsskyddslagen bestämmelse om att tystnadsplikt gäller för den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet.

Den som bryter mot tystnadsplikt och röjer säkerhetsskyddsklassificerade uppgifter kan ställas till ansvar för brott mot Sveriges säkerhet i 19 kap. brottsbalken eller brott mot tystnadsplikten i 20 kap. 3 § brottsbalken.

”Chef för organisationsenhet ansvarar för att den som ska få ta del av säkerhetsskyddsklassificerade uppgifter har utbildats om räckvidden och innebörden av sekretessen och att ett bevis (sekretessbevis) upprättas om att så har skett.”

3 kap. 1 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Sekretessbeviset tecknas först efter att utbildningen har ägt rum. Utbildningen bör genomföras av en person som har kunskap om sekretessbe-

[135] Prop. 2017/18:89 s. 155.
[136] Justitiedepartementets broschyr Offentlighetsprincipen och sekretess – Kortfattat om lagstiftningen s. 8-9.

stämmelserna och som kan förklara deras innebörd. Det är således inte tillräckligt att få läsa sekretessbestämmelsernas innehåll utan att de förklaras.

Ett sekretessbevis är en bekräftelse på att personen har blivit informerad om vad som gäller om sekretess. Att en person undertecknar ett sekretessbevis binder inte personen ifråga om sekretess. En anställd är bunden av sekretessbestämmelserna i OSL oavsett om ett sekretessbevis har undertecknats. I en eventuell rättegång är ett sekretessbevis ett bevis på att den anställde har eller borde ha förstått att han eller hon bröt mot sin tystnadsplikt.

Sekretessbevis får endast upprättas för personer som är anställda vid Försvarsmakten, har uppdrag vid myndigheten eller på grund av tjänsteplikt deltar i myndighetens verksamhet. Sekretessbevis får inte upprättas för en annan myndighets personal då skyddsåtgärden inte är reglerad i en myndighetsöverskridande författning. Det får förutsättas att personal från en annan myndighet har undertecknat ett sekretessbevis vid den myndighet där personalen är anställd. Det kan i samarbeten mellan myndigheter vara nödvändigt att upplysa den deltagande personalen om vilka uppgifter i samarbetet som bedöms omfattas av sekretess. En sådan upplysning kan genomföras utan att sekretessbevis upprättas.

Det finns ingen bestämmelse om att ett sekretessbevis ska upprättas eller att ett befintligt sekretessbevis ska undertecknas på nytt när anställning eller annat deltagande avslutas. Se även avsnitt 6.15 om upplysning om räckvidd och innebörd av sekretess, när anställning eller annat deltagande i säkerhetskänslig verksamhet avslutas.

3.3.2. Behörighetsförteckning

”I 2 kap. 3 § säkerhetsskyddsförordningen (2018:658) finns föreskrifter om vem som är behörig att ta del av säkerhetsskyddsklassificerade uppgifter.

Myndigheten ska dokumentera vilka personer som är behöriga (behörighetsförteckning) att ta del av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell eller högre.”

3 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

”Sådana förteckningar ska föras vid varje organisationsenhet.”

3 kap. 2 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Behörighetsförteckningen används så att endast de personer som står med på förteckningen kan komma att ta del av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, t.ex.:

- när behörigheter läggs in i ett informationssystem, eller

- när en person tar emot en sådan säkerhetsskyddsklassificerad handling eller lagringsmedium från en expedition.

En behörighetsförteckning måste uppdateras löpande när personer blir behöriga eller när deras behörighet upphör. Det finns inget krav att förteckningen ska uppdateras med en viss periodicitet.

Om det inför samverkan med andra myndigheter eller andra organisationsenheter är oklart om en person är behörig, kan det vara lämpligt att kontrollera detta med myndighetens eller enhetens lokala säkerhetsorganisation.

Det kan finnas flera behörighetsförteckningar som är uppdelade på organisatoriska delar eller verksamhetsplatser.

En behörighetsförteckning bör innehålla identifieringsuppgifter så att varje person unikt kan identifieras även efter att förteckningen inte längre används eller efter att personer avslutat sin anställning eller deltagande i Försvarsmaktens verksamhet. Det är därför lämpligt att använda namn och personnummer i förteckningen. FMID får användas istället för personnummer, eftersom den är unikt knuten till en person i Försvarsmakten. Det är lämpligt att det på behörighetsförteckningen framgår vem som har beslutat att en person ska tas med på förteckningen.

Att en person anges på en behörighetsförteckning betyder inte att personen är behörig att ta del av alla säkerhetsskyddsklassificerade uppgifter, personen måste enligt 2 kap. 3 § säkerhetsskyddsförordningen även vara i behov av uppgifterna för att kunna utföra sitt arbete.

Personer behöver inte finnas med i en behörighetsförteckning för att ta del av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklassen begränsat hemlig. Villkoren för behörighet i 2 kap. 3 § säkerhetsskyddsförordningen ska dock vara uppfyllda även för att få ta del av sådana uppgifter.

3.3.3. Utländsk myndighet

”En uppgift för vilken sekretess gäller enligt denna lag får inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte

1. utlämnande sker i enlighet med särskild föreskrift i lag eller förordning,

eller

2. uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.”

8 kap. 3 § OSL

Vägledande förklaring: Bestämmelsen innehåller villkor för när en uppgift som omfattas av sekretess enligt OSL får lämnas till en utländsk myndighet eller en mellanfolklig organisation. Grunden är att sekretessbelagda uppgifter inte ska röjas till en annan stat.

För uppgifter som omfattas av sekretess enligt 15 kap. 2 § OSL (försvarssekretess) finns dessutom särskilda bestämmelser i förordningen om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet. En sådan uppgift får av Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut lämnas till en utländsk myndighet som deltar i ett samarbete inom Försvarsdepartementets område endast om samtliga följande fyra villkor är uppfyllda.

- Samarbetet ska ingå i överenskommelse med den andra staten eller mellanfolkliga organisationen som har ingåtts av regeringen eller en förvaltningsmyndighet efter uppdrag från regeringen.
- Det är enligt den utlämnande myndighetens prövning nödvändigt för att genomföra samarbetet.
- Uppgiften är inte av synnerlig betydelse för rikets säkerhet (kvalificerat hemlig).
- Uppgiften kan inte ge underlag för utveckling av motmedel mot Sveriges försvarssystem.[137]

Om samtliga villkor är uppfyllda behöver inte regeringen tillfrågas före ett lämnande av en uppgift. Om det i Försvarsmakten finns ett behov att delge uppgifter som omfattas av försvarssekretess, men det inte bedöms vara möjligt med hänsyn till villkoren ovan bör HKV LEDS JUR kontaktas.

3.3.4. Utländsk företrädares intyg om säkerhetsklarering

”Om en företrädare för en utländsk myndighet eller en mellanfolklig organisation kommer att ta del av säkerhetsskyddsklassificerade uppgifter ska organisationsenheten kontrollera att företrädaren har ett säkerhetsintyg.

Chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, ansvarar för att en sådan företrädare endast tar del av säkerhetsskyddsklassificerade uppgifter upp till och med den säkerhetsskyddsklass som framgår av intyget.”

3 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: I bilaterala säkerhetsskyddsavtal finns det vanligen bestämmelser om behörighet till information och hur en sådan behörighet ska styrkas. Behörighetsprincipen är densamma i många länder, men det som skiljer sig från svenska förhållanden är att andra länder normalt utfärdar ett intyg som styrker en persons behörighet att ta del av säkerhetsskyddsklassificerade uppgifter (eller mot-

[137] 1 § förordningen om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet.

svarande typ av information i de andra länderna). I Sverige har vi anpassat oss till denna modell när det behövs och vi har även åtagit oss i dessa avtal att följa rutinerna kring uppvisande av intyg om säkerhetsklarering (på engelska Certificate of Personnel Security Clearance, PSCC eller vanligare bara PSC).

Intyget kan antingen uppvisas personligen eller skickas av den organisation som personen företräder eller av en nationell säkerhetsmyndighet. Det förekommer också att denna behörighet intygas som en del i en besöksanmälan. Således behöver inte intyget följa en särskild mall, även om sådana kan underlätta intygandet. Alla dessa sätt är möjliga, men det är organisationsenheten där de säkerhetsskyddsklassificerade uppgifterna ska delges som ansvarar för att den utländska personen i fråga verkligen har ett intyg i någon form. Vid osäkerhet kring utformningen av ett sådant intyg eller avseende utfärdaren bör samverkan ske med säkerhetsskyddsavdelningen vid Must. I vissa särskilda samarbeten förekommer det att ett utbyte av säkerhetsskyddsklassificerade uppgifter föregås av noggranna förberedelser samt att namn på behöriga personer skickas i förväg via särskilt överenskomna kanaler.

I sådana särskilda fall där det är uppenbart att en person som representerar en utländsk myndighet har behörighet till säkerhetsskyddsklassificerade uppgifter i en viss säkerhetsskyddsklass kan detta underlåtas under förutsättning att det också är accepterat, och tillämpas ömsesidigt, av den utländska myndigheten.

FARA!
Att en företrädare för en utländsk myndighet eller en mellanfolklig organisation kan visa upp ett intyg om säkerhetsklarering innebär inte att den utländska företrädaren med automatik ska få ta del av uppgifter som omfattas av sekretess enligt OSL. För att uppgifterna ska få lämnas måste villkor i 8 kap. 3 § OSL vara uppfyllda.

Vid osäkerhet om en utländsk företrädare får ta del av uppgifter som omfattas av sekretess enligt OSL bör samverkan ske med HKV LEDS JUR.

3.4. Sekretessmarkering och märkning med säkerhetsskyddsklass

”En anteckning om hinder att lämna ut en allmän handling får göras endast på en handling som omfattas av en bestämmelse som avses i 2 § andra stycket. Den tillämpliga bestämmelsen ska anges.”

2 kap. 20 § tryckfrihetsförordningen

Vägledande förklaring: En allmän handling får endast sekretessmarkeras om det finns stöd för det i en bestämmelse om sekretess. Skälet till att den tillämpliga sekretessbestämmelsen ska framgå i en sekretessmarkering är att motverka att handlingar får en anteckning i andra fall än när det finns lagliga förutsättningar för det.[138]

[138] Prop. 1975/76:160 s. 209.

”Bestämmelser om sekretessmarkering finns i 5 kap. 5 § offentlighets- och sekretesslagen (2009:400). Bestämmelser om anteckning om säkerhetsskyddsklass finns i 3 kap. 7 § säkerhetsskyddsförordningen (2018:658).”

3 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Paragrafen innehåller en upplysning om vad som gäller enligt lag och förordning. Bestämmelserna beskrivs nedan.

Förutom säkerhetsskyddsklassificerade allmänna handlingar som är av synnerlig betydelse för rikets säkerhet finns det inget krav för myndigheter på att handlingar ska sekretessmarkeras. Oavsett om en säkerhetsskyddsklassificerad handling är en allmän handling eller inte, ska handlingen förses med anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har.

”Om det kan antas att en uppgift i en allmän handling inte får lämnas ut på grund av en bestämmelse om sekretess, får myndigheten markera detta genom att en särskild anteckning (sekretessmarkering) görs på handlingen eller, om handlingen är elektronisk, införs i handlingen eller i det datasystem där den elektroniska handlingen hanteras. Anteckningen ska ange

1. *tillämplig sekretessbestämmelse,*
2. *datum då anteckningen gjordes, och*
3. *den myndighet som har gjort anteckningen.”*

5 kap. 5 § första stycket OSL

Vägledande förklaring: Bestämmelsen om sekretessmarkering är teknikneutral och gäller även för elektroniska handlingar.

En sekretessmarkering är enbart en varningssignal om att det kan finnas uppgifter i en handling som bedöms vara sekretessbelagda enligt OSL. Att sekretessmarkera en handling, eller en del av en handling (avsnitt 3.4.3), innebär inte något bindande avgörande av sekretessfrågan. Om en allmän handling har begärts ut måste därför en sekretessprövning av innehållet göras oavsett om handlingen är sekretessmarkerad eller inte. En sekretessprövning görs i varje enskilt fall och grundas på de uppgifter som förekommer i handlingen. Det är således inte tillåtet att vägra att lämna ut en handling enbart med hänvisning till att den är sekretessmarkerad.

”Om utlämnande till en enskild av en uppgift i en allmän handling som är av synnerlig betydelse för rikets säkerhet enligt förordning ska prövas endast av en viss myndighet, ska en sekretessmarkering göras så snart som möjligt. Av anteckningen ska det framgå vilken myndighet som ska pröva frågan om utlämnande.”

5 kap. 5 § andra stycket OSL

Vägledande förklaring: En myndighet behöver generellt inte sekretessmarkera alla handlingar som innehåller en uppgift som omfattas av sekretess. För handlingar som är av synnerlig betydelse för rikets säkerhet (kvalificerat hemliga) finns dock ett ovillkorligt krav i 5 kap. 5 § OSL på att en sådan handling alltid ska sekretessmarkeras.

”En säkerhetsskyddsklassificerad handling ska förses med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har. Om handlingen innehåller uppgifter med olika säkerhetsskyddsklass ska den högsta säkerhetsskyddsklassen avgöra vilken anteckning handlingen ska ha. Säkerhetspolisen och Försvarsmakten får inom respektive myndighets tillsynsområde meddela föreskrifter om undantag från kravet på anteckning om säkerhetsskyddsklass.”

3 kap. 7 § första stycket säkerhetsskyddsförordningen

Vägledande förklaring: Grunden är att säkerhetsskyddsklass ska anges på säkerhetsskyddsklassificerade handlingar. En sådan anteckning (märkning) är en förutsättning för att alla som kommer i kontakt med handlingen förstår att den är säkerhetsskyddsklassificerad och ska skyddas med säkerhetsskydd. Genom att säkerhetsskyddsklassen anges på handlingen är det tydligt för den som hanterar handlingen vilka krav på säkerhetsskydd som gäller.

Kravet gäller såväl säkerhetsskyddsklassificerade handlingar som är *allmänna handlingar* enligt tryckfrihetsförordningen, som säkerhetsskyddsklassificerade handlingar som *inte* är allmänna handlingar.

Säkerhetsskyddsklass skrivs alltid på svenska.[139] I Sveriges säkerhetsskyddsavtal med andra stater och mellanfolkliga organisationer finns en översättningstabell med parternas klasser på svenska respektive det språk som gäller hos den andra parten eller parterna (avsnitt 3.1.3.3). I avtalen framgår vanligtvis även att de egna nationella beteckningarna ska användas när säkerhetsskyddsklassificerade uppgifter utbyts mellan parterna. En säkerhetsskyddsklassificerad handling som sänds från Sverige till en part märks med säkerhetsskyddsklass på svenska. En inkommande säkerhetsskyddsklassificerad handling från utlandet märks med den säkerhetsskyddsklass på svenska som motsvarar den utländska märkningen.

I internationella samarbeten är praxis att säkerhetsskyddsklassificerade handlingar endast märks med säkerhetsskyddsklasser på engelska, t.ex. RESTRICTED. Om det inte finns något avtal som medger märkning på engelska måste säkerhetsskyddsklassificerade handlingar i samarbetet även märkas med säkerhetsskyddsklass på svenska.

[139] Prop. 2017/18:89 s. 64.

”En säkerhetsskyddsklassificerad handling ska på första sidan förses med en anteckning (märkning) om den högsta säkerhetsskyddsklassen som uppgifterna i handlingen är placerade i. Om handlingen innehåller bilagor, får varje bilaga på första sidan förses med den högsta säkerhetsskyddsklassen som uppgifterna i bilagan är placerade i.”

3 kap. 7 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Märkningen ska alltid finnas på handlingens första sida, även om den sidan inte innehåller någon säkerhetsskyddsklassificerad uppgift. Märkningen är en varningssignal om att den som tagit fram handlingen bedömt att handlingen innehåller någon säkerhetsskyddsklassificerad uppgift. Behovet av varningssignalen som märkningen utgör är lika stort för elektroniska handlingar som för handlingar av papper. Märkningen bör vara tydligt utformad så att personer som kommer i kontakt med handlingen inte kan undgå att se att handlingen är säkerhetsskyddsklassificerad. Märkningen bör därför vara röd och bestå av säkerhetsskyddsklassen utskriven omgiven av en ram. Upp till och med säkerhetsskyddsklassen hemlig bör ramen vara enkel. För säkerhetsskyddsklassen kvalificerat hemlig bör ramen vara dubbel.

En handling i pappersform kan i informationssystem bestå av flera elektroniska handlingar, t.ex. när en pappershandling innehåller en bilaga. För att uppmärksamma att även bilagan innehåller säkerhetsskyddsklassificerade uppgifter får bilagan förses med märkning.

Om en säkerhetsskyddsklassificerad bokpublikation har ett omslag måste omslaget märkas med säkerhetsskyddsklass.

”Övriga sidor i handlingen ska ha samma märkning som på första sidan av handlingen eller bilagan, eller vara märkta med den högsta säkerhetsskyddsklassen som uppgifterna på sidan tillhör.”

3 kap. 7 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med samma märkning avses säkerhetsskyddsklassen på handlingens första sida. Det finns inget hinder mot att varje stycke, bild, tabell etc. i en sida märks med den säkerhetsskyddsklass som gäller för den aktuella delen av sidan.

”En säkerhetsskyddsklassificerad elektronisk handling får istället förses med märkning om säkerhetsskyddsklass på lämpligt sätt med hänsyn till de informationssystem som handlingen behandlas i. En sådan märkning ska då den elektroniska handlingen visas, så långt som möjligt uppfylla kraven i första och andra stycket.”

3 kap. 7 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: För att säkerställa att säkerhetsskyddsklassificerade handlingar innehåller märkningen är det lämpligt att stöd för märkningen ingår i dokumentmallar i informationssystem.

Det är lämpligt att det på varje sida i en presentation i ett informationssystem förses med märkning om den högsta säkerhetsskyddsklass som uppgifterna på sidan är placerade i, eller om sidan inte innehåller någon säkerhetsskyddsklassificerad uppgift.

3.4.1. Märkning på allmänna handlingar

Observera!
Det finns inga krav på markeringarnas storlek eller typsnitt. Det väsentliga är att markeringarna är synliga och tydliga så att de uppfattas av människor som kommer i kontakt med pappershandlingar, elektroniska handlingar m.m.

Moment 3:1 *En märkning med säkerhetsskyddsklass på en allmän handling ska placeras i övre delen på den säkerhetsskyddsklassificerade allmänna handlingens första sida. Säkerhetsskyddsklassen anges med versaler. Märkningen ska vara rektangulär. Upp till och med säkerhetsskyddsklassen hemlig ska ramen vara enkel. För säkerhetsskyddsklassen kvalificerat hemlig ska ramen vara dubbel.*

Vägledande förklaring: Märkningen bör vara röd.

Moment 3:2 *En märkning med säkerhetsskyddsklass på en allmän handling ska innehålla en hänvisning till vilken eller vilka sekretessbestämmelser i OSL som de säkerhetsskyddsklassificerade uppgifterna i den allmänna handlingen omfattas av. I märkningen ska framgå datum för när märkningen gjordes och att det är Försvarsmakten som har gjort märkningen. Försvarsmakten ska anges även på engelska (Swedish Armed Forces).*

Vägledande förklaring: I avsnitt 3.1.3.1 beskrivs vilka sekretessbestämmelser i OSL som säkerhetsskyddsklassificerade uppgifter omfattas av. Med hänsyn till det omfattande internationella samarbetet anges även Försvarsmakten på engelska. Därigenom blir det tydligt för andra stater och mellanfolkliga organisationer att det är Försvarsmakten som har märkt handlingen och att handlingen kommer från Sverige.

Om en säkerhetsskyddsklassificerad allmän handling består av missiv och bilagor, där missivet inte bedöms innehålla någon säkerhetsskyddsklassificerad uppgift, får missivet förses med anteckning om detta. Anteckningen ”DETTA MISSIV INNEHÅLLER INGEN SEKRETESSBELAGD UPPGIFT” bör då användas. Första sidan på missivet för en sådan handling förses alltid med märkning om handlingens säkerhetsskyddsklass.[140] Om ett sådant missiv hanteras i ett informationssystem som inte är avsett för den aktuella säkerhetsskyddsklassen, betyder det inte att säkerhetsskyddsklassificerade uppgifter felaktigt hanterats i systemet.

[140] 3 kap. 7 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd.

Bild 3.4. Exempel på märkning med säkerhetsskyddsklass begränsat hemlig på en allmän handlings första sida.

Bild 3.5. Exempel på märkning med säkerhetsskyddsklass konfidentiell på en allmän handlings första sida.

Bild 3.6. Exempel på märkning med säkerhetsskyddsklass hemlig på en allmän handlings första sida.

Bild 3.7. Exempel på märkning med säkerhetsskyddsklass kvalificerat hemlig på en allmän handling som är av synnerlig betydelse för rikets säkerhet.

Bild 3.8. Exempel på märkning med säkerhetsskyddsklass kvalificerat hemlig på en allmän handling som inte är av synnerlig betydelse för rikets säkerhet. Se vägledande förklaring till moment 3:4.

Moment 3:3 *Om märkningen avser en säkerhetsskyddsklassificerad allmän handling som är av synnerlig betydelse för rikets säkerhet ska märkningen även ange vilken myndighet som enligt 1 § offentlighets- och sekretessförordningen (2009:641) ska pröva begäran om utlämnande av allmän handling.*

Vägledande förklaring: I 1 § OSF används begreppet rikets säkerhet. Begreppet är synonymt med Sveriges säkerhet som används i säkerhetsskyddslagen. Om uppgifterna i en handling har säkerhetsskyddsklassificerats som kvalificerat hemlig utifrån att ett röjande av uppgifterna i handlingen kan medföra en synnerligen allvarlig skada för Sveriges säkerhet, är handlingen av synnerlig betydelse för rikets säkerhet på det sätt som anges i 1 § OSF.[141]

Om uppgifterna i en handling omfattas av ett internationellt åtagande om säkerhetsskydd och har klassificerats som kvalificerat hemlig men ett röjande av uppgifterna inte medför en synnerligen allvarlig skada för *Sveriges säkerhet*, är handlingen inte av synnerlig betydelse för rikets säkerhet på det sätt som anges i 1 § OSF.[142]

Frågan om utlämning av en allmän handling som är av synnerlig betydelse för rikets säkerhet ska i vissa fall prövas av en annan myndighet. För sådana handlingar och som förvaras hos Försvarsmakten gäller enligt 1 § OSF:

- Chefen för Försvarsdepartementet ska pröva utlämnandet om:
  - handlingen innehåller uppgifter som omfattas av sekretess enligt 15 kap. 2 § OSL och
  - uppgifterna inte rör polisens verksamhet för att hindra eller uppdaga brott som rör rikets säkerhet.

- Chefen för Justitiedepartementet ska pröva utlämnandet om:
  - handlingen innehåller uppgifter som omfattas av sekretess enligt 15 kap. 2 § eller 18 kap. 1-3 §§ OSL och
  - uppgifterna rör polisens verksamhet för att hindra eller uppdaga brott som rör rikets säkerhet.

- Chefen för Utrikesdepartementet ska pröva utlämnandet om:
  - handlingen innehåller uppgifter som är omfattas av sekretess enligt 15 kap. 1 § OSL och
  - handlingen har överlämnats av Utrikesdepartementet till en svensk myndighet.

I markeringen används texten ”Frågan om denna handlings utlämnande ska prövas av” följt av vem som enligt 1 § OSF ska pröva utlämnandet. Exempel på märkning med säkerhetsskyddsklass kvalificerat hemlig för en allmän handling där en annan myndighet ska pröva begäran om utlämnande finns i bild 3.7.

[141] 2 kap. 5 § första stycket säkerhetsskyddslagen.
[142] 2 kap. 5 § andra stycket säkerhetsskyddslagen.

Om inte någon annan myndighet ska pröva utlämnandet av handlingen utelämnas texten. Exempel på märkning med säkerhetsskyddsklass kvalificerat hemlig för en sådan allmän handling finns i bild 3.8.

Moment 3:4 *På övriga sidor i en säkerhetsskyddsklassificerad allmän handling ska märkningen bestå av säkerhetsskyddsklassen i versaler med en hänvisning till handlingens första sida. Märkningen ska vara rektangulär. Upp till och med säkerhetsskyddsklassen hemlig ska ramen vara enkel. För säkerhetsskyddsklassen kvalificerat hemlig ska ramen vara dubbel.*

Vägledande förklaring: Den säkerhetsskyddsklass som anges i märkningen kan vara den säkerhetsskyddsklass som framgår av märkningen på handlingens första sida, eller den säkerhetsskyddsklass som avser den högsta säkerhetsskyddsklassen för uppgifterna på den aktuella sidan. Säkerhetsskyddsklassen i märkningen kan således vara lägre än den säkerhetsskyddsklass som anges på första sidan.

Märkningen bör vara röd. Exempel på märkning finns i bilderna 3.9-3.12. Märkning får utformas på annat sätt, så länge som momentet följs.

Bild 3.9. Exempel på märkning med säkerhetsskyddsklass begränsat hemlig på en allmän handlings övriga sidor.

Bild 3.10. Exempel på märkning med säkerhetsskyddsklass konfidentiell på en allmän handlings övriga sidor.

Bild 3.11. Exempel på märkning med säkerhetsskyddsklass hemlig på en allmän handlings övriga sidor.

Bild 3.12. Exempel på märkning med säkerhetsskyddsklass kvalificerat hemlig på en allmän handlings övriga sidor.

Moment 3:5 *En inkommande handling från en annan stat eller en mellanfolklig organisation som är märkt med den statens eller organisationens motsvarighet till säkerhetsskyddsklass, ska placeras i säkerhetsskyddsklass även om Sverige inte omfattas av ett internationellt åtagande om säkerhetsskydd med den andra staten eller organisationen.*

3.4.2. Försvarsmaktens märkning på handlingar som inte är allmänna

Moment 3:6 *En märkning med säkerhetsskyddsklass på en handling som inte är allmän ska placeras i övre delen på den säkerhetsskyddsklassificerade handlingens första sida. I märkningen ska det framgå den säkerhetsskyddsklass som avses.*

Vägledande förklaring: Märkningen får utformas på lämpligt sätt, t.ex. för hand. Exempel på hur märkningen kan se ut finns i bild 3.13. Märkningen bör vara röd.

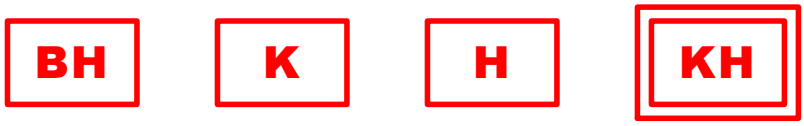


Bild 3.13. Exempel på märkning med säkerhetsskyddsklass på handlingar som inte är allmänna.

Andra myndigheter kan använda andra förkortningar i sin märkning.

3.4.3. Märkning av textstycken, bilder m.m. i en handling

Moment 3:7 *Delar av en säkerhetsskyddsklassificerad handling får märkas med säkerhetsskyddsklass. Varje del ska då märkas med den högsta säkerhetsskyddsklassen för uppgifterna som ingår i delen. Delar av handling får även förses med märkning som talar om att delen inte innehåller någon säkerhetsskyddsklassificerad uppgift.*

Vägledande förklaring: En märkning med säkerhetsskyddsklass på första sidan av en säkerhetsskyddsklassificerad handling är sällan tillräcklig för att läsaren ska förstå vilka uppgifter i handlingen som är säkerhetsskyddsklassificerade.

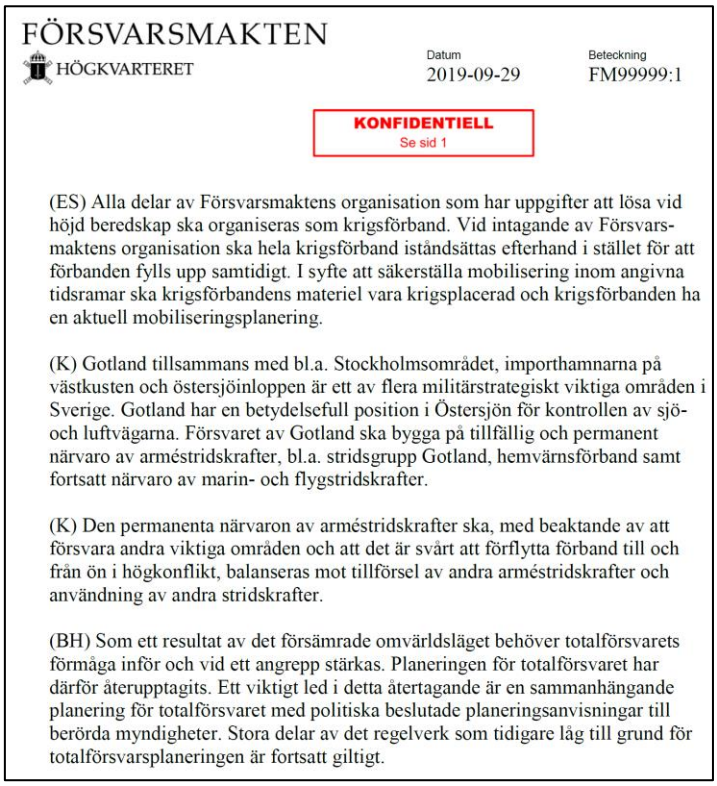
Det kan därför vara lämpligt att märka varje del i en handling med en bedömning om uppgifternas informationsklassificering enligt tabell 3.6. Med del av en handling avses textstycken, bilder, tabeller etc. Märkningen placeras synligt i anslutning till delen så att det är tydligt för läsaren att delen innehåller säkerhetsskyddsklassificerade uppgifter (exempel bild 3.14 och bild 3.15). Märkning i en bild- eller tabellrubrik avser såväl rubriken som bilden eller tabellen.

Tabell 3.6. Märkning av textstycken och märkningens betydelse.

Märkning	Betydelse
(KH)	Den märkta delen av handlingen bedöms innehålla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass kvalificerat hemlig.
(H)	Den märkta delen av handlingen bedöms innehålla säkerhetsskyddsklassificerade uppgifter i högst säkerhetsskyddsklass hemlig.
(K)	Den märkta delen av handlingen bedöms innehålla säkerhetsskyddsklassificerade uppgifter i högst säkerhetsskyddsklass konfidentiell.
(BH)	Den märkta delen av handlingen bedöms endast innehålla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass begränsat hemlig.

Märkning	Betydelse
(SK)	Den märkta delen av handlingen bedöms innehålla sekretessklassificerade uppgifter, men inte säkerhetsskyddsklassificerade uppgifter.
(ES)	Den märkta delen av handlingen bedöms inte innehålla någon uppgift som omfattas av sekretess enligt OSL.

Märkningen av säkerhetsskyddsklasser kan kompletteras med anteckning om vilka stater och mellanfolkliga organisationer som uppgifterna får delges till (avsnitt 3.6.4).



FÖRSVARSMAKTEN

HÖGKVARTERET

Datum 2019-09-29

Beteckning FM99999:1

KONFIDENTIELL
Se sid 1

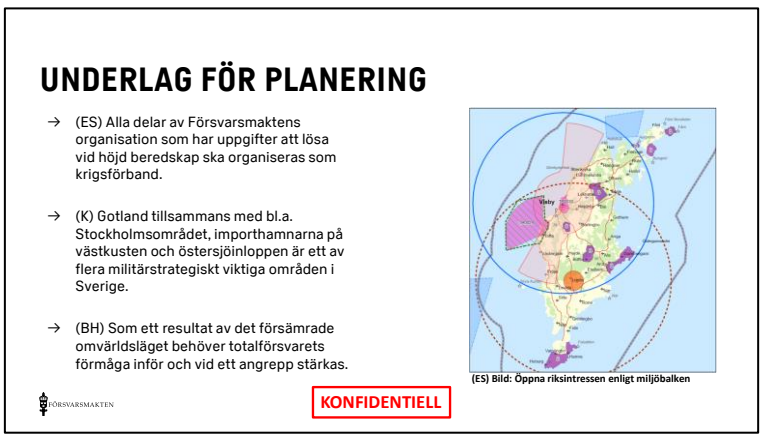
(ES) Alla delar av Försvarsmaktens organisation som har uppgifter att lösa vid höjd beredskap ska organiseras som krigsförband. Vid intagande av Försvarsmaktens organisation ska hela krigsförband iståndsättas efterhand i stället för att förbanden fylls upp samtidigt. I syfte att säkerställa mobilisering inom angivna tidsramar ska krigsförbandens materiel vara krigsplacerad och krigsförbanden ha en aktuell mobiliseringsplanering.

(K) Gotland tillsammans med bl.a. Stockholmsområdet, importhamnarna på västkusten och östersjöinloppen är ett av flera militärstrategiskt viktiga områden i Sverige. Gotland har en betydelsefull position i Östersjön för kontrollen av sjö- och luftvägarna. Försvaret av Gotland ska bygga på tillfällig och permanent närvaro av arméstridskrafter, bl.a. stridsgrupp Gotland, hemvärnsförband samt fortsatt närvaro av marin- och flygstridskrafter.

(K) Den permanenta närvaron av arméstridskrafter ska, med beaktande av att försvara andra viktiga områden och att det är svårt att förflytta förband till och från ön i högkonflikt, balanseras mot tillförsel av andra arméstridskrafter och användning av andra stridskrafter.

(BH) Som ett resultat av det försämrade omvärldsläget behöver totalförsvarets förmåga inför och vid ett angrepp stärkas. Planeringen för totalförsvaret har därför återupptagits. Ett viktigt led i detta återtagande är en sammanhängande planering för totalförsvaret med politiska beslutade planeringsanvisningar till berörda myndigheter. Stora delar av det regelverk som tidigare låg till grund för totalförsvarsplaneringen är fortsatt giltigt.

Bild 3.14. Exempel där varje stycke har märkts med säkerhetsskyddsklass eller med märkning som innebär att stycket inte innehåller någon säkerhetsskyddsklassificerad uppgift.



UNDERLAG FÖR PLANERING

→ (ES) Alla delar av Försvarsmaktens organisation som har uppgifter att lösa vid höjd beredskap ska organiseras som krigsförband.

→ (K) Gotland tillsammans med bl.a. Stockholmsområdet, importhamnarna på västkusten och östersjöinloppen är ett av flera militärstrategiskt viktiga områden i Sverige.

→ (BH) Som ett resultat av det försämrade omvärldsläget behöver totalförsvarets förmåga inför och vid ett angrepp stärkas.

(ES) Bild: Öppna riksintressen enligt miljöbalken

FÖRSVARSMAKTEN

KONFIDENTIELL

Bild 3.15. Exempel på presentation där punkter med text och en bild har märkts med säkerhetsskyddsklass eller märkning att stycket inte innehåller någon säkerhetsskyddsklassificerad uppgift.

3.4.4. Märkning av sekretessklassificerade handlingar

”En allmän handling som är sekretessklassificerad ska på första sidan förses med en särskild anteckning (sekretessmarkering) om att handlingen är sekretessklassificerad. I fråga om en elektronisk handling ska sekretessmarkeringen i stället införas i handlingen eller i det IT-system där den elektroniska handlingen hanteras. Bestämmelser om sekretessmarkering finns i 5 kap. 5 § offentlighets- och sekretesslagen (2009:400).

En sekretessmarkering på en allmän handling ska ha en enkel rektangulär ram.”

3 kap. 1 § första och andra styckena Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

”En sekretessklassificerad handling behöver inte sekretessmarkeras om den ingår i en ordnad samling av handlingar som rör likartad verksamhet och som förvaras skyddad.”

3 kap. 2 § Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Vägledande förklaring: Även handlingar som innehåller uppgifter som omfattas av sekretess enligt OSL, men som *inte* är säkerhetsskyddsklassificerade behöver skyddas. I Försvarsmaktens benämns dessa som *sekretessklassificerade* uppgifter (läs mer om Försvarsmaktens modell för informationsklassificering i avsnitt 3.1.1). För att uppmärksamma att handlingar innehåller sekretessklassificerade uppgifter märks första sidan på allmänna handlingar med en sekretessmarkering enligt exempel i bild 3.16.

Med en ordnad samling av handlingar som rör likartad verksamhet avses handlingar som hanteras avgränsat inom en verksamhet och som är ordnade så att handlingarna går att hänföra till det som handlingarna i huvudsak avser som t.ex. medicinska journaler och personalakter.

Föreskriften ska tolkas restriktivt i fråga om vad som utgör likartad verksamhet. Huvudregeln är att sekretessklassificerade handlingar ska sekretessmarkeras. Med att handlingarna förvaras skyddade avses att det enbart är den personal som hanterar handlingarna i verksamheten som har åtkomst till handlingarna (t.ex. den personal som hanterar medicinska journaler och den personaladministrativa personalen som hanterar personalakter). Normalt har den personal som hanterar sådana handlingar kunskap om de sekretessbestämmelser som är tillämpliga för uppgifterna i verksamheten, varför behovet av sekretessmarkering inte är lika stort som i annan verksamhet.

Bild 3.16. Exempel på märkning på första sidan på en sekretessklassificerad allmän handling.

Bild 3.17. Exempel på märkning på en sekretessklassificerad arbetshandling.

En sekretessklassificerad allmän handling som enligt bestämmelsen inte behöver sekretessmarkeras ska dock sekretessmarkeras om handlingen inte längre ingår i en ordnad samling av handlingar som rör likartad verksamhet. En sekretessklassificerad handling ska inte omfattas av säkerhetsskydd för skydd av sekretessen och får därför inte märkas med säkerhetsskyddsklass.

> *”En handling som inte är allmän får på första sidan förses med en anteckning om att den är sekretessklassificerad. Anteckningen får utformas på lämpligt sätt.”*
>
> 3 kap. 1 § tredje stycket Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Exempel på märkning av en sekretessklassificerad arbetshandling finns i bild 3.17 ovan.

3.4.5. Märkning av lagringsmedier

> *”Ett säkerhetskyddsklassificerat lagringsmedium ska på höljet förses med en anteckning (märkning) om den högsta säkerhetsskyddsklass lagringsmediet är avsett för.”*
>
> 3 kap. 8 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen gäller såväl lagringsmedier som en person har kvitterat för personligt tjänstebruk, som lagringsmedier som används för drift och säkerhetskopiering, t.ex. i en server.

Med hölje avses den yttersta delen som omsluter lagringsmediet, t.ex. utsidan på en hårddiskkassett eller ett USB-minne. Om höljet avlägsnas måste lagringsmediet märkas på nytt, t.ex. när en hårddisk tas ur en hårddiskkassett. Lager av höljen kan ses som matrjosjka, ryska dockor där en docka är fylld med allt mindre delbara dockor.

”Ett säkerhetskyddsklassificerat lagringsmedium som är placerat i säkerhetsskyddsklassen konfidentiell eller högre ska märkas med identifieringsuppgift på höljet.”

3 kap. 13 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Identifieringsuppgiften behövs för att kunna upprätthålla spårbarhet i hanteringen, t.ex. kvittering vid mottagande, inventering och dokumenterad förstöring.

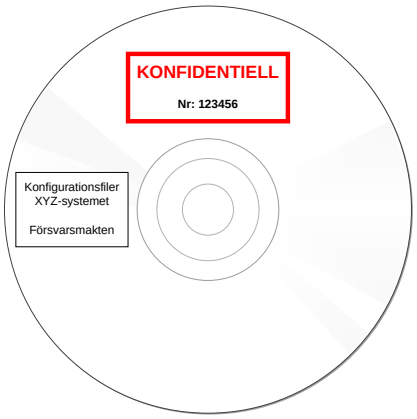


Bild 3.18. Exempel på märkning av av en CD-ROM. Kim Hakkarainen/Försvarsmakten

”Om lagringsmediet är fast monterat i utrustning som omöjliggör märkning på lagringsmediet ska märkningen i stället göras på utrustningen eller annan lämplig plats i anslutning till lagringsmediet.”

3 kap. 8 § andra stycket och 3 kap. 13 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Vissa fast monterade lagringsmedier, vanligtvis sådana som är avsedda för drift eller säkerhetskopiering, är inte alltid möjliga att märka. Om lagringsmedierna inte kan märkas placeras istället märkningen synligt och i så nära anslutning till medierna som möjligt.

Med lämplig plats menas att utrustningen ska märkas så att det klart framgår för en person som befinner sig vid utrustningen att den innehåller säkerhetsskyddsklassificerade lagringsmedier. Lämplig plats att placera märkningen på kan i sådana fall vara en dörr eller lucka till det utrymme där utrustningen är placerad.

Om ett fast monterat lagringsmedium monteras bort måste lagringsmediet alltid märkas med säkerhetsskyddsklass.

Om ett fast monterat lagringsmedium i säkerhetsskyddsklass konfidentiell eller högre monteras bort måste lagringsmediet alltid märkas med identifieringsuppgift.

”Om ett säkerhetskyddsklassificerat lagringsmedium kan antas komma att lämnas över till utländska myndigheter eller leverantörer ska lagringsmediet förses med en märkning om ursprungsland om det inte är olämpligt.”

3 kap. 28 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Sådan märkning kan bestå av texten ”Country of origin: Sweden”. I Försvarsmakten är det tillräckligt att lagringsmediet är märkt med myndighetens namn på engelska, dvs. Swedish Armed Forces.

3.4.6. Äldre märkning med informationssäkerhetsklass

3.4.6.1 Handlingar som är märkta med informationssäkerhetsklass

Om en säkerhetsskyddsklassificerad handling har märkts med informationssäkerhetsklass behöver den inte märkas om med säkerhetsskyddsklass.[143]

3.4.6.2 Arkiverade handlingar

En säkerhetsskyddsklassificerad handling som är arkiverad före den 1 april 2019 behöver inte märkas med säkerhetsskyddsklass.[144] En säkerhetsskyddsklassificerad handling som är märkt med informationssäkerhetsklass och som arkiveras efter den 1 april 2019 behöver heller inte märkas med säkerhetsskyddsklass.

När en sådan arkiverad säkerhetsskyddsklassificerad handling tas ut ur arkivet för att användas märks den med säkerhetsskyddsklass.

3.4.6.3 Äldre handlingar som inte är arkiverade

Äldre säkerhetsskyddsklassificerade handlingar, t.ex. äldre bokpublikationer, får i detta avseende likställas med arkiverade handlingar. När den äldre säkerhetsskyddsklassificerade handlingen tas fram för att distribueras måste den märkas med säkerhetsskyddsklass.

[143] Punkt 4 i ikraftträdande- och övergångsbestämmelserna till Försvarsmaktens föreskrifter om säkerhetsskydd.
[144] Punkt 3 i ikraftträdande- och övergångsbestämmelserna till säkerhetsskyddsförordningen.

3.5. Ändring och borttagning av märkning av säkerhetsskyddsklass

3.5.1. Rutin för ändring och borttagning

> *”Myndigheten ska ha rutiner för ändring respektive borttagning av märkning av säkerhetsskyddsklass.*
>
> *Rutinerna ska minst reglera vem som får besluta om ändringen respektive borttagningen samt hur ändringen respektive borttagningen ska genomföras.*
>
> *Rutinerna ska dokumenteras.”*
>
> 3 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen gäller märkning av säkerhetsskyddsklass på handlingar, inklusive tryckta skrifter och elektroniska handlingar, lagringsmedier och materiel.

Att en ändring eller borttagning av märkning har gjorts kan behöva kommuniceras till den del av myndigheten som ansvarar för registrering ur säkerhetsskyddssynpunkt, så att diarium eller register kan uppdateras. En ändring eller borttagning kan resultera i förändring av säkerhetsskyddsåtgärder, t.ex. kvittering vid mottagande och inventering.

Se avsnitt 3.1.3.4 innan någon ändring eller borttagning av säkerhetsskyddsklass genomförs på en handling som har inkommit från en annan stat eller mellanfolklig organisation.

Se avsnitt 3.5.2 om samverkan inför ändring av eller borttagning av säkerhetsskyddsklassen kvalificerat hemlig.

Moment 3:8 *En ändring eller borttagning av säkerhetsskyddsklass på en tryckt skrift ska beslutas av den chef som, enligt FM ArbO, ansvarar för den aktuella bokpublikationen.*

Moment 3:9 *Organisationsenheten ska i en lokal instruktion reglera vem som får besluta om ändring respektive borttagning av en säkerhetsskyddsklass på en allmän handling, ett lagringsmedium eller annan materiel som förvaras vid organisationsenheten. Instruktionen ska även beskriva hur ändringen eller borttagningen dokumenteras i det diarium som handlingen är diarieförd i eller i det register som används för uppföljning av exemplar av handlingen, lagringsmediet eller materielen.*

Moment 3:10 *Om det vid en organisationsenhet bedöms att en säkerhetsskyddsklassificerad allmän handling, som har upprättats vid någon annan organisationsenhet eller en annan myndighet, inte längre är säkerhetsskyddsklassificerad alternativt ska placeras i en annan säkerhetsskyddsklass än den ursprungliga, ska den organisationsenhet respektive den myndighet som har upprättat handlingen underrättas.*

Moment 3:11 *Ändring på en säkerhetsskyddsklassificerad allmän handling i pappersform utförs genom att beslutet antecknas i anslutning till märkningen, den del av märkning som ska ändras överkorsas. I anteckningen ska det framgå vem som har fattat beslutet och datum när ändringen görs. Därefter anges den nya märkningen i anslutning till överkorsningen.*

Vägledande förklaring:

Bild 3.19. Exempel på ändring av märkning på en säkerhetsskyddsklassificerad allmän handling i pappersform. Kim Hakkarainen/Försvarsmakten

En ändring på en säkerhetsskyddsklassificerad elektronisk handling får ske på lämpligt sätt med hänsyn till det informationssystem som handlingen behandlas i. Om det är möjligt får märkningen tas bort för att ersättas med en ny märkning.

Moment 3:12 *Borttagning på en säkerhetsskyddsklassificerad allmän handling i pappersform utförs genom att beslutet antecknas i anslutning till märkningen. I anteckningen ska det framgå vem som har fattat beslutet och datum när ändringen görs. Därefter överkorsas märkningen.*

Bild 3.20. Exempel på borttagning av märkning på en säkerhetsskyddsklassificerad allmän handling i pappersform. I beslutet är säkerhetsskyddsklassificerad förkortad till SSK.
Kim Hakkarainen/Försvarsmakten

Moment 3:13 *Den som förvarar en säkerhetsskyddsklassificerad handling som inte är allmän får besluta om ändring eller borttagning av säkerhetsskyddsklass på handlingen.*

Vägledande förklaring: Ändringen genomförs på enklaste sätt, t.ex. genom att korsa över och ange den nya säkerhetsskyddsklassen. Beslutet behöver inte antecknas på handlingen.

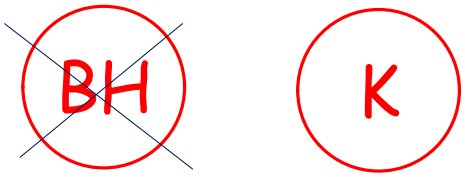


Bild 3.21. Exempel på ändring av säkerhetsskyddsklass på en säkerhetsskyddsklassificerad handling som inte är allmän.
Kim Hakkarainen/Försvarsmakten

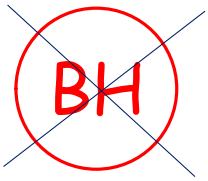


Bild 3.22. Exempel på borttagning av säkerhetsskyddsklass på en säkerhetsskyddsklassificerad handling som inte är allmän.
Kim Hakkarainen/Försvarsmakten

3.5.2. Samverkan innan märkning av kvalificerat hemlig ändras eller tas bort

”Ändring respektive borttagning av märkning av säkerhetsskyddsklass som gäller för en kvalificerat hemlig handling får ske först efter hörande av den myndighet som har upprättat handlingen.

Vid ärende om utlämning av allmän handling enligt tryckfrihetsförordningen får myndigheten höra den myndighet som har upprättat handlingen.”

3 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med kvalificerat hemlig handling avses i bestämmelsen alla säkerhetsskyddsklassificerade handlingar som är placerade i säkerhetsskyddsklassen kvalificerat hemlig.

Moment 3:14 *En ändring av eller borttagning av säkerhetsskyddsklassen kvalificerat hemlig på en säkerhetsskyddsklassificerad handling som har upprättas av Försvarsmakten, får ske först efter att den organisationsenhet som har upprättat handlingen godkänt ändringen eller borttagningen.*

Vägledande förklaring: Uppgifter som är placerade i säkerhetsskyddsklassen kvalificerat hemlig är uppgifter som om de röjs kan medföra synnerligen allvarlig skada för Sveriges säkerhet. Kvalificerat hemlig är den högsta säkerhetsskyddsklassen. Den myndighet eller organisationsenhet som har upprättat handlingen måste därför höras om sin bedömning om uppgifterna fortfarande är placerade i säkerhetsskyddsklassen kvalificerat hemlig och därmed om lämpligheten att genomföra ändringen eller borttagningen.

Den myndighet eller organisationsenhet som har upprättat handlingen kan ge stöd i bedömningen om handlingen fortfarande är placerad i säkerhetsskyddsklassen kvalificerat hemlig. Trots att en myndighet självständigt prövar frågan om utlämnande av en allmän handling enligt tryckfrihetsförordningen finns det inget hinder mot att myndigheter samverkar i bedömningen av uppgifterna.

En säkerhetsskyddsklassificerad handling är placerad i säkerhetsskyddsklassen kvalificerat hemlig antingen på grund av att:

- ett röjande av uppgifterna i handlingen kan medföra synnerlig skada för Sveriges säkerhet, eller
- på grund av ett internationellt säkerhetsskyddsåtagande.

Se även inledningen på avsnitt 3.4 om sekretessmarkering. Om en handling fortsatt bedöms vara placerad i säkerhetsskyddsklassen kvalificerat hemlig *p.g.a. att ett röjande av uppgifterna i handlingen kan medföra synnerligen allvarlig skada för Sveriges säkerhet*, finns regler om vilken myndighet som ska pröva frågan om utlämnande i 1 § OSF.

Av 1 § OSF följer att den myndighet som förvarar en säkerhetsskyddsklassificerad handling som *är placerad i säkerhetsskyddsklassen kvalificerat hemlig p.g.a. ett internationellt åtagande om säkerhetsskydd* ska pröva frågan om utlämnande av handlingen, om ett röjande av uppgifterna i handlingen *inte* kan medföra synnerligen allvarlig skada för Sveriges säkerhet.

3.6. Annan märkning

3.6.1. Beteckning, exemplarnummer m.m.

”En säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre ska på första sidan märkas med handlingens beteckning, exemplarnummer, antal sidor samt bilagor, om sådana följer med. Av bilaga och blad i bok med lösbladssystem ska framgå till vilken handling bilagan respektive bladet hör.

För en säkerhetsskyddsklassificerad elektronisk allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre får märkning enligt första stycket istället göras på lämpligt sätt med hänsyn till de informationssystem som handlingen behandlas. Märkningen behöver inte omfatta exemplarnummer och antal sidor.”

3 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Exemplar av allmänna handlingar i säkerhetsskyddsklassen konfidentiell och högre ska kunna följas upp så att det går att ta reda på var ett exemplar förvaras eller om det förkommit eller förstörts. För att underlätta det arbetet måste handlingen vara märkt med vissa identifierande uppgifter som kan användas i ett register över exemplaren (bild 3.23). Syftet är att uppnå spårbarhet för varje exemplar av sådana handlingar.

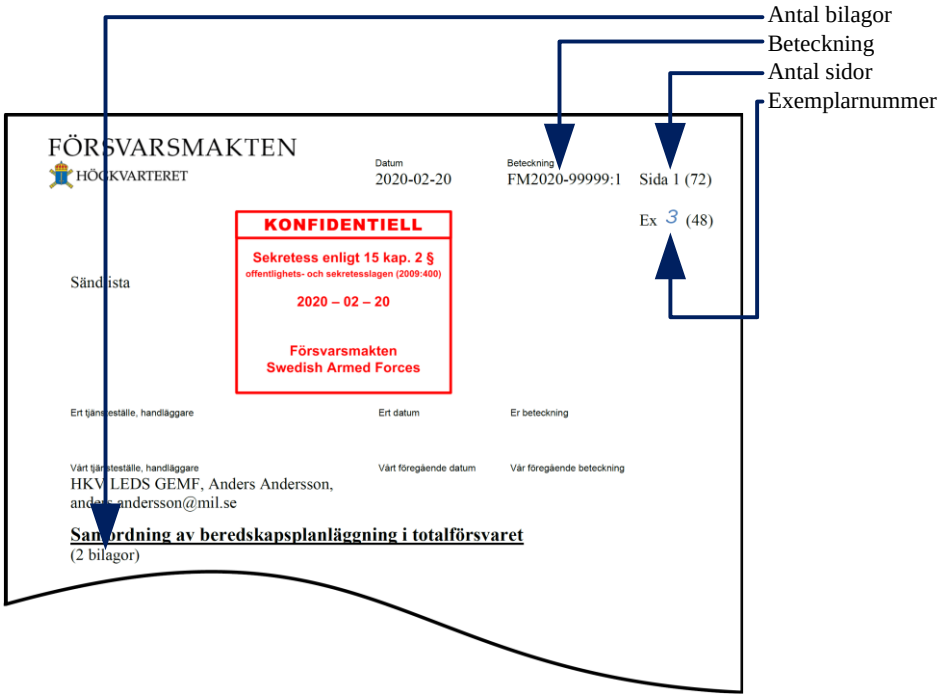


Bild 3.23. Exempel på märkning av en säkerhetsskyddsklassificerad allmän handlings första sida. Kim Hakkarainen/Försvarsmakten

En elektronisk allmän handling behöver inte märkas med exemplarnummer och antal sidor eftersom spårbarheten för åtkomst till handlingen uppnås med säkerhetsloggning. Ska handlingen skrivas ut måste utskriften däremot märkas med exemplarnummer och antal sidor för att kunna följa upp exemplaren som utskrifterna utgör.

3.6.2. Ursprungsland

”Säkerhetsskyddsklassificerade uppgifter som lämnas till en utländsk myndighet eller en mellanfolklig organisation ska omfattas av ett internationellt säkerhetsskyddsåtagande som Sverige har ingått med den andra staten eller organisationen, om det inte finns särskilda skäl för att sådana uppgifter ändå kan lämnas.”

3 kap. 9 § första stycket säkerhetsskyddsförordningen

”Om en säkerhetsskyddsklassificerad handling kan antas komma att lämnas över till utländska myndigheter eller leverantörer, ska den förses med en anteckning om ursprungsland om det inte är olämpligt.”

3 kap. 7 § andra stycket säkerhetsskyddsförordningen

Vägledande förklaring: Eftersom den säkerhetsskyddsklassificerade handlingen är märkt med ursprungsland (Sverige) och säkerhetsskyddsklass står det klart för mot-

tagaren att handlingen ska skyddas med säkerhetsskyddsåtgärder enligt det internationella säkerhetsskyddsåtagande som gäller för det aktuella fallet.

Ursprungsland (Sverige) framgår enligt moment 3:2 i märkning med säkerhetsskyddsklass på allmänna handlingar (avsnitt 3.4.1).

3.6.3. Behöriga utländska myndigheter och organisationer

Att det ska finnas ett internationellt säkerhetsskyddsåtagande är en grundförutsättning för att få lämna säkerhetsskyddsklassificerade uppgifter till en utländsk myndighet eller en mellanfolklig organisation.[145] Saknas ett sådant åtagande är den mottagande myndigheten eller organisationen inte förpliktad att ge uppgifterna ett säkerhetsskydd.

Endast omständigheten att det finns ett säkerhetsskyddsavtal med en annan stat eller en mellanfolklig organisation medför inte att staten eller organisationen kan få ta del av säkerhetsskyddsklassificerade uppgifter.

I 8 kap. 3 § OSL finns villkor för när en uppgift som omfattas av sekretess enligt OSL får lämnas till en utländsk myndighet eller en mellanfolklig organisation. Grunden är att sekretessbelagda uppgifter inte ska röjas till en annan stat (avsnitt 3.3.3).

> *”Om myndigheten har beslutat att en säkerhetsskyddsklassificerad handling får delges till någon utländsk myndighet eller mellanfolklig organisation får handlingens första sida märkas med en sådan upplysning.”*
>
> 3 kap. 27 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Märkningen talar om att de säkerhetsskyddsklassificerade uppgifterna i en handling har bedömts uppfylla villkoren för att få delges. Märkningen bör utformas så att det klart framgår till vilka länder eller mellanfolkliga organisationer uppgifterna får delges. På engelska uttrycks detta normalt med ”RELEASABLE TO” följt av en uppräkning av länder eller mellanfolkliga organisationer.

Märkningen får innehålla en begränsning för den utländska myndigheten eller mellanfolkliga organisationen att delge eller använda handlingen. I säkerhetsskyddsavtal förekommer det ofta ett åtagande att en part som delger information till en annan part kan specificera för vilket ändamål som informationen ska användas (benämns i internationella sammanhang normalt caveat).

I internationella samarbeten där svenska myndigheter deltar kan det finnas säkerhetsskyddsklassificerade uppgifter, som *inte* uppfyller villkoren i 8 kap. 3 § OSL för att få delges till en utländsk myndighet eller mellanfolklig organisation. Det finns inget hinder för att en myndighet som har bedömt att en säkerhetsskyddsklassificerad handling *inte får* delges en annan stat eller mellanfolklig organisation, att märka handlingen med en upplysning om detta.

---

[145] 3 kap. 9 § första stycket säkerhetsskyddsförordningen.

Behovet av märkningen finns även för säkerhetsskyddsklassificerade elektroniska handlingar. En sådan handling får märkas på lämpligt sätt med hänsyn till de informationssystem som handlingen behandlas i.[146]

3.6.4. Märkning om behöriga utländska myndigheter och organisationer

Moment 3:15 *Om en säkerhetsskyddsklassificerad handling i ett internationellt samarbete får delges till en annan stat eller en mellanfolklig organisation, ska handlingen märkas med en anteckning om vilka stater och organisationer som den får delges till.*

Vägledande förklaring: Med ”får delges” avses att det står klart att den säkerhetsskyddsklassificerade handlingen i sin helhet uppfyller villkoren i 8 kap. 3 OSL och förordningen om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet, för att få delges.

En anteckning utformas normalt på engelska och inleds med ”RELEASABLE TO” följt av en uppräkning av stater och mellanfolkliga organisationer. Anteckningen kan förkortas och inleds då med ”REL TO” följt av en uppräkning med förkortningar av staternas och organisationernas namn. Anteckningen anges normalt längst upp på varje sida i en handling.

Om delar av en säkerhetsskyddsklassificerad handling behöver märkas med anteckningen ”RELEASABLE TO” bör anteckningen anges förkortad tillsammans med märkning om säkerhetsskyddsklass i anslutning till textstycken, bilder, tabeller m.m. i handlingen (avsnitt 3.4.3), t.ex. ”(H - REL TO FIN)”.

Moment 3:16 *Om en säkerhetsskyddsklassificerad handling innehåller uppgifter som enligt 8 kap. 3 § OSL* inte får *delges någon annan stat eller mellanfolklig organisation får handlingen märkas med anteckningen FÅR EJ DELGES UTLÄNDSK MYNDIGHET.*

Vägledande förklaring: Märkningen betyder att uppgifter i en sådan handling inte får röjas till en annan stat eller mellanfolklig organisation. Om det vid en förnyad prövning står klart att villkoren i 8 kap. 3 § OSL är uppfyllda, får anteckningen på enklaste sätt överkorsas och uppgifterna delges till den andra staten eller organisationen. Om anteckningen behöver förkortas bör FEDUM användas. FEDUM är en förkortning för FÅR EJ DELGES UTLÄNDSK MYNDIGHET.

Om delar av en säkerhetsskyddsklassificerad handling behöver märkas med anteckningen bör anteckningen anges förkortad tillsammans med märkning om säkerhetsskyddsklass (avsnitt 3.4.3), t.ex. ”(K - FEDUM)”.

[146] 3 kap. 27 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd.

3.6.5. Utländsk märkning om begränsning att delge eller använda information

Moment 3:17 *Har en utländsk myndighet eller en mellanfolklig organisation försett en säkerhetsskyddsklassificerad handling med en anteckning som innebär begränsningar i att delge eller använda handlingen ska anteckningen följas om hinder inte möter enligt svensk rätt.*

Vägledande förklaring: I bilaterala säkerhetsskyddsavtal förekommer det ofta ett åtagande att en part som delger information till en annan part kan specificera för vilket ändamål som informationen ska användas. En sådan specificering, som kan göras genom anteckning på en säkerhetsskyddsklassificerad handling eller i någon form av styrande dokument, ska naturligtvis följas i den mån det inte strider mot svensk rätt att följa specificeringen. Detta innebär att om informationen är delgiven unikt för ett visst materielsamarbete får informationen inte användas i något annat sammanhang. Naturligtvis bestämmer Försvarsmakten (utifrån behörighetsrekvisiten) vilka vid myndigheten som ska delges informationen och bestämmelsen i sig avser inte att begränsa detta på något sätt.

Tabell 3.7. Exempel på caveat.

Organisation	Exempel på caveat
EU	RELEASABLE TO NBG PARTICIPANTS
	RELEASABLE TO NATO
	RELEASABLE TO NORWAY
Nato	RELEASABLE TO SWEDEN AND IRELAND
	RELEASABLE TO THE EU

En anteckning som innebär begränsningar i att delge eller använda säkerhetsskyddsklassificerade handlingar benämns i internationella sammanhang normalt *caveat* (se tabell 3.7 för exempel på caveat). Benämningen kan även användas i andra områden än informationssäkerhet och har då andra betydelser.

Om en allmän handling som är försedd med en sådan angiven begränsning begärs ut måste naturligtvis sekretessen vägas mot offentlighetsintressena. Om en sådan handling inte innehåller någon uppgift som omfattas av sekretess enligt OSL inträffar ett fall där den angivna begränsningen får vika för svensk rätt. Detta kan naturligtvis få betydelse för Sveriges relationer med det upprättande landet, varför sekretessprövningen måste vara mycket noggrann i detta fall. Anteckningen om caveat innebär ofta att handlingen omfattas av sekretess enligt 15 kap. 1 § OSL, den s.k. utrikessekretessen. Anteckningen om caveat på handlingen innebär inte i sig att sekretess föreligger.

3.7. Sändlista för exemplarhantering

”En säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre ska på handlingens sändlista märkas med hur många exemplar av handlingen som har framställts och vilka som är mottagare av respektive exemplar. Motsvarande uppgifter ska anges i diariet där handlingen är diarieförd, eller i ett register för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.

Första stycket gäller inte för säkerhetsskyddsklassificerade elektroniska allmänna handlingar.”

3 kap. 12 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen gäller såväl handlingar som ska distribueras till mottagare utanför Försvarsmakten som mottagare inom myndigheten.

På handlingar som ska till en annan myndighet anges normalt endast myndighetens namn eller organisatorisk del inom myndigheten på sändlistan. Om en handling är avsedd för en viss namngiven person bör det framgå på handlingens sändlista, så att mottagande myndighets registratur vet vem handlingen är avsedd för.

Spårbarheten för åtkomst till en elektronisk allmän handling uppnås med säkerhetsloggning. Det är därför inte meningsfullt att ange exemplarnummer för elektroniska handlingar i den elektroniska handlingens sändlista.

3.8. Registrering för uppföljning

”I det diarium där en säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre är diarieförd ska anges vem som förvarar handlingen eller om handlingen har förkommit, arkiverats eller gallrats. Uppgifterna får istället för i diariet antecknas i ett register för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.

För säkerhetskyddsklassificerade elektroniska allmänna handlingar får det istället anges i vilket informationssystem handlingen behandlas.”

3 kap. 18 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Registreringen är av stor betydelse för informationssäkerheten eftersom den gör det möjligt att upprätthålla kontrollen över en handling under dess livscykel, från att den har kommit in eller upprättats till dess att den har förstörts.

Genom registrering skapas underlag för inventering av handlingar för att kontrollera om handlingarna fortfarande är i behåll eller om de har förlorats. Registret ger även underlag för vilka handlingar som ska förstöras efter att de har återlämnats. Ett register över säkerhetsskyddsklassificerade handlingar behövs även för att i efterhand

kunna avgöra vilka handlingar som en person har haft tillgång till, t.ex. som underlag i en utredning om brott mot Sveriges säkerhet. Om en handling finns i flera exemplar gäller krav på registrering för varje exemplar.

Försvarsmakten kan ha flera diarier och register.

Uppgifter för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar behöver inte anges i ett diarium. Det kan vara lämpligt att använda diariet endast för ärendehantering och offentlighetsinsyn, och ett annat register för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.

3.8.1. Registrering av inlånade handlingar

Säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen konfidentiell eller högre som har lånats in från en annan myndighet måste registreras i ett register för att kunna följa upp innehavet under den tid som handlingen finns hos Försvarsmakten.[147]

3.8.2. Register över lagringsmedier

> *”Myndigheten ska föra ett register över myndighetens säkerhetsskyddsklassificerade lagringsmedier. Av registret ska det framgå lagringsmediets identifieringsuppgifter, vem som förvarar det och om mediet har förkommit, arkiverats eller förstörts.*
>
> *Ett säkerhetsskyddsklassificerat lagringsmedium som används endast en gång för omedelbar överföring av säkerhetskyddsklassificerade uppgifter mellan två informationssystem och som därefter omedelbart förstörs behöver inte föras in i registret.”*
>
> 3 kap. 19 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Det är lämpligt att ett register innehåller upplysning om för vilket informationssystem lagringsmediet är avsett att användas och lagringsmediets säkerhetsskyddsklass. Anledningen är att det vid förlust av ett lagringsmedium ska finnas möjlighet att utreda skadan av förlusten. Försvarsmakten kan ha flera register.

För säkerhetsskyddsklassificerade lagringsmedier som är placerade i säkerhetsskyddsklass konfidentiell och högre används registret även för att möjliggöra inventering. Observera att bestämmelsen inte är begränsad till lagringsmedier som är placerade i säkerhetsskyddsklass konfidentiell och högre. Även begränsat hemliga lagringsmedier ska registreras för att kunna möjliggöra utredningar när sådana lagringsmedier förloras eller återfinns.

[147] Följer av 3 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd.

3.8.3. Register som är undantagna allmänhetens insyn

Inom vissa områden eller för vissa slag av handlingar skulle ett register över allmänna handlingar p.g.a. sekretess enligt OSL endast komma att innehålla datum då handlingarna kom in eller upprättades samt diarienummer. Regeringen får för ett visst register föreskriva att uppgifter om handlingarnas avsändare och mottagare eller beskrivning av handlingens innehåll (ärendemening) *inte får* utelämnas eller särskiljas.[148]

Uppgifterna om en handlings avsändare och mottagare eller ärendemening ska då registreras i registret även om de omfattas av sekretess enligt OSL. Eftersom registret kommer att innehålla uppgifter som omfattas av sekretess enligt OSL kan registret inte hållas tillgängligt för allmänheten. Existensen av ett sådant register är inte en uppgift som omfattas av sekretess enligt OSL eftersom sådana register är angivna i 3 § OSF. Allmänheten kan begära att få ta del av registret och då måste en sekretessprövning göras på samma sätt som för en allmän handling som begärs utlämnad. En positiv effekt ur säkerhetsskyddssynpunkt med separata register, som allmänheten p.g.a. sekretesskäl inte har insyn i, är att tillgången till ett sådant register även ska begränsas inom myndigheten till de personer som behöver tillgång till registret. Det kan även vara nödvändigt att styra behörigheten till uppgifterna i ett sådant register med hänsyn till vilka uppgifter personerna är behöriga till.

Om regeringen har föreskrivit att ett visst register alltid ska innehålla handlingarnas avsändare och mottagare eller ärendemening får registret endast användas för registrering av handlingar som uppfyller de villkor som regeringen föreskrivit. Andra slag av allmänna handlingar ska registreras i ett annat register, normalt ett register som är tillgängligt för allmänheten.

”Följande myndigheter ska i den utsträckning som framgår nedan inte tillämpa 5 kap. 2 § andra stycket offentlighets- och sekretesslagen (2009:400).

Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut	*Diarier över inriktningar enligt lagen (2000:130) om försvarsunderrättelseverksamhet och över underrättelser inom försvarets underrättelse- och säkerhetstjänst.”*

3 § OSF

Vägledande förklaring: Ett exempel på register över allmänna handlingar som regeringen har undantagit från allmänhetens insyn är diarier vid Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut över

[148] 5 kap. 4 § OSL.

underrättelser inom försvarets underrättelse- och säkerhetstjänst.[149] Registret är även avsett för *inriktningar enligt lagen om försvarsunderrättelseverksamhet*.

Ett sådant register är *underrättelse- och säkerhetsdiariet* vid Must. Registret får således endast användas för registrering av allmänna handlingar som utgör sådana underrättelser eller inriktningar. Säkerhetsrapporter (avsnitt 10.2) är ett exempel på underrättelser i säkerhetstjänst. Alla andra slag av allmänna handlingar i underrättelse- och säkerhetstjänst ska registreras i ett register som allmänheten har insyn i.

Undantaget från allmänhetens insyn i sådana register är i Försvarsmakten inte begränsat till Must, utan ska i Försvarsmakten även tillämpas av organisationsenheter.

Observera!
Handlingar från Must som är registrerade i underrättelse- och säkerhetsdiariet vid Must (t.ex. underrättelseorienteringar) får inte registreras i VIDAR eller exemplarhanteras i DIANA.

Att handlingarna är undantagna från att registreras i register som allmänheten har insyn i påverkar inte kraven på exemplarhantering. Underrättelse- och säkerhetscentralen vid Must kan ge organisationsenheterna stöd i lämplig rutin för lokal exemplarhantering av handlingarna.

3.9. Kopiering och utdrag

”Myndigheten ska besluta vilka rutiner som ska tillämpas i samband med kopiering av eller utdrag ur en säkerhetsskyddsklassificerad handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre. Rutinerna ska dokumenteras.

Har en kopia av en säkerhetsskyddsklassficerad allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre gjorts, ska uppgift om detta liksom uppgift om till vem kopian eller utdraget har lämnats antecknas i det register eller liggare där handlingen är diarieförd eller i ett register för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.”

3 kap. 14 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Rutinerna ska förebygga att s.k. svartkopior av fysiska exemplar uppstår. Svartkopior är oregistrerade fysiska kopior av eller utdrag ur säkerhetsskyddsklassificerade allmänna handlingar som ska registreras, dvs. fysiska kopior som Försvarsmakten inte har kontroll över. Svartkopior minskar skyddseffekten av att hanteringen av övriga exemplar är spårbar. En förlust av en svartkopia kan inte uppmärksammas i en inventering av säkerhetsskyddsklassificerade handlingar eftersom uppgift om kopian (exemplaret) saknas i registret över säkerhetsskyddsklassi-

[149] 3 § OSF.

ficerade handlingar. Rutinerna om kopiering och utdrag har därför en stark koppling till krav på registrering och exemplarhantering.

När en säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklass konfidentiell eller högre skrivs ut från ett informationssystem uppstår ett nytt exemplar. Detta nya exemplar ska registreras (avsnitt 3.8).

3.9.1. Rutin för kopiering och utdrag

Moment 3:18 *Organisationsenheten ska ta fram rutiner för hur kopiering av eller utdrag ur fysiska säkerhetsskyddsklassificerade handlingar ska genomföras vid enheten. Rutinerna ska beskriva hur kopiering ska genomföras.*

Vägledande förklaring: En kopiator är normalt ett informationssystem och omfattas därför av de bestämmelser som gäller för informationssystem. Kopiering av säkerhetsskyddsklassificerade handlingar måste genomföras på utrustning som är godkänd ur säkerhetsskyddssynpunkt (ackrediterade). Utrustning som inte är godkänd får inte användas för kopiering. Rutinerna måste säkerställa att endast godkänd utrustning används, t.ex. genom att utrustningarna förses med märkning om vilken högsta säkerhetsskyddsklass den är godkänd för. Rutinerna bör även beskriva vad personalen måste uppmärksamma vid kopiering, t.ex. att inte lämna kvar original och kopior.

Moment 3:19 *För säkerhetsskyddsklassificerade allmänna handlingar i säkerhetsskyddsklass konfidentiell eller högre ska rutinerna dessutom beskriva:*

a) Vem som beslutar att en handling får kopieras (kopieringstillstånd).

b) Hur en kopia eller utdrag ska hanteras så att det nya exemplaret registreras innan det lämnas till den person som ska ta emot det. Rutinerna ska säkerställa att en person som förvarar en handling inte själv får kopiera den.

Vägledande förklaring till punkten a: Ett *kopieringstillstånd* beslutas självständigt inom en organisationsenhet. Det finns inget krav på att ett sådant beslut ska föregås av samverkan för en handling som har upprättats av en annan myndighet eller i Försvarsmakten av en annan organisationsenhet.

Det är inte nödvändigt att det ska vara en chef för den verksamhet som har *upprättat* handlingen som ska besluta om kopiering eller utdrag. Beslut om kopieringstillstånd kan ske nära den verksamhet som har behov av fler kopior, t.ex. om flera personer ska arbeta tillsammans och varje person för arbetet behöver ett eget exemplar av en viss handling.

För att motverka förekomsten av svartkopior, öka spårbarheten och underlätta tillgängligheten till informationstillgångar, är det lämpligt att en chef i den verksamhet där ett exemplar av den fysiska handlingen *förvaras* beslutar om kopieringstillstånd. Även chefer som har fattat beslut om fördelning av ärenden i en verksamhet bör kunna fatta beslut om kopieringstillstånd.

Rutinerna för kopiering eller utdrag måste säkerställa att den person som kopieringstillståndet avser uppfyller behörighetskraven i 2 kap. 3 § säkerhetsskyddsförordningen, t.ex. att personen behöver uppgifterna för att kunna utföra sitt arbete.

Tips!
Krångla inte till det. Restriktiva rutiner för kopieringstillstånd, betingade av nit om ett gott säkerhetsskydd, kan försvåra och fördröja informationshanteringen så att det mer skadar än gör nytta.

För en handling som inte uppfyller villkoren i 2 kap. tryckfrihetsordningen för att vara en allmän handling, finns inga krav på exemplarhantering. En s.k. arbetshandling får därför kopieras av den person som förvarar handlingen, om det behövs för arbetet, utan att det finns ett kopieringstillstånd.

Vägledande förklaring till punkten b: Säkerhetsskydd ska skydda säkerhetskänslig verksamhet mot bl.a. spioneri. Rutinerna för kopiering och utdrag ska därför utformas så att det är någon annan person som kopierar eller gör utdraget, än den person som förvarar den fysiska handlingen. Det normala i Försvarsmakten är att kopieringen genomförs av expedition vid organisationsenheten, stabsexpedition i en kontingent i utlandet eller liknande funktion för informationshantering.

Rutinerna måste också säkerställa att det nya fysiska exemplaret registreras, innan det lämnas till den person som ska ta emot det (avsnitt 3.11). Registrering av exemplar (avsnitt 3.8) är en förutsättning för att kunna följa upp innehavet genom inventering (avsnitt 3.13).

3.10. Distribution

3.10.1. Rutiner för distribution

”Myndigheten ska ha rutiner för hur säkerhetsskyddsklassificerade handlingar och lagringmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre ska distribueras inom och utom myndigheten. Rutinerna ska dokumenteras. Myndigheten ska se till att nödvändiga skyddsåtgärder vidtas under distributionen.”

3 kap. 25 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Säkerhetsskyddsklassificerade uppgifter bör, ur säkerhetsskyddssynpunkt, i första hand överföras elektroniskt i informationssystem, krypterade med kryptografiska funktioner som har godkänts av Försvarsmakten, mellan avsändande och mottagande parter. Om det inte är möjligt får uppgifterna skrivas ut på en fysisk handling eller lagras på ett lagringsmedium som distribueras fysiskt.

Kravet i bestämmelsens första stycke gäller, enligt 3 kap. 3 och 4 §§ Försvarsmaktens föreskrifter om säkerhetsskydd, även för tryckta skrifter och materiel som inne-

håller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell. Kravet gäller, enligt tredje stycket i bestämmelsen, inte för elektroniska handlingar. Rutinerna utformas så att handlingarna och lagringsmedierna skyddas så att obehöriga inte kan ta del av uppgifterna när de distribueras. Öppna postfack för begränsat hemliga handlingar är ett exempel på intern distribution där nödvändiga skyddsåtgärder inte har vidtagits, eftersom obehöriga kan ta del av uppgifterna.

För distribution utanför Försvarsmakten behöver rutinerna även utformas så att distributionen sker mellan avsändande och mottagande myndighets registraturer, för att säkerställa att handlingar och lagringsmedier registreras. Personadresserade försändelser är inte lämpliga och ska undvikas, eftersom sådan adressering ökar sannolikheten för att handlingar och lagringsmedier inte kommer att registreras. Av samma skäl bör personlig överlämning till mottagare undvikas.

Om skyddet för handlingarna och lagringsmedierna blir lägre under distribution utanför Försvarsmakten, jämfört med när de hanteras inom myndigheten, riktas skyddsåtgärderna på att upptäcka förseningar av, förlust av och påverkan på försändelser. Rutinerna för distribution utanför myndigheten bör innehålla åtgärder för att upptäcka om ett emballage under distributionen har öppnats eller ersatts med ett nytt emballage.

För säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen begränsat hemlig finns inget krav att nödvändiga skyddsåtgärder ska vidtas under distribution. Sådana handlingar och lagringsmedier får dock omfattas av skyddsåtgärder som gäller för handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre.

Moment 3:20 *Om organisationsenheten utför distribution av fysiska säkerhetsskyddsklassificerade handlingar, lagringsmedier och materiel som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, ska enheten ta fram rutiner för distributionen.*

Moment 3:21 *Rutiner för distribution ska minst innehålla:*

a) Åtgärder för iordningsställande, avsändning, mottagning och kontroll av emballage och försändelser.

b) Åtgärder för uppföljning av att försändelser har kommit fram samt upptäckt av förseningar och förlust.

c) Åtgärder för spårbarhet av vilka handlingar, tryckta skrifter, lagringsmedier och materiel som finns i en försändelse.

d) Åtgärder när:

1) försändelser har försenats eller förlorats,

2) innehåll i försändelser inte överensstämmer med det förväntade, samt

3) *försändelser eller emballage har påverkats.*

Vägledande förklaring: Dokumenthanteringsenheten vid Försvarsmaktens HR-centrum (FM HRC DokhE) stödjer organisationsenheterna med dokumenthantering, inklusive distribution. Försvarets bok och blankettförråd (FBF) vid Försvarsmaktens centrallager hanterar distribution av publikationer. Om en organisationsenhet endast använder sådana tjänster och inte har behov av egen rutin, behöver organisationsenheten inte ta fram en rutin för distribution.

3.10.2. Godkänd distributör

”En försändelse med säkerhetsskyddsklassificerade handlingar eller lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre ska sändas med en distributör som har godkänts av myndigheten. En sådan distributör ska kunna verifiera att försändelsen har levererats till mottagaren.”

3 kap. 25 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ska godkänna sådan distributör.”

3 kap. 6 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: En distributör får vara en utomstående part som tillhandahåller tjänsten att genomföra fysisk distribution av en försändelse till mottagaren.

För säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen begränsat hemlig finns inget krav att distributören ska ha godkänts. Det finns inte heller något hinder mot att sådana handlingar och lagringsmedier skickas med en distributör som har godkänts för handlingar och lagringsmedier som är placerade i högre säkerhetsskyddsklasser.

Försvarsmaktens beslut 2017 om godkännande av distributör innebär att Postnord får användas för Försvarsmaktens distribution inom Sverige av säkerhetsskyddsklassificerade handlingar, tryckta skrifter, lagringsmedier och materiel upp till och med säkerhetsskyddsklass hemlig, om de sänds med tilläggstjänsterna REK eller VÄRDE.[150]

Beslutet innebär att Försvarsmakten inte får använda Postnord för att sända säkerhetsskyddsklassificerade handlingar, tryckta skrifter, lagringsmedier och materiel i säkerhetsskyddsklassen kvalificerat hemlig. Försvarsmakten får ta emot säkerhetsskyddsklassificerade handlingar, tryckta skrifter, lagringsmedier och materiel i sä-

[150] Godkännande av distributör för postdistribution av hemliga handlingar” (FM2015-8736:1).

kerhetsskyddsklassen kvalificerat hemlig som har sänts med Postnord av andra myndigheter och företag.

För signalskyddstjänsten gäller särskilda bestämmelser för distribution av signalskyddsnycklar.

3.10.3. Distribution till och från utlandet

”För försändelser till och från utlandet med säkerhetsskyddsklassificerade handlingar och som inte skyddas av kryptografiska funktioner enligt 5 §, ska Utrikesdepartementets kurirförbindelser anlitas. Säkerhetspolisen och Försvarsmakten får inom respektive myndighets tillsynsområde meddela föreskrifter om undantag från kravet i första stycket.”

3 kap. 10 § säkerhetsskyddsförordningen

”En myndighet får inom ramen för ett samarbete med ett annat land eller en mellanfolklig organisation komma överens om att distribuera säkerhetsskyddsklassificerade handlingar på annat sätt än vad som föreskrivs i 3 kap. 10 § första stycket säkerhetsskyddsförordningen.”

3 kap. 29 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen avser distribution mellan en svensk myndighet och en utländsk myndighet, ett utländskt företag eller en mellanfolklig organisation.

Med *annat sätt* avses t.ex. kurir som inte ingår i de diplomatiska kurirförbindelserna eller distribution genom kommersiella kurirföretag.

Det är inte alltid möjligt att använda Utrikesdepartementets kurirförbindelser. Behöver en svensk myndighet distribuera säkerhetsskyddsklassificerade handlingar utanför Utrikesdepartementets kurirförbindelser, måste distributionen uppfylla bestämmelser om distribution i det säkerhetsskyddsavtal som Sverige har ingått med det andra landet eller mellanfolkliga organisationen.

I vissa av Sveriges säkerhetsskyddsavtal framgår att de ingående parternas behöriga säkerhetsmyndigheter först ska godkänna distribution som ska genomföras på annat sätt. Det kan t.ex. röra sig om distribution av säkerhetsskyddsklassificerade handlingar som rör ett specifikt samarbete mellan Sverige och ett annat land och där transportvägen mellan länderna anses tillräckligt säker även utan det skydd som Utrikesdepartementets kurirförbindelser ger.

I andra säkerhetsskyddsavtal finns mer detaljerade bestämmelser om vilken distribution, förutom diplomatiska kanaler, som är tillåten. Ett exempel är Sveriges säkerhets-

skyddsavtal med Frankrike[151], Spanien[152], Storbritannien[153] och Tyskland[154] där det framgår att kurirföretag i brådskande fall får anlitas för distribution av säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklass konfidentiell, under förutsättning att kurirföretaget uppfyller krav som anges i säkerhetsskyddsavtalen. I de fyra säkerhetsskyddsavtalen framgår också att begränsat hemliga handlingar ska distribueras enligt avsändarens nationella bestämmelser och att detta kan innebära distribution med kurirföretag.

”En myndighet får också inom ramen för egen verksamhet som bedrivs i utlandet distribuera säkerhetsskyddsklassificerade handlingar på annat sätt än vad som föreskrivs i 3 kap. 10 § första stycket säkerhetsskyddsförordningen, om distributionen är under myndighetens kontroll och omfattas av säkerhetsskyddsåtgärder för att försvåra och upptäcka obehörig åtkomst till handlingarna.”

3 kap. 29 § tredje stycket
Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen avser en svensk myndighets verksamhet utomlands. Bestämmelsen innebär att Utrikesdepartementets kurirförbindelser inte behöver anlitas för distribution för egen verksamhet som myndigheter bedriver i utlandet.

3.10.4. Försvarsmaktens distribution till och från utlandet

Moment 3:20 och moment 3:21 i avsnitt 3.10.1 gäller även för distribution till och från utlandet.

För distribution av säkerhetsskyddsklassificerade handlingar till en svensk kontingent i utlandet kan inte alltid Utrikesdepartementets kurirförbindelser användas. Distributionen kan i sådana fall genomföras som en transport av säkerhetsskyddsklassificerade handlingar. Distribution underlättas av att transporten genomförs av Försvarsmaktens personal i militärt fartyg, luftfartyg eller fordon.

[151] SÖ 2007:2, artikel 7.3.
[152] SÖ 2006:18, artikel 8.2.
[153] SÖ 2007:66, artikel 8.2.
[154] SÖ 2016:5, artikel 8.2.

3.11. Kvittering vid mottagande

”När en säkerhetsskyddsklassificerad allmän handling eller ett säkerhetsskyddsklassificerat lagringsmedium som är placerat i säkerhetsskyddsklassen konfidentiell eller högre tas emot ska mottagandet kvitteras med underskrift, namnförtydligande och datum. Ett namnförtydligande får vara en kod.

När en säkerhetsskyddsklassificerad allmän handling eller ett säkerhetsskyddsklassificerat lagringsmedium återlämnas ska detta antecknas på kvittokopian. Kvittokopian för en handling som är placerad i säkerhetsskyddsklassen konfidentiell eller hemlig ska bevaras i minst 10 år. Kvittokopian för en handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig ska bevaras i minst 25 år.

Mottagande av en säkerhetskyddad elektronisk handling behöver dock inte kvitteras om mottagandet sker i ett informationssystem där det i en säkerhetslogg noteras vem som tagit del av handlingen.”

3 kap. 15 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Kvittering vid mottagande möjliggör spårbarhet av vilka personer som tagit emot ett exemplar av en handling eller ett lagringsmedium. Kvitteringen och den registrering som sker är väsentlig för att veta vem som förvarar ett visst exemplar av en handling eller ett lagringsmedium. Det är också en förutsättning för att kunna följa upp innehavet och, om något saknas, vara ett underlag för utredning om vad som har hänt. Ett exempel på kod är FMID.

För handlingar gäller krav på kvittering endast säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklass konfidentiell eller högre. För lagringsmedier görs ingen skillnad på mediets status som allmän handling enligt tryckfrihetsförordningen.

Det är lämpligt att kvittot förvaras av myndighetens registratur, eller motsvarande funktion, till dess att personen lämnar tillbaka den handling eller lagringsmedium som kvittot avser. Vid återlämning är det lämpligt att personen får kvittot så att personen efteråt kan visa att handlingen eller lagringsmediet har återlämnats.

Anledningen till att kvitto ska bevaras hos myndigheten i 10 respektive 25 år är relaterat till preskriptionstiden för brott som kan sammankopplas med en säkerhetsskyddsklassificerad handling. Preskriptionstiden för brottet grov obehörig befattning med hemlig handling är 10 år.

En underskrift kan vara elektronisk.

Med ”säkerhetskyddad elektronisk handling” i bestämmelsen avses säkerhetsskyddsklassificerad elektronisk handling.

”Vad som föreskrivs i 15 § gäller inte när arkiv-, expeditions-, sambands- eller tryckeripersonal tar emot en sådan säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium för registrering, kopiering, distribution, arkivering eller förstöring, om inte den som lämnar över handlingen begär det. Vad som föreskrivs i 15 § gäller inte heller för personal som arbetar med drift av informationssystem för sådana säkerhetsskyddsklassificerade lagringsmedier som hanteras i driften av informationssystemen.”

3 kap. 16 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: De angivna personalkategorierna hanterar regelbundet en stor mängd handlingar och lagringsmedier. Personalen får därmed anses ha haft möjlighet att ta del av de säkerhetsskyddsklassificerade uppgifterna och därmed är det inte heller rationellt att upprätthålla kvitteringskravet för dessa personalkategorier. Även om personalkategorierna har till arbetsuppgift att hantera handlingarna och lagringsmedierna betyder det inte att de ska ta del av uppgifterna.

Personal vid bokförråd som hanterar utlåning och distribution av säkerhetsskyddsklassificerade publikationer likställs i detta avseende med expeditionspersonal.

3.12. Kvittering vid muntlig delgivning eller genom visning

”Myndigheten ska ha rutiner för hur kvittering ska göras om uppgifter i en säkerhetsskyddklassificerad allmän handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig, lämnas muntligt eller genom visning. Rutinerna ska dokumenteras.”

3 kap. 17 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen gäller muntlig överföring av uppgifter och visning. Ett exempel när kvittering ska ske är i mötessammanhang där en presentation som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen kvalificerat hemlig presenteras. Presentationen måste uppfylla villkoren i tryckfrihetsförordningen för att vara en allmän handling, t.ex. om en presentation har färdigställts, och därmed upprättats, före mötet.

Ett annat exempel när kvittering ska ske är när innehavaren av en säkerhetsskyddklassificerad allmän handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig visar innehållet i handlingen för en kollega.

3.12.1. Rutin vid muntlig delgivning eller genom visning

Moment 3:22 *När uppgifter i en säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig, lämnas muntligt eller genom visning, ska kvittering genom namnteckning och namnförtydligande ske på delgivningskvitto eller lista. På delgivningskvittot eller listan anges det datum när upp-*

gifterna lämnades eller visades. Kvittot eller listan ska om möjligt förvaras tillsammans med handlingen.

Moment 3:23 *Kvitton och listor ska hållas ordnade vid expeditioner eller arkiv så att det är möjligt att undersöka vilka personer som har kvitterat att de, muntligen eller genom visning, har tagit del av uppgifterna.*

Vägledande förklaring: Enligt RA-MS 2018:42 får kvitton och listor gallras 25 år efter utgången av det år då handlingen har återlämnats.

Det är lämpligt att en expedition alltid fäster en delgivningslista på en sådan handling. På så sätt behöver inte innehavaren av handlingen tänka på att finna en sådan blankett i samband med att delgivning av uppgifter ur handlingen.

Tidigare kvitterades muntlig delgivning och visning av uppgifter i en allmän hemlig handling som hade placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre. Något sådant krav finns inte längre för upp till och med säkerhetsskyddsklassen hemlig.

Observera!
Det finns inget krav i Försvarsmakten att kvittera muntlig delgivning eller visning ur säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklasserna begränsat hemlig, konfidentiell eller hemlig.

3.13. Inventering

Inventering innebär en regelbunden kontroll av att varje exemplar av en handling är i behåll eller om de har förlorats. Inventeringen syftar till att upprätthålla spårbarheten i hanteringen av handlingar som införts genom sändlistor, registrering, numrering av exemplar, och kvittering vid mottagande. En positiv effekt av inventering är att innehavare av handlingar anstränger sig för att behålla kontrollen över dessa.

”Säkerhetsskyddsklassificerade handlingar som innehåller uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska inventeras minst en gång per år. Säkerhetsskyddsklassificerade handlingar som innehåller uppgifter i säkerhetsskyddsklassen hemlig eller konfidentiell ska inventeras i den omfattning som anges i Säkerhetspolisens föreskrifter eller, om det gäller verksamhet som hör till Försvarsmaktens tillsynsområde, Försvarsmaktens föreskrifter.

För arkiverade handlingar gäller kravet på inventering enbart för handlingar i säkerhetsskyddsklassen kvalificerat hemlig.

Hos myndigheter och annan verksamhet som offentlighets- och sekretesslagen (2009:400) är tillämplig på gäller kravet på inventering endast för allmänna handlingar.”

3 kap. 8 § säkerhetsskyddsförordningen

”Säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig ska inventeras en gång per år.

Säkerhetskyddsklassificerade elektroniska handlingar behöver inte inventeras.”

3 kap. 21 § andra och tredje styckena
Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Uppgifter om vilka exemplar som ska inventeras finns i det diarium eller register där exemplaren är registrerade enligt 3 kap. 18 § Försvarsmaktens föreskrifter om säkerhetsskydd (avsnitt 3.8).

För att en inventering ska få avsedd effekt är det lämpligt att det är någon annan än den person som har kvitterat handlingarna, som kontrollerar om handlingarna är i behåll eller om de saknas. Om en handling består av flera lösa bilagor eller lagringsmedier måste även dessa kontrolleras. Normalt är det inte nödvändigt att räkna varje sida i en handling, om det inte finns tydliga indikationer på att handlingen inte längre är intakt, t.ex. när sidor lossnat.

I 3 kap. 8 § säkerhetsskyddsförordningen framgår att kravet på inventering inte gäller arkiverade säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig. Arkiverade säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklassen kvalificerat hemlig ska inventeras.

Även *tryckta skrifter* som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell eller högre ska inventeras, enligt 3 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd. Exempel på tryckta skrifter är bokpublikationer, reglementen, manualer och handböcker. Ett annat exempel är kartor och sjökort.

Det är fysiska föremål (såsom handlingar i pappersform, tryckta skrifter, lagringsmedier och materiel) som ska inventeras för att kontrollera om föremålen är i behåll eller om de har förlorats. Att inventera elektroniska handlingar är normalt inte meningsfullt, t.ex. att de elektroniska handlingarna är kvar på ett lagringsmedium. Elektroniska handlingar kan dessutom finnas i flera kopior i ett informationssystem. Händelser när säkerhetsskyddsklassificerade elektroniska handlingar hanteras i ett informationssystem loggas i systemets säkerhetsloggning enligt 4 kap. 17 § Försvarsmaktens föreskrifter om säkerhetsskydd (avsnitt 4.8.3).

Även säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen konfidentiell eller högre som har lånats från en annan myndighet ska, enligt 3 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd, inventeras.

Om en prioritering av vilka säkerhetsskyddsklassificerade handlingar som avses inventeras behöver göras, bör den utgå från handlingarnas högsta säkerhetsskyddsklass.

”Ett säkerhetsskyddsklassificerat lagringsmedium som är placerat i säkerhetsskyddsklassen konfidentiell eller högre ska inventeras en gång per år.”

3 kap. 22 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Ett lagringsmedium kan innehålla en mycket stor mängd uppgifter samtidigt som det yttre utförandet kan vara mycket litet. Förlust av ett lagringsmedium som innehåller säkerhetsskyddsklassificerade uppgifter kan därför medföra skador för Sveriges säkerhet i mycket stor omfattning.

I motsats till konventionella handlingar används inte ett lagringsmediums status enligt tryckfrihetsförordningen för att styra vilket säkerhetsskydd lagringsmediet ska ha. Ett skäl är att säkerhetskopior enligt 2 kap. 13 § andra stycket tryckfrihetsförordningen är undantagna från att vara allmänna handlingar.

Även *materiel* som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell eller högre ska inventeras, enligt 3 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd. Säkerhetsskyddsklassificerade lagringsmedier och materiel bör inventeras samtidigt som de säkerhetsskyddsklassificerade allmänna handlingarna inventeras.

Ett lagringsmedium har oftast ett serienummer som är åtkomligt för avläsning genom det gränssnitt som det är anslutet med. I informationssystem kan det vara lämpligt att använda tekniska funktioner för att läsa av serienummer på fast monterade lagringsmedier för att genomföra inventeringen.

Om ett lagringsmedium saknas vid en inventering och inte kan återfinnas efter eftersökning, måste händelsen rapporteras enligt 2 kap. 10 § första stycket 2 säkerhetsskyddsförordningen.

3.13.1. Rutin för inventering

Moment 3:24 *Organisationsenheten ska ha dokumenterade rutiner för hur inventering av säkerhetsskyddsklassificerade handlingar, tryckta skrifter, lagringsmedier och materiel ska gå till.*

Vägledande förklaring: I det fall en handling består av flera lösa bilagor eller lagringsmedier måste även dessa kontrolleras. Om handlingen har gått sönder, t.ex. om sidor lossnat, bör en noggrannare kontroll av att handlingen är intakt ske. Att räkna varje sida i en hemlig handling, inklusive bilagor, bör endast genomföras när det finns tydliga indikationer på att handlingen inte är intakt. I detta avseende bör noggrannheten i inventeringen vara större för handlingar m.m. som är placerade i säkerhetsskyddsklass kvalificerat hemlig.

I böcker som består av lösbladssystem, samt i ohäftade handlingar, bör varje blad kontrolleras.

Dokumenthanteringsenheten vid Försvarsmaktens HR-centrum (FM HRC DokhE) stödjer organisationsenheterna med dokumenthantering, inklusive inventering av säkerhetsskyddsklassificerade handlingar. Om en organisationsenhet endast använder den tjänsten och inte har behov av egen rutin, behöver organisationsenheten inte ta fram en rutin för inventering av de handlingar som inventeras av FM HRC DokhE.

Ett äldre beslut[155] om hur hemliga handlingar ska inventeras motsvarar rutiner i momentet.

Moment 3:25 *Inventering ska protokollföras av en inventeringsförrättare. Ett inventeringsprotokoll upprättas för varje person som har inventerats. I protokollet ska det framgå vilka exemplar av handlingar, tryckta skrifter, lagringsmedier och materiel som är i behåll och vilka som saknas.*

Moment 3:26 *Inventering av säkerhetsskyddsklassificerade allmänna handlingar, tryckta skrifter, lagringsmedier och materiel som har placerats i säkerhetsskyddsklassen kvalificerat hemlig ska utföras av två inventeringsförrättare som är anställda i Försvarsmakten.*

Vägledande förklaring: Ingen av inventeringsförrättarna får vara den person som ska få sina handlingar, tryckta skrifter, lagringsmedier och materiel inventerade. Att en person genomför inventering innebär inte att personen är behörig att ta del av uppgifterna i handlingarna m.m. Även om personerna som genomför inventeringen inte ska ta del av uppgifterna är det ofrånkomligt att detta kan ske under ett inventeringstillfälle. Personal som genomför inventeringen ska därför i övrigt ha till arbetsuppgift att hantera säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass kvalificerat hemlig.

Personerna som genomför inventeringen behöver inte kvittera att de genom visning har delgivits uppgifter ur handlingarna. Uppgift om vilka personer som har genomfört inventeringen bör framgå på inventeringsprotokollet.

Moment 3:27 *Om en säkerhetsskyddsklassificerad handling, en tryckt skrift, ett lagringsmedium eller materiel trots eftersökning inte kan återfinnas vid inventering ska detta rapporteras som en säkerhetshotande händelse.*

Rapportering beskrivs i avsnitt 10.2.1.

3.13.2. Inventering i arkiv

Handlingar som är placerade i säkerhetsskyddsklass kvalificerat hemlig och som förvaras i en förseglad låda i ett arkiv kan inventeras genom att kontrollera att lådan är i behåll, samt att lådan och förseglingen är intakt. En sådan försegling måste dock vara av en sådan typ att det ska kunna upptäckas om den ursprungliga förseglingen har ersatts med en ny. Det är också nödvändigt att förteckningar över innehållet i en sådan låda hålls aktuella vid en expedition. Det kan t.ex. i det register där en hand-

[155] 2 kap. 15 § Försvarsmaktens interna bestämmelser (FIB 2015:2) om säkerhetsskydd och skydd av viss materiel.

ling är diarieförd framgå i vilken låda handlingen är placerad. När en sådan låda iordningsställs bör två personer samtidigt delta i arbetet, inklusive förseglingen av lådan och registrering av handlingarna.

3.14. Återlämning

”När en säkerhetsskyddsklassificerad allmän handling eller ett säkerhetsskyddsklassificerat lagringsmedium återlämnas ska detta antecknas på kvittokopian. Kvittokopian för en handling som är placerad i säkerhetsskyddsklassen konfidentiell eller hemlig ska bevaras i minst 10 år. Kvittokopian för en handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig ska bevaras i minst 25 år.”

3 kap. 15 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Moment 3:28 *När en säkerhetsskyddsklassificerad allmän handling, en tryckt skrift, ett lagringsmedium eller materiel som är placerat i säkerhetsskyddsklass konfidentiell eller högre inte längre behövs för arbetet, ska handlingen, den tryckta skriften, lagringsmediet eller materielen återlämnas.*

Moment 3:29 *Återlämning görs till den expedition eller servicedisk där handlingen, den tryckta skriften, lagringsmediet eller materielen är diarieförda eller registrerade för att kunna följas upp.*

Vägledande förklaring: I avsnitt 3.8 beskrivs registrering för uppföljning av säkerhetsskyddsklassificerade handlingar och lagringsmedier.

När en handling eller ett lagringsmedium lämnas tillbaka är det lämpligt att originalkvittot återlämnas till mottagaren, eftersom det är det enda han eller hon har för att bevisa att den handlingen eller lagringsmediet är återlämnat.

Det finns inget krav ur säkerhetsskyddssynpunkt att en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium som är placerat i säkerhetsskyddsklass begränsat hemlig ska återlämnas till en expedition. Om det är fråga om en allmän handling ska dock originalet återlämnas för att bevaras.

Moment 3:30 *När en persons anställning eller uppdrag i Försvarsmakten avslutas ska samtliga säkerhetsskyddsklassificerade handlingar, tryckta skrifter, lagringsmedier och materiel som personen förvarar återlämnas, förstöras eller lämnas kvar inom organisationsenheten.*

3.15. Återlämning av en lånad handling

Moment 3:31 *En säkerhetsskyddsklassificerad handling som har lånats från en annan myndighet ska återlämnas till den utlånande myndigheten när handlingen inte längre behövs för arbetet. Att en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklass konfidentiell eller högre har återlämnats ska dokumenteras i det register som används för uppföljning av exemplar av handlingen i Försvarsmakten.*

3.16. Arkivering

”För gallring av säkerhetsskyddsklassificerade allmänna handlingar gäller särskilda bestämmelser som meddelas av Riksarkivet.”

3 kap. 23 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen är en påminnelse om att säkerhetsskyddsklassificerade allmänna handlingar endast får gallras enligt de regler som återfinns i arkivlagen och meddelade gallringsbeslut.

En myndighet har skyldighet att arkivera allmänna handlingar oavsett handlingarnas klassificering. Arkivet är en del av kulturarvet vilket alltid ska beaktas när handlingar gallras. Myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de bl.a. tillgodoser rätten att ta del av allmänna handlingar.[156]

Riksarkivet har bl.a. meddelat:

- Riksarkivets föreskrifter (RA-MS 2018:42) och allmänna råd om gallring hos Fortifikationsverket, Försvarets materielverk, Försvarsmakten, Totalförsvarets forskningsinstitut och Totalförsvarets rekryteringsmyndighet. Föreskrifterna omfattar bevarande och gallring av handlingar om säkerhet och säkerhetsskydd.
- Riksarkivets föreskrifter (RA-FS 2018:3) och allmänna råd om återlämnande eller gallring av handlingar vid upphandling. Föreskrifterna omfattar bl.a. handlingar för säkerhetsskyddad upphandling.
- Riksarkivets föreskrifter (RA-MS 2014:38) om bevarande i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten hos Försvarsmakten.

3.17. Förstöring

”Förstöring av säkerhetsskyddsklassificerade handlingar och lagringsmedier ska ske så att återskapande av uppgifterna omöjliggörs.”

3 kap. 24 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen gäller såväl allmänna handlingar som handlingar som inte är allmänna. Hur förstöringen sker är upp till Försvarsmakten att avgöra. Förstöring av handlingar i pappersform kan t.ex. göras med dokumentförstörare eller bränning. Det är lämpligt rutiner tas fram för hur förstöring går till och som beskriver vilka metoder som ska användas.

Intill dess att förstöringen är genomförd ska handlingarna och lagringsmedierna förvaras enligt kraven i 5 kap. 12-19 §§ Försvarsmaktens föreskrifter om säkerhetsskydd.

[156] 3 § arkivlagen.

Av bestämmelsen följer att det inte är tillräckligt att förstöring görs så att ett återskapande endast försvåras. Metoder för förstöring måste utgå från de fysiska egenskaper hos det som ska förstöras, så att ett återskapande av uppgifterna efter förstöring inte är möjligt.

3.17.1. Krav på restprodukter

Moment 3:32 *Vid förstöring av en säkerhetsskyddsklassificerad handling i pappersform eller motsvarande material får restprodukten utgöras av spån med en area som är mindre än 18 mm² och en bredd av högst 1,2 mm.*

Observera!
Krav på restprodukternas storlek gäller för alla säkerhetsskyddsklasser.

Vägledande förklaring: Bestämmelsen motsvarar tidigare krav att restprodukter får utgöras av spån med en bredd av högst 1,2 mm och en längd av högst 15 mm. Kravet har formulerats om för att lättare kunna jämföras med standarder. Restprodukter enligt nivå P-7 i standarden DIN-66399 uppfyller kravet i bestämmelsen. Standarden SS-EN 15713:2009 innehåller inte krav på restprodukternas storlek.

Bestämmelsen innebär att förstöring i Försvarsmakten även får ske på ett sätt som ger restprodukter som inte utgörs av spån, t.ex. bränning där restprodukten utgörs av aska. I sådana fall gäller fortfarande att det ska vara omöjligt att återskapa uppgifterna.

3.17.2. Dokumenterad förstöring

”Förstöring av säkerhetsskyddsklassificerade allmänna handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre ska dokumenteras.”

3 kap. 24 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen gäller alla exemplar av en handling. När en handling eller ett lagringsmedium har förstörts upphör behovet att upprätthålla kontrollen över dessa.

Att dokumentera att en handling eller ett lagringsmedium har förstörts är, ur säkerhetsskyddssynpunkt, det sista steget i livscykeln för handlingar och lagringsmedier. I avsnitt 3.8 beskrivs krav på att förstöringen dokumenteras i diarier eller register för uppföljning.

3.17.3. Förstöring av kvalificerat hemliga handlingar

Moment 3:33 *Förstöring av en säkerhetsskyddsklassificerad allmän handling, en tryckt skrift, ett lagringsmedium eller materiel som har placerats i säkerhetsskyddsklassen kvalificerat hemlig ska skriftligen intygas av två, vid förstöringen samtidigt närvarande, personer som är anställda i Försvarsmakten.*

Vägledande förklaring: Omfattningen av säkerhetsskyddsklassificerade allmänna handlingar i pappersform eller motsvarande är normalt liten. Det är ur säkerhetsskyddssynpunkt bättre att handlingarna förstörs vid den expedition som hanterar handlingarna och av expeditionens personal.

3.17.4. Förstöring i krig och stridssituationer

Informationstillgångar kan om de faller i orätta händer orsaka skada för Sverige. I lagen (1992:1402) om undanförsel och förstöring finns bestämmelser som främst ska tillämpas när Sverige är i krig. Bestämmelserna i lagen omfattar även manuella eller informationssystembaserade informationstillgångar.[157] Lagen gäller före arkivlagens bestämmelser om vilka handlingar som får gallras.[158] När planläggning för undanförsel och förstöring genomförs är det nödvändigt att den även omfattar säkerhetsskyddsklassificerade handlingar och lagringsmedier.

I stridssituationer, t.ex. när Försvarsmakten genomför en militär insats, kan situationer förekomma där en militär chef även på förhållandevis låg nivå av taktiska skäl måste besluta att handlingar och lagringsmedier ska förstöras. Någon föreskrift som medger en sådan förstöring finns inte idag. Ett sådant handlande får bedömas i efterhand med utgångspunkt i de allmänna reglerna om nöd i brottsbalken.[159] Det är sannolikt av större vikt att uppgifter som kan hjälpa en motståndare inte röjs till denne.

3.18. Förvaring

Bestämmelser om förvaring av säkerhetsskyddsklassificerade handlingar, säkerhetsskyddsklassificerade tryckta skrifter, säkerhetsskyddsklassificerade lagringsmedier och säkerhetsskyddsklassificerad materiel beskrivs i kapitel 5 om fysisk säkerhet.

3.19. Medförande

”Myndigheten ska besluta i vilken omfattning säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre får medföras från myndighetens lokaler eller områden. Beslutet ska dokumenteras.”

3 kap. 20 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

”Ett sådant medförande får endast göras om det är nödvändigt för verksamheten.”

3 kap. 3 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

[157] Prop. 1992/93:78 s. 1.
[158] 10 § tredje stycket arkivlagen.
[159] Prop. 1992/93:78 s. 6.

Vägledande förklaring: Med medförande avses när en person för sitt arbete behöver transportera och förvara handlingar eller lagringsmedier utanför Försvarsmaktens lokaler eller områden.

Andra staters underrättelsetjänster kan lättare komma över säkerhetsskyddsklassificerade uppgifter utanför Försvarsmaktens lokaler, som normalt är skyddsobjekt med kontrollerat tillträde och bevakning. Utanför lokalerna och områdena ökar sannolikheten även för att de medförda handlingarna och lagringsmedierna av misstag förloras och inte kan återfinnas.

Bestämmelserna syftar till att motverka att anställda tar med sig handlingar och lagringsmedier trots att den anställdes arbetsuppgifter inte motiverar det. Huvudregeln bör vara att handlingar och lagringsmedier inte ska tas med från ordinarie arbetsplats, eftersom skyddet alltid blir sämre utanför Försvarsmaktens lokaler och områden. Verksamheten kan dock ha behov av att medföra handlingar och lagringsmedier.

Att bestämmelserna inte tar upp säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen begränsat hemlig, innebär att sådana handlingar och lagringsmedier får medföras – om inte Försvarsmakten bestämt något annat.

Kravet i bestämmelserna gäller, enligt 3 kap. 3-4 §§ Försvarsmaktens föreskrifter om säkerhetsskydd, även för tryckta skrifter och materiel som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell.

Moment 3:34 *Organisationsenheten ska i en lokal instruktion reglera beslut om medförande av säkerhetsskyddsklassificerade handlingar eller lagringsmedier som har placerats i säkerhetsskyddsklassen konfidentiell eller högre utanför Försvarsmaktens lokaler eller områden. Detsamma gäller för medförande från ett militärt fartyg, luftfartyg eller från ett fordon, som befinner sig utanför Försvarsmaktens lokaler eller områden.*

Instruktionen ska minst beskriva

a) generella beslut om medförande samt,

b) hur beslut fattas när ett generellt beslut saknas.

Vägledande förklaring: En lokal instruktion får utformas för att tillåta medförande av säkerhetsskyddsklassificerade handlingar och lagringsmedier mellan platser där det finns behov av medförande. Instruktionen bör ta hänsyn till för vilket ändamål den säkerhetsskyddsklassificerade handlingen eller lagringsmediet medförs och till vilka platser den handlingen eller lagringsmediet ska medföras. Något beslut att medföra säkerhetsskyddsklassificerade handlingar och lagringsmedier behöver inte fattas för varje handling och lagringsmedium. Instruktionen kan utformas så att beslut om medförande delegeras inom enheten. Instruktionen utformas så att det i efterhand är möjligt att kunna avgöra om ett medförande har varit tillåten.

Exempel
Högkvarteret är i Stockholm grupperat på flera skilda platser, bl.a. på Lidingövägen 24 och Banérgatan 62. Möten genomförs på båda platserna och personalen behöver därför ta med sig säkerhetsskyddsklassificerade handlingar mellan platserna.

Den lokala instruktionen för Högkvarteret (rutinhandboken) får *utformas så att det inte behövs något särskilt tillstånd att medföra säkerhetsskyddsklassificerade handlingar mellan de två platserna.*

Exempel
Vid Karlsborgs fästning finns flera militära verksamheter i olika byggnader inom fästningsområdet. Fästningsområdet är till stora delar öppet för allmänheten. Fästningsområdet är en del av Försvarsmaktens områden. Medförande av säkerhetsskyddsklassificerade handlingar mellan byggnaderna behöver inte regleras i en lokal instruktion.

Om det vid organisationsenheten finns behov att medföra säkerhetsskyddsklassificerade handlingar eller lagringsmedier utanför Sverige måste den lokala instruktionen reglera beslut för sådant medförande. Det finns inte längre något krav på skriftligt samråd med Must för medförande utomlands. Se även moment 3:36.

Ett äldre beslut[160] om medförande av en hemlig handling utanför Försvarsmaktens lokaler eller områden m.m., får fortsätta att gälla.

Moment 3:35 *Om det av något beslut om verksamhetens genomförande följer att en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium ska medföras utanför Försvarsmaktens lokaler eller områden, behövs inte något särskilt beslut om medförande enligt den lokala instruktionen.*

Vägledande förklaring: Detta kan t.ex. vara fråga om att en anställd av sin chef muntligen ges arbetsuppgiften att delta i ett möte vid en annan myndighet där uppgifter som finns i en säkerhetsskyddsklassificerad handling kommer att diskuteras. Den anställde behöver medföra den säkerhetsskyddsklassificerade handlingen för att kunna delta i mötet.

”Säkerhetsskyddsklassificerade handlingar och lagringsmedier som medförs från myndigheten ska vara under kontroll eller förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av handlingarna respektive lagringsmedierna inom myndighetens lokaler.”

3 kap. 20 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

[160] 2 kap. 10 § Försvarsmaktens interna bestämmelser (FIB 2015:2) om säkerhetsskydd och skydd av viss materiel.

Vägledande förklaring: Att säkerhetsskyddsklassificerade handlingar och lagringsmedier ska vara under kontroll betyder att *ingen obehörig kan komma åt de medförda handlingarna eller lagringsmedierna utan att personen som medför dem upptäcker det*. Bestämmelsen gäller oavsett vilken säkerhetsskyddsklass handlingarna eller lagringsmedierna är placerade i.

Exempel på när säkerhetsskyddsklassificerade handlingar eller lagringsmedier *står under kontroll* är:

- Handlingarna eller lagringsmedierna läggs i en väska, portfölj eller liknande som personen bär med sig överallt under hela medförandet.
- Under övernattning på hotell eller i bostad hålls väskan eller portföljen låst. Dessutom låses väskan eller portföljen fast med en vajer i nära anslutning till sängen, så att ett eventuellt tillgrepp under natten försvåras och lättare kan upptäckas. Den person som medför handlingar och lagringsmedier stannar kvar i hotellrummet eller bostaden under hela den tid som väskan eller portföljen är fastlåst med vajern.
- På flygplan tas väskan eller portföljen med som handbagage. Om den läggs i bagagehylla hålls bagagehyllan under uppsikt.

Exempel på när säkerhetsskyddsklassificerade handlingar eller lagringsmedier *inte står under kontroll* är:

- En väska, portfölj eller liknande som innehåller handlingar eller lagringsmedier lämnas obevakad en kortare stund på en restaurang, i en bil, på ett hotellrum eller i bostaden.
- En sådan väska eller portfölj lämnas in för effektförvaring, t.ex. i en förvaringsbox på en järnvägsstation eller bemannad effektförvaring på hotell.
- Under övernattning på hotell hålls väskan eller portföljen låst. Dessutom låses väskan eller portföljen fast med en vajer i nära anslutning till sängen. Personen som medför handlingar och lagringsmedier lämnar hotellrummet under en kortare tid, men låter väskan eller portföljen vara kvar i hotellrummet.
- Handlingar eller lagringsmedier läggs i en resväska som checkas in på en flygplats.
- Handlingar eller lagringsmedier förvaras i ett säkerhetsfack på ett hotellrum.

De exempel som beskrivits är inte uttömmande.

Det är lämpligt att förvara säkerhetsskyddsklassificerade handlingar och lagringsmedier i ett förseglat emballage (kuvert eller säkerhetskuvert). Ett eventuellt försök till intrång i emballaget kan därmed lättare uppmärksammas. Under ett medförande (t.ex. en tjänsteresa) där man kommer att använda handlingar eller lagringsmedier är det lämpligt att ta med sig några tomma säkerhetspåsar som kan användas.

”En säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium som har medförts utanför myndighetens lokaler eller områden ska snarast möjligt återföras eller överlämnas till den som ska förvara handlingen eller lagringsmediet.”

3 kap. 20 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen gäller även för säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen begränsat hemlig.

3.19.1. Medförande utomlands

Moment 3:36 *Innan säkerhetsskyddsklassificerade handlingar och lagringsmedier som har placerats i säkerhetsskyddsklassen konfidentiell eller högre medförs utanför Sverige ska organisationsenheten upprätta en förteckning över handlingarna och lagringsmedierna. I förteckningen ska anges om någon av handlingarna eller lagringsmedierna ska överlämnas utomlands. När det gäller de handlingar som ska återföras till Sverige ska organisationsenheten, när handlingarna har återförts, kontrollera att dessa är desamma som de som enligt förteckningen ska återföras.*

3.19.2. Medförande till bostad

Bestämmelser om medförande av säkerhetsskyddsklassificerade handlingar och lagringsmedier gäller även för medförande till bostad, t.ex. för arbete i hemmet under en pandemi. Bestämmelserna innebär att det inte behövs något särskilt beslut för att få medföra säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklass begränsat hemlig.

För att kunna arbeta med säkerhetsskyddsklassificerade handlingar och lagringsmedier i bostaden måste säkerhetskyddsåtgärder för arbetet finnas i bostaden, t.ex. förvaring (avsnitt 5.3.5).

3.20. Transporter

”En myndighet ska besluta hur transporter av säkerhetsskyddsklassificerade handlingar och lagringsmedier ska genomföras. Beslutet ska dokumenteras.”

3 kap. 26 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Skyddsåtgärderna behöver anpassas efter hur stor mängd handlingar och lagringsmedier som ska transporteras, deras placering i säkerhetsskyddsklass, var transporten går och förhållanden under transporten.

Transporter beskrivs i avsnitt 5.7.

3.20.1. Åtgärder inför transport av handlingar och lagringsmedier

Moment 3:37 *Inför en skyddad transport ska säkerhetsskyddsklassificerade handlingar och lagringsmedier förpackas i emballage som förseglas så att mottagaren kan upptäcka att emballage har öppnats eller ersatts under transporten.*

Vägledande förklaring: Det är ur säkerhetsskyddssynpunkt inte tillräckligt att enbart använda behållare med lås eftersom dessa kan dyrkas. Förseglingen måste vara utformad så att det med blotta ögat går att upptäcka om en försegling har öppnats eller ersatts med en ny försegling (t.ex. numrerad plombering).

Moment 3:38 *Inför en skyddad transport ska åtgärder vidtas så att det finns spårbarhet för vilka säkerhetsskyddsklassificerade handlingar och lagringsmedier som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre som ska transporteras.*

Vägledande förklaring: Syftet med momentet är att det efter en transport ska vara möjligt att avgöra vilka handlingar eller lagringsmedier som ingått i ett emballage som har förlorats, öppnats eller påverkats under transporten.

3.21. Gemensam användning

I Försvarsmakten förekommer verksamheter som innebär att flera personer har ett behov att gemensamt använda säkerhetsskyddsklassificerade handlingar och lagringsmedier. Det är i sådan verksamhet inte möjligt att låta varje person ha ett personligt exemplar och låta personerna kvittera handlingarna eller lagringsmedierna mellan sig. Ett exempel på verksamhet där behov av gemensam användning finns är ledningscentraler samt drift- och underhåll i Försvarsmaktens anläggningar. Ett annat exempel är staber under höjd beredskap.

”Om det finns ett oundgängligt behov att gemensamt använda fysiska säkerhetsskyddsklassificerade handlingar och lagringsmedier som förvaras hos en organisationsenhet, får chefen för organisationsenheten, eller den chefen för organisationsenheten bestämmer, besluta vilka personer som ska ingå i en grupp som gemensamt ska använda handlingarna och lagringsmedierna. Ett beslut om gemensam användning ska dokumenteras.”

3 kap. 4 § första stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Ett beslut om gemensam användning som har fattats med stöd av äldre bestämmelser får fortsätta att gälla.

Moment 3:39 *Den person som med stöd av ett beslut om gemensam användning har kvitterat mottagandet av en handling eller ett lagringsmedium som ska användas gemensamt, ska tillsammans med var och en av dem som ingår i gruppen, svara för att säkerhetsskyddet upprätthålls vid hantering av den säkerhetsskyddsklassificerade handlingen eller lagringsmediet.*

Vägledande förklaring: När en person, som för gruppens räkning har kvitterat mottagandet av en handling eller ett lagringsmedium som ska användas gemensamt, inte längre ingår i gruppen behöver omkvittering inte genomföras.

Moment 3:40 *Om gemensam användning tillämpas ska organisationsenheten ta fram rutiner för gemensam användning. Rutinerna ska minst innehålla:*

a) Vilka befattningar vid enheten som får besluta om inrättande eller avveckling av en grupp, att en person ska ingå, eller inte längre ska ingå, i en grupp samt att en viss säkerhetsskyddsklassificerad handling eller lagringsmedium ska användas gemensamt av en viss grupp.

b) Åtgärder för beslut om inrättande eller avveckling av en grupp för gemensam användning.

c) Åtgärder för beslut att en person ska ingå, eller inte längre ska ingå, i en grupp. Åtgärderna ska säkerställa att det i efterhand går att avgöra vilka personer som har ingått i en grupp och tidpunkter för in- och utträde ur gruppen.

d) Åtgärder för samråd med en annan organisationsenhet eller myndighet om en person som avses ingå i en grupp inte är anställd vid enheten.

e) Åtgärder för beslut att en viss säkerhetsskyddsklassificerad handling eller lagringsmedium ska användas gemensamt av en viss grupp. Åtgärderna ska säkerställa att det i efterhand går att avgöra vilka handlingar och lagringsmedier som kunnat användas av personer i en grupp och tidpunkt för beslut.

f) Åtgärder för hur en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium ska tas emot av en grupp.

g) Åtgärder för förvaring av säkerhetsskyddsklassificerade handlingar och lagringsmedier. Åtgärderna ska säkerställa att endast personer som ingår i en grupp kan komma in i förvaringsutrymmen för handlingar och lagringsmedier som gruppen gemensamt använder. Åtgärderna ska även säkerställa dokumentation över vilka förvaringsutrymmen som en grupp förvarar handlingar och lagringsmedier i.

h) Åtgärder för inventering av säkerhetsskyddsklassificerade handlingar och lagringsmedier som används gemensamt.

i) Åtgärder för hur en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium ska lämnas tillbaka från en grupp.

j) Åtgärder när någon som ingår i en grupp upptäcker:

1) *att en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium saknas, kan ha röjts eller obehörigen har ändrats, samt*

2) *någon annan brist i säkerhetsskyddet för den gemensamma användningen.*

Vägledande förklaring: Gemensam användning tillämpas restriktivt och användas endast om det är *oundgängligen* nödvändigt med hänsyn till verksamheten och personernas *avgränsade* arbetsuppgifter. Gemensam användning får användas för handlingar och lagringsmedier som är placerade i säkerhetsskyddsklass upp till och med kvalificerat hemlig.

Varje person som ingår i en grupp ska vara behörig att ta del av samtliga säkerhetsskyddsklassificerade uppgifter i de handlingar och lagringsmedier som är avsedda för gemensam användning. Personer som ingår i gruppen får utan inbördes kvittenser använda de säkerhetsskyddsklassificerade handlingarna eller lagringsmedierna.

Det är lämpligt att varje grupp ges en beteckning så att olika grupper kan åtskiljas. Det är också lämpligt att det i beslut om gemensam användning framgår för vilket syfte gruppen inrättats.

Det är lämpligt att det av anteckning på den säkerhetsskyddsklassificerade handlingen eller lagringsmediet, t.ex. genom en märkning, framgår att den är avsedd för gemensam användning samt beteckning på gruppen för vilken handlingen är avsedd.

På motsvarande sätt bör det i register, där den säkerhetsskyddsklassificerade handlingen eller lagringsmediet är registrerat, även framgå att handlingen eller lagringsmediet är avsedd för gemensam användning samt beteckning på gruppen för vilken handlingen är avsedd.

Samförvaringsbeslut behövs inte för ett förvaringsutrymme för handlingar och lagringsmedier som används gemensamt. Tillräcklig spårbarhet uppnås genom rutiner i moment 3:40 g.

Bestämmelser om inventering (avsnitt 3.13) av säkerhetsskyddsklassificerade handlingar och lagringsmedier gäller även när handlingar och lagringsmedier används gemensamt.

Personnummer eller FMID kan användas i beslut för vilka personer som ska ingå i en grupp.

3.22. Utlån

Det saknas generella bestämmelser om utlåning av allmänna handlingar. I arkivlagen framgår indirekt att en myndighet får låna ut allmänna handlingar.[161] Arkivhandlingar får lånas ut till andra myndigheter för tjänsteändamål.[162]

Utlåning kan vara lämpligt om den lånande myndigheten har begränsad förmåga att upprätthålla säkerhetsskydd för säkerhetsskyddsklassificerade handlingar. Efter att den lånande myndigheten inte längre har behov av en säkerhetsskyddsklassificerad handling återlämnas den till den utlånande myndigheten.

Moment 3:41 *Om en säkerhetsskyddsklassificerad allmän handling lånas ut till en myndighet eller ett företag ska det i diariet där handlingen är diarieförd anges vem som har lånat handlingen och om handlingen har återlämnats. Uppgifterna får istället för i diariet antecknas i ett register för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.*

Moment 3:42 *Om ett säkerhetsskyddsklassificerat lagringsmedium lånas ut till en myndighet eller ett företag ska det i register över Försvarsmaktens säkerhetsskyddsklassificerade lagringsmedier framgå vem som har lånat mediet och om mediet har återlämnats.*

Vägledande förklaring: Syftet är att lånet ska följas upp så att säkerhetsskyddsklassificerade handlingar och lagringsmedier återlämnas.

Se även avsnitt 3.2.5 om säkerhetsskydd för lånade säkerhetsskyddsklassificerade handlingar hos en inlånande myndighet som omfattas av Försvarsmaktens föreskrifter om säkerhetsskydd.

[161] 12 § andra stycket och 15 § andra stycket arkivlagen.
[162] 7 § arkivförordningen (1991:446).

4. Informationssäkerhet i och kring informationssystem

Observera!
Utöver de bestämmelser som förklaras i kapitlet gäller även Försvarsmaktens interna bestämmelser (FIB 2017:8) om it-säkerhet och Försvarsmaktens interna bestämmelser (FIB 2017:11) om it-verksamhet, som inte beskrivs i kapitlet.

Bestämmelserna i FIB 2017:8 och FIB 2017:11 är framtagna före den nya säkerhetsskyddslagen men gäller om de inte strider mot säkerhetsskyddslagen, säkerhetsskyddsförordningen och Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.

Utöver bestämmelser finns även andra styrdokument såsom it-processen som beskriver Försvarsmaktens arbetssätt om it-tjänster.

4.1. Grunder

”Med informationssystem avses ett system av sammansatt mjuk- och hårdvara som behandlar information.”

1 kap. 5 § säkerhetsskyddsförordningen

Vägledande förklaring: Exempel på informationssystem är en dator eller ett nätverk av datorer med tillhörande operativsystem och applikationsprogramvara. Även t.ex. smarta mobiltelefoner, skrivare och digitala kopiatorer är (eller kan ingå i) informationssystem.

”Vad som anges om informationssystem gäller även för sådana informationssystem som utgörs endast av ett elektroniskt kommunikationsnät.”

4 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

”Informationssäkerhet ska

1. förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och

2. förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.”

2 kap. 2 § säkerhetsskyddslagen

Vägledande förklaring: Första punkten tar sikte på skyddet av säkerhetsskyddsklassificerade uppgifter. Om ett informationssystem ska hantera säkerhetsskyddsklassificerade uppgifter ska informationssystemets säkerhetsfunktioner anpassas för att förebygga att sådana uppgifter inte röjs för obehöriga, ändras, görs otillgängliga eller förstörs. Förekommer uppgifter som har delats in i olika säkerhetsskyddsklasser ska

systemet vara inrättat med säkerhetsfunktioner som svarar upp mot den högsta skyddsnivån.[163]

Andra punkten tar framför allt sikte på skyddsåtgärder för att tillgodose behov av tillgänglighet och riktighet i fråga om uppgifter och informationssystem som inte utgör eller innehåller säkerhetsskyddsklassificerade uppgifter, men som har avgörande betydelse för t.ex. styrning, reglering och övervakning av för Sverige viktiga samhällsfunktioner inom t.ex. el- och vattenförsörjning, digital infrastruktur och sådana sammanställningar av uppgifter, t.ex. folkbokföringsregistret, som är av grundläggande betydelse för ett fungerande samhälle. Med uppgifter och informationssystem avses i detta sammanhang såväl uppgifter som de tekniska system som används för att i olika avseenden elektroniskt behandla uppgifter.[164]

4.2. Åtgärder inför driftsättning

4.2.1. Identifiera säkerhetskrav

”Innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift ska verksamhetsutövaren genom en särskild säkerhetsskyddsbedömning ta ställning till vilka säkerhetskrav i systemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Säkerhetsskyddsbedömningen ska dokumenteras.”

3 kap. 1 § säkerhetsskyddsförordningen

Vägledande förklaring: *Särskild säkerhetsskyddsbedömning* (SSB) är det begrepp som ersätter begreppet *säkerhetsmålsättning* som tidigare har använts i Försvarsmakten.

”Den särskilda säkerhetsskyddsbedömningen ska utgå från verksamhetens säkerhetsskyddsanalys och omfatta vilka hot och sårbarheter som finns i och kring systemet samt en beskrivning av den säkerhetskänsliga verksamhet som systemet ska stödja.

Myndigheten ska i den särskilda säkerhetsskyddsbedömningen, utöver krav på skydd mot röjande av de säkerhetsskyddsklassificerade uppgifter som kommer att hanteras i informationssystemet, också ta ställning till den säkerhetskänsliga verksamhetens krav på tillgänglighet till informationssystemet, och de uppgifter som behandlas i det, och verksamhetens krav på riktighet för dessa uppgifter.”

4 kap. 5 § första och andra styckena Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen gäller alla informationssystem som har betydelse för säkerhetskänslig verksamhet, även om de inte hanterar säkerhetsskydds-

[163] Prop. 2017/18:89 s. 138.
[164] Prop. 2017/18:89 s. 138.

klassificerade uppgifter. Detta betyder att man måste ta ställning till den säkerhetskänsliga verksamhetens behov av tillgång till systemet och av riktigheten för uppgifter i det för att avgöra om systemet omfattas av bestämmelsen. Sådana system som är avsedda att hantera säkerhetsskyddsklassificerade uppgifter har alltid betydelse för säkerhetskänslig verksamhet och omfattas alltså alltid av bestämmelsen.

Källor till krav på skydd mot röjande, krav på tillgänglighet och riktighet kan finnas i andra författningar. Ett exempel är att bestämmelsen i 8 kap. 3 § OSL (avsnitt 3.3.3) om sekretess för en utländsk myndighet måste identifieras som krav för ett informationssystem som utländsk personal ska använda. Bestämmelsen kan innebära att det behöver finnas administrativa och tekniska skyddsåtgärder som säkerställer att Försvarsmakten följer 8 kap. 3 § OSL. Ett annat exempel är att det i 17 § Försvarsmaktens interna bestämmelser om it-verksamhet finns bestämmelser om kontinuitetsplanering.

Försvarsmakten har genom krav på godkända säkerhetsfunktioner (KSF) tagit fram grundkrav för informationssystem. De grundkrav som gäller för ett visst informationssystem kan refereras till i den särskilda säkerhetsskyddsbedömningen för systemet. Krav som tillkommer för det specifika informationssystemet dokumenteras i SSB för systemet. I KSF ställs krav på att det ska finnas en *it-säkerhetsspecifikation* (ITSS) som används för ytterligare kravdefiniering samt under utveckling, evaluering och ackreditering av ett informationssystem.

Även fristående datorer som endast används av en användare, och som inte har någon koppling till omvärlden genom t.ex. USB eller CD/DVD, omfattas av föreskriften. Sådana datorer kan anses ingå i ett system av myndighetens alla fristående datorer av samma typ och en särskild säkerhetsskyddsbedömning behöver alltså inte göras för varje dator för sig.

4.2.2. Förbereda drift, förvaltning, underhåll, övervakning och incidenthantering

> *”En myndighet som avser att använda ett informationssystem i säkerhetskänslig verksamhet ska besluta vilka rutiner, resurser och kompetenser för drift, förvaltning, underhåll, övervakning och hantering av incidenter som är nödvändiga ur säkerhetsskyddssynpunkt under hela systemets livscykel. Beslutet ska dokumenteras.”*
>
> 4 kap. 10 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Försvarsmakten ska känna till vilka resurser som krävs för drift och förvaltning av systemet så att dessa kan säkerställas. Om tillräckliga resurser inte finns kan säkerheten i ett informationssystem inte upprätthållas över tid och driftsättning av ett informationssystem kan då behöva skjutas upp till dess att tillräckliga resurser kan säkerställas.

4.2.3. Granskning av skyddsåtgärder

> *”Myndigheten ska granska och godkänna att skyddsåtgärderna i och kring informationssystemet uppfyller de säkerhetskrav som har identifierats i den särskilda säkerhetsskyddsbedömningen och att åtgärderna som beskrivs i 15–27 §§ har implementerats och ger avsedd förmåga. I granskningen ska systemets säkerhetsförmåga testas. Granskningen och godkännandet ska dokumenteras.”*
>
> 4 kap. 6 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: I Försvarsmakten är godkännandet en del av ackrediteringen av ett informationssystem (avsnitt 4.2.5).

> *”Säkerhetsskyddschefen ska i enlighet med 4 kap. 6 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd granska att skyddsåtgärderna i och kring ett informationssystem uppfyller de säkerhetskrav som har identifierats i den särskilda säkerhetsskyddsbedömningen för systemet, och att åtgärderna som beskrivs i 4 kap. 15–27 §§ samma författning har implementerats och ger avsedd förmåga.”*
>
> 11 kap. 22 § FM ArbO

Vägledande förklaring: I Must interna styrdokument har bemyndigandet att besluta om granskningen delegerats till chefen för säkerhetskontoret vid Must. Genom den dokumenterade granskningen uppnås förtroende (assurans) till att ett informationssystem uppfyller specificerade säkerhetskrav.

De skyddsåtgärder som beskrivs i 4 kap. 15–27 §§ Försvarsmaktens föreskrifter om säkerhetsskydd är inte uttömmande men beskriver en uppsättning åtgärder som normalt täcker de flesta behov. Resultatet av den särskilda säkerhetsskyddsbedömningen (SSB) kan vara att ytterligare åtgärder bedöms vara nödvändiga, t.ex. åtgärder för fysisk säkerhet och personalsäkerhet.

Skyddsåtgärder innehåller ofta tekniska säkerhetsfunktioner i informationssystemen men kan också vara administrativa eller organisatoriska, särskilt i kombination med fysisk säkerhet och begränsat tillträde till de platser där informationssystemet finns.

Om det finns generella krav på åtgärderna som beskrivs i 4 kap. 15–27 §§ Försvarsmaktens föreskrifter om säkerhetsskydd genomförs granskningen, inklusive testning, mot de generella kraven. I Försvarsmakten har chefen för Must beslutat KSF som är grundkrav för informationssystem i Försvarsmakten. KSF innehåller f.n. dock inte alla krav för de skyddsåtgärder som anges i 4 kap. 15–27 §§ Försvarsmaktens föreskrifter om säkerhetsskydd.

Granskning består av tester av tekniska åtgärder samt undersökning av administrativa och organisatoriska åtgärder. Granskning syftar till att:

- Bekräfta att säkerhetskraven är uppfyllda.
- Informationssystemets säkerhetsförmågor är korrekt implementerade.
- Informationssystemets säkerhetsförmågor inte kan kringgås eller manipuleras.
- Informationssystemets säkerhetsförmågor fungerar som det är tänkt.
- Informationssystemets säkerhetsförmågor inte har dolda funktioner som kan utföra icke önskvärda åtgärder.

Kravet på att granskningen ska dokumenteras innebär att:

- Genomförandet av tester och resultat av genomförda tester ska dokumenteras.
- Genomförandet av undersökningar av administrativa och organisatoriska åtgärder och resultat av undersökningarna ska dokumenteras.

Dokumentation från testerna och undersökningarna är en del av underlaget för granskning och det godkännande från säkerhetsskyddssynpunkt (ackreditering) som ska göras enligt 3 kap. 3 § säkerhetsskyddsförordningen. Det är inte möjligt att godkänna ett informationssystem från säkerhetsskyddssynpunkt, förrän det finns dokumentation från granskningen som visar att:

- säkerhetskrav som har identifierats i SSB är uppfyllda och
- åtgärderna som beskrivs i 4 kap. 15–27 §§ Försvarsmaktens föreskrifter om säkerhetsskydd har implementerats och ger avsedd förmåga.

Med test avses främst provning av ett informationssystem och dess tekniska skyddsåtgärder. Det är alltså inte tillräckligt med enbart en granskning av dokumentation som beskriver informationssystemet.

”De personer som ansvarar för utvecklingen av systemet får inte ansvara för granskningen och godkännandet av skyddsåtgärderna.”

4 kap. 6 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Syftet med bestämmelsen är att säkerställa ett visst oberoende mellan utvecklare och granskare. Att låta den som utvecklat en skyddsåtgärd också granska den innebär en stor risk för att sårbarheter förbises.

”Myndigheten ska genom granskning eller på annat sätt förvissa sig så långt möjligt om att hård- och mjukvara som ska användas i informationssystem som har betydelse för säkerhetskänslig verksamhet bedöms vara tillförlitlig ur säkerhetsskyddsynpunkt.”

4 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Det är inte möjligt att helt förvissa sig om att en hård- eller mjukvara är tillförlitlig. Det är däremot viktigt att göra en helhetsbedömning av om tillförlitligheten är tillräcklig för att man ska kunna använda hård- eller mjukvaran i ett informationssystem som är av betydelse för säkerhetskänslig verksamhet.

För att få förtroende för en leverantör måste leverantören ha en utvecklings-, test- och tillverkningsprocess med en dokumenterad livscykelmodell för utveckling, integration och testning som omhändertar säkerhetsaspekter. Det kan även vara nödvändigt att granska om livscykelmodellen är ändamålsenlig och om leverantören följer den.

Försvarsmakten har en strategi för säker leverantörskedja (secure supply chain).[165]

4.2.4. Begäran om samråd

”Innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren skriftligen samråda med Säkerhetspolisen. Om verksamhetsutövaren hör till Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1, ska denne i stället samråda med Försvarsmakten.

Samrådsskyldigheten gäller även i fråga om andra informationssystem än sådana som anges i första stycket, om obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig.”

3 kap. 2 § säkerhetsskyddsförordningen

Vägledande förklaring: Eftersom det av 7 kap. 1 § första stycket 1 säkerhetsskyddsförordningen följer att Försvarsmakten utövar tillsyn av Försvarsmaktens säkerhetsskydd, ska samråd enligt 3 kap. 2 § säkerhetsskyddsförordningen även tas för Försvarsmaktens informationssystem. I Försvarsmakten uppnås samråd normalt genom det yttrande som Must lämnar enligt 13 kap. 4 § Försvarsmaktens interna bestämmelser om it-säkerhet.

”En begäran om samråd enligt 3 kap. 2 § säkerhetsskyddsförordningen (2018:658) ska ställas till Försvarsmaktens högkvarter. De uppgifter som Försvarsmakten efterfrågar ska tillhandahållas av den begärande myndigheten.”

4 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Försvarsmakten kan bl.a. efterfråga den särskilda säkerhetsskyddsbedömningen, dokumentation som beskriver hur skyddsåtgärderna i och kring informationssystemet uppfyller ställda säkerhetskrav och den dokumenterade granskning som ska finnas enligt 4 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd.

[165] FM2015-10969:29.

”Chefen för militära underrättelse- och säkerhetstjänsten bemyndigas att lämna Försvarsmaktens samråd enligt 3 kap. 2 § säkerhetsskyddsförordningen vid andra myndigheters driftsättande av informationssystem.”

11 kap. 18 § 3 FM ArbO

Vägledande förklaring: Vid Must är det säkerhetsskyddsavdelningen som bereder ärenden om samråd.

4.2.5. Godkännande från säkerhetsskyddssynpunkt (ackreditering)

”Ett informationssystem som ska användas i säkerhetskänslig verksamhet får inte tas i drift förrän det har godkänts från säkerhetsskyddssynpunkt av verksamhetsutövaren. Godkännandet ska dokumenteras.”

3 kap. 3 § säkerhetsskyddsförordningen

”Av 13 kap. 1 och 3 §§ Försvarsmaktens interna bestämmelser (FIB 2017:8) om it-säkerhet framgår att FM CIO, eller den han eller hon bestämmer, beslutar om central ackreditering av it-system.”

8 kap. 38 § FM ArbO

Vägledande förklaring: Bestämmelsen är en upplysning om vad som står i Försvarsmaktens interna bestämmelser om it-säkerhet.

”Ett informationssystem får inte godkännas från säkerhetssynpunkt (ackrediteras) innan åtgärderna enligt 6 § har godkänts.”

4 kap. 8 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: I avsnitt 4.2.3 beskrivs granskning av skyddsåtgärderna som 6 § i bestämmelsen hänvisar till. Åtgärderna avser:

- skyddsåtgärderna i och kring ett informationssystem som har identifierats i den särskilda säkerhetsskyddsbedömningen för informationssystemet, samt
- skyddsåtgärderna som beskrivs i 4 kap. 15–27 §§ Försvarsmaktens föreskrifter om säkerhetsskydd.

Det är Försvarsmaktens säkerhetsskyddschef som har uppgiften att genomföra granskningen.[166]

[166] 11 kap. 22 § FM ArbO.

”Innan ett it-system som är avsett för behandling av hemliga uppgifter får ackrediteras centralt, ska militära underrättelse- och säkerhetstjänsten i Högkvarteret yttra sig i fråga om säkerheten i systemet.”

11 kap. 4 § första stycket Försvarsmaktens interna bestämmelser om it-säkerhet

Vägledande förklaring: Yttrandet avser den granskning som anges i 4 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd och som beskrivs i avsnitt 4.2.3.

4.3. Förvaltning och underhåll

”Myndigheten ska fortlöpande förvalta och underhålla de informationssystem som har betydelse för säkerhetskänslig verksamhet så att säkerhetsskyddet i och kring systemen kan upprätthållas.”

4 kap. 10 § andra stycket Försvarsmaktens föreskrifter o säkerhetsskydd

4.4. Dokumentation

”Myndigheten ska dokumentera de informationssystem som har betydelse för säkerhetskänslig verksamhet. System som är av särskild betydelse vid höjd beredskap ska dokumenteras särskilt.”

4 kap. 11 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med särskild betydelse vid höjd beredskap avses det som är mer kritiskt för verksamheten i det läget. Syftet med att belysa just detta är att ge underlag för att dimensionera säkerhetsskyddet för dessa system efter de förutsättningar som råder vid höjd beredskap.

”Dokumentationen ska beskriva systemets hård- och mjukvara, systemets kommunikation och beroenden, informationsflöden och datautbyten samt de skyddsåtgärder som avser systemet och vad som i övrigt är av betydelse för att kunna upprätthålla säkerheten i och kring systemet.”

4 kap. 11 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: För att ett informationssystems säkerhetsskydd ska kunna upprätthållas under systemets livslängd är det nödvändigt att kontinuerligt hålla dokumentation över systemet och säkerhetsåtgärderna uppdaterad. För att kontrollera att säkerhetsskyddet är tillräckligt kan det finnas behov av att genomföra nya hot- och sårbarhetsanalyser för systemet.

4.5. Hantering av säkerhetsskyddsklassificerade lagringsmedier

”Ett säkerhetsskyddsklassificerat lagringsmedium får endast hanteras i ett informationssystem som uppfyller de krav som gäller för hantering av uppgifter i den högsta säkerhetsskyddsklass som någon av uppgifterna på lagringsmediet har placerats i eller kan komma att placeras i.”

4 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Ett lagringsmedium som t.ex. är avsett att innehålla eller som innehåller sådana säkerhetsskyddsklassificerade uppgifter som har placerats i säkerhetsskyddsklassen hemlig får inte hanteras i ett informationssystem som är avsett för behandling av uppgifter som är placerade i en lägre säkerhetsskyddsklass (konfidentiell eller begränsat hemlig). Ett informationssystem som är avsett för behandling av sådana uppgifter har inte ett tillräckligt säkerhetsskydd för att kunna hantera uppgifter som är placerade i säkerhetsskyddsklassen hemlig.

”Ett säkerhetsskyddsklassificerat lagringsmedium som innehåller eller har innehållit säkerhetsskyddsklassificerade uppgifter på nivån hemlig eller kvalificerat hemlig får inte återanvändas i ett informationssystem som är avsett för behandling av säkerhetsskyddsklassificerade uppgifter som är placerade i en lägre säkerhetsskyddsklass.”

4 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Ett lagringsmedium som tidigare använts för uppgifter i en viss säkerhetsskyddsklass får inte användas i system som inte är avsedda för denna nivå, även om de aktuella uppgifterna har tagits bort. Borttagning av data från ett lagringsmedium lämnar ofta spår som gör det möjligt att återskapa uppgifterna.

”Ett säkerhetsskyddsklassificerat lagringsmedium som innehåller säkerhetsskyddsklassificerade uppgifter på nivån begränsat hemlig eller konfidentiell får återanvändas i ett informationssystem om myndigheten har rutiner för att säkerställa att inga säkerhetsskyddsklassificerade uppgifter längre kan utläsas ur lagringsmediet.”

4 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Lagringsmediet får även återanvändas i sådana informationssystem som inte är avsedda för behandling av säkerhetsskyddsklassificerade uppgifter under förutsättning att åtgärder har vidtagits för att säkerställa att inga säkerhetsskyddsklassificerade uppgifter kan utläsas ur lagringsmediet.

4.6. Övervakning

”Myndigheten ska kontinuerligt övervaka de informationssystem som är anslutna till ett elektroniskt kommunikationsnät, och som har betydelse för säkerhetskänslig verksamhet, för att kunna upptäcka, analysera och bedöma förändringar och händelser som kan indikera skadlig eller obehörig påverkan, åtkomst eller nyttjande, eller försök till detta, eller obehörig dataöverföring till eller från systemet.”

4 kap. 12 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Övervakningen är en del i incidenthanteringen som krävs enligt 1 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd; det som upptäcks genom övervakningen ska tas om hand med de rutiner som Försvarsmakten har dokumenterat.

Med kontinuerlig övervakning avses inte att alla system ska vara konstant övervakade under dygnets alla timmar. I den särskilda säkerhetsskyddsbedömningen bör det analyseras hur den kontinuerliga bevakningen av det aktuella informationssystemet ska göras, mot bakgrund av den säkerhetskänsliga verksamhet som informationssystemet finns i eller vilken säkerhetsskyddsklass uppgifterna som behandlas i systemet är placerade i.

Syftet med att undanta system som inte är anslutna till elektroniska kommunikationsnät är att inte kräva kontinuerlig övervakning av system som inte är kontinuerligt uppkopplade eftersom det antagligen inte är praktiskt genomförbart. Sådana system bör istället regelbundet kontrolleras på annat sätt.

4.7. Åtgärder vid förändringar i och kring informationssystem

”De skyddsåtgärder i och kring ett informationssystem som ska användas i säkerhetskänslig verksamhet ska fortlöpande anpassas för att möta förändringar i hot och ny kunskap om sårbarheter. Vid behov ska den särskilda säkerhetsskyddsbedömningen och dokumentationen av informationssystemet uppdateras.”

4 kap. 13 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Om ny kunskap om hot eller sårbarheter pekar på att säkerhetsskyddet måste anpassas så ska detta göras. Mindre ändringar, som t.ex. säkerhetsuppdateringar av programvara som kan göras utan någon påtaglig risk för att skyddet försämras kan normalt göras utan att uppdatera den särskilda säkerhetsskyddsbedömningen. Systemets dokumentation ska dock uppdateras så att den är aktuell och korrekt.

”Ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska godkännas ur säkerhetsskyddssynpunkt på nytt om det sker förändringar i eller kring systemet som negativt kan påverka säkerheten i systemet. Ett sådant godkännande ska föregås av uppdatering av den särskilda säkerhetsskyddsbedömningen och granskning enligt 5–6 §§.”

4 kap. 14 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Vid större förändringar finns alltid en risk att skyddet oavsiktligt nedsätts, varför en granskning av förändringen är viktig. En uppdatering av den särskilda säkerhetsskyddsbedömningen behöver inte betyda att analysen görs om från grunden, utan kan utgå från den förändring som skett och ta ställning till hur denna påverkar bedömningen.

4.8. Säkerhetsförmågor

4.8.1. Säkerhetskrav för informationssystem som används i säkerhetskänslig verksamhet

”En verksamhetsutövare som ansvarar för ett informationssystem som ska användas i säkerhetskänslig verksamhet ska vidta lämpliga skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av informationssystemet. Verksamhetsutövaren ska också se till att spårbarhet finns för händelser som är av betydelse för säkerheten i systemet.”

3 kap. 4 § första stycket säkerhetsskyddsförordningen

”Försvarsmaktens säkerhetsskyddschef beslutar de krav på skyddsåtgärder i och kring informationssystem som krävs för användning av system i Försvarsmakten.”

11 kap. 24 § 5 FM ArbO

4.8.2. Autentisering och behörighetskontroll

”För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att verifieraanvändares identitet och behörighet innan dessa ges tillgång till systemet, samt styra åtkomst till uppgifter, funktioner och resurser i systemet enbart till de användare som har tilldelats behörighet till dessa.

Vad som gäller för användare i första stycket gäller också för informationssystem och processer i informationssystem som ges tillgång till uppgifter, funktioner och resurser.”

4 kap. 15 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Åtgärderna är främst riktade mot hot från ”insidan”, dvs. från personer som har tillgång till informationssystemet eller de utrymmen där systemet används. Åtkomststyrningen är inte begränsad till vem som får använda systemet utan behörighet ska kontrolleras även för funktioner och åtkomst till uppgifter i systemet (utom i de fall alla användare av systemet faktiskt är behöriga till alla uppgifter och funktioner).

Olika delar av ett informationssystem ska inte fritt kunna utbyta information utan att försäkra sig om att de kommunicerar med rätt motpart och att denna har rätt till den efterfrågade tjänsten eller informationen. Detta kan t.ex. gälla schemalagda körningar för att flytta data eller utföra andra transaktioner mellan olika system eller delsystem. När åtgärder utförs mellan delsystem för en användares räkning, t.ex. en databasoperation, bör detta i första hand utföras med användarens identitet och behörigheter för att säkerställa rätt behörighet.

”Tilldelning av identiteter och behörigheter i informationssystem som ska användas i säkerhetskänslig verksamhet ska vara möjlig att granska för att avgöra vilka användare eller resurser som har tillgång till systemet och vilka behörigheter som de har tilldelats i systemet. Myndigheten ska regelbundet granska behörigheterna för att se till att de är ändamålsenliga och aktuella.”

4 kap. 16 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Behörigheter som oavsiktligt behålls när personal slutar eller byter befattning medför lätt att användare har större rättigheter i informationssystemet än nödvändigt. Detta innebär en ökad risk både vid insiderangrepp och om en extern angripare på något sätt kan agera med en annan användares behörighet i systemet. För att kunna göra kontroller av att behörighetstilldelningen är ändamålsenlig behöver både beslut om tilldelade behörigheter och faktiska behörigheter i systemet kunna granskas.

4.8.3. Säkerhetsloggning

”För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att registrera händelser i eller kring systemet som är av betydelse för säkerheten i säkerhetsloggar. En analys av säkerhetsloggar ska genomföras regelbundet för informationssystem som är avsedd att användas av flera personer. Analysen ska dokumenteras.”

4 kap. 17 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Säkerhetsloggning är manuell eller automatisk registrering, eller både och, av händelser som är av betydelse för säkerheten i eller kring ett informationssystem.

Vad som utgör händelser som har betydelse för säkerheten behöver analyseras för varje informationssystem. Det kan t.ex. röra sig om in- och utloggningar, förändringar av behörighetsinställningar och åtkomst, överföring av information, uttag eller utskrifter av känsliga uppgifter.

Bestämmelsen omfattar endast säkerhetsloggar vilket innebär att Försvarsmakten kan avgöra vilken annan loggning utöver säkerhetsloggning som är av intresse för verksamheten, men som inte har med säkerheten att göra. Det är lämpligt att försöka separera sådana loggar från säkerhetsloggar men det kan förekomma att samma logg innehåller poster som hänför sig till säkerhetshändelser och poster som främst är av intresse ur ett driftsperspektiv.

Säkerhetsloggarna ska kunna användas både för att indikera intrång eller annan otillåten påverkan och för att utreda sådana händelser.

”Säkerhetsloggar och säkerhetskopior av dessa ska skyddas så att de finns tillgängliga när de behövs, att deras riktighet bevaras och att obehörig åtkomst försvåras.”

4 kap. 18 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med skydd avses även fysiska skyddsåtgärder.

4.8.4. Intrångsskydd och intrångsdetektering

”För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att detektera och avvärja intrång, försök till intrång eller skadlig inverkan på systemet samt detektera och avvärja obehörig kommunikation med systemet.”

4 kap. 19 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Intrångsskydd är administrativa eller tekniska åtgärder, eller både och, som vidtas för att skydda informationssystem mot obehörig åtkomst från ett elektroniskt kommunikationsnät.

Intrångsdetektering är administrativa eller tekniska åtgärder, eller både och, som vidtas för att detektera intrång, eller försök till intrång eller förberedelse till intrång.

”Myndigheten ska se till att informationssystem som har betydelse för säkerhetskänslig verksamhet separeras från övriga informationssystem som inte omfattas av krav på säkerhetsskydd.”

4 kap. 20 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Separationen mellan informationssystem kan vara antingen fysisk eller logisk. Med fysisk separation menas att informationssystemen använder helt olika fysiska infrastrukturer, dvs. olika datorer, servrar, lagringskomponenter, nätverkskomponenter och kablar. Fysisk separation gör det relativt lätt att genom inspektion säkerställa att separationen finns och ger normalt en hög assurans för att separationen upprätthålls. Med logisk separation menas att separationen upprätthålls genom tekniska åtgärder i informationssystemen, t.ex. regler i brandväggar eller nätverksprodukter, eller genom kryptering med olika nycklar. Med logisk separation finns alltid en risk för sårbarheter i de tekniska funktionerna eller misstag vid konfigurationen som gör att separationen inte upprätthålls. Sådana sårbarheter kan vara mycket svåra att upptäcka.

4.8.5. Skydd mot skadlig kod

”För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att försvåra och upptäcka inmatning, försök till inmatning, exekvering eller försök till exekvering av skadlig kod eller annan obehörig kod i systemet.”

4 kap. 21 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Syftet med åtgärden är att förhindra att skadlig kod används för att obehörigen påverka informationssystemet. Eftersom det inte går att säkert avgöra vad syftet med en kod som förs in i systemet är måste åtgärden omfatta all obehörig kod, dvs. all kod som inte beslutats ska användas i systemet. Åtgärderna ska också ta sikte både på att koden förs in i systemet och att koden faktiskt exekveras – detta utgör ett försvar på djupet för att förhindra angrepp om skadlig kod trots åtgärderna ändå kommit in i systemet.

En skyddsåtgärd som skyddar mot skadlig kod behöver inte nödvändigtvis vara ett datorprogram. Skydd kan även åstadkommas på annat sätt. Konfigurationsstyrning samt styrning av vilka processer eller program som tillåts exekveras i en dator kan vara ett sätt att skydda sig mot skadlig kod.

4.8.6. Bevarande av riktighet

”För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att upptäcka och försvåra obehörig förändring (bevarande av riktighet) av informationssystemet och dess säkerhetsskydd.”

4 kap. 22 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Skyddsåtgärder för bevarande av riktighet består ofta av kontroll av checksummor eller digitala signaturer men även behörighetskontroll kan användas som en del i skyddet. Alla program och data i ett informationssystem kan inte skyddas på samma sätt eller till samma nivå så vilka skyddsåtgärder som ska vidtas måste framgå av den särskilda säkerhetsskyddsbedömningen.

4.8.7. Säkerhetskopiering

”För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att säkerhetskopiera och vid behov återställa mjukvara, konfigurationsdata och andra uppgifter som är av betydelse för verksamheten, informationssystemets funktion eller säkerhetsskyddet, och som inte lätt kan återskapas på annat sätt.

Kontroll av att säkerhetskopior kan återläsas ska genomföras regelbundet.”

4 kap. 23 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Data som inte behöver säkerhetskopieras kan t.ex. vara sådant som kan hämtas från en masterdatakälla i ett annat system eller sådant som uppdateras kontinuerligt från en extern sensor och där historiken inte behöver sparas. Programvara som lätt kan installeras om från installationsmedia behöver naturligtvis inte heller säkerhetskopieras, däremot kan konfigurationsdata som förändras över tiden behöva säkerhetskopieras.

Hur ofta säkerhetskopiering görs och hur länge kopiorna sparas måste bedömas för varje informationssystem utifrån verksamhetens krav på tillgänglighet. Sådana krav bör framgå av den särskilda säkerhetsbedömningen.

”Säkerhetskopior ska förvaras åtskilt från informationssystemet och skyddas så att de finns tillgängliga när de behövs, att deras riktighet bevaras och att obehörig åtkomst till säkerhetskopiorna försvåras.”

4 kap. 24 § Försvarsmaktens föreskrifter om säkerhetsskydd

4.8.8. Skydd mot röjande signaler

> *”En verksamhetsutövare som ansvarar för ett informationssystem enligt första stycket ska beakta risken för röjande signaler och vidta lämpliga skyddsåtgärder för systemet om*
>
> *1. informationssystemet avses behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller*
>
> *2. obehörig åtkomst till informationssystemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig.”*
>
> 3 kap. 4 § andra stycket säkerhetsskyddsförordningen

> *”I 3 kap. 4 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om skyddsåtgärder mot röjande signaler. En myndighet ska besluta om säkerhetskrav för skydd mot röjande signaler (RÖS). Beslutet ska dokumenteras.”*
>
> 4 kap. 25 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Röjande signaler (RÖS) är icke önskvärda elektromagnetiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs.

Skydd mot röjande signaler kan uppnås genom att främst använda RÖS-inmätt utrustning i kombination med avstånd mellan verksamhetsutövarens prerimeterskydd till byggnad/lokal som verksamhetsutövaren inte har kontroll över. RÖS-inmätt utrustning är sådan utrustning som har kända egenskaper avseende på hur långt de röjande signalerna strålar.

Utöver avståndet mellan utrustning och eventuell avlyssnare tas hänsyn till hur mycket de röjande signalerna dämpas av den egna byggnadens byggnadsmaterial. Armerad betong dämpar t.ex. mycket mer än fönsterglas. Generellt är det bra att eftersträva att placera denna typ av utrustning så centralt som möjligt i byggnaden och, om möjligt, gärna under mark. För en mer exakt bedömning av en byggnads dämpande egenskaper kan en dämpningsmätning utföras.

I vissa fall behöver tekniska system separeras från varandra för att inte röjande signalerna ska kunna sändas ut externt genom öppna system som exempelvis en radiosändare.

Skydd mot röjande signaler kan även uppnås genom att använda ett så kallat RÖS-skyddat utrymme. Ett sådant utrymme omges av ett sammanhängande metallhölje, genomföringar och ledningar, vilket förhindrar att röjande signaler kommer ut. RÖS-skyddade utrymmen (RÖS-kabinetter) kan också upprättas i mindre skala för utrustning.

4.8.9. Skydd mot obehörig avlyssning

> *”Innan säkerhetsskyddsklassificerade uppgifter behandlas i ett informationssystem utanför verksamhetsutövarens kontroll ska denne försäkra sig om att säkerhetsskyddet för uppgifterna i systemet är tillräckligt.*
>
> *Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll ska uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.”*
>
> 3 kap. 5 § säkerhetsskyddsförordningen

Vägledande förklaring: Med *utanför verksamhetsutövarens kontroll* avses att verksamhetsutövaren:

- inte har fysisk kontroll över den elektroniska kommunikationens medium (normalt kabel eller radio) eller
- inte har fysisk eller logisk kontroll över kommunikationsutrustning.

Avsaknaden av fysisk kontroll gör det möjligt för en antagonist att komma åt mediet eller kommunikationsutrustningen (lägga sin hand på kabel eller utrustning samt ta emot radiosignaler) i syfte att avlyssna de säkerhetsskyddsklassificerade uppgifter som kommuniceras i mediet eller genom utrustningen. Kommunikation med radio är normalt alltid utanför verksamhetsutövarens kontroll eftersom radiosignalernas utbredning i praktiken möjliggör avlyssning. Kommunikation med kablar är utanför verksamhetsutövarens kontroll om verksamhetsutövaren inte fysiskt kan skydda kabeln i hela dess längd.

Avsaknaden av logisk kontroll gör det möjligt för en antagonist att påverka (datorintrång för att ändra konfiguration eller funktion) utrustningen i syfte att avlyssna de säkerhetsskyddsklassificerade uppgifter som kommuniceras genom utrustningen.

Enligt bestämmelsen ska därför uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten. Ett sådant skydd kan endast uppnås med signalskyddstjänst. Signalskyddstjänst regleras i bl.a. Försvarsmaktens föreskrifter om signalskyddstjänsten.

Bestämmelsen är tillämplig på informationssystem för kommunicering av alla former av information, t.ex. tal (telefoni över kabel eller radio), textmeddelanden, bilder, filöverföring, sensordata, styrinformation för maskiner som data. Bestämmelsen är tillämplig såväl när säkerhetsskyddsklassificerade uppgifter kommuniceras till ett annat informationssystem, som när sådana uppgifter kommuniceras till en annan del av samma informationssystem.

Att uppgifterna skyddas med kryptografiska funktioner kan t.ex. innebära att enskilda meddelanden krypteras innan de kommuniceras eller att alla uppgifter som kommuniceras är krypterade.

Bestämmelser om signalskydd finns i Försvarsmaktens föreskrifter (FFS 2019:9) om signalskyddstjänsten och Försvarsmaktens interna bestämmelser (FIB 2008:3) om signalskyddstjänsten.

”I 3 kap. 5 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om när säkerhetsskyddsklassificerade uppgifter ska skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att försvåra att uppgifter kommer obehöriga till del, ändras eller förstörs vid kommunikation mellan informationssystemets delsystem eller vid kommunikation till andra informationssystem.”

4 kap. 26 § Försvarsmaktens föreskrifter om säkerhetsskydd

4.8.9.1 Undantag från krav på godkända kryptografiska funktioner

”Försvarsmakten får om det finns särskilda skäl också besluta om undantag från kraven i 5 § andra stycket. Försvarsmakten ska samråda med Säkerhetspolisen innan ett beslut om undantag meddelas om det gäller verksamhet som hör till Säkerhetspolisens tillsynsområde och med Regeringskansliet (Utrikesdepartementet) om kravet följer av ett internationellt säkerhetsskyddsåtagande.”

3 kap. 6 § andra stycket säkerhetsskyddsförordningen

”Chefen för militära underrättelse- och säkerhetstjänsten leder beredningen av ärenden om undantag enligt 3 kap. 6 § säkerhetskyddsförordningen (2018:658).”

11 kap. 5 § första stycket FM ArbO

”Chefen för militära underrättelse- och säkerhetstjänsten beslutar i ärenden om undantag enligt 3 kap. 6 § andra stycket säkerhetsskyddsförordningen.”

11 kap. 12 § 11 FM ArbO

Vägledande förklaring: Ärenden om undantag från krav på godkända kryptografiska funktioner bereds av säkerhetskontoret vid Must tillsammans med juridiska avdelningen vid ledningsstaben i Högkvarteret. Samverkan med Must innan en hemställan skickas in rekommenderas.

Moment 1:4 i avsnitt 1.10.1 innehåller krav på vad som ska anges i en begäran om undantag enligt 3 kap. 6 § säkerhetskyddsförordningen.

4.8.10. Säkerhetskonfiguration

”Ett informationssystem som ska användas i säkerhetskänslig verksamhet ska konfigureras för att minska sårbarheter genom att ta bort eller stänga av funktioner och tjänster som inte behövs, använda lämpliga och möjliga säkerhetsfunktioner i systemet samt konfigurera systemet utifrån vedertagna rekommendationer.”

4 kap. 27 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Syftet med åtgärden är att säkerställa att risken för sårbarheter i ett informationssystem är så låg som möjligt. Genom att ta bort eller stänga av funktioner eller tjänster som inte används minskas risken att dessa exponeras för en angripare som kan använda tjänsten, eller en sårbarhet i den, för egna syften. På samma sätt minskar man risken för sårbarheter i systemet genom att använda de skyddsåtgärder som systemet erbjuder och konfigurera systemet utefter rekommendationer. Källor för vedertagna rekommendationer kan vara tillverkaren, välrenommerade säkerhetsföretag eller svenska eller utländska myndigheter. Vilka rekommendationer som ska följas för sådana operativsystem, applikationsprogramvaror m.m. bör fastställas.

4.9. Undantag från krav på skyddsåtgärder

Se även avsnitt 1.10.2 om undantag. I bilaga 2 finns en sammanställning av vem som leder beredning av samt vem som beslutar i ärenden om undantag från bestämmelser i författningar.

”Säkerhetspolisen och Försvarsmakten får inom respektive myndighets tillsynsområde meddela föreskrifter om undantag från kraven i 4 § första stycket.”

3 kap. 6 § första stycket säkerhetsskyddsförordningen

Se avsnitt 4.8.1 om krav på skyddsåtgärder.

”Myndigheten får ansöka om undantag från 3 kap. 4 § första stycket säkerhetsskyddsförordningen (2018:658) enligt det förfaringssätt som Försvarsmakten bestämmer.”

4 kap. 28 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: En ansökan om undantag från en eller flera bestämmelser ska ställas till säkerhetskontoret vid Must.

”Överbefälhavaren beslutar i ärenden om undantag enligt 3 kap. 6 § första stycket säkerhetsskyddsförordningen (2018:658).”

6 kap. 1 § 24 FM ArbO

4.10. Beredning av och beslut om undantag för informationssystem

Se först avsnitt 1.10.1 och 1.10.5 om undantag från bestämmelser i författningar. I bilaga 2 finns en sammanställning över vem som leder beredning av samt vem som beslutar i ärenden om undantag från bestämmelser i författningar.

”Chefen för militära underrättelse- och säkerhetstjänsten leder beredningen av ärenden om undantag från

1. Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd, förutom i fråga om ärenden som bereds enligt 8 kap. 35 §, och

2. Försvarsmaktens föreskrifter (FFS 2019:9) om signalskyddstjänsten, och

3. övriga föreskrifter rörande säkerhetsskydd.”

11 kap. 5 § andra stycket FM ArbO

”FM CIO ska avväga verksamhetsnytta, ekonomi, säkerhet, därtill kopplad risk-hantering och incidenthantering avseende it-system och information i it-system i Försvarsmakten.”

8 kap. 34 § andra stycket FM ArbO

”FM CIO leder beredningen av Försvarsmaktens ärenden om undantag från Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd avseende it-säkerhet och Försvarsmaktens interna bestämmelser (FIB 2017:8) om it-säkerhet.”

8 kap. 35 § FM ArbO

Vägledande förklaring: Innebörden är att undantagsberedningar för Försvarsmaktens informationssystem leds av CIO. Chefen för Must leder undantagsberedningar i ärenden från andra myndigheter.[167] En hemställan från någon enhet i Försvarsmakten om undantag från Försvarsmaktens föreskrifter säkerhetsskydd, Försvarsmaktens interna bestämmelser om säkerhetsskydd och Försvarsmaktens interna bestämmelser om it-säkerhet ska ställas till FM CIO i ärenden som rör informationssäkerhet.

[167] 11 kap. 5 § andra stycket 1 FM ArbO.

I sådana ärenden deltar säkerhetskontoret vid Must och juridiska avdelningen vid ledningsstaben i Högkvarteret.

Om ett ärende om undantag för ett informationssystem inte avser föreskrifter om it-säkerhet i Försvarsmaktens föreskrifter om säkerhetsskydd eller Försvarsmaktens interna bestämmelser om it-säkerhet, är det chefen för Must som leder beredningen om undantag.

”Chefen för militära underrättelse- och säkerhetstjänsten leder beredningen av ärenden om undantag enligt 3 kap. 6 § säkerhetskyddsförordningen (2018:658).”

11 kap. 5 § första stycket FM ArbO

Vägledande förklaring: I 3 kap. 6 § säkerhetsskyddsförordningen finns bestämmelser om undantag från krav i:

- 3 kap. 4 § första stycket säkerhetsskyddsförordningen om skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på ett informationssystem som ska användas i säkerhetskänslig verksamhet, skyddsåtgärder för obehörig avlyssning av, åtkomst till och nyttjande av systemet, samt spårbarhet för händelser som är av betydelse för säkerheten i systemet.[168] Skyddsåtgärderna beskrivs i avsnitt 4.8.1.

- 3 kap. 5 § andra stycket säkerhetsskyddsförordningen att säkerhetsskyddsklassificerade uppgifter ska skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten, när uppgifterna kommuniceras utanför verksamhetsutövarens kontroll.[169]

”Chefen för militära underrättelse- och säkerhetstjänsten leder beredningen av ärenden om undantag enligt 3 kap. 6 § säkerhetskyddsförordningen (2018:658).”

11 kap. 5 § första stycket FM ArbO

”Överbefälhavaren beslutar
24. i ärenden om undantag enligt 3 kap. 6 § första stycket säkerhetskyddsförordningen (2018:658).”

6 kap. 1 § 24 FM ArbO

[168] 3 kap. 4 § första stycket säkerhetsskyddsförordningen.
[169] 3 kap. 5 § andra stycket säkerhetsskyddsförordningen.

Vägledande förklaring: ÖB beslutar om undantag på krav på skyddsåtgärder som anges i 3 kap. 4 § första stycket säkerhetsskyddsförordningen. Skyddsåtgärderna beskrivs i avsnitt 4.8.1.

”Chefen för militära underrättelse- och säkerhetstjänsten leder beredningen av ärenden om undantag från

1. Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd, förutom i fråga om ärenden som bereds enligt 8 kap. 35 §, och

2. Försvarsmaktens föreskrifter (FFS 2019:9) om signalskyddstjänsten, och

3. övriga föreskrifter rörande säkerhetsskydd.”

11 kap. 5 § andra stycket FM ArbO

”Försvarsmakten får medge undantag från föreskrifterna i denna författning.

Överbefälhavaren, eller den han eller hon bestämmer, fattar beslut i ärenden om undantag.”

12 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

5. Fysisk säkerhet

5.1. Grunder

Fysisk säkerhet är en del av säkerhetsskyddet och måste vara integrerat med personalsäkerhet och informationssäkerhet för att säkerhetsskyddet i sin helhet ska vara tillfredställande. Till exempel kan fysiska skyddsåtgärder motverka insiders genom försvårande åtgärder och styrning av behörighet till byggnader och lokaler. Likaså är fysisk säkerhet beroende av tillfredställande informationssäkerhet, inte minst när det gäller information relaterat till fysiska skyddsåtgärder som passagekontrollsystem.

> *”Fysisk säkerhet ska*
>
> *1. förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs, och*
>
> *2. förebygga skadlig inverkan på sådana områden, byggnader, anläggning eller objekt som avses i 1.”*
>
> 2 kap. 3 § säkerhetsskyddslagen

Vägledande förklaring: I första punkten tydliggörs att fysisk säkerhet inte enbart innebär att förebygga att obehöriga får tillträde till platser utan att åtgärden också kan avse byggnader och anläggningar av olika slag samt objekt, t.ex. fordon. Även delar av t.ex. en anläggning innefattas.[170]

I andra punkten tydliggörs att åtgärden kan avse också ett skydd mot sådan skadlig inverkan som kan orsakas utan ett obehörigt tillträde. Det skulle exempelvis kunna röra sig om att en kabel för samhällsviktig elektronisk kommunikation skyddas genom ett robust hölje eller larm eller åtgärder för att skydda ett objekt mot obemannade luftfartyg, s.k. drönare.[171]

Exempel på åtgärder avseende fysisk säkerhet för att förhindra skadlig inverkan mot sådana områden, byggnader, anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs är skalskydd, påkörningsskydd eller andra barriärer som fysiskt hindrar en bil att t.ex. forcera en vägg eller köra på människor, ballistiskt skydd och skyddsåtgärder mot anlagd brand eller påverkan med hjälp av kemikalier.[172]

Begreppet ”fysisk säkerhet” i 2018 års säkerhetsskyddslag har ett vidare tillämpningsområde än begreppet ”tillträdesbegränsning” i 1996 års säkerhetsskyddslag.

[170] Prop. 2017/18:89 s. 138.
[171] Prop. 2017/18:89 s. 138.
[172] Prop. 2017/18:89 s. 72.

”Områden, byggnader och andra anläggningar eller objekt där säkerhetsskyddsklassificerade uppgifter förvaras eller annars behandlas, eller där säkerhetskänslig verksamhet i övrigt bedrivs, ska vara försedda med funktioner för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan utifrån ett identifierat säkerhetsskyddsbehov.”

4 kap. 1 § säkerhetsskyddsförordningen

Vägledande förklaring: Det finns ett starkt samband mellan att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan. Upptäckt måste ske så tidigt som möjligt, t.ex. vid ett obehörigt tillträde, i syfte att ge hanterande enheter tillräckligt mycket tid att komma på plats för att hindra eller omhänderta en angripare innan oacceptabla konsekvenser för Sveriges säkerhet hinner uppstå.

”Myndigheten ska vidta de fysiska säkerhetsskyddsåtgärder som krävs för att skydda säkerhetsklassificerade uppgifter och säkerhetskänslig verksamhet. Detta omfattar även detektering av farliga ämnen, vapen samt avlyssnings- och störutrustning.”

5 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Fysiska säkerhetsskyddsåtgärder omfattar bl.a. byggnadstekniska åtgärder, teknisk och personell bevakning samt möjlighet att ingripa.

Med farliga ämnen avses sjukdomsalstrande substanser eller toxiska ämnen, samt olika former av CBRNE-ämnen (kemiska, biologiska inkl. toxiner, radiologiska, nukleära och explosivämnen), spräng- och tändmedel och ammunition. Med avlyssningsutrustning avses varianter av akustisk, elektronisk och visuell avlyssning. Med störutrustning avses elektroniska störvapen såsom elektromagnetisk puls (EMP) och högeffektpulsad mikrovåg (HPM) samt radiosändare.

Behovet av detektering måste anpassas till fred, kris och krig. I Försvarsmakten behöver behovet anpassas till beredskapslägen.

Säkerhetsklassificerade uppgifter i bestämmelsen avser säkerhetsskyddsklassificerade uppgifter.

5.2. Organisationsenhetens bestämmelser om fysisk säkerhet

”Vid varje organisationsenhet ska det finnas bestämmelser om den fysiska säkerheten för områden, byggnader och andra anläggningar eller objekt vid organisationsenheten.

Chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, beslutar bestämmelser om den fysiska säkerheten.

För områden, byggnader och andra anläggningar eller objekt som disponeras gemensamt av två eller flera organisationsenheter ska Försvarsmaktens produktionschef, eller den produktionschefen bestämmer, besluta vilken eller vilka chefer för organisationsenheterna som beslutar bestämmelser om den fysiska säkerheten. De utpekade cheferna får delegera bemyndigandet att besluta bestämmelser om den fysiska säkerheten.”

4 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring till första stycket: Bestämmelserna anges lämpligen i en lokal instruktion. Exempel på punkter som kan ingå i en sådan instruktion:

- Eventuell indelning i administrativa zoner eller säkerhetszoner.
- Rutiner för tjänstekort och passerbevis m.m.
- Rutiner för tillträde (inklusive beslut om tillträdesrätt) till områden, byggnader och andra anläggningar eller objekt.
- Besöksrutiner.
- Rutiner för förvaring av säkerhetsskyddsklassificerade handlingar och lagringsmedier.
- Rutiner för förvaring av säkerhetskänslig materiel.
- Rutiner för nycklar, kort och koder, inklusive förvaring av huvud- och reservnycklar och förteckning över nycklar, kort och koder.
- Rutiner vid öppning av ett förvaringsutrymme utan närvaro av den person som har tilldelats utrymmet.
- Rutiner för larm och bevakning.
- Skyddsåtgärder som ska vidtas vid larm.
- Vilka utrymmen som är godkända för regelbunden muntlig delgivning.
- Rutiner för användning av utrymmen som är godkända för regelbunden muntlig delgivning.
- Rutiner för förteckning över vilka som är behöriga att komma in i utrymmen som är godkända för regelbunden muntlig delgivning.
- Rutiner för detektering av och skydd mot farliga ämnen, vapen samt avlyssnings- och störutrustning.
- Rutiner för hantering av post och gods.

Instruktionen behöver inte vara ett eget dokument utan kan bestå av flera dokument. Huvudsaken är att vad som gäller för den fysiska säkerheten lokalt är dokumenterat i en instruktion och att det finns rutiner för den fysiska säkerheten.

Delar av instruktionen kan komma att innehålla säkerhetsskyddsklassificerade uppgifter. I sådant fall bör instruktionen delas upp i flera dokument för att underlätta personalens åtkomst till de delar som inte innehåller några säkerhetsskyddsklassificerade uppgifter.

Vägledande förklaring till tredje stycket: Produktionschefen har även uppgiften att leda garnisonssamordning och ska utse garnisonschef.[173] Beslut som har fattats med stöd av äldre bestämmelser får fortsätta att gälla.

5.3. Tillträde och förvaring

> *”Myndigheten ska ha rutiner för tillträde till myndighetens områden, byggnader och andra anläggningar eller objekt. Rutinerna ska dokumenteras.”*
>
> 5 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Rutinerna kan framgå i organisationsenhetens instruktion för fysisk säkerhet.

5.3.1. Tillträdesansvarig chef

> *”Chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, ska besluta om tillträde till områden, byggnader och andra anläggningar eller objekt vid organisationsenheten (tillträdesansvarig chef).*
>
> *För områden, byggnader och andra anläggningar eller objekt som disponeras gemensamt av två eller flera organisationsenheter ska Försvarsmaktens produktionschef, eller den produktionschefen bestämmer, besluta vilken eller vilka chefer för organisationsenheterna som ska vara tillträdesansvarig chef.”*
>
> 4 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

5.3.2. Beslut om tillträde

Moment 5:1 *Beslut om tillträde enligt 4 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd ska innefatta it-utrymmen vid organisationsenheten där det behandlas säkerhetsskyddsklassificerade uppgifter eller bedrivs annan säkerhetskänslig verksamhet.*

Vägledande förklaring: Skydd för it-utrymmen beskrivs i avsnitt 5.6.

[173] 9 kap. 7 § 9 och 14 kap. 9 § FM ArbO.

”När myndigheten medger en person tillträde till myndighetens områden, byggnader och andra anläggningar eller objekt där det bedrivs verksamhet som kräver säkerhetsskydd ska myndigheten se till att personen genom besökstillstånd eller på annat sätt har fått myndighetens tillstånd till tillträde och att personen har styrkt sin identitet. Vid myndigheten ska det för varje besökare antecknas dennes namn, personnummer, passnummer eller nummer på annan identitetshandling, den myndighet, organisation eller motsvarande som besökaren företräder och dagen för besöket. Sådana anteckningar ska bevaras i minst 10 år.

Första stycket ska dock tillämpas med beaktande av allmänhetens rätt att utan att uppge sin identitet ta del av allmänna handlingar.”

5 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Identitet fastställs med stöd av godkänd identitetshandling. Enligt 3 kap. 2 § Försvarsmaktens interna bestämmelser (FIB 2017:7) om tjänstekort och vissa behörighetshandlingar godtas endast följande för att styrka identitet inom Försvarsmakten.

- identitetskort som uppfyller kraven enligt Standardiseringskommissionens i Sverige normer[174] (SIS), Svensk Standard (SS) 61 43 14,
- svenska pass,
- svenska körkort, och
- tjänstekort enligt förordningen (1958:272) om tjänstekort.

En utländsk besökare har normalt inte sådana identitetshandlingar och får därför identifieras med en identitetshandling som har utfärdats av en annan stat eller mellanfolklig organisation.

I 13 § Försvarsmaktens skyddsföreskrifter finns bestämmelser om att det i bevakningsplanen för ett skyddsobjekt särskilt ska anges vilka kriterier som ska ligga till grund för att medge någon person tillträde till skyddsobjektet.

I 14 § Försvarsmaktens skyddsföreskrifter framgår förutsättningarna för att kunna medge tillträde till ett skyddsobjekt.

När en person vill ta del av allmänna handlingar behöver personen inte uppge sin identitet, varje person har rätt att vara anonym i en sådan situation.[175]

[174] Numera Svenska institutet för standarder.
[175] 2 kap. 18 § tryckfrihetsförordningen.

5.3.3. Administrativa zoner och säkerhetszoner

> *”Myndigheten får besluta att områden, byggnader och andra anläggningar eller objekt ska vara en administrativ zon och en säkerhetszon. Beslutet ska dokumenteras.”*
>
> 5 kap. 13 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen är avsedd att ge myndigheterna ett alternativt sätt att utforma den fysiska säkerheten. Beslutet måste dock föregås av en säkerhetsskyddsplanering.

Säkerhetszoner kan medföra enklare och effektivare hantering och förvaring av information och verksamhet utifrån att det totala skyddet och kontrollen medger lägre skyddskrav inne i en säkerhetszon.

Ett exempel på en administrativ zon är Försvarsmaktens Högkvarter, där hela området från staketet och byggnaden som helhet utgör en sådan administrativ zon. I byggnaden kompletteras skyddet med flera säkerhetszoner, med styrning av tillträdet, t.ex. olika ledningscentraler. Med säkerhetszon avses t.ex. utrymmen som kräver särskild behörighet för tillträde, där säkerhetskänslig verksamhet bedrivs. För en säkerhetszon kan Försvarsmakten bestämma att t.ex. servicepersonal för bl.a. it-drift och lokalvård inte får lämnas ensamma.

> *”I bilaga 2 till denna författning anges de krav som gäller för administrativ zon respektive säkerhetszon.”*
>
> 5 kap. 14 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: De specifika kraven som gäller för zonerna framgår av bilaga 2 i Försvarsmaktens föreskrifter om säkerhetsskydd.

5.3.3.1 Jämförelsetabell förvaring

Tabell 5.2 nedan visar krav på skyddsnivåer och larm för förvaringsutrymmen för säkerhetsskyddsklassificerade handlingar och lagringsmedier beroende på om utrymmena är placerade utanför en administrativ zon eller en säkerhetszon, i en administrativ zon eller i en säkerhetszon.[176]

Skyddsnivå 4 kan uppnås om ett utrymme som uppfyller krav för skyddsnivå 3 och som är försett med larm samt att en särskild avdelad styrka kan vara på plats inom sådan tid att ett intrång i utrymmet kan försvåras.[177]

[176] 5 kap. 15-17 §§ Försvarsmaktens föreskrifter om säkerhetsskydd.
[177] Skyddsnivå 4 i bilaga 1 till Försvarsmaktens föreskrifter om säkerhetsskydd.

Tabell 5.2. Jämförelsetabell.

	Utanför zoner	Administrativ zon	Säkerhetszon
Begränsat hemlig	Skyddsnivå 1		
Konfidentiell	Lägst skyddsnivå 3 Larm	Skyddsnivå 3	Skyddsnivå 2 Larm
Hemlig			
Kvalificerat hemlig	Skyddsnivå 4 Larm		

5.3.3.2 Beslut om administrativa zoner och säkerhetszoner

> *”I 5 kap. 13 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd och i bilaga 2 till föreskrifterna finns bestämmelser om beslut om administrativ zon och säkerhetszon.*
>
> *Tillträdesansvarig chef fattar sådana beslut.”*
>
> 4 kap. 6 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Bemyndigandet får inte delegeras.

Vägledande förklaring: Beslut om administrativa zoner och säkerhetszoner kan finnas i organisationsenhetens instruktion för den fysiska säkerheten (avsnitt 5.2).

5.3.4. Krav på förvaringsutrymmen

> *”I bilaga 1 till denna författning anges de krav som gäller för respektive skyddsnivå. Ett förvaringsutrymme för säkerhetsskyddsklassificerade handlingar och säkerhetsskyddsklassificerade lagringsmedier ska uppfylla de krav som gäller för skyddsnivå 1, 2, 3 eller 4.”*
>
> 5 kap. 12 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: I bilagan finns krav på utformning av utrymmen, krav på larm och åtgärd vid larm. I krav för skyddsnivåerna 2, 3 och 4 framgår att utrymmenas omslutningsytor får bestå av andra material med motsvarande motståndskraft.

Beroende på de förvarade handlingarnas eller lagringsmediernas säkerhetsskyddsklass ska den fysiska säkerheten kunna motstå försök till intrång under viss tid. Utrymmen delas därför in i skyddsnivå 1, 2, 3 eller 4. Ju högre säkerhetsskyddsklass desto kraftigare konstruerat förvaringsutrymme krävs. Ju kraftigare konstruerat utrymmet är, och därmed dess sammanhängande förmåga att motstå angrepp, desto högre skyddsnivå har det.

5.3.5. Förvaring av säkerhetsskyddsklassificerade handlingar och lagringsmedier

”En säkerhetsskyddsklassificerad handling och ett säkerhetsskyddsklassificerat lagringsmedium som är placerade i säkerhetsskyddsklassen begränsat hemlig ska vara under kontroll eller förvaras inlåsta i ett förvaringsutrymme eller i en låst lokal som endast den som är behörig att ta del av handlingen eller lagringsmediet har tillträde till. Lokalen eller förvaringsutrymmet ska uppfylla de krav som gäller för skyddsnivå 1 vid förvaring i eller utanför en administrativ zon eller en säkerhetszon.”

5 kap. 15 § Försvarsmaktens föreskrifter om säkerhetsskydd

”En säkerhetsskyddsklassificerad handling och ett säkerhetsskyddsklassificerat lagringsmedium som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig ska vara under kontroll eller förvaras inlåsta i ett förvaringsutrymme som uppfyller de krav som gäller för skyddsnivå 2 i en säkerhetszon eller skyddsnivå 3 i en administrativ zon. Om en sådan handling eller ett sådant lagringsmedium inte förvaras i någon zon ska handlingen eller lagringsmediet förvaras i ett larmat utrymme i lägst skyddsnivå 3.”

5 kap. 16 § Försvarsmaktens föreskrifter om säkerhetsskydd

”En säkerhetsskyddsklassificerad handling och ett säkerhetsskyddsklassificerat lagringsmedium som är placerade i säkerhetsskyddsklassen kvalificerat hemlig ska vara under kontroll eller förvaras inlåsta i ett larmat utrymme i skyddsnivå 4 vid förvaring i eller utanför en administrativ zon eller en säkerhetszon.”

5 kap. 17 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Säkerhetsskyddsklassificerade handlingar får förvaras utanför en administrativ zon eller en säkerhetszon. Rådande omvärldsläge och förändrade hotbild är motiv för att förvaringsutrymmen ska vara försedda med larm om säkerhetsskyddsklassificerade handlingar placerade i säkerhetsskyddsklass konfidentiell eller högre förvaras i utrymmena.

I avsnitt 5.4.2 beskrivs skyddsåtgärder som ska vidtas vid larm.

Se avsnitt 3.19 om medförande för vad som avses med ”vara under kontroll”.

I avsnitt 5.2.4 beskrivs administrativ zon och säkerhetszon.

5.3.6. Samförvaring

”I 5 kap. 9 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd finns bestämmelser om vem som får inneha en nyckel, ett kort eller en kod.

Chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, får besluta att ett förvaringsutrymme får användas av flera personer. Ett sådant samförvaringsbeslut ska dokumenteras.”

4 kap. 6 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Samförvaring avser enbart åtkomst till ett förvaringsutrymme. Ett samförvaringsbeslut innebär inte att personerna är behöriga att ta del av uppgifter som någon annan förvarar i utrymmet. Samförvaring är inte lämpligt när flera personer från skilda verksamheter gemensamt ska förvara säkerhetsskyddsklassificerade handlingar som de sinsemellan inte är behöriga till.

Om personerna inte är behöriga att ta del av samtliga säkerhetsskyddsklassificerade uppgifter som förvaras i förvaringsutrymmet, bör förvaringsutrymmet innehålla låsbara innerfack så att varje person kan tilldelas ett personligt innerfack.

Ett samförvaringsbeslut som har fattats med stöd av äldre bestämmelser får fortsätta att gälla.

5.3.7. Jämförelsetabell i fördröjningstid för förvaringsutrymmen

Moment 5:2 *Tabell 5.1 ska användas för att fastställa den tid en särskild avdelad styrka har till sitt förfogande innan ett intrång har skett i ett nivåreglerat förvaringsutrymme.*

Tabell 5.1. Jämförelsetabell.

Fördröjningstid i minuter mot angrepp	Skyddsnivå enligt bilaga 1 i FFS 2019:2	Grade* enligt SS-EN 1143	Svensk standard SS 3492 SS 3493 SS 3150	Stöldskyddsföreningens norm SSF 3492
10	3	----	SS 3492 SS 3493	SSF 3492
15	3	0		
20	3	I		
30	3	II		

Fördröjningstid i minuter mot angrepp	Skyddsnivå enligt bilaga 1 i FFS 2019:2	Grade* enligt SS-EN 1143	Svensk standard SS 3492 SS 3493 SS 3150	Stöldskyddsföreningens norm SSF 3492
40	3	III	SS 3150 50 svp	
60	4	IV	SS 3150 100 svp	
90	4	V	SS 3150 120 svp	
120	4	VI	SS 3150 170 svp	
150	4	VII	SS 3150 280 svp	

Vägledande förklaring: Utrymmen som inte är testade enligt Europanormen (SS-EN) eller Svensk standard (SS), men som har en fastställd skyddsnivå har en motståndskraft som motsvarar angrepp i 10 minuter för skyddsnivå 3 och 60 minuter för skyddsnivå 4.

Kassuner som är uppställda på grusbädd (skyddsnivå 3) har en motståndskraft som motsvarar angrepp i 30 minuter. Kassuner som är uppställda och förankrade på hårdgjord yta (t.ex. betong) har en motståndskraft som motsvararar angrepp i 60 minuter (skyddsnivå 4). Detta gäller för kassun m/67 och m/83.

5.3.8. Beslut om avvikelse vid förvaring av säkerhetsskyddsklassificerade handlingar och lagringsmedier

> *”Myndigheten får fatta beslut som avviker från 15–17 §§ under förutsättning att motsvarande skydd kan upprätthållas. Beslutet ska dokumenteras.”*
>
> 5 kap. 18 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Om ett förvaringsutrymme för säkerhetsskyddsklassificerade handlingar eller lagringsmedier inte uppfyller krav för den skyddsnivå som gäller för utrymmet, kan utrymmet ändå få användas om åtgärder vidtas för att upprätthålla motsvarande skydd. Sådana åtgärder kan framgå i säkerhetsskyddsplaneringen,

t.ex. kan placering och närhet till en särskilt avdelad styrka vara ingångsvärden för att uppnå ett motsvarande skydd.

> *”Chef för organisationsenhet får besluta om sådana avvikelser.”*
>
> 4 kap. 12 § andra stycket
> Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Ett beslut om avvikelse från 5 kap. 15-17 §§ Försvarsmaktens föreskrifter om säkerhetsskydd kan framgå av organisationsenhetens säkerhetsskyddsplan eller en särskild säkerhetsskyddsplan. I planen måste det framgå att det är fråga om en sådan avvikelse. Åtgärder för att upprätthålla motsvarande skydd måste också anges i planen.

5.3.9. Förvaring av säkerhetskänslig materiel

> *”Med* säkerhetskänslig materiel *avses i denna författning materiel som inte innehåller säkerhetsskyddsklassificerade uppgifter, men som har en sådan betydelse för Försvarsmaktens säkerhetskänsliga verksamhet att en förlust av materielen allvarligt påverkar den säkerhetskänsliga verksamheten.”*
>
> 1 kap. 2 § andra stycket
> Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Säkerhetskänslig materiel kan t.ex. vara materiel som används i insatsorganisationen. Genom säkerhetsskyddsanalysen identifieras vilken materiel i verksamheten som är säkerhetskänslig materiel. En sådan identifiering kan göras i Försvarsmaktens säkerhetsskyddsanalys, i en organisationsenhets, en lednings säkerhetsskyddsanalys eller i en särskild säkerhetsskyddsanalys.

Att förlust av materielen allvarligt ska påverka den säkerhetskänsliga verksamheten är ett kvalificeringskrav, så att inte merparten av all materiel bedöms vara säkerhetskänslig materiel. Med ”allvarligt påverkar den säkerhetskänsliga verksamheten” avses inte detsamma som att förlusten ”medför en allvarlig skada för Sveriges säkerhet” enligt 2 kap. 5 § säkerhetsskyddslagen.

> *”Säkerhetskänslig materiel ska förvaras i ett förvaringsutrymme som uppfyller de krav som gäller för skyddsnivå 1–4 enligt bilaga 1 till Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.”*
>
> 4 kap. 1 § första stycket
> Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 5:3 *Säkerhetskänslig materiel ska förvaras i ett förvaringsutrymme som ska placeras i någon av följande skyddsnivåer.*

Skyddsnivå 1 gäller för förvaring av en ringa mängd säkerhetskänslig materiel.
Skyddsnivå 2 gäller för förvaring av en mindre mängd säkerhetskänslig materiel.
Skyddsnivå 3 gäller för förvaring av en större mängd säkerhetskänslig materiel.
Skyddsnivå 4 gäller för förvaring av mycket stora mängder säkerhetskänslig materiel.

I avsnitt 2.4 beskrivs skydd av materiel som inte ska omfattas av säkerhetsskydd.

5.3.10. Beslut om avvikelse vid förvaring av säkerhetskänslig materiel

”Chef för organisationsenhet får fatta beslut som avviker från kraven under förutsättning att motsvarande skydd kan upprätthållas.”

4 kap. 10 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

5.3.11. Nycklar, kort och koder

”Nycklar, kort och koder som var för sig ger tillträde till säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig verksamhet ska vara under kontroll eller förvaras i motsvarande skyddsnivå som de ger tillträde till.”

5 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Om reservnycklar, reservkort eller uppgifter om kod ska förpackas så ska det förslagsvis göras i ett förseglat och ej genomlysbart kuvert av den som har ansvar för förvaringsutrymmet.

Begreppet *under kontroll* innebär t.ex. att det dagliga användandet sker på ett sådant sätt att ingen obehörig kan komma åt dessa. Begreppet kan även innebära att innehavaren alltid bär nyckel och kort på sig, att anteckning om kod inte förvaras tillsammans med kortet eller att den personliga koden döljs vid användandet. Se även den förklarande texten i avsnitt 3.19 om hur säkerhetsskyddsklassificerade handlingar och lagringsmedier är under kontroll när de medförs.

Om enbart en nyckel behövs för att någon ska ge sig tillträde till säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig verksamhet måste nyckeln förvaras i ett utrymme med motsvarande skyddsnivå under den tid nyckeln inte är under kontroll.

Vid bruk av tvåfaktorsautentisering (t.ex. kort och kod) ställs inte dessa förvaringskrav på kortet förutsatt att koden inte förvaras tillsammans med kortet.

”En nyckel, ett kort eller en kod får innehas endast av den som har ansvaret för utrymmet, om inte myndigheten har beslutat annat.”

5 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Syftet med bestämmelsen är att förhindra obehöriga att få tillgång till utrymmena. Ett sådant beslut kan t.ex. innefatta att flera personer får tillträde till ett sådant utrymme. Beslutet ska dokumenteras, vilket framgår av 21 § myndighetsförordningen (2007:515). Se även avsnitt 5.3.6 om samförvaring.

”Det ska finnas en förteckning över samtliga nycklar, kort och koder till områden, byggnader eller utrymmen som

1. innehåller säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell eller högre, eller

2. används för säkerhetskänslig verksamhet om en inträffad skada kan vara mer än inte obetydlig för Sveriges säkerhet.

Av förteckningen ska framgå till vem och när en nyckel, ett kort eller en kod har lämnats samt var reservnyckel och kod eller kort i reserv förvaras.”

5 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Syftet är att ha den ordning som gäller säkerhetsskyddsklassificerade handlingar och lagringsmedier även ska gälla för nycklar, kort och koder.

”Sådana förteckningar ska föras vid varje organisationsenhet.”

4 kap. 7 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Det kan finnas flera förteckningar över nycklar, kort och koder vid en organisationsenhet.

”Om det finns anledning att anta att en nyckel eller ett kort har förlorats eller kopierats, att en kod har röjts eller att en nyckel, kort eller kod har använts av någon obehörig person, ska förhållandet omedelbart rapporteras till myndighetens säkerhetsskyddschef eller till den han eller hon bestämmer.”

5 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd

Moment 5:4 *Vid organisationsenheten ska en förteckning föras över nycklar, kort och koder till områden, byggnader eller utrymmen som används för säkerhetskänslig verksamhet där en inträffad skada lägst kan vara inte obetydlig för Sveriges säkerhet.*

Moment 5:5 *Sådana nycklar, kort och koder som anges i 5 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd och moment 5:4 ska inventeras en gång per år.*

Moment 5:6 *En nyckel som ännu inte har lämnats till den som ska ansvara för ett förvaringsutrymme ska förvaras av säkerhetschefen, eller av den han eller hon bestämmer.*

Moment 5:7 *En anteckning om en kod till ett kombinationslås eller en anteckning om en kod som används tillsammans med ett passerbevis ska förvaras i ett förseglat emballage. Emballaget ska vara så beskaffat att det är omöjligt att ta del av anteckningen utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget. Anteckningen med emballage ska förvaras på samma sätt som gäller för säkerhetsskyddsklassificerade handlingar eller säkerhetskänslig materiel som förvaras i det utrymme som koden går till.*

Moment 5:8 *Om en person ska vara borta från organisationsenheten en längre tid ska han eller hon överlämna nyckeln till förvaringsutrymmet till säkerhetschefen, eller till den säkerhetschefen bestämmer. Nyckeln ska förvaras på samma sätt som anges i moment 5:7.*

Moment 5:9 *En kod eller en reservnyckel får endast i vittnes närvaro användas av någon annan än den som har ansvar för förvaringsutrymmet. I organisationsenhetens bestämmelser för fysisk säkerhet ska förutsättningar för en sådan användning anges.*

Vägledande förklaring: Se avsnitt 5.2 om organisationsenhetens bestämmelser om den fysiska säkerheten.

Moment 5:10 *I ett avtal om inköp av ett flyttbart förvaringsutrymme, en dörr till ett förvaringsutrymme eller ett lås ska det säkerställas att nyckeln till utrymmet eller låset levereras separat och direkt till organisationsenheten samt att leveransen sker enligt vad som gäller för säkerhetsskyddsklassificerade handlingar i lägst den säkerhetsskyddsklassen som förvaringsutrymmet är avsett för.*

Moment 5:11 *Ett sådant förhållande som anges i 5 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd ska vid organisationsenheten rapporteras som en säkerhetshotande händelse.*

Rapportering beskrivs i avsnitt 10.2.1.

5.3.12. Förvaring av huvudnycklar och reservnycklar

> *”Om myndigheten har beslutat att personalen under kortare tid får lämna säkerhetsskyddsklassificerade handlingar eller säkerhetsskyddsklassificerade lagringsmedier framme i ett låst arbetsrum, ska huvudnycklar och reservnycklar förvaras så att ingen obehörig kan komma åt dem.”*
>
> 5 kap. 19 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Om personalen beviljas att under kortare tid, t.ex. lunch, få lämna säkerhetsskyddsklassificerade handlingar framme i arbetsrummet och inte

behöva låsa in dem i ett säkerhetsskåp måste det säkerställas att inga obehöriga har tillgång till rummet. Detta innebär att t.ex. nycklar, inklusive huvudnycklar, måste förvaras på ett säkert sätt. Nycklar ska vara under kontroll eller förvaras inlåsta i ett utrymme med samma skyddsnivå som det arbetsrum för vilka de är avsedda. Nycklar som inte används bör förvaras i förseglad säkerhetspåse eller liknande.

Bevakningspersonal som inte är behörig att ta del av information eller verksamhet, kan ändå beslutas vara behöriga till utrymmen, eftersom det ingår i deras arbetsuppgifter att kontrollera och stödja vid behov.

”Chef för organisationsenhet, eller den chef för organisationsenhet bestämmer, fattar sådana beslut avseende egen organisationsenhet.”

4 kap. 8 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Beslutet om att personalen under kortare tid får lämna säkerhetsskyddsklassificerade handlingar eller säkerhetsskyddsklassificerade lagringsmedier framme i ett låst arbetsrum kan finnas i organisationsenhetens instruktion för den fysiska säkerheten (avsnitt 5.2).

Moment 5:12 *En reservnyckel till ett förvaringsutrymme ska förvaras i ett förseglat emballage. Emballaget ska vara så beskaffat att det är omöjligt att avläsa nyckelaxet utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget.*

Moment 5:13 *Ett emballage som innehåller en reservnyckel ska förvaras på samma sätt som gäller för de handlingar, lagringsmedier eller den materiel som förvaras i det utrymme som nyckeln går till.*

5.3.13. Utländska besök till Försvarsmakten

”Innan ett beslut om att ge en utlänning tillträde får fattas ska insatschefen, eller den insatschefen bestämmer, ha lämnat tillstånd för tillträdet. Ett sådant tillstånd behövs inte i fråga om verksamhet som

1. anges i lagen (2000:130) om försvarsunderrättelseverksamhet, eller

2. avser militär säkerhetstjänst vid den militära underrättelse- och säkerhetstjänsten i Högkvarteret.

Tillstånd från insatsledningen behövs inte om det är fråga om en utlännings tillträde till områden, byggnader och andra anläggningar eller objekt som vid tillfället är tillgängliga för allmänheten eller som utlänningen måste komma till för att kunna ställa en begäran om att få ta del av allmänna handlingar.”

4 kap. 3 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Ärenden om utländska besök bereds av tillståndssektionen vid insatsstabens avdelning för genomförande av operationer (INSS J3 Tillstånd).

”Försvarsmakten skall skaffa Regeringskansliets tillstånd innan myndigheten anordnar besök av en utlänning vid en krigsstabsplats eller en ledningscentral eller vid ett förband eller annan enhet under pågående beredskapsuppdrag eller krigsförbandsövning.”

1 § första stycket förordningen (1996:442) om utländska besök vid vissa myndigheter inom Försvarsdepartementets verksamhetsområde

Vägledande förklaring: När beslut om att ett besök av utländska medborgare har lämnats till en organisationsenhet, innefattar detta i regel endast tillstånd att besöka den organisationsenhet som har ansökt hos Högkvarteret. Chefen för organisationsenheten eller, i förekommande fall tillträdesansvarig chef, bestämmer vilka delar av organisationsenheten som får besökas eller inte får besökas. Ett sådant ställningstagande måste grunda sig på organisationsenhetens säkerhetsskyddsplanering alternativt den särskilda säkerhetsskyddsplanen för det aktuella besöket.

”Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut skall skaffa Regeringskansliets tillstånd innan myndigheterna anordnar besök av en utlänning som har en befattning som motsvarar en befattning inom Försvarsmakten som överbefälhavare eller ställföreträdande myndighetschef, högre militär chef i Högkvarteret eller en befattning som motsvarar en befattning som chef för Försvarets materielverk eller Totalförsvarets forskningsinstitut.”

2 § förordningen om utländska besök vid vissa myndigheter inom Försvarsdepartementets verksamhetsområde

”Tillstånd enligt 1 och 2 §§ samt rapport enligt 4 § behövs inte om besöket är föranlett av att utlänningen skall

1. förbereda, delta i eller följa upp verksamhet inom ramen för en överenskommelse mellan Sverige och andra stater om samarbete inom totalförsvarets område,

2. förbereda, delta i eller följa upp en affärsförhandling,

3. göra en anmälan eller en uppvaktning eller på något annat sätt medverka i endast protokollära sammanhang, eller

4. delta i ett samkväm eller annan liknande verksamhet.”

5 § förordningen om utländska besök vid vissa myndigheter inom Försvarsdepartementets verksamhetsområde

”Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut behöver inte skaffa tillstånd enligt 1 och 2 §§ eller lämna rapport enligt 4 § när de bedriver sådan verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Försvarsmakten behöver inte heller skaffa ett sådant tillstånd eller lämna en sådan rapport när den bedriver militär säkerhetstjänst.”

5 a § förordningen om utländska besök vid vissa myndigheter inom Försvarsdepartementets verksamhetsområde

5.4. Bevakning

”Bevakning med personal eller tekniska bevakningssystem ska finnas vid alla passerställen till platser där det bedrivs säkerhetskänslig verksamhet.”

5 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Ett tekniskt bevakningssystem i form av ett passagekontrollsystem kan med fördel användas vid passerställen som används av organisationsenhetens personal. Vid platser dit besökare kan förväntas komma bör bevakningen företrädesvis vara personell.

Personell och teknisk bevakning syftar till att upptäcka obehörigt tillträde eller skadlig inverkan mot säkerhetskänslig verksamhet.

Personell bevakning kan bestå av till exempel skyddsvaktspersonal som utför fast bevakning vid ingångar och entréer, eller som patrullerar med oförutsägbara mönster.

Teknisk bevakning kan ske både som inre och yttre bevakning och kan utföras som perimeterskydd, skalskydd, volymskydd och punktskydd.

5.4.1. Skydd för tekniska bevakningssystem

”Om ett tekniskt bevakningssystem avser

1. utrymmen där säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklassen konfidentiell eller högre förvaras och behandlas, eller

2. platser där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan vara mer än inte obetydlig för Sveriges säkerhet,

ska säkerhetsskyddet av de centrala delarna i det tekniska bevakningssystemet uppfylla de krav på förvaring som gäller för lägst skyddsnivå 2.

Myndigheten ska utreda vilket säkerhetsskydd som behövs för att säkerställa bevakningssystemets funktionalitet. En sådan utredning ska dokumenteras.”

5 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med de centrala delarna av det tekniska bevakningssystemet avses styrdator men inte detektorer, kontakter, kortläsare eller ringklockor. Det tekniska bevakningssystemet ska inte kunna manipuleras eller på annat sätt påverkas.

I Försvarsmakten är ett tekniskt bevakningssystem ett informationssystem (system av sammansatt mjuk- och hårdvara som behandlar information).[178] Ett tekniskt bevakningssystem omfattas av bestämmelser för informationssystem, bl.a. ackreditering. Bestämmelser om informationssystem beskrivs i kapitel 4.

Moment 5:14 *Organisationsenhetens tekniska bevakningssystem för platser där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan vara inte obetydlig för Sveriges säkerhet, ska säkerhetsskyddet av de centrala delarna i det tekniska bevakningssystemet uppfylla de krav på förvaring som gäller för lägst skyddsnivå 2.*

Vägledande förklaring: Det kan t.ex. vara ett passagekontrollsystem till utrymmen där säkerhetsskyddsklassificerade uppgifter förvaras eller hanteras. Det kan även vara ett larmsystem där detektion av ett intrång medför en insats från en särskilt avdelad styrka som har till uppgift att undersöka den detekterade händelsen.

Moment 5:15 *Organisationsenheten ska vidta de skyddsåtgärder som behövs för att*

a) säkerställa att ett tekniskt bevakningssystem inte kan manipuleras i syfte att någon obehörig ska kunna ta sig in i utrymmen, samt

b) kontinuitet för det tekniska bevakningssystemets funktion.

Vägledande förklaring: Skyddsåtgärderna kan bestå av en kombination av tekniska, administrativa och fysiska åtgärder så att ett nödvändigt skydd uppnås. Reservkraft, redundanta förbindelser för larmöverföring och sabotageskydd är exempel på åtgärder.

5.4.2. Åtgärder vid larm

> *”Myndigheten ska besluta vilka skyddsåtgärder som ska vidtas vid larm från områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. Beslutet ska dokumenteras.”*
>
> 5 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Det är nödvändigt att inför ett beslut analysera vilka åtgärder som bedöms lämpliga vid larm. Beroende på avstånd till objektet eller andra försvårande omständigheter kan annan åtgärd än insats vara aktuell.

Åtgärder som vidtas vid larm för att skydda säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig verksamhet från att avslöjas eller på annat sätt röjas, kan t.ex. vara:

[178] 1 kap. 5 § säkerhetsskyddsförordningen.

- Koppla om elektronisk kommunikation.
- Genomföra insats mot det område, den byggnad eller den anläggning eller objekt där larm har utlösts.

”Krav på larm i 5 kap. 16-17 §§, 22 § andra och tredje styckena samt 5 kap. 24 § i den nya författningen avseende larm ska börja gälla den 1 april 2022.”

Punkt 8 i ikraftträdande- och övergångsbestämmelse till Försvarsmaktens förskrifter om säkerhetsskydd

Vägledande förklaring: Punkten innebär att organisationsenheter i Försvarsmakten till den 1 april 2022 ska säkerställa att förvaringsutrymmen enligt 5 kap. 16-17 §§, 22 § andra och tredje styckena samt 5 kap. 24 § i Försvarsmaktens förskrifter om säkerhetsskydd är larmade.

”Chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, ska besluta sådana skyddsåtgärder för områden, byggnader och andra anläggningar eller objekt som hör till organisationsenheten.”

4 kap. 5 § andra stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Ett beslut om vilka skyddsåtgärder som ska vidtas vid larm kan ingå i organisationsenhetens säkerhetsskyddsplan eller en särskild säkerhetsskyddsplan. Organisationsenhetens interna styrning av hur detta ska ordnas kan ingå i enhetens bestämmelser om den fysiska säkerheten (avsnitt 5.2).

Termineringen av larm kan ske lokalt hos egen vakt, eller motsvarande, eller centralt i Försvarsmaktens larmcentral (FMLC).

5.5. Utrymmen för muntlig delgivning

”Myndigheten ska besluta vilka utrymmen som är godkända för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell eller högre.

Av beslutet ska det framgå hur det säkerställs att endast behörig personal har tillträde till utrymmet samt vilken utrustning som får medföras eller finnas i utrymmet.

Beslutet ska dokumenteras.”

5 kap. 20 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Innan ett utrymme kan godkännas för muntlig regelbunden delgivning av säkerhetsskyddsklassificerade uppgifter måste en sårbarhetsanalysanalys (avsnitt 5.5.3) genomföras. Av analysen bör det framgå vad som krävs för att ett

utrymme ska vara godkänt för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter. För att ett utrymme ska vara godkänt för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter bör det ha vidtagits erforderliga åtgärder mot obehörig avlyssning.

Exempel på lokaler där regelbunden delgivning kan förekomma är enskilda utrymmen som konferens-, mötes- eller kontorslokaler (inklusive tjänsterum) som återkommande används för muntlig delgivning av säkerhetsskyddsklassificerade uppgifter. Det kan också vara en möteslokal som återkommande över tiden används för planerade och icke planerade mötesgenomgångar. Det kan också röra sig om ledningsrum eller ledningscentraler som JOC (Joint Operations Center) eller JIOC (Joint Intelligence Operations Center).

Endast den anledningen att utrustning (t.ex. datorer för internetbaserad lärplattform med mikrofon och kamera) är godkänd för att användas inom Försvarsmakten, innebär inte att den är lämplig att användas i ett utrymme för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter.

5.5.1. Sårbarheter kopplat till utrymmen för muntlig delgivning

I utrymmen finns olika svagheter i skyddet mot avlyssning som innebär att andra, än de som befinner sig i utrymmet, kan överhöra, få insyn i, eller tekniskt avlyssna ett samtal. Sårbarheterna kan påverkas och reduceras genom att tekniska, administrativa eller fysiska säkerhetsskyddsåtgärder vidtas.

5.5.1.1 Fysiska sårbarheter

Exempel på fysiska sårbarheter som kan ge möjlighet till obehörig avlyssning kan vara utrymmets ljudisolering i väggar, fönster, dörrar, tak och golv, ventilation (rör, schakt m.m.). Även kabelkanaler som inte är tätade kan leda ljud mellan utrymmen eller vidare i en byggnad.

Utrymmets konstruktion och val av material kan medge att ljud kan fortplantas i byggnaden på ett oönskat sätt. Stomljud från glas- och väggpartier kan avlyssnas med riktad mikrofon, t.ex. lasermikrofon. En sådan behöver aldrig monteras på byggnaden utan kan fånga upp vibrationer från ljud på långt avstånd.

Ett utrymmes placering kan utgöra en sårbarhet om utrymmet är placerat vid yttervägg. Om ett utrymme är placerat i ett flervåningshus där obehöriga finns under, över eller vid sidan av utrymmet kan även detta vara en sårbarhet.

Det är även viktigt att beakta den tekniska utrustning och de inventarier som finns i ett utrymme. Ju mer teknisk utrustning och inventarier som finns i utrymmet desto svårare kan det vara att upptäcka avlyssningsutrustning. Avlyssningsutrustning kan enkelt installeras i både möbler och teknisk utrustning.

5.5.1.2 Tekniska sårbarheter

Exempel på tekniska sårbarheter som gör det möjligt att obehörigen avlyssna ett utrymme kan vara datorer, fasta telefoner, mobiltelefoner, digitala klockor, radiosändare, högtalare i utrymmet. Sårbarheten ökar om den tekniska utrustningen kan kommunicera elektroniskt via kabel eller trådlöst utanför utrymmet.

En antagonist som har fått fysisk tillgång till teknisk utrustning eller som kan påverka den tekniska utrustningen på distans, skulle kunna manipulera utrustningen för att avlyssna utrymmet. Det kan t.ex. ske via fast internetuppkoppling eller att utrustningen i ett tidigare skede haft en nätverkskoppling, där en antagonist t.ex. har aktiverat utrustningens mikrofon eller högtalare så det går att avlyssna samtal. Det kan även ske genom installation av skadlig kod i datorer och mobiltelefoner.

Fast telefoni (såväl analoga telefoner som ip-telefoner) och mobiltelefoner kan manipuleras så att de i viloläge fångar upp samtal och för ljudet vidare via tele- eller ip-nät. Mobiltelefoner och trådlösa telefoner är radiosändare som kan avlyssnas på långa avstånd, även från platser som är belägna utanför byggnaden.

5.5.2. Organisationsenhetens säkerhetsskyddsplanering

I moment 2:4 (avsnitt 2.3.3.1) finns kravet att det i organisationsenhetens säkerhetsskyddsplanering ska framgå vilka utrymmen som ska användas för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell eller högre.

Har en organisationsenhet godkänt utrymmen före den 1 januari 2021, gäller godkännandet längst till den 31 december 2022.[179]

5.5.3. Sårbarhetsanalys för identifiering av åtgärder

Moment 5:16 *Vilka åtgärder som behöver vidtas för att ett utrymme ska kunna godkännas ska identifieras i en sårbarhetsanalys. Identifierade åtgärder ska genomföras innan utrymmet godkänns.*

Vägledande förklaring: Sårbarhetsanalysen i momentet är inte en säkerhetsskyddsanalys eftersom säkerhetsskyddsanalysens nio steg inte behöver genomföras. Det är endast en analys för att identifiera sårbarheter som finns i fastighetens konstruktion, utrymmets placering och omgivande miljö. Andra ingångsvärden i sårbarhetsanalysen är de muntliga uppgifternas högsta säkerhetsskyddsklass och krav enligt moment nedan. Planering av säkerhetsskyddsåtgärder för ett utrymme kan ingå i organisationsenhetens säkerhetsskyddsplan, alternativt i en särskild säkerhetsskyddsplan för ett utrymme.

Resultat av sårbarhetsanalysen är åtgärder som behöver vidtas. Sårbarhetsanalysen måste normalt genomföras innan ett konstruktionsarbete påbörjas. Det är organisationsenheten som ansvarar för att genomföra sårbarhetsanalysen.

[179] Punkten 3 i ikraftträdande- och övergångsbestämmelser till Försvarsmaktens interna bestämmelser om säkerhetsskydd.

5.5.4. Sårbarhetsbedömning

Moment 5:17 *Om ett utrymme för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre avses användas vid organisationsenheten, ska en sårbarhetsbedömning genomföras. En begäran om sårbarhetsbedömning ska göras till underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2).*

5.5.5. Samråd

Moment 5:18 *Efter att en sårbarhetsbedömning enligt moment 5:17 har genomförts ska organisationsenheten begära samråd med säkerhetsskyddsavdelningen vid Must. Ett samråd ska inhämtas:*

a) Innan ett konstruktionsarbete påbörjas av ett befintligt eller ett nytt utrymme.

b) Innan ett godkännande av ett befintligt eller ett nytt utrymme, i det fall ett konstruktionsarbete inte kommer att genomföras.

Moment 5:19 *En begäran om samråd ska innehålla:*

a) Beskrivning av den säkerhetskänsliga verksamhet som ska använda utrymmet.

b) Vilka typer av säkerhetsskyddsklassificerade uppgifter som ska behandlas i utrymmet.

c) Den verksamhetsansvariges hotbild för den egna säkerhetskänsliga verksamheten.

d) Bedömda sårbarheter för utrymmet och dess omgivning. Resultat från sårbarhetsbedömning beställd av underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2) ska bifogas.

e) Vilka åtgärder som har identifierats i sårbarhetsanalysen enligt moment 5:16 och hur dessa kommer att uppfyllas.

f) Situationsplan för byggnaden och dess omgivning.

g) Vilken teknisk utrustning och inventarier som ska finnas i utrymmet.

Vägledande förklaring: Med typer av säkerhetsskyddsklassificerade uppgifter i punkten b avses en övergripande beskrivning av uppgifterna, t.ex. försvarsplanering.

Samråd görs för att undvika kostsamma investeringar i utrymmen som inte kommer att kunna godkännas.

5.5.6. Krav på utrymmen

Moment 5:20 *Ett utrymme som är avsett att användas för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell eller högre, ska uppfylla följande krav.*

a) Utrymmet ska vara placerat i en administrativ zon. Om utrymmet är avsett för delgivning av kvalificerat hemliga uppgifter ska utrymmet vara en säkerhetszon.

b) Utrymmet ska vara larmat.

c) För att reducera möjligheter till obehörig avlyssning ska administrativa-, fysiska- och tekniska åtgärder vidtas. Åtgärderna ska dokumenteras.

d) En förteckning över vilka personer som är behöriga till utrymmet ska upprättas.

e) Utrymmet ska vara försett med loggning på personnivå över vilken behörig personal som har haft tillträde till utrymmet.

f) Det ska i utrymmet finnas en förteckning över vilken teknisk utrustning som får finnas i, eller som får medföras in i utrymmet.

g) Det ska i utrymmet finnas en förteckning över vilken inredning som får finnas i, eller som får medföras in i utrymmet.

h) Personal som ska vara behörig till utrymmet ska vara utbildade i bestämmelser och rutiner kring användning av utrymmet och dess säkerhetsskydd.

5.5.7. Beslut om godkännande

”Enligt 5 kap. 20 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd ska myndigheten besluta vilka utrymmen som är godkända för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell eller högre.

Chef för organisationsenhet, eller den chef för organisationsenhet bestämmer, fattar sådana beslut avseende utrymmen inom egen organisationsenhet.”

4 kap. 9 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Beslut om vilka utrymmen som är godkända för regelbunden muntlig delgivning, och uppgifter om dess placering, är normalt en uppgift som omfattas av sekretess enligt 18 kap. 8 § OSL och är en säkerhetsskyddsklassificerad uppgift. Underlag som tas fram i arbetet inför ett beslut (planer, hemställan etc.) måste därför ges erforderligt säkerhetsskydd redan från arbetets start.

Moment 5:21 *Efter beslut om godkännande har fattats ska hemställan om tekniskt säkerhetsskyddsundersökning tillställas underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2).*

Vägledande förklaring: En teknisk säkerhetsskyddsundersökning (TSU) innefattar att man ser över såväl tekniska förhållanden som administrativa rutiner, utbildning och hantering av utrymmet. Därför genomförs TSU så snart som möjligt efter att utrymmet är godkänt och taget i drift.

5.5.8. Kontroll av utrymmen för muntlig delgivning

Moment 5:22 *Utrymmen som har godkänts för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell och högre, ska regelbundet kontrolleras. Sådana kontroller ska även genomföras efter ett obehörigt intrång eller misstanke om sådant intrång.*

Vägledande förklaring: Kontroll av ett utrymme syftar till att upprätthålla utrymmets säkerhetsskydd över tid och förhindra eller upptäcka möjlighet till, eller faktisk påverkan av utrymmets skydd mot obehörig avlyssning.

Kontroll är en del i det regelbundna säkerhetsskyddsarbetet och innebär att systematiskt undersöka integriteten i utrymmets säkerhetsskydd. Ju högre säkerhetsskyddsklass som ett utrymme är godkänt för, desto tätare och mer ingående bör genomförandet av kontrollen vara.

Kontroll av godkända utrymmen bör finnas som ett avsnitt i den interna kontrollplanen. Periodicitet för kontroll av godkända utrymmen bör identifieras i en säkerhetsskyddsplan eller en särskild säkerhetsskyddsplan. För varje godkänt utrymme bör det finnas en lista med vad som ska kontrolleras och som används för att dokumentera en kontroll.

Exempel på kontrollpunkter är:

- Utformningen av säkerhetsskyddet för utrymmet.
- Utformningen av rutiner för användning av utrymmet.
- Utrymmets inre och yttre omslutningsytor och deras fysiska skick och integritet.
- Inredning och teknisk utrustning i utrymmet.
- Behörigheter för tillträde till utrymmet.

Om brister upptäcks vid en kontroll måste korrigerande åtgärder vidtas samt vid behov även säkerhetsrapport upprättas.

En kontroll av utrymmen för muntlig delgivning är inte sådana kontroller som beskrivs i kapitel 9 om kontroll av säkerhetsskydd.

5.5.9. Muntlig delgivning i högst säkerhetsskyddsklass begränsat hemlig

Moment 5:23 *Innan ett utrymme används för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter i högst säkerhetsskyddsklass begränsat hemlig ska följande beaktas.*

a) Utrymmets utformning och placering.

b) Vilken teknisk utrustning som finns i, eller får medföras in i utrymmet.

c) Den tekniska utrustningens möjlighet till kommunikation med omvärlden.

Vägledande förklaring: I organisationsenhetens instruktion för fysisk säkerhet (avsnitt 5.2) bör det framgå vilka byggnader eller utrymmen där det inte är lämpligt att genomföra regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är begränsat hemliga.

5.6. Skydd för it-utrymmen

”I bilaga 1 till denna författning anges de krav som gäller för respektive skyddsnivå. It-utrymmen ska uppfylla de krav som gäller för skyddsnivå 2, 3 eller 4.”

5 kap. 21 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: It-utrymmen där säkerhetsskyddsklassificerade uppgifter behandlas eller där säkerhetskänslig verksamhet bedrivs ska delas in i skyddsnivå 2-4. Ju kraftigare konstruerat it-utrymmet är, och därmed dess sammanhängande förmåga att motstå angrepp, desto högre skyddsnivå har det. Ju högre säkerhetsskyddsklass desto kraftigare konstruerat it-utrymme, d.v.s. en högre skyddsnivå.

”Om det i it-utrymmen behandlas uppgifter som är placerade i säkerhetsskyddsklassen begränsat hemlig ska it-utrymmena uppfylla de krav som gäller för skyddsnivå 2.

Om det i it-utrymmen behandlas uppgifter som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig ska it-utrymmena uppfylla de krav som gäller för skyddsnivå 3 samt förses med larm.

Om det i it-utrymmen behandlas uppgifter som är placerade i säkerhetsskyddsklassen kvalificerat hemlig ska it-utrymmena uppfylla de krav som gäller för skyddsnivå 4 samt förses med larm.”

5 kap. 22 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Syftet med detektionskravet är att få vetskap om någon aktör har försökt eller gett sig tillgång till de säkerhetsskyddsklassificerade uppgifterna. Skyddsåtgärderna kan variera beroende på t.ex. på utrymmets placering och om det finns en särskild avdelad styrka som kan göra en insats. Det kan även vara en

teknisk funktion som säkerställer att inga säkerhetsskyddsklassificerade uppgifter behandlas i it-utrymmet vid detektion.

Vid detektion av intrång i ett it-utrymme som är försett med larm vidtas de skyddsåtgärder som i förväg har beslutats.

”It-utrymmen ska förses med ett system för inpassering. Av systemet ska det framgå när och vem som har haft tillträde till utrymmet samt andra händelser som är av betydelse för säkerheten.”

5 kap. 23 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Syftet med bestämmelsen är att ha kontroll över tillträde till, och därmed även verksamhet i, utrymmen och lokaler som innehåller tele- och dataväxlar, korskopplingar, dataservrar och motsvarande installationer. Med begreppet system för inpassering menas ett passagekontrollsystem som medger säkerhetsloggning av tillträde. Passagekontrollsystemet bör monteras i anslutning till den eller de dörrar som leder in till utrymmena eller lokalerna. Alla som besöker it-utrymmet bör se till att de antingen loggas i systemet eller på annat sätt. Det är lämpligt att loggarna analyseras.

Det är lämpligt att det även finns en manuell lista för loggning av besökare i de fall dessa inte loggas digitalt. För it-utrymmen som inte är försedda med tekniskt system för inpasseringskontroll får inpasseringskontrollen inte begränsas till en besöksliggare som ifylls av besökaren själv. Om en besöksliggare måste användas är det viktigt att det är en annan person som säkerställer att de som ska ges tillträde har rätt identitet och är behöriga att komma in i it-utrymmet.

Exempel på andra händelser kan vara passage med nyckel och misslyckade passager.

I moment 5:1 framgår att beslut om tillträde ska innefatta it-utrymmen.

”Ett it-utrymme där säkerhetskänslig verksamhet bedrivs där en inträffad skada kan vara mer än inte obetydlig för Sveriges säkerhet, ska uppfylla de krav som gäller för skyddsnivå 3 samt förses med larm.”

5 kap. 24 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Bestämmelsen tar sikte på it-utrymmen där det inte behandlas säkerhetsskyddsklassificerade uppgifter, men där det bedrivs säkerhetskänslig verksamhet (med krav på tillgänglighet och riktighet). Det handlar om skydd för säkerhetskänsliga informationssystem, dvs. system som har ett skyddsvärde av andra

skäl, t.ex. elektroniska kommunikationsnät eller system för styrning av kraftförsörjning.[180]

Moment 5:24 *Ett it-utrymme där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan medföra en skada för Sveriges säkerhet som inte är obetydlig, ska uppfylla de krav som gäller för skyddsnivå 3 samt förses med larm.*

Vägledande förklaring: Bestämmelsen utökar kravet i 5 kap. 24 § Försvarsmaktens föreskrifter om säkerhetsskydd till att omfatta all säkerhetskänslig verksamhet oavsett vilken skada som kan inträffa i utrymmet.

Moment 5:25 *Ett it-utrymme där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan vara ringa för Sveriges säkerhet ska uppfylla de krav som gäller för skyddsnivå 2.*

5.6.1. Beslut om avvikelse för skydd av it-utrymmen

”Myndigheten får fatta beslut som avviker från 21–22 och 24 §§ under förutsättning att motsvarande skyddsnivå kan upprätthållas. Beslutet ska dokumenteras.”

5 kap. 25 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Om ett it-utrymme inte uppfyller krav för den skyddsnivå som gäller för utrymmet eller inte kan förses med larm, kan utrymmet ändå få användas om åtgärder vidtas för att upprätthålla motsvarande skydd. Sådana åtgärder kan framgå i säkerhetsskyddsplaneringen. Åtgärderna kan t.ex. vara personell bevakning samt placering och närhet till en särskilt avdelad styrka.

”Chef för organisationsenhet får besluta om sådana avvikelser.”

4 kap. 13 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Ett beslut om avvikelse från 5 kap. 21-22 och 24 §§ Försvarsmaktens föreskrifter om säkerhetsskydd kan framgå av organisationsenhetens säkerhetsskyddsplan eller en särskild säkerhetsskyddsplan. I planen måste det framgå att det är fråga om en sådan avvikelse. Åtgärder för att upprätthålla motsvarande skydd måste också anges i planen.

5.7. Transporter

”En myndighet ska besluta hur transporter av säkerhetsskyddsklassificerade handlingar och lagringsmedier ska genomföras. Beslutet ska dokumenteras.”

3 kap. 26 § Försvarsmaktens föreskrifter om säkerhetsskydd

[180] Prop. 2017/18:89 s. 70.

Vägledande förklaring: Skyddsåtgärderna behöver anpassas efter hur stor mängd handlingar och lagringsmedier som ska transporteras, deras placering i säkerhetsskyddsklass, var transporten går och förhållanden under transporten.

Med transport avses inte medförande (avsnitt 3.19) eller distribution (avsnitt 3.10).

Med skyddad transport avses i detta reglemente en sådan transport av säkerhetsskyddsklassificerade handlingar, lagringsmedier eller säkerhetskänslig materiel som vid varje transporttillfälle ska vara anpassad till det särskilda skydd som krävs enligt den särskilda säkerhetsskyddsanalys som ska göras (moment 5:26). Skyddad transport används när analysen visar att mängden handlingar, lagringsmedier eller materiel är sådan att distribution på annat sätt inte är lämplig ur säkerhetsskyddssynpunkt och därför inte får ske.

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, beslutar hur sådana transporter ska genomföras. Säkerhetsskyddschefen, eller den säkerhetsskyddschefen bestämmer, beslutar även hur transporter av säkerhetskänslig materiel ska genomföras.”

4 kap. 11 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 5:26 En *organisationsenhet som avser att sända säkerhetsskyddsklassificerade handlingar, lagringsmedier eller säkerhetskänslig materiel ska göra en särskild säkerhetsskyddsanalys för att fastställa transportnivå för den aktuella transporten. Innan en sådan transport genomförs ska säkerhetsskyddsanalysen granskas och godkännas av organisationsenhetens säkerhetschef eller den säkerhetschefen bestämmer.*

Vägledande förklaring: I den särskilda säkerhetsskyddsanalysen måste hänsyn tas till mängden säkerhetsskyddsklassificerade handlingar, lagringsmedier och säkerhetskänslig materiel.

Vissa fordon och transporter kan i sig beslutas vara skyddsobjekt.

Moment 5:27 *En skyddad transport för säkerhetsskyddsklassificerade handlingar, lagringsmedier och säkerhetskänslig materiel ska placeras i någon av följande transportnivåer.*

a) ***Transportnivå 1*** *gäller för transport av säkerhetsskyddsklassificerade handlingar som är placerad i säkerhetsskyddsklassen begränsat hemlig, samt för transport av en ringa mängd säkerhetskänslig materiel.*

   Transportutrymmet ska vara låst och skyddat mot insyn. En internationell vägtransport ska ha följebil.

b) ***Transportnivå 2*** *gäller för transport av en mindre mängd säkerhetsskyddsklassificerade handlingar som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig eller ringa mängd kvalificerat hemlig, samt för transport av en mindre mängd säkerhetskänslig materiel.*

Transporten ska utföras med

- *tillträdesskyddad container eller ett annat transportutrymme av motsvarande standard, eller*
- *vapenlåda med larm, eller*
- *transportutrymme som är låst och skyddat mot insyn.*

En vägtransport ska ha följebil.

c) ***Transportnivå 3*** *gäller för transport av en större mängd säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig eller mindre mängd kvalificerat hemlig. Transportnivå 3 gäller även för transport av en större mängd säkerhetskänslig materiel.*

Transporten ska utföras med

- *tillträdesskyddad container som är utrustad med fjärröverfört larm eller ett annat transportutrymme av motsvarande standard som är utrustat med fjärröverfört larm, eller*
- *tillträdesskyddad container som åtföljs av en följebil eller ett annat transportutrymme av motsvarande standard som åtföljs av en följebil, eller*
- *låst transportutrymme som är skyddat från insyn och som åtföljs av en transportskyddsstyrka.*

En internationell vägtransport ska ha följebil.

Personsäkerhetslarm ska medföras i det fordon som transporterar säkerhetsskyddsklassificerade handlingar, lagringsmedier eller säkerhetskänslig materiel. Personsäkerhetslarm ska också medföras av transportskyddsstyrka och i följebil, om sådana används.

d) ***Transportnivå 4*** *gäller för transport av mycket stora mängder säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig samt för transport av en större mängd säkerhetsskyddsklassificerade handlingar som är placerade i säkerhetsskyddsklassen kvalificerat hemlig. Transportnivå 4 gäller även för transport av mycket stora mängder säkerhetskänslig materiel.*

Transporten ska utföras med

- *tillträdesskyddad container som är utrustad med fjärröverfört larm eller ett annat transportutrymme av motsvarande standard som är utrustat med fjärröverfört larm, eller*
- *tillträdesskyddad container som åtföljs av en transportskyddsstyrka eller ett annat transportutrymme av motsvarande standard som åtföljs av en transportskyddsstyrka, eller*
- *låst transportutrymme som är skyddat från insyn och som åtföljs av polis eller av minst två transportskyddsstyrkor.*

Vägtransport i transportnivå 4 ska ha följebil.

Personsäkerhetslarm ska medföras i det fordon som transporterar säkerhetsskyddsklassificerade handlingar, lagringsmedier eller säkerhetskänslig materiel i transportnivå 4. Personsäkerhetslarm ska också medföras av transportskyddsstyrka och i följebil.

Moment 5:28 *Inför en skyddad transport i transportnivå 2-4 ska den organisationsenhet som ansvarar för att planera transporten upprätta en särskild säkerhetsskyddsplan.*

Moment 5:29 *Innan en skyddad transport i transportnivå 2-4 påbörjas, ska den organisationsenhet som organiserar transporten informera mottagaren av godset, berörda polisregioner och berörda regionala staber om att transporten ska genomföras.*

Moment 5:30 *Vid en skyddad transport ska om möjligt nycklar eller koder till förvaringsutrymmen som ingår i transporten skickas till mottagaren i en separat försändelse. Om nycklar eller koder inte kan skickas till mottagaren i en separat försändelse, ska de under transporten vara under kontroll av personal i följebil, transportskyddsstyrkan eller transportfordonet.*

Moment 5:31 *Vid uppehåll under transporten ska det skydd som gäller för transporten upprätthållas.*

Vägledande förklaring: Ett längre uppehåll måste i första hand förläggas till Försvarsmaktens skyddsobjekt. I andra hand får uppehållet förläggas till ett annat militärt område, anläggning eller objekt som är inhägnat och bevakat, under förutsättning att transportutrymmet är utrustat med fjärröverfört larm eller är under kontroll av en skyddsstyrka som är utrustad med personsäkerhetslarm.

Om uppehållet inte kan förläggas till Försvarsmaktens skyddsobjekt, annat militärt område, anläggning eller objekt får uppehållet förläggas till ett annat obevakat område, anläggning eller objekt. Transportutrymmet måste i sådant fall vara utrustat med fjärröverfört larm och stå under kontroll antingen av en skyddsstyrka som är utrustad med personsäkerhetslarm eller av polis.

REGLEMENTE

Inom Sverige är normalt ett militärt område, en anläggning eller ett objekt beslutade vara skyddsobjekt enligt skyddslagen (2010:305). Med ett annat militärt område, anläggning eller objekt avses t.ex. områden, anläggningar och objekt utanför Sverige.

6. Säkerhetsprövning

”Personalsäkerhet ska
1. förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig, och
2. säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd.”

2 kap. 4 § säkerhetsskyddslagen

Vägledande förklaring: Personalsäkerhet är aktuell dels vid deltagande i verksamheter där tillgång ges till säkerhetsskyddsklassificerade uppgifter, dels i verksamheter som av annan anledning är säkerhetskänsliga, exempelvis deltagande i verksamhet vid ett skyddsobjekt.[181]

Detta kapitel beskriver endast säkerhetsprövning. Utbildning och övning beskrivs i kapitel 7.

6.1. Grunder

”Den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas.”

3 kap. 1 § första meningen säkerhetsskyddslagen

Vägledande förklaring: Av 3 kap. 1 § säkerhetsskyddslagen följer att Försvarsmaktens personal[182] och andra som deltar i Försvarsmaktens säkerhetskänsliga verksamhet ska säkerhetsprövas. En säkerhetsprövning ska genomföras oavsett om deltagandet är placerat i säkerhetsklass eller inte. Säkerhetsprövningen ska anpassas till den säkerhetskänsliga verksamhet som avses oavsett vilken typ av deltagande som det gäller (t.ex. anställning, säkerhetsskyddad upphandling, utbildning, utbytes- eller växeltjänstgöring, praktik eller militära befattningar såsom värnpliktig och hemvärnsoldat).

”Säkerhetsprövningen syftar till att klarlägga om en person kan antas vara lojal mot de intressen som skyddas i denna lag och i övrigt pålitlig från säkerhetssynpunkt. Vid säkerhetsprövningen ska sådana omständigheter beaktas som kan antas innebära sårbarheter i säkerhetshänseende.”

3 kap. 2 § säkerhetsskyddslagen

[181] Prop. 2017/18:89 s. 139.
[182] Försvarsmaktens personal definieras i förordningen om Försvarsmaktens personal.

Vägledande förklaring: Säkerhetsprövning handlar ytterst om att bedöma om en person har tillräckliga förutsättningar och personlig lämplighet att genom anställning eller på annat sätt delta i säkerhetskänslig verksamhet. En helhetsbedömning ska göras som baseras på ett allsidigt underlag och som tydligt relateras till verksamheten och anställningen.[183]

Utifrån ett riskreduceringsperspektiv kan olika krav ställas på lojalitet, pålitlighet och sårbarhet. Detta kan t.ex. innebära att en individ kan placeras på en befattning i säkerhetsklass trots att en viss sårbarhet och vissa brister i lojalitet och pålitlighet finns, men att dessa kan hanteras med andra skyddsåtgärder. Det kan även innebära att en person inte tillåts delta i den säkerhetskänsliga verksamheten, t.ex. om levnadsbakgrund inte kan klargöras eller om deltagandet överför en alltför stor sårbarhet till individen.

”Säkerhetsprövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas och ska innefatta en grundutredning samt registerkontroll och särskild personutredning i den omfattning som anges i 13, 14 och 17 §§. Om det finns särskilda skäl får säkerhetsprövningen göras mindre omfattande.

Säkerhetsprövningen ska följas upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.”

3 kap. 3 § säkerhetsskyddslagen

Vägledande förklaring: Särskilda skäl kan avse om den som prövningen handlar om redan tidigare har prövats på motsvarande sätt och ytterligare utredning därför inte bedöms kunna tillföra något nytt i sak (avsnitt 6.8.8 och avsnitt 6.9.10).[184]

I avsnitt 6.8 finns mer information om grundutredning och i avsnitt 6.11 beskrivs uppföljning av säkerhetsprövning.

Säkerhetsprövningsprocessen beskrivs som ett flödesschema i bild 6.1.

En säkerhetsprövning inleds alltid med en grundutredning. Denna består som minst av en säkerhetsprövningsintervju, kontroll av betyg och intyg samt referenstagning. Grundutredningen kan även kompletteras med ytterligare åtgärder och information.

Efter genomförd grundutredning ska en sammanfattande bedömning göras av det som framkommit. Organisationsenheten ska bedöma om personen uppfyller kraven för en godkänd säkerhetsprövning eller inte. Om personen inte bedöms uppfylla kraven för en godkänd säkerhetsprövning så avslutas säkerhetsprövningsprocessen.

[183] Prop. 2017/18:89 s. 143.
[184] Prop. 2017/18:89 s. 144.

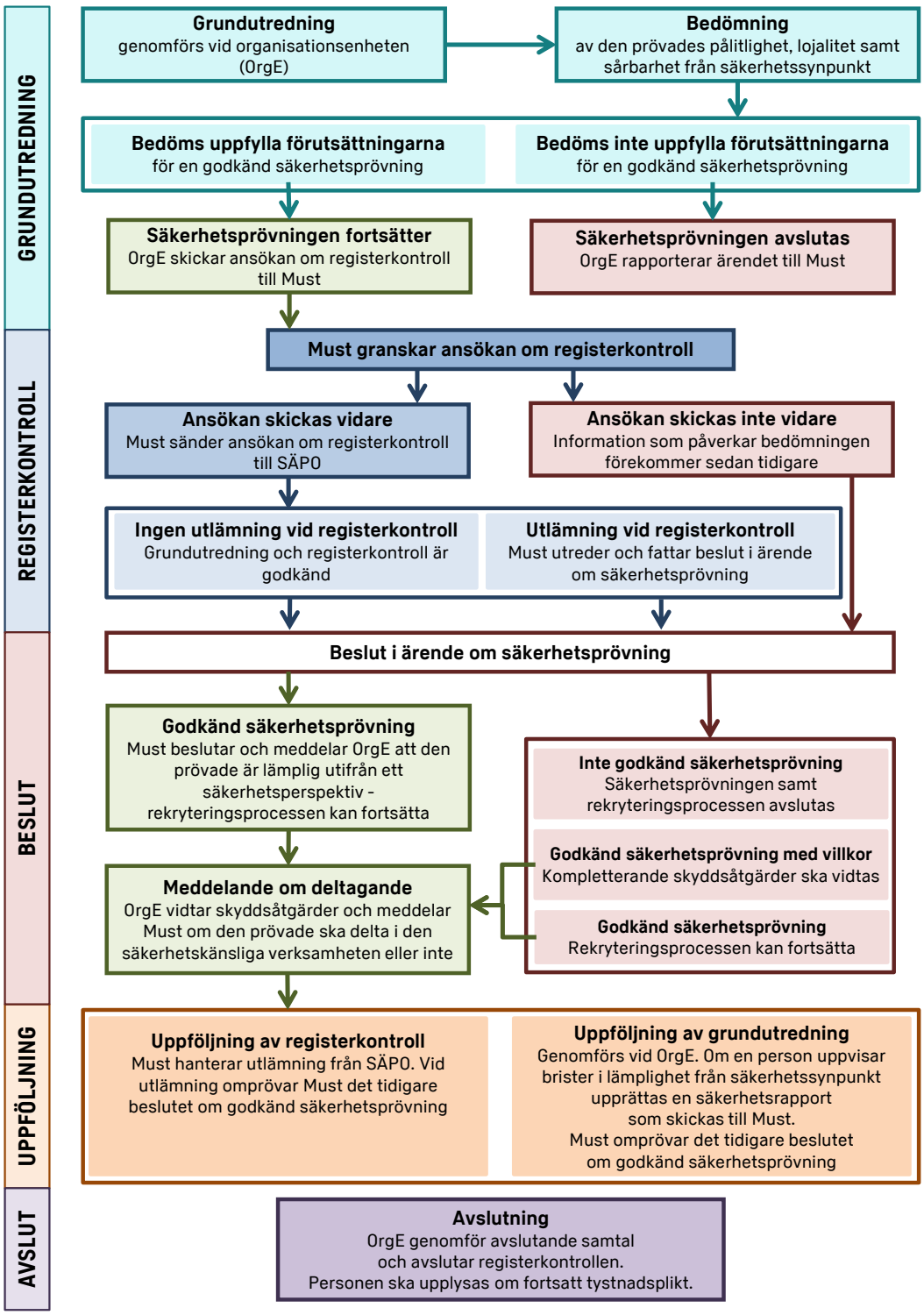


Bild 6.1. Flödesschema för säkerhetsprövningsprocessen. Maria Lind och Sanna Jonsson/Försvarsmakten

Om personen bedöms uppfylla kraven för en godkänd säkerhetsprövning och befattningen är placerad i säkerhetsklass ska en ansökan om registerkontroll skickas till

säkerhetsprövningssektionen. Om befattningen är placerad i säkerhetsklass 1 eller 2 ingår även en särskild personutredning.[185] För det fall befattningen inte är placerad i säkerhetsklass ska i stället en ansökan om deltagande i säkerhetskänslig verksamhet skickas till säkerhetsprövningssektionen.

Efter genomförd registerkontroll ska ett beslut i ärende om säkerhetsprövning fattas. Beslutet fattas vid säkerhetsprövningssektionen och kan hanteras på två sätt, via ett meddelande i registerkontrollrutinen eller genom ett skriftligt beslut. Organisationsenheten ska sedan vidta eventuella skyddsåtgärder samt meddela säkerhetsprövningssektionen om personen kommer att delta i den säkerhetskänsliga verksamheten eller inte.

Om personen, efter beslut om godkänd säkerhetsprövning, har påbörjat deltagande i den säkerhetskänsliga verksamheten fortsätter säkerhetsprövningen genom att organisationsenheten följer upp personen. Detta genomförs bl.a. genom daglig uppföljning i verksamheten och uppföljande samtal. Registerkontrollen genomförs även löpande under tiden för deltagandet. Om det finns anledning att anta att personen inte längre uppfyller kraven för en godkänd säkerhetsprövning, kan det tidigare beslutet om godkänd säkerhetsprövning omprövas.

När en person avslutar sitt deltagande i den säkerhetskänsliga verksamheten ska säkerhetsprövningen avslutas. Detta görs genom ett avslutande samtal samt en påminnelse om fortsatt tystnadsplikt.

6.2. Befattningsanalys

> *”Myndigheten ska analysera vilka anställningar samt annat deltagande i myndighetens säkerhetskänsliga verksamhet som ska placeras i säkerhetsklass, samt vilket övrigt deltagande i den säkerhetskänsliga verksamheten som endast ska vara föremål för säkerhetsprövning. Myndigheten ska därvid särskilt beakta 3 kap. 10 § säkerhetsskyddslagen (2018:585).*
>
> *Myndigheten ska vidare utgå från myndighetens säkerhetsskyddsanalys och särskilt beakta förekomsten av internationella åtaganden om säkerhetsskydd. Av analysen ska skälet till placering i säkerhetsklass framgå.*
>
> *Analysen ska dokumenteras.”*
>
> 6 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: En analys av den säkerhetskänsliga verksamheten utifrån ett befattningsperspektiv är grunden till säkerhetsprövning. Med *befattning* avses i säkerhetsprövningssammanhang anställningar, annat deltagande i Försvarsmaktens säkerhetskänsliga verksamhet samt sådana aktiviteter som ger tillgång till Försvarsmaktens säkerhetskänsliga verksamhet eller säkerhetsskyddsklassificerad information. Befattningsanalysen omfattar därmed även befattningar som avser deltagande i

[185] 3 kap. 17 § säkerhetsskyddslagen.

säkerhetskänslig verksamhet och som ingår i en säkerhetsskyddad upphandling (avsnitt 6.17.1 och kapitel 8).

> *”I 6 kap. 3 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd finns bestämmelser om analys av anställningar och annat deltagande i säkerhetskänslig verksamhet (befattningsanalys).*
>
> *Varje organisationsenhet ska genomföra en befattningsanalys som ska utgå från organisationsenhetens säkerhetsskyddsanalys. Befattningsanalysen ska uppdateras när en anställning eller ett deltagande i säkerhetskänslig verksamhet tillkommer vid enheten eller väsentligen ändras.*
>
> *Försvarsmaktens säkerhetsskyddschef får besluta närmare bestämmelser om hur en sådan befattningsanalys ska genomföras.”*
>
> 5 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Befattningsanalysen ska ingå som en del av säkerhetsskydds- och verksamhetsskyddsplaneringen (kapitel 2). Det är den organisationsenhet som ansvarar för verksamheten som ansvarar för att en befattningsanalys genomförs.

Moment 6:1 *Vid frivillig försvarsverksamhet ska en befattningsanalys genomföras av den organisationsenhet som stödjer verksamheten genom t.ex. utlåning av lokaler, materiel eller instruktörer.*

Vägledande förklaring: Om man i befattningsanalysen kommer fram till att den frivilliga försvarsverksamheten deltar i Försvarsmaktens säkerhetskänsliga verksamhet, ansvarar organisationsenheten för att säkerhetsprövning och i förekommande fall registerkontroll genomförs. Ett sådant exempel är Grundläggande soldatutbildning för frivillig personal (GU-F).

Moment 6:2 *Befattningsanalysen ska genomföras utifrån olika säkerhetslägen, dvs. fred, höjd beredskap och krig.*

Moment 6:3 *Befattningsanalysen ska även innefatta befattningar där personerna krigsplaceras.*

Moment 6:4 *Av befattningsanalysen ska säkerhetsklass och grunden för placering i säkerhetsklass framgå för varje befattning.*

Vägledande förklaring: Avsikten med befattningsanalysen är att komma fram till om befattningen innebär deltagande i säkerhetskänslig verksamhet och vilken säkerhetsklass som kan vara aktuell. Den genomförs även för att komma fram till om verksamheten kan skyddas på något annat sätt än genom placering i säkerhetsklass, t.ex. genom åtgärder inom fysisk säkerhet (såsom att begränsa tillträde inom en byggnad) och informationssäkerhet (såsom behörighetskontroll i informationssy-

stem).[186] Vid osäkerhet om vilken säkerhetsklass som en befattning ska placeras i bör den lägre säkerhetsklassen väljas.

Det bör observeras att en person får ta del av säkerhetsskyddsklassificerade uppgifter upp till nivån begränsat hemlig utan att befattningen behöver vara placerad i säkerhetsklass. Detsamma gäller om en person, till följd av sitt deltagande i verksamheten, endast har möjlighet att orsaka en ringa skada för Sveriges säkerhet.

Om en krigsplacering ställer särskilda krav, t.ex. att befattningen bör placeras i en högre säkerhetsklass, ska befattningsanalysen svara på om en sådan placering kan genomföras vid t.ex. höjd beredskap, eller om vissa befattningar ska placeras i en högre säkerhetsklass även i fredstid. Likaså ska befattningsanalysen även genomföras för befattningar i krigsorganisationen som i fredstid inte är bemannade. I sådana fall ska analysen svara på om säkerhetsprövningen kan genomföras vid höjd beredskap, eller om vissa befattningar ska omfattas av säkerhetsprövning även i fredstid. Särskild hänsyn ska tas till om säkerhetsskyddet kan uppnås via andra skyddsåtgärder än placering i säkerhetsklass.

Vid en befattningsanalys är det viktigt att identifiera sådana säkerhetsskyddsvärden som den egna verksamheten är beroende av, men som den verksamhetsansvarige själv (t.ex. chef för en organisationsenhet) inte ansvarar för. Det vill säga att befattningsinnehavaren får tillgång till säkerhetsskyddsvärden som ägs eller ansvaras för av någon annan än den egna organisationsenheten. Det kan t.ex. röra sig om tillträde eller tillgång till en annan organisationsenhets anläggningar, system eller funktioner, eller kontinuerligt deltagande i internationell verksamhet på uppdrag av en annan organisationsenhet. Av denna anledning ska samtliga befattningar i Försvarsmaktens verksamhet analyseras, även om säkerhetsskyddsanalysen kommit fram till att vissa verksamheter inte bedriver säkerhetskänslig verksamhet.

Slutligen ska befattningsanalysen även ta hänsyn till om befattningen innefattar internationella säkerhetsskyddsåtaganden (avsnitt 1.7.4), som t.ex. internationell tjänstgöring, eller tillgång till uppgifter som Sverige genom säkerhetsskyddsavtal har åtagit sig att skydda.[187]

Moment 6:5 *När en organisationsenhet har uppdaterat en befattningsanalys ska den sändas till säkerhetsprövningssektionen vid Must.*

Moment 6:6 *När en befattningsanalys har uppdaterats ska organisationsenheten säkerställa att de personer, som enligt analysen har en befattning som är placerad i säkerhetsklass, är registerkontrollerade för den säkerhetsklassen.*

Vägledande förklaring: Av 6 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd följer att befattningsanalysen måste uppdateras om en organisationsenhet får en ny befattning eller om befattningens innehåll väsentligen förändras. Den nya befattningsanalysen ska sändas till säkerhetsprövningssektionen, innan säkerhetspröv-

[186] 3 kap. 10 § säkerhetsskyddslagen.
[187] Prop. 2017/18:89 s. 46

ningen av personen som ska placeras på befattningen inleds. Detta sker genom att *Förteckning befattningsanalys* skickas in på nytt.

> *”Varje organisationsenhet ska med grund i befattningsanalysen lämna förslag till militära underrättelse- och säkerhetstjänsten i Högkvarteret på vilka anställningar och annat deltagande i säkerhetskänslig verksamhet vid den egna enheten som*
>
> *1. ska placeras i säkerhetsklass,*
>
> *2. ska bemannas av personer som ska vara föremål för säkerhetsprövning utan registerkontroll, eller*
>
> *3. endast ska vara föremål för registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen (2018:585).”*
>
> 5 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: När organisationsenheten har genomfört befattningsanalysen ska ett förslag enligt 5 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd sändas till säkerhetsprövningssektionen.

Moment 6:7 *Vid redovisning av en befattningsanalys ska dokumentmallen* Förteckning befattningsanalys *användas.*

Vägledande förklaring: Dokumentmallen fås av säkerhetsprövningssektionen, och sänds in via IS UNDSÄK.

6.2.1. Säkerhetsklasser

Vilken säkerhetsklass som en anställning eller något annat deltagande i säkerhetskänslig verksamhet ska placeras i, är beroende av i vilken utsträckning en person i sin befattning tar del av säkerhetsskyddsklassificerade uppgifter, vilken säkerhetsskyddsklass uppgifterna är placerade i och vilken möjlighet personen har att, genom sitt deltagande i verksamheten, orsaka skada för Sveriges säkerhet.

En anställning eller något annat deltagande i säkerhetskänslig verksamhet placeras i säkerhetsklass enligt villkoren i 3 kap. 6-8 §§ säkerhetsskyddslagen. Villkoren framgår i tabell 6.1.

En befattning ska inte placeras i säkerhetsklass om den anställde eller den som på annat sätt deltar i verksamheten får del av uppgifter i säkerhetsskyddsklassen *begränsat hemlig*, eller till följd av sitt deltagande i verksamheten endast har möjlighet att orsaka en *ringa skada* för Sveriges säkerhet. I detta fall ska personen genomgå säkerhetsprövning men inte vara föremål för registerkontroll. Personer, som genom anställning eller annat deltagande i Försvarsmaktens verksamhet, endast kommer att ta del av *sekretessklassificerade* uppgifter (avsnitt 3.1.1) ska endast säkerhetsprövas om personen i övrigt kommer att delta i säkerhetskänslig verksamhet.

Tabell 6.1. Säkerhetsklasser enligt villkoren i 3 kap. 6-8 §§ säkerhetsskyddslagen.

Säkerhetsklass	Får del av säkerhetsskyddsklassificerade uppgifter	Till följd av deltagande i verksamheten har möjlighet att orsaka skada för Sveriges säkerhet
1	I en omfattning som *inte är ringa* får del av uppgifter i säkerhetsskyddsklassen *kvalificerat hemlig*.	*Synnerligen allvarlig* skada
2	I *ringa omfattning* får del av uppgifter i säkerhetsskyddsklassen *kvalificerat hemlig*. I en *omfattning som inte är ringa* får del av uppgifter i säkerhetsskyddsklassen *hemlig*.	*Allvarlig* skada
3	I *ringa omfattning* får del av uppgifter i säkerhetsskyddsklassen *hemlig*. Får del av uppgifter i säkerhetsskyddsklassen *konfidentiell*.	*Inte obetydlig* skada
Ingen säkerhetsklass	Får endast del av uppgifter i säkerhetsskyddsklassen *begränsat hemlig*.	*Ringa* skada

Även om strävan är att placera befattningarna i så låg säkerhetsklass som möjligt, ska hänsyn tas till den säkerhetskänsliga verksamhetens betydelse. Om en person som genom en befattning har tillträde till en anläggning har säkerhetsprövats med registerkontroll för skyddet mot terrorism, enligt tidigare säkerhetsskyddslagstiftning, ska befattningen nu normalt placeras i säkerhetsklass 3.

En placering i högre säkerhetsklass kan vara motiverad om ett deltagande i en verksamhet innebär att en person behöver anförtros tillgång till vissa anläggningar eller system av kritisk betydelse för landets grundläggande funktioner, exempelvis elförsörjning.[188]

6.2.2. Beslut om placering i säkerhetsklass 1

> *”Regeringen beslutar om placering i säkerhetsklass om inget annat anges i 8–12 §§.”*
>
> 5 kap. 6 § säkerhetsskyddsförordningen

[188] Prop. 2017/18:89 s. 147.

”Om en kommun, ett landsting eller en sådan myndighet som anges i 8 eller 11 § bedömer att det finns behov av att placera en anställning eller annat deltagande i säkerhetsklass 1, ska myndigheten, kommunen eller landstinget begära att regeringen beslutar om en sådan placering.”

5 kap. 7 § första meningen säkerhetsskyddsförordningen

”Kommuner, landsting och de myndigheter som anges i bilagan till denna förordning beslutar om

1. placering i säkerhetsklass 2 och 3 i fråga om anställning eller annat deltagande i den egna verksamheten, och

2. placering i säkerhetsklass 2 och 3 i fråga om anställning eller uppdrag hos en leverantör som de har ingått ett säkerhetsskyddsavtal enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585) med.”

5 kap. 8 § första stycket säkerhetsskyddsförordningen

”Försvarsmaktens säkerhetsskyddschef bemyndigas att hos regeringen, i enlighet med 5 kap. 7 § säkerhetsskyddsförordningen (2018:658), begära att en anställning eller annat deltagande ska placeras i säkerhetsklass 1.”

5 kap. 4 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Försvarsmakten får *inte* besluta vilka anställningar eller annat deltagande i Försvarsmaktens säkerhetskänsliga verksamhet som ska placeras i säkerhetsklass 1. Detta innebär att innan en ansökan om registerkontroll i säkerhetsklass 1 görs till Säkerhetspolisen ska det hos Försvarsmakten finnas ett regeringsbeslut om att befattningen är placerad i säkerhetsklass 1.[189] Organisationsenheten ska därmed, i enlighet med 5 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd, i befattningsanalysen föreslå vilka befattningar som ska placeras i säkerhetsklass 1. Detta gäller även befattningar som avser deltagande i säkerhetskänslig verksamhet och som ingår i en säkerhetsskyddad upphandling (avsnitt 6.17).

Genom bemyndigande i Must interna styrdokument är det chefen för säkerhetsprövningssektionen som, till regeringen, begär att en anställning eller annat deltagande ska placeras i säkerhetsklass 1. Säkerhetsprövningssektionen analyserar och sammanställer Försvarsmaktens behov av befattningar som ska placeras i säkerhetsklass 1. Efter att regeringen har beslutat om vilka befattningar som ska vara placerade i säkerhetsklass 1, meddelar säkerhetsprövningssektionen beslutet till organisationsenheten.

[189] 6 kap. 8 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

Moment 6:8 *Om regeringen beslutar att en befattning inte får placeras i säkerhetsklass 1 ska chefen för säkerhetsprövningssektionen vid Must istället besluta om placering av befattningen i säkerhetsklass 2.*

Vägledande förklaring: I ett sådant fall är det upp till den organisationsenhet där befattningen finns att se till att även andra skyddsåtgärder vidtas, t.ex. begränsning av tillgång till säkerhetsskyddsklassificerad information i nivå kvalificerat hemlig.

6.2.3. Beslut om placering i säkerhetsklass 2 och 3

> *”Kommuner, landsting och de myndigheter som anges i bilagan till denna förordning beslutar om*
>
> *1. placering i säkerhetsklass 2 och 3 i fråga om anställning eller annat deltagande i den egna verksamheten, och*
>
> *2. placering i säkerhetsklass 2 och 3 i fråga om anställning eller uppdrag hos en leverantör som de har ingått ett säkerhetsskyddsavtal enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585) med.”*
>
> 5 kap. 8 § första stycket säkerhetsskyddsförordningen

> *”Av 5 kap. 8 § säkerhetsskyddsförordningen (2018:658) framgår att Försvarsmakten beslutar om placering i säkerhetsklass 2 och 3 i fråga om anställning eller annat deltagande i den egna verksamheten.*
>
> *Sådana beslut fattas av Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddchefen bestämmer.”*
>
> 5 kap. 3 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Genom bemyndigande i Must interna styrdokument är det chefen för säkerhetsprövningssektionen som beslutar vilka anställningar och annat deltagande i säkerhetskänslig verksamhet som ska placeras i säkerhetsklass 2 och 3.

Organisationsenheten ska därför i befattningsanalysen, lämna förslag på vilka befattningar som ska placeras i säkerhetsklass 2 och 3.

Moment 6:9 *Om chefen för säkerhetsprövningssektionen har beslutat att en befattning inte ska placeras i den säkerhetsklass som organisationsenheten föreslagit ska organisationsenheten följa det beslutet.*

Vägledande förklaring: Chefen för säkerhetsprövningssektionen kan besluta att en befattning ska placeras i en högre säkerhetsklass än organisationsenheten föreslagit. I ett sådant fall ska organisationsenheten se till att personen som bemannar befattningen har en säkerhetsprövning och registerkontroll för rätt säkerhetsklass. Om beslutet istället innebär att en befattning placeras i lägre säkerhetsklass än den organisationsenheten föreslagit är det upp till organisationsenhet att se till att även andra skydds-

åtgärder vidtas, t.ex. begränsning av tillgång till säkerhetsskyddsklassificerad information.

6.2.4. Beslut om befattning som inte placeras i säkerhetsklass

En följd av att chefen för säkerhetsprövningssektionen beslutar om vilka anställningar eller annat deltagande i säkerhetskänslig verksamhet som ska placeras i säkerhetsklass 2 och 3 blir att chefen för säkerhetsprövningssektionen även indirekt beslutar om vilka befattningar som inte placeras i säkerhetsklass. Organisationsenheten ska därför, enligt 5 kap. 2 § andra punkten Försvarsmaktens interna bestämmelser om säkerhetsskydd, även lämna förslag på vilka befattningar som ska bemannas av personer som ska vara föremål för säkerhetsprövning utan registerkontroll.

6.2.5. Registerkontroll utan placering i säkerhetsklass

”Om det finns särskilda skäl, får registerkontroll av någon som ska delta i säkerhetskänslig verksamhet göras utan föregående placering i säkerhetsklass. Vid en sådan kontroll får de uppgifter om den kontrollerade som anges i 14 § tredje stycket hämtas.

Regeringen får meddela föreskrifter om sådan registerkontroll som avses i första stycket. Föreskrifterna får dock inte gälla för riksdagen och dess myndigheter.”

3 kap. 15 § säkerhetsskyddslagen

”En registerkontroll av den som ska delta i säkerhetskänslig verksamhet får göras utan placering i säkerhetsklass om det finns särskilda skäl. Regeringen beslutar om registerkontroll enligt första stycket. Vid större evenemang, statsbesök eller andra liknande händelser med närvaro av någon för vars personskydd Säkerhetspolisen ansvarar, får beslut om registerkontroll i stället fattas av Säkerhetspolisen.”

5 kap. 13 § säkerhetsskyddsförordningen

Vägledande förklaring: En person, som ska delta i säkerhetskänslig verksamhet av tillfällig karaktär och som inte uppfyller kraven för placering i säkerhetsklass, kan bli föremål för registerkontroll om det föreligger särskilda skäl. Sådan verksamhet är ytterst ovanlig i Försvarsmakten då det främst rör verksamhet som Säkerhetspolisen ansvarar för, men skulle kunna gälla tillfällig verksamhet som vissa internationella konferenser. När en sådan verksamhet är aktuell i Försvarsmakten ska en befattningsanalys göras även för dessa befattningar. Till grund för bedömningen av särskilda skäl ska särskild vikt läggas vid den aktuella hotbildsanalysen. Dokumenterad kriminalitet eller samröre med kriminella organisationer ska även utgöra en del av bedömningsgrunden. Det är regeringen eller Säkerhetspolisen som beslutar om en befattning ska vara föremål för registerkontroll utan placering i säkerhetsklass.

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, bemyndigas att:

2. hos regeringen eller Säkerhetspolisen begära att registerkontroll ska göras utan placering i säkerhetsklass enligt 5 kap. 13 § säkerhetsskyddsförordningen.”

5 kap. 18 § 2 Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Det är säkerhetsprövningssektionen som bereder ärenden till regeringen eller Säkerhetspolisen avseende befattningar som ska vara föremål för registerkontroll, men som inte placeras i säkerhetsklass, enligt 5 kap. 13 § säkerhetsskyddsförordningen.

Av 5 kap. 2 § tredje punkten Försvarsmaktens interna bestämmelser om säkerhetsskydd framgår att det är organisationsenheten som ska lämna förslag på vilka befattningar vid den egna enheten som endast ska vara föremål för registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen.

Organisationsenheten skickar en begäran till säkerhetsprövningssektionen om behovet av att framställa till regeringen eller Säkerhetspolisen. Av begäran ska det framgå varför befattningen inte placeras i säkerhetsklass samt vilka särskilda skäl som föreligger för registerkontroll. Regeringens eller Säkerhetspolisens beslut meddelas säkerhetsprövningssektionen, som i sin tur meddelar organisationsenheten. Först därefter kan organisationsenheten ansöka om registerkontroll. En sådan registerkontroll sker enligt ordinarie rutin (avsnitt 6.9.9).

Moment 6:10 *Om regeringen eller Säkerhetspolisen beslutar att en befattning inte ska vara föremål för registerkontroll enligt 5 kap. 13 § säkerhetsskyddsförordningen ska organisationsenheten genomföra en förnyad befattningsanalys.*

Vägledande förklaring: Den förnyade befattningsanalysen ska svara på vilka övriga skyddsåtgärder som ska vidtas för att de särskilda skälen ska kunna omhändertas på annat sätt än genom en registerkontroll.

6.2.6. Förteckning över befattningar

”Myndigheten ska förteckna vilka anställningar och annat deltagande i den säkerhetskänsliga verksamheten som har placerats i säkerhetsklass, eller som endast ska föregås av registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen (2018:585).”

6 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd

”Av 6 kap. 4 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd framgår att myndigheten ska förteckna vilka anställningar och annat deltagande i den säkerhetskänsliga verksamheten som har placerats i säkerhetsklass, eller som endast ska föregås av registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen (2018:585).

En sådan förteckning ska föras av Försvarsmaktens säkerhetsskyddschef.”

5 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Förteckningen förs av säkerhetsprövningssektionen. Till grund för förteckningen används organisationsenheternas befattningsanalyser i form av underlaget *Förteckning befattningsanalys* som lämnats in till säkerhetsprövningssektionen.

Moment 6:11 *Varje organisationsenhet ska löpande föra en förteckning över vilka personer som har en befattning som är placerad i säkerhetsklass. Organisationsenhetens förteckning ska även innehålla vilka personer som:*

a) enbart får del av begränsat hemliga uppgifter,

b) till följd av sitt deltagande i säkerhetskänslig verksamhet har möjlighet att orsaka endast ringa skada för Sveriges säkerhet.

Vägledande förklaring: Syftet med förteckningen är att få spårbarhet över vem som deltar i säkerhetskänslig verksamhet. Förteckningen förs i registerkontrollrutinen (RK-rutinen) i IS UNDSÄK och hålls uppdaterad av organisationsenheten.

6.2.7. Metod för befattningsanalys

Metod för säkerhetsskyddsanalys beskrivs närmare i kapitel 2. I steg 2 i metod för säkerhetsskyddsanalys bryts den säkerhetskänsliga verksamheten ner i *system*, *funktioner* och *anläggningar*. Befattningsanalysen genomförs med utgångspunkt i *funktioner* och med antagandet att en befattning är kopplad till en eller flera funktioner. Befattningar kan även hänföras till *system* och *anläggningar*. Exempelvis är en specifik befattning en del av en verksamhets *funktion*, men samtidigt kommer den som innehar befattningen att använda *system* samt ges tillträde till *anläggningar*.

I steg 3 i säkerhetsskyddsanalysen värderas de identifierade säkerhetsskyddsvärdena, med syfte att bedöma hur skyddsvärda de är, dvs. vad konsekvenserna blir av att säkerhetsskyddsvärdena förloras. Värderingen av konsekvensnivå utgår från en femgradig skala som i befattningsanalysen ska användas för att placera befattningar i eller utanför säkerhetsklass.

Slutligen är det inför en befattningsanalys viktigt att identifiera sådana säkerhetsskyddsvärden som den egna verksamheten är beroende av, men som den verksamhetsansvarige själv (t.ex. chef för en organisationsenhet) inte ansvarar för. Det vill säga att befattningsinnehavaren får tillgång till säkerhetsskyddsvärden som ägs eller

ansvaras för av någon annan än den egna organisationsenheten. Analys av befattning beskrivs som ett flödesschema i bild 6.2.

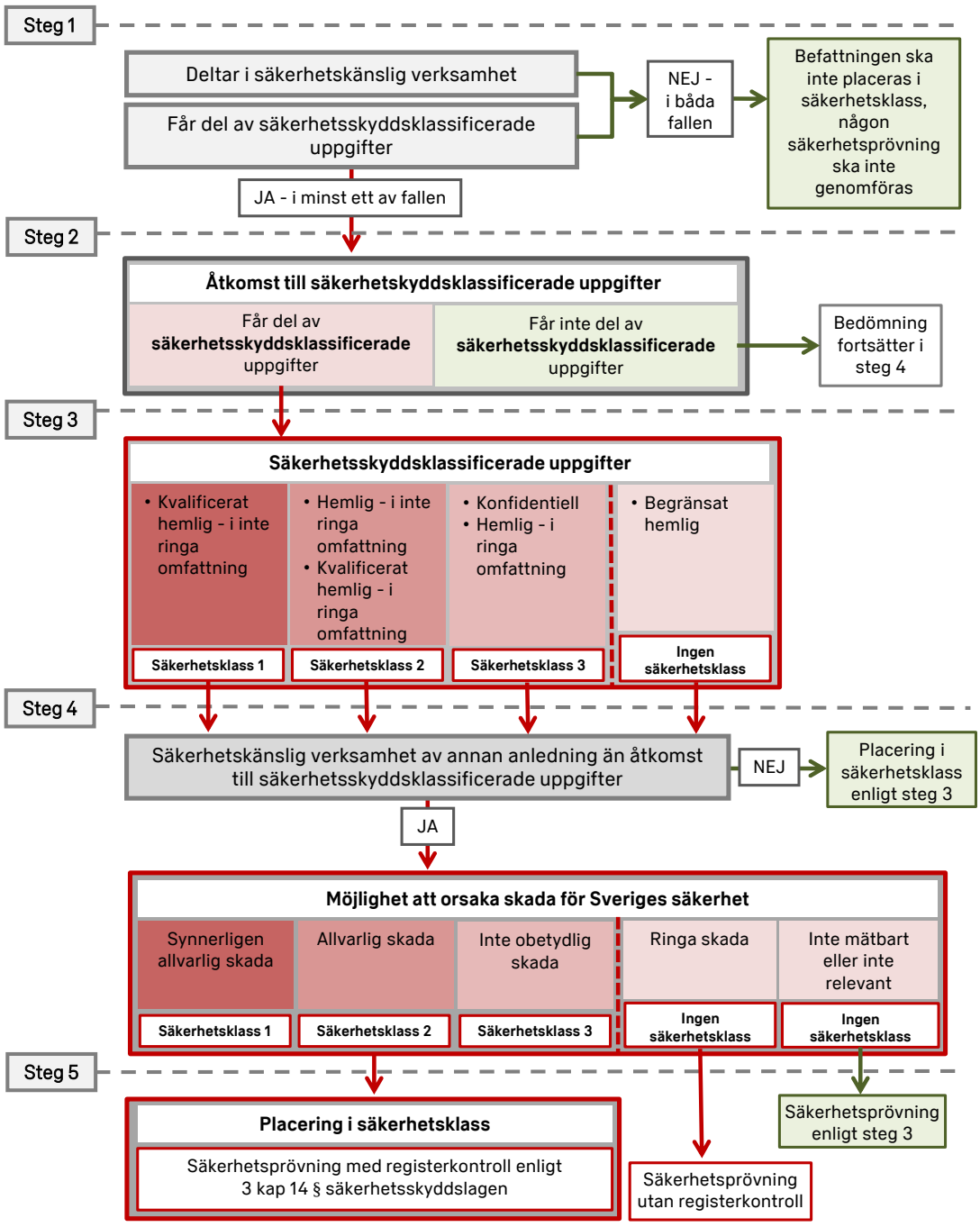


Bild 6.2. Flödesschema för analys av befattning. Maria Lind och Sanna Jonsson/Försvarsmakten

Utifrån flödesschemat kan processen för analys av befattning genomföras på följande sätt.

I säkerhetsskyddsanalysen är befattningar en del av en *funktion* (avsnitt 2.5.2) som i befattningsanalysen bryts ner till befattningsgrupper. Om verksamheten är strukturerad så att enskilda befattningsinnehavare deltar på olika sätt i den säkerhetskänsliga verksamheten ska befattningsgrupperna brytas ned i enskilda poster och analyseras enskilt. Flödesschemat kan användas för både grupper av befattningar och för enskilda befattningar. Beskrivningen utgår dock från att en enskild befattning analyseras.

Steg 1 – Bedömning av deltagande i säkerhetskänslig verksamhet

Mot bakgrund av vad som framkommit i verksamhetsbeskrivningen (avsnitt 2.5.1) ska en analys genomföras för att komma fram till vilka delar av verksamheten som är säkerhetskänsliga och som därmed ska ges ett säkerhetsskydd, samt vilken verksamhet som enbart omfattas av verksamhetsskydd.

Med detta som utgångspunkt delas sedan verksamheten upp i befattningar. Analysen ska svara på vilka befattningar som innebär deltagande i säkerhetskänslig verksamhet samt vilka befattningar som ger tillgång till säkerhetsskyddssklassificerande uppgifter. I detta skede ska det även identifieras om befattningen innebär att personen får tillgång till säkerhetskänslig verksamhet eller får del av säkerhetsskyddsklassificerade uppgifter utanför den egna verksamheten.

Om en befattning innebär att en person inte bedöms delta i säkerhetskänslig verksamhet eller få del av säkerhetsskyddsklassificerade uppgifter, ska ingen säkerhetsprövning genomföras.

Steg 2 – Åtkomst till säkerhetsskyddsklassificerade uppgifter

Om en befattning innebär att en person får del av uppgifter som omfattas av sekretess enligt OSL ska en bedömning göras av vilken typ av uppgifter det rör sig om. Om befattningen inte ger tillgång till *säkerhetsskyddsklassificerade uppgifter* utan endast till *sekretessklassificerade uppgifter*, eller till uppgifter som inte omfattas av sekretess enligt OSL, så utgår steg 3 och analysen fortsätter enligt steg 4.

Om en befattning däremot innebär att en person får del av säkerhetsskyddsklassificerade uppgifter så fortsätter analysen enligt steg 3.

Steg 3 – Omfattning av säkerhetsskyddsklassificerade uppgifter

Om en person, i sin befattning, får del av säkerhetsskyddsklassificerade uppgifter ska analysen svara på vilken säkerhetsskyddsklass uppgifterna har och i vilken omfattning befattningsinnehavarenkommer att ta del av dem. Med detta som utgångspunkt ska befattningen antingen placeras i säkerhetsklass 1, 2 eller 3, eller inte placeras i säkerhetsklass.

Innebär befattningen att en person får del av säkerhetsskyddsklassificerade uppgifter i nivån *begränsat hemlig* ska befattningen inte placeras i säkerhetsklass av den anledningen, men analysen ska fortsätta med en bedömning av skada i steg 4.

Om befattningsanalysen kommer fram till att befattningen ska placeras i säkerhetsklass, med anledning av tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *konfidentiellt* och uppåt, ska analysen kompletteras med en bedömning av skada i steg 4.

Steg 4 - Bedömning av möjlighet att orsaka skada för Sveriges säkerhet

Om befattningen innebär att en person tar del av säkerhetsskyddsklassificerade uppgifter men i övrigt inte deltar i säkerhetskänslig verksamhet, ska analysen avslutas i detta steg. Bedömningen av huruvida befattningen ska placeras i säkerhetsklass utgår enbart från vad som framkommit i steg 3.

Innebär befattningen deltagande i verksamhet som är säkerhetskänslig av annan anledning än att den ger tillgång till säkerhetsskyddsklassificerade uppgifter ska den skada som kan uppstå bedömas. Bedömningen görs utifrån den konsekvensnivå som konstaterats i steg 3 i metod för säkerhetsskyddsanalys (avsnitt 2.5.3). Konsekvensen av skadan bedöms enligt tabell 6.2 nedan och ger placering i säkerhetsklass 1, 2 eller 3, alternativt att befattningen inte ska placeras i säkerhetsklass.

Steg 5 – Bedömning av placering i säkerhetsklass

Slutligen ska analysen utmynna i en sammanvägd bedömning av vad som framkommit i steg 3 och 4. Om man i befattningsanalysen, enligt steg 3 och 4, inte kommer fram till samma säkerhetsklass ska befattningen placeras i den högre säkerhetsklassen (enligt tabell 6.2).

Tabell 6.2. Placering i säkerhetsklass.

Konsekvensnivå		Grund för säkerhetsprövning	Säkerhetsklass	Åtgärd
5	Synnerligen allvarlig skada	▪ Får del av KH-uppgifter i inte ringa omfattning ▪ Har möjlighet att orsaka synnerligen allvarlig skada för Sveriges säkerhet	1	Säkerhetsprövning med registerkontroll
4	Allvarlig skada	▪ Får del av KH-uppgifter i ringa omfattning ▪ Får del av H-uppgifter i inte ringa omfattning ▪ Har möjlighet att orsaka allvarlig skada för Sveriges säkerhet	2	Säkerhetsprövning med registerkontroll
3	Inte obetydlig skada	▪ Får del av H-uppgifter i ringa omfattning ▪ Får del av K-uppgifter ▪ Har möjlighet att orsaka inte obetydlig skada för Sveriges säkerhet	3	Säkerhetsprövning med registerkontroll

2	Ringa skada	▪ Får del av BH-uppgifter ▪ Har möjlighet att endast orsaka ringa skada för Sveriges säkerhet	Ingen säkerhetsklass	Säkerhetsprövning utan registerkontroll
1	Inte mätbart eller inte relevant		Ingen säkerhetsklass	Ingen säkerhetsprövning

Nedan följer tre exempel på hur analysen ska genomföras.

Exempel
Befattning 1 vid organisationsenhet A:

- *Har tillgång till system i konsekvensnivå 2 (skada som inte är ringa) vid organisationsenhet A.*
- *Ges tillträde till anläggning i konsekvensnivå 2 (skada som inte är ringa) vid organisationsenhet A.*
- *Hanterar i en omfattning som inte är ringa säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass hemlig.*

Befattningsanalys: Befattning 1 ska placeras i säkerhetsklass 2 med anledning av att personer i befattningen får tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass hemlig i en omfattning som inte är ringa.

Exempel
Befattning 3 vid organisationsenhet B:

- *Har tillgång till system i konsekvensnivå 1 (möjlighet att orsaka ringa skada) vid organisationsenhet B.*
- *Hanterar sekretessklassificerade uppgifter.*

Befattning 3 vid organisationsenhet B samverkar med organisationsenhet A:

- *Hanterar säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell.*

Befattningsanalys: Befattning 3 ska placeras i säkerhetshetsklass 3, med anledning av att befattningen ger tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell.

Exempel
Befattning 2 vid organisationsenhet A:

- *Har tillgång till system i konsekvensnivå 2 (skada som inte är ringa) vid organisationsenhet A.*
- *Ges tillträde till anläggningar i konsekvensnivå 3, men aggregerat i konsekvensnivå 4 (allvarlig skada) vid organisationsenhet A.*
- *Hanterar säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklasserna konfidentiell, samt hemlig i en omfattning som är ringa.*

Befattning 2 vid organisationsenhet A samverkar med organisationsenhet B:

- *Ges tillträde till anläggning i konsekvensnivå 3 (inte obetydlig skada) vid organisationsenhet B.*
- *Hanterar säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig, i en omfattning som är ringa.*

Befattningsanalys: Befattning 2 ska placeras i säkerhetshetsklass 2, med anledning av att befattningen har tillgång till anläggningar där personen kan orsaka allvarlig skada för Sveriges säkerhet.

6.3. Ansvar för säkerhetsprövning i Försvarsmakten

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ska leda och samordna Försvarsmaktens säkerhetsprövningar enligt säkerhetskyddslagen (2018:585) och säkerhetsskyddsförordningen (2018:658).”

5 kap. 7 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

”Försvarsmaktens säkerhetsskyddschef ansvarar för att säkerhetsprövning genomförs inför

1. anställning i befattningsnivå OF 5, respektive befattningsnivå CF 5 för civila tjänstemän, eller högre,

2. befordran till befattningsnivå OF 5 eller högre,

3. byte av befattning inom befattningsnivå OF 5, respektive befattningsnivå CF 5 för civila tjänstemän, eller högre,

4. konstituering till befattningsnivå OF 5, eller högre, och

5. anställning som försvarsattaché.

Ansvaret omfattar inte de anställningar som nämns i 24 § förordningen (2007:1266) med instruktion för Försvarsmakten.

Försvarsmaktens säkerhetsskyddschef får besluta att säkerhetsskyddschefen ansvarar för säkerhetsprövning i fler fall än de som framgår i 1–5.”

5 kap. 8 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

”I övriga fall än de som regleras i 8 § ansvarar chef för organisationsenhet för att grundutredning genomförs vid egen organisationsenhet, samt att säkerhetsprövningen följs upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.

I ansvaret ingår att

1. besluta vilka som får genomföra grundutredning och uppföljning,

2. besluta vilka personer som i övrigt är behöriga att ta del av uppgifter som förekommer i ärenden om säkerhetsprövning, och

3. se till att personal som arbetar med säkerhetsprövning har relevant utbildning och är lämpliga för uppgiften i enlighet med 6 kap. 2 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.”

5 kap. 11 § första och andra styckena
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Säkerhetsprövningssektionen leder och samordnar Försvarsmaktens säkerhetsprövningar.

Chefen för en organisationsenhet ansvarar för att åtgärder vidtas vid egen organisationsenhet, och det arbetet leds vanligtvis av organisationsenhetens säkerhetschef.

Chefen för organisationsenheten ska besluta lokal arbetsordning för styrning och kontroll av den egna verksamheten.[190]

För att säkerhetsprövningen ska fungera vid en organisationsenhet är det viktigt att det finns en tydlig ansvarsfördelning i den lokala arbetsordningen, där det klargörs vem som har vilket ansvar och vad ansvaret innebär. Inom Högkvarteret måste lokal arbetsordning vara tydlig vad gäller uppdelning av ansvar för säkerhetsprövning.

> *”Myndigheten ska förebygga och vidta rimliga skyddsåtgärder för att minska sårbarheter hos personer som deltar i myndighetens säkerhetskänsliga verksamhet.”*
>
> 6 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd

> *”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, beslutar om den som säkerhetsprövningen gäller uppfyller kraven för en godkänd säkerhetsprövning. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”*
>
> 5 kap. 14 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

> *”Ett beslut om godkänd säkerhetsprövning ska omprövas om den prövningen gäller, inte längre uppfyller kraven för godkännandet. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”*
>
> 5 kap. 15 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Genom ett bemyndigande i Must interna styrdokument är det chefen för säkerhetsprövningssektionen som beslutar i ärenden om säkerhetsprövning. Ett beslut i ärende om säkerhetsprövning kan omfatta villkor i form av olika skyddsåtgärder.

Moment 6:12 *Om chef för en organisationsenhet har beslutat om tillfälliga skyddsåtgärder ska det meddelas till säkerhetsprövningssektionen vid Must.*

Vägledande förklaring: Inom ramen för arbetsledningsrätten och inom ramen för övriga mandat kan chefen för en organisationsenhet besluta om tillfälliga skyddsåtgärder kopplat till den som är föremål för säkerhetsprövning. Tillfälliga skyddsåtgärder kan behövas under tiden för en utredning eller efter ett beslut i ärende om säkerhetsprövning eller omprövning av beslut i ärende om säkerhetsprövning. Beslut om tillfälliga skyddsåtgärder bör förenas med ett slutdatum.

[190] 1 kap. 3 § FM ArbO.

Tillfälliga skyddsåtgärder kan vara särskild uppföljning (avsnitt 6.10.2.1), säkerhetssamtal (avsnitt 6.13.1), skyddssamtal (avsnitt 6.11.2), samt restriktioner (avsnitt 6.10.2.2).

Om tillfälliga åtgärder vidtas rapporteras det enligt rutin i avsnitt 6.4.

”I enskilda fall får Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ta över ansvaret för genomförande av grundutredning och uppföljning enligt 11 §.”

5 kap. 13 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Säkerhetsprövningssektionen kan i vissa fall ta över ansvaret för en säkerhetsprövning helt eller delvis, och även besluta om hur en säkerhetsprövning ska genomföras i ett enskilt fall. När säkerhetsprövningssektionen tar över ansvaret för en säkerhetsprövning kan t.ex. en organisationsenhet som inte har ansvaret i det specifika fallet utses att genomföra vissa åtgärder.

Syftet med regeln är att säkerställa att relevanta åtgärder vidtas i särskilda situationer. Det kan röra sig om situationer när jäv förekommer eller att ett särskilt deltagande skiljer sig så mycket från den vanliga verksamheten, att bestämmelser om ansvar för säkerhetsprövning inte är tillämpliga utan måste anpassas. Det kan även innebära att särskilda åtgärder måste genomföras inom ramen för en utredning.

Observera!
Ansvar för säkerhetsprövning måste finnas i organisationsenhetens lokala arbetsordning.

Ansvar som behöver regleras kan vara vilket ansvar lokal säkerhetsorganisation, anställande chefer och HR-funktionen har. Det finns inget hinder för ett samarbete mellan lokal säkerhetsorganisation och HR-funktion eller mellan organisationsenheters säkerhetsorganisationer. Det kan t.ex. röra sig om information om vilken personal som slutar i Försvarsmakten eller byter organisationsenhet, eller information om utbildningar och tjänstenivåer.

Vid samarbete måste hänsyn tas till att uppgifter från en säkerhetsprövning alltid ska delges restriktivt och att uppgifterna vanligtvis omfattas av sekretess enligt OSL. För att få del av uppgifter från en säkerhetsprövning krävs även en särskild behörighet (avsnitt 6.5). Kravet gäller även för personal utanför militär säkerhetstjänst, t.ex. inom HR-funktionen.

6.4. Säkerhetsrapportering i personärende

”Varje organisationsenhet ska rapportera brister i pålitlighet, lojalitet och omständigheter som kan innebära sårbarheter i säkerhetshänseende inför och under tiden för en persons anställning eller deltagande i säkerhetskänslig verksamhet.

Rapportering ska göras till Försvarsmaktens säkerhetsskyddschef eller den säkerhetsskyddschefen bestämmer.

Om brister eller omständigheter har rapporterats om en person ska varje organisationsenhet på begäran av Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, lämna ytterligare information om den person som rapporteringen rör.”

8 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 6:13 *Rapportering enligt 8 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd ska göras till säkerhetsprövningssektionen vid Must.*

Vägledande förklaring: Rapporteringskravet gäller även när organisationsenheten bedömer att en persons deltagande i säkerhetskänslig verksamhet inte påverkas. Uppgifter som ska rapporteras kan uppkomma under grundutredningen, t.ex. vid referenstagning eller säkerhetsprövningsintervju, eller vid en uppföljning och under det avslutande samtalet. Det kan även vara fråga om tips och information från öppna källor såsom internet och sociala medier.

Exempel på när en person kan brista i pålitlighet, lojalitet eller om det finns omständigheter som kan innebära sårbarheter i säkerhetshänseende kan vara om personen förekommer som misstänkt i polisutredning eller säkerhetsrapportering i Försvarsmakten, har kontakter inom organiserad brottslighet eller författningshotande verksamhet. Exempel på författningshotande verksamhet är terrorism eller annan verksamhet som genom ideologiskt motiverad brottslighet hotar våra grundläggande demokratiska funktioner, oavsett om de bakomliggande orsakerna är politiska eller religiösa.

En uppgift som rapporteras kan vara så allvarlig att det innebär att personen inte längre kan delta i den säkerhetskänsliga verksamheten. Uppgiften kan även vara av sådan art att personen får delta i den säkerhetskänsliga verksamheten, men under vissa villkor (avsnitt 6.10.2).

Moment 6:14 *Organisationsenheten ska på begäran av säkerhetsprövningssektionen vid Must lämna den information som finns om en person vid organisationsenheten, om hinder inte möter på grund av bestämmelse om sekretess i offentlighets- och sekretesslagen.*

Vägledande förklaring: Enligt 8 kap. 2 § OSL gäller sekretess mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra. I normalfallet betraktas inte organisationsenheter som självstän-

diga i förhållande till varandra.[191] Det kan dock finnas hinder att lämna vissa uppgifter, t.ex. uppgifter som inom hälso- och sjukvården omfattas av sekretess enligt 25 kap. 1 § OSL.

Moment 6:15 *Information om brister i pålitlighet, lojalitet och omständigheter som kan innebära sårbarheter i säkerhetshänseende, samt annan information som begärs av säkerhetsprövningssektionen vid Must, ska hanteras på ett sådant sätt att endast de som är behöriga att ta del av informationen kan få tillgång till den.*

Observera!

Vid säkerhetsrapportering av personärenden ska behörighetsmall
HKV MUST SÄKK SÄKS PERSONÄRENDEN
alltid användas i IS UNDSÄK.

Vägledande förklaring: Normalt används IS UNDSÄK för säkerhetsrapportering i personärende. Men rapporten kan även komma in via t.ex. e-post, telefon och brev. Om personärendet är en del av en säkerhetsrapport ska personuppgifterna skyddas särskilt. Därför ska de läggas i en kommentar med begränsad läsbehörighet (läsbar för behörighetsmallen ovan). Om personärendet inte är en del av ett annat ärende som säkerhetsrapporterats ska informationen läggas i en handling i IS UNDSÄK, som rekommenderas till säkerhetsprövningssektionen (enligt behörighetsmall ovan).

Eftersom personuppgifterna inte ska spridas till obehöriga ska läsbehörigheten vara begränsad till de som har behov av uppgifterna för att vidta åtgärder, t.ex. organisationsenhetens säkerhetschef och enskilda handläggare. Generella behörighetsmallar, som sprider uppgifterna till personer som inte är behöriga, får inte användas.

6.5. Behörighet att genomföra säkerhetsprövning

”Myndigheten ska se till att den som genomför säkerhetsprövning har relevant utbildning och är lämplig för uppgiften.”

6 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Säkerhetsprövning innebär ett kontinuerligt intrång i den personliga integriteten, vilket ställer särskilda krav på Försvarsmakten och på de som ska genomföra säkerhetsprövning. Därför är det viktigt att de personer som arbetar med säkerhetsprövning för Försvarsmakten har rätt utbildning och är bedömda som lämpliga att arbeta med uppgiften.

[191] Handbok för dokument och ärendehantering i Försvarsmakten Förhandsutgåva Del 1 och 2 (H FM DÄR 2013) sid. 28.

”I övriga fall än de som regleras i 8 § ansvarar chef för organisationsenhet för att grundutredning genomförs vid egen organisationsenhet, samt att säkerhetsprövningen följs upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.

I ansvaret ingår att

1. besluta vilka som får genomföra grundutredning och uppföljning,

2. besluta vilka personer som i övrigt är behöriga att ta del av uppgifter som förekommer i ärenden om säkerhetsprövning, och

3. se till att personal som arbetar med säkerhetsprövning har relevant utbildning och är lämpliga för uppgiften i enlighet med 6 kap. 2 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.

5 kap. 11 § första och andra styckena
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 6:16 *En person är behörig att vidta åtgärder inom ramen för säkerhetsprövning först efter att den har genomgått relevant utbildning samt bedömts som lämplig.*

Vägledande förklaring: Att genomföra någon del av säkerhetsprövning kan t.ex. avse säkerhetsprövningsintervjuer, uppföljande samtal, administrativa åtgärder eller ansvara för en utredning i personärende.

Vilka som har beslutats vara behöriga ska förtecknas enligt moment 6:21 i avsnitt 6.5.1.1. Ett beslut som har fattats med stöd av äldre bestämmelser får fortsätta att gälla. Om en person ska genomföra säkerhetsprövning åt en annan organisationsenhet är det lämpligt att den organisationsenheten kontrollerar att personen har genomgått relevant utbildning och har bedömts som lämplig. Kontrollen sker genom samverkan mellan organisationsenheternas säkerhetschefer.

Om en person ska genomföra grundutredning och uppföljning åt en annan organisationsenhet måste chefen för den andra organisationsenheten besluta att personen får genomföra grundutredning och uppföljning vid enheten.

”I enskilda fall får Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ta över ansvaret för genomförande av grundutredning och uppföljning enligt 11 §.”

5 kap. 13 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Genom ett bemyndigande i Must interna styrdokument följer att säkerhetsprövningssektionen får ta över ansvaret för genomförande av grundutredning och uppföljning enligt 5 kap. 13 § Försvarsmaktens interna bestämmelser om säkerhetsskydd.

Att ta över ansvaret kan innebära att säkerhetsprövningssektionen i enskilda fall utser en person för att genomföra en grundutredning eller uppföljning. Det kan också innebära att säkerhetsprövningssektionen beslutar att uppgifter som har framkommit under en säkerhetsprövning får lämnas till en annan person än den som chefen för en organisationsenhet har beslutat vara behörig till uppgifterna.

Säkerhetsprövningssektionen kan även, med stöd av 5 kap. 13 § Försvarsmaktens interna bestämmelser om säkerhetsskydd, besluta att en person inte är lämplig att genomföra säkerhetsprövning. En sådan person får då inte arbeta med säkerhetsprövning i Försvarsmakten, oavsett vilket beslut som chefen för en organisationsenhet har fattat.

En person som inte är lämplig att genomföra säkerhetsprövning är t.ex. någon som saknar relevant utbildning, men det kan även vara en person som har uppvisat oförståelse för den personliga integriteten, hanterat uppgifter inom ramen för säkerhetsprövning felaktigt, underlåtit att genomföra delar av säkerhetsprövningen, underlåtit att vidta åtgärder eller som själv omfattats av ett beslut i ärende om säkerhetsprövning med villkor. Det kan även vara en person som av någon annan anledning inte vill eller kan utföra uppgiften.

Moment 6:17 *Vid varje organisationsenhet ska det minst finnas en befattning som är utsedd att ansvara för registerkontrollhantering. Innan en person får tillgång till RK-rutinen i IS UNDSÄK ska säkerhetsprövningssektionen vid Must ha godkänt personen.*

6.5.1. Utbildning

”Myndigheten ska regelbundet utbilda och öva myndighetens personal och andra som deltar i den säkerhetskänsliga verksamheten i säkerhetsskydd. Omfattningen och innehållet ska utgå från myndighetens säkerhetsskyddsplan.

7 kap. 2 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

”Myndigheten ska se till att den som genomför säkerhetsprövning har relevant utbildning och är lämplig för uppgiften.”

6 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

”Försvarsmaktens säkerhetsskyddschef får besluta närmare bestämmelser om utbildning i säkerhetsprövning.”

5 kap. 20 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 6:18 *Personer som*

a) administrerar registerkontroller,

b) genomför samtal och intervjuer,

c) genomför grundutredning,

d) genomför uppföljning av säkerhetsprövning,

e) genomför utredningar eller tar del av utredningsinformation,

f) handlägger den dokumentation som finns om den som säkerhetsprövningen gäller,

g) genomför bedömningar inför beslut i ärenden om säkerhetsprövning,

h) beslutar i ärenden om säkerhetsprövning, eller

i) utbildar i säkerhetsprövning

ska ha genomgått en av Försvarsmaktens säkerhetsskyddschefs godkända utbildningar innan de deltar i ärenden som rör säkerhetsprövning.

Vägledande förklaring: Säkerhetsprövningssektionen ansvarar för utbildning i säkerhetsprövning i Försvarsmakten samt godkänner utbildningar som genomförs av andra. Enligt 7 kap. 2 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd ska personal och andra som deltar i den säkerhetskänsliga verksamheten regelbundet utbildas i säkerhetsskydd. Utbildningen ska genomföras fortlöpande så att individens kompetens upprätthålls. Periodiciteten ska utgå från Försvarsmaktens säkerhetsskyddsplan. Ett exempel när en uppdaterad utbildning måste genomföras är om brister i kompetens upptäcks eller om regelverk har förändrats.

Moment 6:19 *Chefen för en organisationsenhet ska besluta vilka som ska utbilda i säkerhetsprövning vid organisationsenheten.*

6.5.1.1 Dokumentation av behörighet och utbildning

> *”Myndigheten ska föra en förteckning över de anställda och andra som har genomgått utbildning i säkerhetsskydd, samt vilken utbildning som genomförts och när. En genomförd övning ska dokumenteras.”*
>
> 7 kap. 2 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

”Chef för organisationsenhet ansvarar för att

1. personal vid den egna enheten utbildas och övas i säkerhetsskydd,

2. föra förteckning över de som har genomgått utbildning i säkerhetsskydd, och

3. dokumentera genomförda övningar.”

6 kap. 1 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Av 7 kap. 2 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd följer att det ska finnas en förteckning över vilka personer som har genomgått utbildning i säkerhetsprövning.

Moment 6:20 *Organisationsenheten ska förteckna vilka som har genomgått utbildning i säkerhetsprövning, vilken utbildning som genomförts och när den genomfördes. Förteckningen ska meddelas till säkerhetsprövningssektionen vid Must i IS UNDSÄK.*

Vägledande förklaring: Säkerhetsprövningssektionen ansvarar för att en förteckning finns för Försvarsmaktens räkning.

Moment 6:21 *En förteckning enligt moment 6:20 ska även innefatta vilka vid organisationsenheten som är behöriga att genomföra grundutredning och uppföljning, samt vilka personer som i övrigt är behöriga att ta del av uppgifter som förekommer i ärenden om säkerhetsprövning.*

6.6. Svenskt medborgarskap

”En anställning i staten, en kommun eller ett landsting som är placerad i säkerhetsklass 1 eller 2 får endast innehas av den som är svensk medborgare.

Om det finns särskilda skäl får regeringen i enskilda fall medge undantag från kravet på svenskt medborgarskap.”

3 kap. 11 § säkerhetsskyddslagen

Vägledande förklaring: Kravet på svenskt medborgarskap gäller endast anställning och inga andra former av deltagande. Det finns inte något krav att en person endast ska ha svenskt medborgarskap, utan en person kan vara medborgare i flera länder.

Svenskt medborgarskap är inte ett krav för placering i säkerhetsklass 3, även om placeringen gäller anställning. Observera att det i andra författningar finns krav på svenskt medborgarskap för militära befattningar oavsett vilken säkerhetsklass befattningen är placerad i (se faktarutan nedan).

FAKTA!
Bestämmelser om svenskt medborgarskap för militära befattningar finns i:

- 4 § förordningen (2015:613) om militär grundutbildning.
- 9 § 1 officersförordningen (2007:1268).
- 4 § förordningen (1994:524) om frivillig försvarsverksamhet.
- 5 § andra stycket hemvärnsförordningen (1997:146).
- 5 § lagen (1994:260) om offentlig anställning.

När det råder höjd beredskap får regeringen föreskriva om *allmän tjänsteplikt*, om det behövs för att verksamhet som är av särskild vikt för totalförsvaret ska kunna upprätthållas.[192] Om regeringen beslutar att allmän tjänsteplikt ska råda och fullgöras vid Försvarsmakten kommer civila arbetstagare, som ingår i Försvarsmaktens krigsorganisation, att likställas som militär personal.[193] Eftersom svenskt medborgarskap är ett krav för militära befattningar (se faktarutan) måste medborgarskap beaktas när en civil arbetstagare ska bemanna en befattning i Försvarsmakten som innebär krigsplacering.

6.7. Samtycke och information till den som ska prövas

Moment 6:22 *En person som ska säkerhetsprövas ska få information om att säkerhetsprövning ska genomföras och vad den omfattar. Personen ska även informeras om nödvändigheten av att anmäla förändringar i personliga förhållanden.*

Vägledande förklaring: Informationen ska lämnas till personen vid säkerhetsprövningsintervjun om så tidigare inte skett.

”Registerkontroll och särskild personutredning får göras endast om den som säkerhetsprövningen gäller har lämnat sitt samtycke. Samtycket ska anses gälla också kontroller och utredningar under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.”

3 kap. 18 § säkerhetsskyddslagen

”Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska dokumentera att samtycke till registerkontroll och särskild personutredning har lämnats av den som säkerhetsprövningen gäller.”

6 kap. 11 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Moment 6:23 *Den organisationsenhet som genomför säkerhetsprövningen ska informera den prövade om vad registerkontroll innebär och ansvarar för att den prö-*

[192] 6 kap. 1 § lagen (1994:1809) om totalförsvarsplikt.
[193] 2 kap. 2 § 10 förordningen (1996:927) om Försvarsmaktens personal.

vade lämnar sitt samtycke inför registerkontroll. Om den prövade inte lämnar sitt samtycke ska grundutredningen avslutas.

Moment 6:24 *En organisationsenhet ska registrera samtycket i RK-rutinen i IS UNDSÄK samt på dokumentmallen* Intervjuguide säkerhetsprövningsintervju *inför ansökan om registerkontroll.*

Vägledande förklaring: Informationen till den prövade ska minst omfatta:

- Vilka register som kommer att kontrolleras. Uppgifter hämtas från belastningsregistret, misstankeregistret samt register där uppgifter som behandlas med stöd av polisdatalagen hämtas.

- Att kontrollen utförs löpande under hela tiden som deltagandet i den säkerhetskänsliga verksamheten pågår.

- Att personen ska lämna sitt samtycke samt att grundutredningen avslutas om samtycke inte lämnas.

- Att vid säkerhetsklass 1 och 2 gäller samtycket även för medkontrollerad (make, maka eller sambo). Den medkontrollerade behöver alltså inte lämna samtycke. Med sambo avses två personer som stadigvarande bor tillsammans i ett parförhållande och har gemensamt hushåll.[194] Enligt Säkerhetspolisen kan ett par vara att betrakta som sambos trots att de är folkbokförda på olika adresser, t.ex. om de växelvis bor på olika adresser och har delad ekonomi.[195]

Se mer information om dokumentation av registerkontroll och samtycke i avsnitt 6.16.3.

6.7.1. Återtagning av tidigare lämnat samtycke

Moment 6:25 *Om den prövade under grundutredningens genomförande återtar ett tidigare lämnat samtycke, ska grundutredningen avslutas.*

Moment 6:26 *Om den prövade, efter genomförd registerkontroll, återtar sitt samtycke ska säkerhetsprövningen avslutas och ett avslutande samtal ska genomföras med den prövade. Säkerhetsprövningssektionen vid Must ska informeras innan registerkontrollen avslutas.*

Vägledande förklaring: Det avslutande samtalet ska genomföras på sådant sätt att omständigheterna kring varför personen valt att återta sitt samtycke utreds. Läs mer om avslutande samtal i avsnitt 6.15. Säkerhetsprövningssektionen meddelar organisationsenheten när registerkontrollen kan avslutas.

[194] 1 § sambolagen (2003:376).
[195] Säkerhetspolisens vägledning i säkerhetsskydd – Personalsäkerhet (juni 2019), kapitel 5.2.3.

6.8. Grundutredning

”Säkerhetsprövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas och ska innefatta en grundutredning samt registerkontroll och särskild personutredning i den omfattning som anges i 13, 14 och 17 §§. Om det finns särskilda skäl får säkerhetsprövningen göras mindre omfattande.”

3 kap. 3 § första stycket säkerhetsskyddslagen

”Med grundutredning enligt 3 kap. 3 § säkerhetsskyddslagen (2018:585) avses en utredning om personliga förhållanden av betydelse för säkerhetsprövningen. Utredningen ska omfatta betyg, intyg, referenser och uppgifter som den som prövningen gäller har lämnat, samt andra uppgifter i den utsträckning det är relevant för prövningen. Vid behov ska en identitetskontroll göras.”

5 kap. 2 § säkerhetsskyddsförordningen

”En grundutredning inför en anställning eller annat deltagande i säkerhetskänslig verksamhet som är placerad i säkerhetsklass ska innefatta en säkerhetsprövningsintervju.”

6 kap. 5 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med grundutredning avses att uppgifter hämtas in om personliga förhållanden av betydelse för säkerhetsprövningen, innan personen deltar i den säkerhetskänsliga verksamheten.[196] Grundutredningen ska innehålla kontroll av betyg, intyg och referenstagning samt att uppgifter från den som kontrollen avser hämtas in, t.ex. genom en säkerhetsprövningsintervju. Registerkontroll och särskild personutredning ingår inte i grundutredningen, utan är fristående moment i säkerhetsprövningsprocessen, och genomförs efter grundutredningen.

Omfattningen av grundutredningen anpassas till vilken typ av deltagande i säkerhetskänslig verksamhet som det är fråga om. Fler åtgärder ingår i en grundutredning mot placering på befattning i säkerhetsklass 1 och 2 jämfört med en befattning i säkerhetsklass 3. I och med att organisationsenheten skickar in en ansökan om registerkontroll, eller en ansökan om deltagande i säkerhetskänslig verksamhet utan placering i säkerhetsklass, till säkerhetsprövningssektionen är grundutredningen avslutad. Säkerhetsprövningssektionen kan dock besluta om att grundutredningen ska kompletteras innan registerkontrollen genomförs eller innan ansökan om deltagande i säkerhetskänslig verksamhet godkänns.

[196] Prop. 2017/18:89 s. 143-144.

Kravet på genomförande av grundutredning finns även när en person redan deltar i Försvarsmaktens verksamhet, se avsnitt 6.8.7. En grundutredning kan även göras mindre omfattande om det finns särskilda skäl, se avsnitt 6.8.8.

Observera!
En grundutredning ska alltid ha gjorts innan en registerkontroll genomförs och grundutredningen ska alltid dokumenteras.

”I övriga fall än de som regleras i 8 § ansvarar chef för organisationsenhet för att grundutredning genomförs vid egen organisationsenhet, samt att säkerhetsprövningen följs upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.”

5 kap. 11 § första stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Det är den organisationsenhet som ansvarar för den säkerhetskänsliga verksamheten som ansvarar för att en grundutredning genomförs innan en person deltar i verksamheten. En grundutredning ska även i vissa fall göras vid frivillig försvarsverksamhet. I sådant fall ansvarar den organisationsenhet med vilken personen som prövas avser att teckna avtal med, för genomförandet.

En grundutredning bör påbörjas så snart som möjligt inför ett deltagande. Det finns inget hinder att påbörja grundutredningen för flera kandidater vid en rekrytering, t.ex. kan en kontroll av betyg och intyg som genomförts av HR-funktionen ingå som en del av grundutredningen. Av integritetsskäl bör säkerhetsprövningsintervjun genomföras med så få kandidater som möjligt, varför det i de flesta fall är lämpligt att endast genomföra säkerhetsprövningsintervjun med slutkandidaten. När det gäller befattningar som är placerade i säkerhetsklass får registerkontroll endast genomföras för den person som avses placeras på befattningen (avsnitt 6.9).

Moment 6:27 *Om befattningen är placerad i säkerhetsklass 1 eller 2 ska grundutredningen även omfatta:*

a) personens ekonomiska förhållanden, och

b) personens förekomst på internet och sociala medier som är allmänt tillgängliga och som har betydelse för säkerhetsprövningen

Vägledande förklaring: En grundutredning ska även bestå av andra uppgifter i den utsträckning det är relevant för prövningen och ska vara mer djupgående ju högre säkerhetsklass befattningen är placerad i. Det kan t.ex. vara relevant med en mer djupgående kontroll av en medkontrollerad. Om befattningen är placerad i säkerhetsklass 3 eller om befattningen avser ett deltagande som inte är placerat i säkerhetsklass får grundutredningen omfatta personens ekonomiska förhållanden, och perso-

nens förekomst på internet och sociala medier som är allmänt tillgängliga om det behövs för säkerhetsprövningen. En grundutredning ska alltid kompletteras när det uppkommit frågetecken som behöver utredas närmare för att en bedömning av informationen ska kunna genomföras. Likaså kan kompletteringar behövas om uppgifter lämnas ut efter registerkontroll.

Tips!
I Försvarsmaktens handbok om säkerhetsprövning (H SÄK Säkprövn) finns stöd för hur du kontrollerar uppgifter samt genomför referenstagning.

Moment 6:28 *När en person, som redan deltar i Försvarsmaktens säkerhetskänsliga verksamhet, byter organisationsenhet ska den mottagande organisationsenheten inhämta information om säkerhetsprövningen från den avlämnande organisationsenheten.*

Vägledande förklaring: Inhämtning av information görs lämpligen genom att den mottagande organisationsenheten kontaktar säkerhetschefen vid den avlämnande organisationsenheten. Överlämning av information kan göras antingen muntligt eller skriftligt. Dokumentation från säkerhetsprövningen ska dock bevaras vid den avlämnande organisationsenheten (avsnitt 6.16). Det finns inga hinder mot att en kopia överlämnas till den mottagande organisationsenheten.

”Om det under eller efter genomförd grundutredning enligt 11 § står klart att den som prövningen gäller inte uppfyller kraven för en godkänd säkerhetsprövning ska chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, avsluta säkerhetsprövningen och rapportera bedömningen enligt rutinerna i 8 kap. 5 §.”

5 kap. 12 § första stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Om en säkerhetsprövning avbrutits under eller efter genomförd grundutredning ska det alltid rapporteras till säkerhetsprövningssektionen (avsnitt 6.4 och 6.8.5).

”Grundutredningen ska dokumenteras.”

6 kap. 5 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Dokumentationen består av underlag som den prövade lämnat, som CV, betyg och intyg samt anteckningar som har gjorts vid granskning av dessa. Dokumentationen består även av anteckningar och underlag från referenstagning och kontroll av öppna källor och underlag från genomförd säkerhetsprövningsintervju (avsnitt 6.8.1), samt *Sammanfattande dokumentation - grundutredning* (avsnitt 6.8.2).

Om den prövade efter genomförd grundutredning inte bedöms uppfylla kraven för en godkänd säkerhetsprövning ska dokumentationen sändas till säkerhetsprövningssektionen (avsnitt 6.8.5). Om säkerhetsprövningen ska fortsätta ska dokumentationen bevaras vid organisationsenheten.

Läs mer om dokumentationskrav samt arkivering vid grundutredning i avsnitt 6.16.2.

6.8.1. Säkerhetsprövningsintervju

> *”En grundutredning inför en anställning eller annat deltagande i säkerhetskänslig verksamhet som är placerad i säkerhetsklass ska innefatta en säkerhetsprövningsintervju.”*
>
> 6 kap. 5 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Moment 6:29 *Vid säkerhetsprövningssektionen vid Must får det beslutas om ytterligare säkerhetsprövningsintervjuer inom ramen för en grundutredning.*

Vägledande förklaring: Säkerhetsprövningsintervjun syftar till att inhämta information från individen om de personliga förhållandena av betydelse för säkerhetsprövningen.[197] Säkerhetsprövningsintervjun ska alltid genomföras innan registerkontroll, men det finns inget hinder mot att genomföra ytterligare intervjuer med personen efter en registerkontroll för att klargöra omständigheter som framkommit där. Om så skett ska detta framgå av dokumentationen. Registerkontroll ska dock inte genomföras om det efter säkerhetsprövningsintervjun står klart att den som prövningen gäller inte uppfyller kraven för en godkänd säkerhetsprövning.[198]

Moment 6:30 *En säkerhetsprövningsintervju ska ha minst den omfattning som man vid säkerhetsprövningssektionen vid Must har bestämt. Säkerhetsprövningsintervjun ska i övrigt ha den omfattning som behövs för att bedöma den prövades pålitlighet och lojalitet samt om det föreligger några sårbarheter i säkerhetshänseende.*

Vägledande förklaring: Omfattningen av säkerhetsprövningsintervjun kan anpassas till den verksamhet som avses, men ska alltid innefatta de fastställda frågeområdena. Frågeområdena framgår i dokumentmallen *Intervjuguide säkerhetsprövningsintervju*. Den prövades lämplighet från säkerhetssynpunkt kan påverkas av förhållanden som inte direkt gäller den prövade själv utan en nära anhörig, som en make, maka, sambo eller partner. Det är därför viktigt att utreda den prövades lojalitetsband till en nära anhörig samt om det föreligger något beroendeförhållande till en maka, make, sambo eller partner som kan medföra en sårbarhet i säkerhetshänseende, eller påverka pålitligheten och lojalitet.

[197] 5 kap. 2 § säkerhetsskyddsförordningen.
[198] 5 kap. 3 § säkerhetsskyddsförordningen.

Tips!
I Försvarsmaktens handbok om säkerhetsprövning (H SÄK Säkprövn) finns stöd för hur du genomför en säkerhetsprövningsintervju.

Moment 6:31 *Vid en säkerhetsprövningsintervju ska anteckningar föras.*

Vägledande förklaring: Anteckningarna kan föras på dokumentmallen *Intervjuguide säkerhetsprövningsintervju* och utgör då den dokumentation som ska bevaras från säkerhetsprövningsintervjun. Om anteckningarna inte förts på *Intervjuguide säkerhetsprövningsintervju* ska dokumentmallen fyllas i efter intervjun, och övriga anteckningar kan därefter förstöras. Dokumentmallen får kompletteras med extra sidor. Uppgifterna som inhämtas vid intervjutillfället omfattas av försvarssekretess enlig 15 kap. 2 § OSL och därför måste informationssystem som är godkända för sådana uppgifter användas om uppgifterna hanteras digitalt. Dokumenten kan även omfattas av annan sekretess till skydd för den enskilde, t.ex. 35 kap. 1 § OSL (enskilds personliga och ekonomiska förhållanden vid registerkontroll) och 38 kap. 4 § OSL (enskilds personliga och ekonomiska förhållanden i försvarsunderrättelseverksamhet och den militära säkerhetstjänsten).

Moment 6:32 *Efter en säkerhetsprövningsintervju ska en bedömning göras av de uppgifter som har framkommit. Bedömningen ska dokumenteras med hjälp av dokumentmallen* Intervjuguide säkerhetsprövningsintervju.

Vägledande förklaring: Bedömningen som genomförs efter intervjun ingår sedan i den sammanfattande bedömningen av individen.

6.8.2. Sammanfattande bedömning av en grundutredning

Moment 6:33 *Resultatet av grundutredningen ska sammanställas på dokumentmallen* Sammanfattande dokumentation grundutredning.

Moment 6:34 *En grundutredning ska avslutas med en sammanfattande bedömning. Bedömningen ska genomföras innan framställan om registerkontroll och ska dokumenteras på dokumentmallen* Sammanfattande dokumentation grundutredning.

Vägledande förklaring: En sammanfattande bedömning ska alltid göras, även om befattningen inte är placerad i säkerhetsklass. Dokumentmallen *Sammanfattande dokumentation grundutredning* tillhandahålls av säkerhetsprövningssektionen.

Av dokumentet *Sammanfattande dokumentation grundutredning* måste det framgå

- om den prövade kan antas vara lojal mot de intressen som skyddas i säkerhetsskyddslagen och
- i övrigt är pålitlig från säkerhetssynpunkt, samt
- om det finns omständigheter som innebär sårbarheter i säkerhetshänseende.

Om det har framkommit information som påverkat bedömningen samt om det föreligger något uppföljningsbehov, ska även det framgå av dokumentet. Av dokumentmallen ska det även framgå vilka åtgärder som har vidtagits och när de har genomförts.

Efter att en grundutredning har genomförts finns det tre vägval beroende på vad som hittills har kommit fram om den prövade:

- Att fortsätta säkerhetsprövningen (avsnitt 6.8.3).
- Att fortsätta säkerhetsprövningen med kompletterande skyddsåtgärder (avsnitt 6.8.4).
- Att avsluta säkerhetsprövningen (avsnitt 6.8.5).

6.8.3. Säkerhetsprövningen ska fortsätta

”En ansökan om registerkontroll får göras endast om den som säkerhetsprövningen gäller kan antas komma att anställas eller på annat sätt delta i den aktuella verksamheten. Om det finns synnerliga skäl får en ansökan göras utan ett sådant antagande.”

5 kap. 14 § säkerhetsskyddsförordningen

Vägledande förklaring: I Försvarsmakten finns sällan synnerliga skäl till att ansöka om registerkontroll utan att det kan antas att personen kan komma att anställas eller delta i verksamheten. En registerkontroll ska aldrig användas som ett sållningsinstrument vid en säkerhetsprövning, utan en grundutredning med en efterföljande bedömning att personen antas uppfylla förutsättningarna för en godkänd säkerhetsprövning ska vara genomförd innan ansökan om registerkontroll sänds in. Bedömningen om särskilda skäl föreligger genomförs vid säkerhetsprövningssektionen innan ansökan om registerkontroll skickas in av organisationsenheten.

”Om säkerhetsprövningen inte avslutats enligt 12 § första stycket ska chef för en organisationsenhet, eller den chefen för organisationsenheten bestämmer, i förekommande fall göra en framställan om registerkontroll hos den militära underrättelse- och säkerhetstjänsten i Högkvarteret.”

5 kap. 16 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Om den sammanfattande bedömningen av en grundutredning visar att den prövade uppfyller förutsättningarna för en godkänd säkerhetsprövning och därmed bedöms kunna delta i den säkerhetskänsliga verksamheten, ska säkerhetsprövningen fortsätta. Om befattningen är placerad i säkerhetsklass ska en ansökan om registerkontroll sändas till säkerhetsprövningssektionen (avsnitt 6.9.2).

Om befattningen inte är placerad i säkerhetsklass ska en ansökan om deltagande i säkerhetskänslig verksamhet sändas till säkerhetsprövningssektionen (moment 6:40 i avsnitt 6.8.9).

6.8.4. Säkerhetsprövningen ska fortsätta med kompletterande skyddsåtgärder

Om det under grundutredningen framkommit brister som påverkat bedömningen av en persons pålitlighet eller lojalitet samt om det framkommit omständigheter som kan innebära en sårbarhet i säkerhetshänseende ska särskilda åtgärder vidtas. Säkerhetsprövningen ska då antingen avslutas (avsnitt 6.8.5), eller fortsätta. Det är organisationsenheten som gör bedömningen i detta steg.

Av dokumentmallen *Sammanfattande dokumentation grundutredning* ska det i korthet framgå vad som har framkommit och hur uppgifterna bedömts. Där ska det även framgå om det finns uppföljningsbehov eller om skyddsåtgärder behöver vidtas för att personen ska kunna delta i den avsedda verksamheten, t.ex. restriktioner eller särskild uppföljning.

Moment 6:35 *Dokumentmallen* Sammanfattande dokumentation grundutredning *ska sändas till säkerhetsprövningssektionen vid Must. Bedömningen ska kompletteras med en säkerhetsrapport i personärende med uppgifter om:*

a) vilka åtgärder som har vidtagits inom ramen för säkerhetsprövningen,

b) brister i den prövades lojalitet, pålitlighet eller omständigheter som kan innebära sårbarheter i säkerhetshänseende, och

c) kompletterande skyddsåtgärder som kan uppväga den prövades brister eller sårbarheter.

Vägledande förklaring: Rapporten ska innehålla en beskrivning av de omständigheter som har framkommit under grundutredningen samt organisationsenhetens bedömning av informationen. Med rapporten kan även underlag medfölja som t.ex. den dokumenterade säkerhetsprövningsintervjun eller uppgifter från referenstagning. Om befattningen är placerad i säkerhetsklass ska en ansökan om registerkontroll sändas till säkerhetsprövningssektionen (avsnitt 6.9.2).

Om befattningen inte är placerad i säkerhetsklass, ska ansökan om deltagande i säkerhetskänslig verksamhet skickas in till säkerhetsprövningssektionen (moment 6:40 i avsnitt 6.8.9).

6.8.5. Säkerhetsprövningen ska avslutas

> *”Om det redan efter grundutredningen står klart att den som prövningen gäller inte uppfyller kraven för en godkänd säkerhetsprövning enligt 3 kap. 2 § säkerhetsskyddslagen (2018:585), ska registerkontroll och särskild personutredning inte göras.”*
>
> 5 kap. 3 § andra meningen säkerhetsskyddsförordningen

> *”Om det under eller efter genomförd grundutredning enligt 11 § står klart att den som prövningen gäller inte uppfyller kraven för en godkänd säkerhetsprövning ska chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, avsluta säkerhetsprövningen och rapportera bedömningen enligt rutinerna i 8 kap. 5 §.”*
>
> 5 kap. 12 § första stycket
> Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Om det under eller efter grundutredningen står klart att personen, av säkerhetsrelaterade skäl, inte kan placeras på avsedd befattning ska organisationsenheten avsluta säkerhetsprövningen. En grundutredning kan avslutas i alla steg, t.ex. efter granskning av betyg och intyg, eller efter säkerhetsprövningsintervjun. Av integritetsskäl är det viktigt att organisationsenheten inte fortsätter med grundutredningen när det står klart att personen inte kommer att uppfylla kraven för en godkänd säkerhetsprövning.

Moment 6:36 *Om organisationsenheten avslutar säkerhetsprövningen av säkerhetsrelaterade skäl, ska dokumentationen av grundutredningen sändas till säkerhetsprövningssektionen vid Must, tillsammans med* Sammanfattande dokumentation grundutredning. *Dokumentationen ska kompletteras med en säkerhetsrapport i personärende med uppgifter om:*

a) vilka åtgärder som vidtagits inom ramen för säkerhetsprövningen, och

b) brister i den prövades lojalitet, pålitlighet eller omständigheter som kan innebära sårbarheter i säkerhetshänseende.

Vägledande förklaring: Dokumentationen sparas vid säkerhetsprövningssektionen (avsnitt 6.16.2). Detta säkerställer att en person som på nytt ska säkerhetsprövas kommer att genomgå en fördjupad grundutredning, där de omständigheter som låg till grund för den tidigare bedömningen utreds. Detta innebär även att uppgifter om en person kommer att bedömas på ett likvärdigt sätt när personen säkerhetsprövas av olika organisationsenheter. Säkerhetsprövningssektionen ger stöd i dessa ärenden.

Även i de fall den prövade väljer att ta tillbaka sin ansökan och säkerhetsprövningen av säkerhetsrelaterade skäl har avslutats, ska moment 6:36 följas.

Vad som ingår i dokumentation av grundutredning framgår även i avsnitt 6.16.2.

6.8.6. Grundutredning inför grund- och repetitionsutbildning

Grundutredning inför värnplikt genomförs av Totalförsvarets rekryteringsmyndighet[199] inom ramen för mönstring, för befattningar som är placerade i säkerhetsklass 3 och befattningar som inte är placerade i säkerhetsklass. Totalförsvarets rekryteringsmyndighet redovisar resultatet av grundutredningen till säkerhetsprövningssektionen.

Om den aktuella befattningen är placerad i säkerhetsklass sänder Totalförsvarets rekryteringsmyndighet en ansökan om registerkontroll till säkerhetsprövningssektionen. Säkerhetsprövningssektionen ansöker sedan om registerkontroll enligt vanlig rutin (avsnitt 6.9.2).

Om befattningen inte är placerad i säkerhetsklass begär Totalförsvarets rekryteringsmyndighet registerutdrag enligt 15 § förordning (1999:1134) om belastningsregister samt 4 § förordning (1999:1135) om misstankeregister för Försvarsmaktens räkning. Säkerhetsprövningssektionen bedömer information som har framkommit efter registerutdrag.

Totalförsvarets rekryteringsmyndighet kan inte placera en individ i en befattningsgrupp eller skriva in personen för tjänstgöring innan den prövade bedömts som lämplig efter genomförd mönstring, eventuell registerkontroll är klar, och säkerhetsprövningen är godkänd.

Moment 6:37 *Om en totalförsvarspliktig som är inskriven för värnplikt ska placeras på en befattning i säkerhetsklass 1 eller 2 ska grundutredningen genomföras av den organisationsenhet där den värnpliktige ska placeras. Grundutredningen och registerkontrollen ska vara genomförda innan den värnpliktige får delta i säkerhetskänslig verksamhet som kräver placering i säkerhetsklass 1 eller 2.*

Vägledande förklaring: Det är lämpligt att grundutredningen påbörjas direkt efter inställelsen till organisationsenheten. Innan en värnpliktig kan påbörja befattningsutbildningen ska det finnas en godkänd säkerhetsprövning för rätt säkerhetsklass.

6.8.7. När ska grundutredningen göras om?

En grundutredning gäller tillsvidare och följs upp kontinuerligt under tiden för deltagandet i den säkerhetskänsliga verksamheten (avsnitt 6.11). Det finns dock tillfällen när en grundutredning ska göras om, även om personen tidigare genomgått en grundutredning.

Moment 6:38 *En grundutredning ska göras om vid följande tillfällen.*

a) När en person placeras på en ny befattning med andra arbetsuppgifter, oavsett om befattningarna är placerade i samma säkerhetsklass.

[199] Den 1 februari 2021 ändras myndighetens namn till Totalförsvarets plikt- och prövningsverk.

b) När en person får förändrade arbetsuppgifter i sin nuvarande befattning som, efter en befattningsanalys, påverkar placeringen i säkerhetsklass.

c) När en registerkontroll ska förnyas för en person som redan är placerad på en befattning i säkerhetsklass 1 eller 2, och där registerkontrollen är genomförd före den 1 april 2019.

d) När en person byter organisationsenhet (oavsett befattning).

e) När en värnpliktig ska placeras på en befattning efter avslutad grundutbildning. Kravet gäller dock inte i det fall den värnpliktige endast krigsplaceras.

Vägledande förklaring: Även om grundutredningen ska göras om i sin helhet enligt ovanstående, finns tillfällen där grundutredningen kan göras mindre omfattande (avsnitt 6.8.8). Att grundutredningen görs om innebär i de flesta fall även att en ny registerkontroll ska genomföras (avsnitt 6.9.4).

6.8.8. När får grundutredningen vara mindre omfattande?

> *”Säkerhetsprövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas och ska innefatta en grundutredning samt registerkontroll och särskild personutredning i den omfattning som anges i 13, 14 och 17 §§. Om det finns särskilda skäl får säkerhetsprövningen göras mindre omfattande.”*
>
> 3 kap. 3 § första stycket säkerhetsskyddslagen

Vägledande förklaring: Särskilda skäl kan avse om den som prövningen gäller redan tidigare har prövats på motsvarande sätt och ytterligare utredning därför inte bedöms kunna tillföra något nytt i sak.[200] Särskilda skäl för att göra undantag från krav på registerkontroll, kan vara om den prövade redan registerkontrollerats på motsvarande sätt (avsnitt 6.9.10).

En grundutredning kan göras mindre omfattande i vissa delar. Kontroll av betyg och intyg samt referenstagning kan t.ex. ha genomförts av HR-funktionen inför en anställning. I sådana fall kan det inom ramen för grundutredningen kontrolleras vad som har framkommit och om kontrollen eller referenstagningen behöver kompletteras. En anställningsintervju kan dock aldrig ersätta en säkerhetsprövningsintervju.

I vissa fall kan en tidigare grundutredning även gälla för deltagande i annan verksamhet, t.ex. om en grundutredning är genomförd för en befattning i säkerhetsklass 2 och personen tillfälligt ska ha en annan befattning som är placerad i säkerhetsklass 3. För att detta ska vara möjligt krävs att grundutredningen nyligen är utförd samt att det kan uteslutas att det förekommer ytterligare information om personen som skulle påverka beslutet om godkänd säkerhetsprövning.

[200] Prop. 2017/18:89 s. 144.

Moment 6:39 *Om en organisationsenhet bedömer att en grundutredning ska göras mindre omfattande ska det anmälas till säkerhetsprövningssektionen vid Must.*

Vägledande förklaring: Genom ett bemyndigande i Must interna styrdokument är det chefen för säkerhetsprövningssektionen som beslutar om det föreligger särskilda skäl enligt 3 kap. 3 § första stycket säkerhetsskyddslagen. En sådan anmälan kan gälla enskilda fall som t.ex. vid ett befattningsbyte där arbetsuppgifterna inte förändras, eller vid tillfällig verksamhet. En anmälan kan även gälla grundutredningen som helhet, t.ex. att en rutin har upprättats som innebär att kontroll av betyg och intyg alltid genomförs av HR-funktionen. Anmälan görs i IS UNDSÄK, genom att en hemställan sänds till säkerhetsprövningssektionen.

För information om när grundutredningen kan göras mindre omfattande vid säkerhetsskyddad upphandling se avsnitt 6.17.3.

6.8.9. Ansökan om deltagande utan placering i säkerhetsklass

Om en person i sin befattning enbart kommer att delta i säkerhetskänslig verksamhet och där befattningen till följd av detta inte är placerad i säkerhetsklass, ska grundutredningen genomföras enligt avsnitt 6.8. Någon registerkontroll ska inte genomföras i dessa fall.

Moment 6:40 *Om befattningen inte är placerad i säkerhetsklass ska en ansökan om deltagande i säkerhetskänslig verksamhet skickas till säkerhetsprövningssektionen vid Must.*

Moment 6:41 *En ansökan om deltagande i säkerhetskänslig verksamhet ska innehålla personuppgifter, kontrollorsak och kontrollorsakstext. Vid ansökan ska nivå ”Ej RK” väljas.*

Vägledande förklaring: Vid ansökan används de kontrollorsaker som beskrivs i moment 6:47. Säkerhetsprövningssektionen granskar uppgifterna och fattar ett beslut i ärende om säkerhetsprövning. Efter beslutet ska organisationsenheten meddela säkerhetsprövningssektionen om personen ska delta i den säkerhetskänsliga verksamheten eller inte. Om beslutet meddelats skriftligen ska organisationsenheten skyndsamt vidta eventuella skyddsåtgärder.

En organisationsenhet kan även ansöka om deltagande i säkerhetskänslig verksamhet utan placering i säkerhetsklass, efter ett beslut i ärende om säkerhetsprövning som innebär att en person inte längre uppfyller kraven för en godkänd säkerhetsprövning i befattning som är placerad i säkerhetsklass.

För mer information om beslut i ärende om säkerhetsprövning se avsnitt 6.10.

6.9. Kontroll i register

6.9.1. Registerkontroll och särskild personutredning

> *”Med registerkontroll avses i denna lag att uppgifter hämtas från register som omfattas av lagen (1998:620) om belastningsregister eller lagen (1998:621) om misstankeregister. Med registerkontroll avses också att uppgifter som behandlas med stöd av polisdatalagen (2010:361) hämtas.”*
>
> 3 kap. 13 § säkerhetsskyddslagen

Vägledande förklaring: Närmare bestämmelser om registerkontroll och särskild personutredning regleras i Säkerhetspolisens föreskrifter om säkerhetsskydd. Bestämmelserna om hur en framställan om registerkontroll ska genomföras samt samtycke finns i 6 kap. 7-16 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd. Dessa gäller även för Försvarsmakten och andra myndigheter som hör till Försvarsdepartementet samt Fortifikationsverket och Försvarshögskolan.[201]

> *”Registerkontroll ska göras om anställningen eller deltagandet i verksamheten har placerats i säkerhetsklass. Uppgifter ska löpande hämtas under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.”*
>
> 3 kap. 14 § första stycket säkerhetsskyddslagen

Vägledande förklaring: Registerkontroll innebär i praktiken att Säkerhetspolisen genomför en kontinuerlig bevakning av tillkommande uppgifter i de register som är aktuella för registerkontroll (s.k. spontanuppföljning).[202]

> *”En särskild personutredning ska göras vid en registerkontroll som avser sådan anställning eller annat deltagande i verksamhet som har placerats i säkerhetsklass 1 eller 2. Utredningen ska omfatta en undersökning av den kontrollerades ekonomiska förhållanden. I övrigt ska utredningen ha den omfattning som behövs.”*
>
> 3 kap. 17 § säkerhetsskyddslagen

Vägledande förklaring: Det är Säkerhetspolisens uppgift att genomföra särskilda personutredningar.[203] Den särskilda personutredningen är inte en del av registerkontrollen utan ett separat moment. En särskild personutredning omfattar även den medkontrollerades ekonomiska förhållanden.[204]

---

[201] 7 kap. 4 § första stycket 2 säkerhetsskyddsförordningen och 1 kap. 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd.
[202] Säkerhetspolisens vägledning i säkerhetsskydd – Personalsäkerhet (juni 2019), kapitel 5.2.7.
[203] 5 kap. 18 § säkerhetsskyddsförordningen.
[204] Säkerhetspolisens vägledning i säkerhetsskydd – Personalsäkerhet (juni 2019), kapitel 5.2.1.

Observera!
Inför registerkontroll ska den prövade lämna sitt samtycke (avsnitt 6.7).

Moment 6:42 *Organisationsenheten ska minst en gång om året, samt vid behov, genomföra översyn och säkerställa att endast de som deltar i verksamheten på en säkerhetsklassad befattning är registerkontrollerade samt att de har en registerkontroll i rätt säkerhetsklass.*

Vägledande förklaring: En registerkontroll ska avslutas när personen inte längre deltar i den befattningsspecifika verksamheten. Översynen genomförs för att säkerställa att endast de som deltar i verksamheten har en aktiv registerkontroll i rätt säkerhetsklass. Översynen ska enligt moment 6:6 i avsnitt 6.2 även genomföras efter att befattningsanalysen har uppdaterats eller förändrats.

Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, bemyndigas att

1. ansöka om registerkontroll hos Säkerhetspolisen enligt 5 kap. 15 § säkerhetsskyddsförordningen (2018:685),

2. hos regeringen eller Säkerhetspolisen begära att registerkontroll ska göras utan placering i säkerhetsklass enligt 5 kap. 13 § säkerhetsskyddsförordningen,

3. hos Säkerhetspolisen ansöka om en förnyad registerkontroll enligt 6 kap. 14 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2), och

4. hos Säkerhetspolisen anmäla att registerkontroll ska avslutas samt anmäla ändring av den registerkontrollerades förhållanden enligt 6 kap. 15 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).

5 kap. 18 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Säkerhetsprövningssektionen ansöker om registerkontroll hos Säkerhetspolisen. Vid säkerhetsprövningssektionen finns Försvarsmaktens kontaktpersoner gentemot Säkerhetspolisen i ärenden om registerkontroll och särskild personutredning.[205]

6.9.2. Framställan om registerkontroll

”Säkerhetspolisen ska utföra en registerkontroll efter ansökan från den som beslutat om placering i säkerhetsklass eller från en sådan verksamhetsutövare som avses i 9 § eller från den som i annat fall beslutat om registerkontroll.”

5 kap. 15 § första stycket säkerhetsskyddsförordningen

[205] 6 kap. 16 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

”Om säkerhetsprövningen inte avslutats enligt 12 § första stycket ska chef för en organisationsenhet, eller den chefen för organisationsenheten bestämmer, i förekommande fall göra en framställan om registerkontroll hos den militära underrättelse- och säkerhetstjänsten i Högkvarteret.”

5 kap. 16 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 6:43 *Organisationsenheten ska framställa om registerkontroll hos säkerhetsprövningssektionen vid Must.*

Vägledande förklaring: Registerkontroller i Försvarsmakten hanteras digitalt i RK-rutinen i IS UNDSÄK. Säkerhetsprövningssektionen bestämmer vilka uppgifter som ska registreras i RK-rutinen.

Moment 6:44 *En ansökan om registerkontroll ska innehålla:*

a) De personuppgifter som Säkerhetspolisen efterfrågar.

b) Säkerhetsklass.

c) Kontrollorsak och kontrollorsakstext.

d) Vid säkerhetsskyddad upphandling ska uppdrag, företag och befattning i företaget anges.

Vägledande förklaring: Säkerhetspolisen efterfrågar bl.a. personuppgifter: personnummer, efternamn, samtliga förnamn, telefonnummer, passnummer (för utländska medborgare), födelseort och födelseland (om ej Sverige), nuvarande och tidigare medborgarskap, senaste bostadsadress i utlandet samt folkbokföringsadress.

Moment 6:45 *Vid säkerhetsklass 1 och 2 ska ansökan kompletteras med* Bilaga – Särskild personutredning för säkerhetsklass 1 och 2. *Bilagan ska skickas till säkerhetsprövningssektionen vid Must, efter att ansökan om registerkontroll har lagts in i RK-rutinen i IS UNDSÄK.*

Vägledande förklaring: Bilagan, som tillhandahålls av Säkerhetspolisen, sänds med rekommenderad post till säkerhetsprövningssektionen. Framställan om registerkontroll kan inte skickas till Säkerhetspolisen förrän bilagan har kommit säkerhetsprövningssektionen tillhanda.

Moment 6:46 *Om ett deltagande i en säkerhetskänslig verksamhet är tidsbegränsat ska detta framgå vid ansökan om registerkontroll och en sluttid ska anges i RK-rutinen i IS UNDSÄK.*

Observera!
I Försvarsmakten har det tidigare funnits en princip, som inneburit att yrkesofficerare, specialistofficerare och reservofficerare alltid har haft en registerkontroll i säkerhetsklass 3, oavsett om de har haft en annan registerkontroll med placering i högre säkerhetsklass, en så kallad ”grundtrea”.

Principen med ”grund trea” ska inte längre användas. Detta innebär att yrkesofficer, specialistofficer och reservofficer som är placerade på en befattning i säkerhetsklass 1 eller 2, endast ska ha en registerkontroll i säkerhetsklass 1 eller 2, och en eventuell ”grundtrea” ska därmed avslutas.

”Av framställan om registerkontroll ska kontrollorsaken framgå tydligt, t.ex. vilken typ av säkerhetskänslig verksamhet personen avses delta i samt vilka arbetsuppgifter han eller hon avses få.”

6 kap. 12 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Moment 6:47 *Endast följande kontrollorsaker för registerkontroll får användas.*

- *AVTALSPERSONAL - för avtalspersonal, samt för person som deltar i frivillig försvarsverksamhet i syfte att teckna avtal (såsom grundläggande soldatutbildning för frivilliga, GU-F) enligt förordningen (1994:524) om frivillig försvarsverksamhet. Vilken frivillig försvarsorganisation som är aktuell ska anges i kontrollorsakstexten.*

- *BEFÄLFÖRSTÄRKNINGSAVTAL – används vid tillfälligt behov av militär personal i fredsorganisationen, men som inte innebär kommendering eller placering av yrkesofficerare. Anställningen görs med stöd av 1 § p 3 förordningen (FFS 1987:8) om frivillig tjänstgöring vid Försvarsmakten.*

- *BEREDSKAP I NBG – ska i dagsläget inte användas.*

- *BEREDSKAP I REGISTERFÖRBAND - för person i registerförband, när personen saknar annan relevant registerkontroll.*

- *BESÖK/INPASSAGE – används när placering i säkerhetsklass krävs för exempelvis tillträde till skyddsobjekt. Används endast i det fall någon av de andra kontrollorsakerna inte är tillämpliga. Registerkontrollen ska vara tidsbegränsad.*

- *CIVIL ANSTÄLLNING - för civilt anställd personal. Kontrollorsaken ska även användas för en civilanställd som är placerad på en militär befattning.*

- *GRUPPBEFÄL, SOLDAT, SJÖMAN - för gruppbefäl, soldat och sjöman (GSS), oavsett om personen är kontinuerligt (K) eller tidvis (T) tjänstgö-*

rande. Vilken typ av befattning som avses ska specificeras i kontrollorakstexten.

- *HEMVÄRNSSOLDAT - för hemvärnssoldater och hemvärnsmusiker som tecknat avtal enligt hemvärnsförordningen (1997:146).*

- *HEMVÄRNSVETERAN - för hemvärnsveteran i befattning som är placerad i säkerhetsklass.*

- *INSTRUKTÖR VID HEMVÄRNET - för instruktör vid Hemvärnet, när denne saknar annan relevant registerkontroll.*

- *KRIGSPLACERING - för krigsplacerad som saknar annan relevant registerkontroll.*

- *OFFICER i säkkl 1 och 2 - för officer och specialistofficer i säkerhetsklass 1 och 2. För civilt anställd personal som är placerad på en militär befattning används kontrollorsak ”CIVIL ANSTÄLLNING”.*

- *OFFICERSUTBILDNING - används för personer som ska genomföra någon form av officersutbildning. Registerkontrollen ska vara tidsbegränsad.*

- *REKRYT - för värnpliktig enligt lagen (1994:1809) om totalförsvarsplikt. (kontrollorsaken kommer att ändras till VÄRNPLIKTIG alternativt TOTALFÖRSVARSPLIKTIG).*

- *SECURITY CLEARANCE – kan utfärdas efter ansökan av en annan stat eller en mellanfolklig organisation. Kontrollorsaken får endast användas av säkerhetsprövningssektionen vid Must.*

- *SUA-ARBETE - för personal hos leverantör som omfattas av säkerhetsskyddad upphandling, samt leverantörens ledning, styrelse och säkerhetsskyddschef. Kontrollorsaken ska kompletteras med uppgifter om företag, befattning i företaget, samt vilket uppdrag eller projekt det gäller. Om uppdraget är tidsbegränsat ska även registerkontrollen vara tidsbegränsad.*

- *UTBILDNING/KURS/ÖVNING - för deltagare i utbildning, kurs eller övning som saknar annan relevant registerkontroll. Registerkontrollen ska vara tidsbegränsad.*

- *UTLANDSTJÄNSTGÖRING – kontrollorsaken ska användas vid internationell insats i det fall annan relevant registerkontroll inte finns. Registerkontrollen ska vara tidsbegränsad, och ange vilken insats det gäller t.ex. ”Mali 12”. Kontrollorsaken ska inte användas för korta internationella tjänsteresor (exempelvis vid konferenser och möten) om annan relevant registerkontroll finns. För att en registerkontroll ska vara relevant ska den vara framställd*

för en befattning där det i befattningsanalysen tagits höjd för internationell tjänstgöring.

- *YRKESOFFICER, RESERVOFFICER - för officer och specialistofficer, oavsett om de är kontinuerligt (K) eller tidvis (T) tjänstgörande. För civilt anställd som är placerade på en militär befattning används kontrollorsak "CIVIL ANSTÄLLNING".*

- *ÖVRIGT - används i undantagsfall när ovanstående kontrollorsaker inte är tillämpbara.*

Moment 6:48 *Kontrollorsaken ska kompletteras med en beskrivning av orsaken till placering i säkerhetsklass, samt vilken befattning som avses. En sådan beskrivning av orsaken till placering i säkerhetsklass får endast begränsas i omfattning efter beslut vid säkerhetsprövningssektion vid Must.*

Vägledande förklaring: Beskrivningen av vilken typ av säkerhetskänslig verksamhet som personen ska delta i och vilka arbetsuppgifter som personen kommer att ha ska anges i fältet "Kontrollorsakstext" i RK-rutinen. Kontrollorsakstexten får inte innehålla förkortningar.

Två exempel på godkänd beskrivning

Kontrollorsak: Civil anställning
Kontrollorsakstext: Expeditionshandläggare, hanterar säkerhetsskyddsklassificerade handlingar upp till och med kvalificerat hemlig.

Kontrollorsak: Yrkesofficer, reservofficer
Kontrollorsakstext: Yrkesofficer, arbetar med totalförsvarsplanering och har tillgång till anläggning av kritisk betydelse för Sveriges säkerhet.

Två exempel på en beskrivning som inte är godkänd

Kontrollorsak: Yrkesofficer, reservofficer
Kontrollorsakstext: YO ORGE STAB

Kontrollorsak: Utlandstjänstgöring
Kontrollorsakstext: Logistic clerk /STEX

6.9.3. Framställan om registerkontroll vid säkerhetsskyddad upphandling

> *”Framställan om registerkontroll av personal hos en leverantör som verksamhetsutövaren har ingått säkerhetsskyddsavtal med, får göras först när avtalet har anmälts till Säkerhetspolisen.*
>
> *En framställan om registerkontroll får innehålla hänvisning till endast ett säkerhetsskyddsavtal.”*
>
> 6 kap. 9 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Moment 6:49 *Den som har tecknat ett säkerhetsskyddsavtal ska ansöka om registerkontroll av leverantörens personal hos säkerhetsprövningssektionen vid Must. Underlag för säkerhetsskyddad upphandling ska vara säkerhetsprövningssektionen vid Must tillhanda senast två veckor innan ansökan om registerkontroll.*

Vägledande förklaring: Ansökan görs via registrering av uppdrag och säkerhetsskyddsavtal i SUA-rutinen i IS UNDSÄK. Efter registrering i SUA-rutinen ska ett SUA-underlag skrivas ut och skickas till säkerhetsprövningssektionen. För att ansökan om registerkontroll ska kunna genomföras måste SUA-rutinen innehålla uppgifter om vilket affärsavtal som säkerhetsskyddsavtalet är kopplat till.

Anmälan om säkerhetsskyddsavtal beskrivs i avsnitt 8.13.

6.9.4. När ska registerkontrollen göras om?

> *”Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska se till att en förnyad registerkontroll görs när någon som innehar en säkerhetsklassad befattning får en annan befattning som inte omfattas av tidigare kontrollorsak eller den befintliga befattningen blir inplacerad i en annan säkerhetsklass. Detsamma gäller, såvitt avser registerkontrollerade personer i säkerhetsklass 1 eller 2, om den kontrollerade ingått äktenskap eller inlett ett samboförhållande efter den senaste registerkontrollen.”*
>
> 6 kap. 14 § Säkerhetspolisens föreskrifter om säkerhetsskydd

”När en anställning eller något annat deltagande som föranlett en placering i säkerhetsklass upphör, ska chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, skyndsamt underrätta militära underrättelse- och säkerhetstjänsten i Högkvartetet.

Detsamma gäller, såvitt avser registerkontrollerade personer som innehar en befattning i säkerhetsklass 1 eller 2, om

1. den registerkontrollerade personen ingått äktenskap eller inlett ett sambo-förhållande efter den senaste registerkontrollen, eller

2. den registerkontrollerade personens äktenskap upplösts eller om sambo-förhållandet har upphört.”

5 kap. 17 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Det är den organisationsenhet som tidigare har ansökt om registerkontroll som ansvarar för att en ny ansökan inkommer till säkerhetsprövningssektionen.

KOM IHÅG!
Enligt tidigare regelverk förnyades registerkontroller i säkerhetsklass 1 vart tredje år och i säkerhetsklass 2 vart femte år. Registerkontroller genomförda efter den 1 april 2019 har inget avslutningsdatum, med anledning av att kravet på förnyad kontroll tagits bort i nya lagstiftningen.

Registerkontroller i säkerhetsklass 1 och 2 som är genomförda fram till och med den 31 mars 2019 har ett automatiskt avslutningsdatum. Den organisationsenhet som ansökt om registerkontroll ska genomföra en förnyad kontroll i god tid innan den pågående kontrollen automatiskt avslutas. Om en sådan registerkontroll innehåller felaktig kontrollorsakstext (felaktig information om arbetsuppgifter) ska kontrollen snarast förnyas.

Moment 6:50 *Om en befattnings placering i säkerhetsklass har ändrats till en annan säkerhetsklass får inte den befintliga registerkontrollen avslutas förrän den nya registerkontrollen har godkänts vid säkerhetsprövningssektionen vid Must.*

6.9.5. Flytt av registerkontroll mellan organisationsenheter

Moment 6:51 *En organisationsenhet kan begära flytt av en registerkontroll:*

a) Om den befintliga befattningen flyttas till en annan organisationsenhet p.g.a. en organisationsförändring och befattningsanalysen inte förändras.

b) Om en person byter arbetsplats till en annan organisationsenhet och befattningsanalysen, kontrollorsak och arbetsuppgifter är desamma.

Vägledande förklaring till punkten a: Avser att personen enbart byter organisationsenhet, men inte befattning, samt att kontrollorsak och arbetsuppgifter är desamma.

Vägledande förklaring till punkten b: Flytt av en registerkontroll ska inte genomföras vid t.ex. tillfälliga bemanningsuppdrag. Istället ska den organisationsenhet där personen ska genomföra uppdraget ansöka om en ny tidsbegränsad registerkontroll. En person som genomför ett tillfälligt bemanningsuppdrag kan ha flera registerkontroller under tiden för uppdraget.

Moment 6:52 *Den mottagande organisationsenheten ska hemställa om flytt av registerkontroll hos säkerhetsprövningssektionen vid Must samt meddela den avlämnade organisationsenheten om att flytt av registerkontroll kommer att genomföras.*

Vägledande förklaring: Flytt av registerkontroll genomförs vid säkerhetsprövningssektionen. Vid säkerhetsprövningssektionen kan beslut fattas om att registerkontrollen ska göras om istället för att flyttas, t.ex. om kontrollorsakstexten är ofullständig eller om andra felaktigheter upptäcks.

6.9.6. Avanmälan eller ändring av den kontrollerades förhållanden

”Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska skriftligen underrätta Säkerhetspolisen om den kontrollerade inte längre har en befattning som är inplacerad i säkerhetsklass. Detsamma gäller, såvitt avser registerkontrollerade personer i säkerhetsklass 1 eller 2, om den kontrollerades äktenskap har upplösts eller om samboförhållandet har upphört. Underrättelsen ska ske på av Säkerhetspolisen anvisad blankett.”

6 kap. 15 § Säkerhetspolisens föreskrifter om säkerhetsskydd

”Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska se till att en förnyad registerkontroll görs när någon som innehar en säkerhetsklassad befattning får en annan befattning som inte omfattas av tidigare kontrollorsak eller den befintliga befattningen blir inplacerad i en annan säkerhetsklass. Detsamma gäller, såvitt avser registerkontrollerade personer i säkerhetsklass 1 eller 2, om den kontrollerande ingått äktenskap eller inlett ett samboförhållande efter den senaste registerkontrollen.”

6 kap. 14 § Säkerhetspolisens föreskrifter om säkerhetsskydd

”När en anställning eller något annat deltagande som föranlett en placering i säkerhetsklass upphör, ska chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, skyndsamt underrätta militära underrättelse- och säkerhetstjänsten i Högkvartetet.

Detsamma gäller, såvitt avser registerkontrollerade personer som innehar en befattning i säkerhetsklass 1 eller 2, om

1. den registerkontrollerade personen ingått äktenskap eller inlett ett sambo-förhållande efter den senaste registerkontrollen, eller

2. den registerkontrollerade personens äktenskap upplösts eller om sambo-förhållandet har upphört.”

5 kap. 17 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, bemyndigas att

3. hos Säkerhetspolisen ansöka om en förnyad registerkontroll enligt 6 kap. 14 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2), och

4. hos Säkerhetspolisen anmäla att registerkontroll ska avslutas samt anmäla ändring av den registerkontrollerades förhållanden enligt 6 kap. 15 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).”

5 kap. 18 § 3 och 4 Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Säkerhetsprövningssektionen ansöker om förnyad registerkontroll samt anmäler avslut och ändring av en registerkontroll till Säkerhetspolisen.

Varje organisationsenhet ansvarar för att uppgifterna i en persons registerkontroll är korrekta, vad gäller personer som deltar i egen verksamhet. Varje person är enskilt ansvarig för att meddela förändringar som påverkar uppgifterna i en registerkontroll. Den organisationsenhet som framställt om registerkontroll ansvarar för att varje individ informeras som sina skyldigheter.

Avanmälan av en registerkontroll görs till säkerhetsprövningssektionen genom att den avslutas i RK-rutinen i IS UNDSÄK. Om avanmälan endast gäller medkontrollerad ska registerkontrollen inte avslutas för den huvudkontrollerade. Medkontrollerad ska istället avregistreras i den befintliga registerkontrollen.

6.9.7. Avanmälan av registerkontroll vid säkerhetsskyddad upphandling

Moment 6:53 *Den som har ingått ett säkerhetsskyddavtal ansvarar för att registerkontrollen avslutas när uppdraget avslutas eller upphör.*

Vägledande förklaring: Efter att den som ansvarar för ett säkerhetsskyddsavtal har avslutat registerkontrollen ansvarar säkerhetsprövningssektionen för att avanmäla

registerkontrollen hos Säkerhetspolisen. Säkerhetspolisen ska även meddelas om att säkerhetsskyddsavtalet har avslutats eller upphört.[206] Det genomförs genom att uppdraget avslutas i SUA-rutinen i IS UNDSÄK och ett SUA-underlag skrivs ut och skickas till säkerhetsprövningssektionen, som sedan ansvarar för att meddela Säkerhetspolisen. Avslutat uppdrag ska även meddelas säkerhetsskyddsavdelningen vid Must (avsnitt 8.15).

6.9.8. Resultat från registerkontroll

Säkerhetspolisen informerar säkerhetsprövningssektionen om resultatet av en registerkontroll. Säkerhetsprövningssektionen meddelar i sin tur resultatet till den organisationsenhet som har ansökt om registerkontroll.

6.9.8.1 Ingen utlämning från Säkerhetspolisen

Om det inte finns några uppgifter från registerkontrollen fattas ett beslut i ärende om säkerhetsprövning vid säkerhetsprövningssektionen. Efter mottagande av beslutet ska organisationsenheten meddela säkerhetsprövningssektionen om personen ska delta i den säkerhetskänsliga verksamheten eller inte (avsnitt 6.10.3).

6.9.8.2 Utlämning från Säkerhetspolisen

Om en person förekommer i något av de register som kontrolleras vid registerkontroll, kan Säkerhetspolisen komma att lämna ut uppgiften till säkerhetsprövningssektionen. Vid säkerhetsprövningssektionen bereds detta och ett beslut i ärende om säkerhetsprövning beslutas. Beslutet meddelas i detta fall skriftligen (avsnitt 6.10).

Säkerhetsprövningssektionen ansvarar för att, enligt 6 kap. 13 § Säkerhetspolisens föreskrifter om säkerhetsskydd, underrätta Säkerhetspolisen om att personen är godkänd vid säkerhetsprövningen eller inte.

6.9.9. Registerkontroll utan placering i säkerhetsklass

I vissa fall kan registerkontroll genomföras utan att befattningen är placerad i säkerhetsklass. En sådan registerkontroll får genomföras när det finns särskilda skäl, enligt 3 kap. 15 § säkerhetsskyddslagen (avsnitt 6.2.5), och genomförs enligt ordinarie rutin för registerkontrollansökan.

6.9.10. Undantag från registerkontroll

> *”Säkerhetsprövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas och ska innefatta en grundutredning samt registerkontroll och särskild personutredning i den omfattning som anges i 13, 14 och 17 §§. Om det finns särskilda skäl får säkerhetsprövningen göras mindre omfattande.”*
>
> 3 kap. 3 § första stycket säkerhetsskyddslagen

[206] 7 kap 12 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2)

Vägledande förklaring: Huvudregeln är att säkerhetsprövningen ska innefatta en registerkontroll om befattningen är placerad i säkerhetsklass.[207] Särskilda skäl för att göra undantag från registerkontroll kan vara om den prövade redan har registerkontrollerats på motsvarande sätt.[208] Ett undantag kan t.ex. göras om en likvärdig registerkontroll finns – det vill säga rätt säkerhetsklass, samma kontrollorsak och likvärdiga arbetsuppgifter. Vid säkerhetsprövningssektionen avgörs om det i det enskilda fallet finns särskilda skäl.

Moment 6:54 *Om en organisationsenhet bedömer att en registerkontroll inte behöver göras enligt 3 kap. 3 § första stycket säkerhetsskyddslagen, ska det anmälas till säkerhetsprövningssektionen vid Must som bestämmer om registerkontroll inte behöver göras.*

6.9.11. Registerutdrag

Om det behövs för en lämplighetsbedömning inför antagning till vissa militära utbildningar samt internationella insatser kan grundutredningen även kompletteras med ett registerutdrag.[209] Om befattningen är placerad i säkerhetsklass genomförs registerkontroll istället för registerutdrag. I de fall detta avser totalförsvarspliktiga som skrivs in eller är inskrivna för värnplikt lämnas registerutdraget ut efter begäran av Totalförsvarets rekryteringsmyndighet.[210]

6.10. Beslut i ärende om säkerhetsprövning

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, beslutar om den som säkerhetsprövningen gäller uppfyller kraven för en godkänd säkerhetsprövning. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”

5 kap. 14 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

”Ett beslut om godkänd säkerhetsprövning ska omprövas om den prövningen gäller, inte längre uppfyller kraven för godkännandet. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”

5 kap. 15 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Ett beslut i ärende om säkerhetsprövning fattas inför deltagande i säkerhetskänslig verksamhet, men kan även omprövas under tiden för deltagandet (avsnitt 6.10.1). Genom interna styrdokument på Must är bemyndigandet att fatta beslut i ärende om säkerhetsprövning delegerat till chefen för säkerhetspröv-

[207] 3 kap. 14 § säkerhetsskyddslagen.
[208] Prop. 2017/18:89 s. 144.
[209] 10 och 15 §§ förordningen (1999:1134) om belastningsregister, samt 4 § 16-17 förordningen (1999:1135) om misstankeregister.
[210] Den 1 februari 2021 ändras myndighetens namn till Totalförsvarets plikt- och prövningsverk.

ningssektionen. Chef för en organisationsenhet kan inte besluta i ärende om säkerhetsprövning eller ompröva ett sådant beslut, däremot kan chefen avsluta en säkerhetsprövning under grundutredningen (avsnitt 6.8.5).

Observera!
Beslut i ärende om säkerhetsprövning kan inte fattas av chefen för en organisationsenhet.

Beslut i ärende om säkerhetsprövning hanteras på två sätt. I det fall där en person uppfyller kraven för en godkänd säkerhetsprövning, och där det inte framkommit några brister i pålitlighet, lojalitet eller sårbarhet i säkerhetshänseende, meddelas beslutet direkt i RK-rutinen i IS UNDSÄK. I de fall där det framkommit brister i pålitlighet, lojalitet eller sårbarhet i säkerhetshänseende meddelas beslutet skriftligen (tidigare benämndes sådana beslut ”Säkerhetsskyddsbeslut i personärende”).

Ett beslut i ärende om säkerhetsprövning har något av de fem lydelser som anges i tabell 6.3.

Tabell 6.3. Lydelser i beslut i ärende om säkerhetsprövning. [ ] anger alternativ. <specifik befattning> anger att benämningen på en befattning skrivs ut.

I det fall en person uppfyller kraven för en godkänd säkerhetsprövning och beslutet inte meddelas skriftligen	
1	Godkänd säkerhetsprövning.

I det fall beslutet meddelas skriftligen	
2	Uppfyller kraven för en godkänd säkerhetsprövning avseende befattning i [säkerhetsklass 1] [säkerhetsklass 2] [säkerhetsklass 3] [säkerhetskänslig verksamhet].
3	Uppfyller kraven för en godkänd säkerhetsprövning avseende befattning i [säkerhetsklass 1] [säkerhetsklass 2] [säkerhetsklass 3] [säkerhetskänslig verksamhet], med följande villkor.
4	Uppfyller inte kraven för en godkänd säkerhetsprövning avseende befattning i [säkerhetsklass 1] [säkerhetsklass 2] [säkerhetsklass 3] [säkerhetskänslig verksamhet].
5	Uppfyller inte kraven för en godkänd säkerhetsprövning avseende <specifik befattning>.

Beslut enligt punkt 5 fattas när en person har bedömts vara särskilt sårbar i en specifik befattning, men kan placeras på en annan befattning i samma säkerhetsklass.

Exempel på beslut i ärende om säkerhetsprövning enligt punkt 3
Uppfyller kraven för godkänd säkerhetsprövning avseende befattning i säkerhetsklass 3 med följande villkor.

Restriktioner: Får inte hantera vapen, ammunition och sprängmedel.

Exempel på beslut i ärende om säkerhetsprövning enligt punkt 5
Uppfyller inte kraven för en godkänd säkerhetsprövning avseende befattning expeditionshandläggare vid Ledningsregementet.

Ett beslut i ärende om säkerhetsprövning kan förenas med villkor om ytterligare skyddsåtgärder såsom särskild uppföljning (avsnitt 6.10.2.1), restriktioner (avsnitt 6.10.2.2), säkerhetssamtal (avsnitt 6.13.1), samt skyddssamtal (6.11.2). Av beslut i ärende om säkerhetsprövning kan det även framgå vem som ska genomföra vissa skyddsåtgärder. Ett beslut i ärende om säkerhetsprövning gäller alltid tillsvidare, vilket innebär att även de villkor som ingår i beslutet gäller tillsvidare, om inte annat angivits.

Om brister upptäcks vad gäller pålitlighet, lojalitet och sårbarhet i säkerhetshänseende för en person som har en godkänd säkerhetsprövning ska organisationsenheten påbörja en utredning och meddela säkerhetsprövningssektionen (avsnitt 6.13). Utredningen kan komma att ligga till grund för omprövning av beslut i ärende om säkerhetsprövning.

Moment 6:55 *Organisationsenheten ska skyndsamt ansöka om deltagande i säkerhetskänslig verksamhet, om:*

a) en person som är anställd i Försvarsmakten inte uppfyller kraven för en godkänd säkerhetsprövning för en befattning placerad i säkerhetsklass, och

b) personen ändå ska delta i Försvarsmaktens säkerhetskänsliga verksamhet.

Vägledande förklaring: Se rutin i avsnitt 6.8.9 om ansökan om deltagande utan placering i säkerhetsklass.

Observera!
Beslut i ärende om säkerhetsprövning omfattas av sekretess enligt 15 kap. 2 § OSL.

6.10.1. Omprövning av beslut i ärende om säkerhetsprövning

> *”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, beslutar om den som säkerhetsprövningen gäller uppfyller kraven för en godkänd säkerhetsprövning. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”*
>
> 5 kap. 14 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

> *”Ett beslut om godkänd säkerhetsprövning ska omprövas om den prövningen gäller, inte längre uppfyller kraven för godkännandet. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”*
>
> 5 kap. 15 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Genom interna styrdokument vid Must är bemyndigandet att ompröva beslut i ärende om säkerhetsprövning delegerat till chefen för säkerhetsprövningssektionen. Ett sådant beslut meddelas skriftligen.

Ett beslut i ärende om säkerhetsprövnings omprövas i följande fall.

- Om det under tiden för en persons deltagande framkommer brister i pålitlighet, lojalitet eller sårbarhet i säkerhetshänseende.
- Om organisationsenheten bedömer att en person som inte har en godkänd säkerhetsprövning åter kan placeras på en befattning som är placerad i säkerhetsklass.
- Om ett tidigare beslut omfattas av villkor och organisationsenheten bedömer att det inte längre finns behov av ett eller flera villkor.

Ett beslut i ärende om säkerhetsprövning med innebörden att en person inte uppfyller kraven för en godkänd säkerhetsprövning, eller om beslutet omfattas av villkor kan endast ändras om de omständigheter som låg till grund för det tidigare beslutet har förändrats. För att det ska vara möjligt att bedöma om personen uppfyller kraven för en godkänd säkerhetsprövning, med eller utan villkor, krävs att tidigare beslutade skyddsåtgärder har genomförts (avsnitt 6.10.2) samt att det finns en dokumenterad uppföljning av den prövade (avsnitt 6.11).

Moment 6:56 *Om ett beslut om godkänd säkerhetsprövning ska omprövas, ska chef för organisationsenheten hemställa om omprövning hos säkerhetsprövningssektionen vid Must. Hemställan ska innehålla den dokumentation som finns om den prövade, samt en bedömning av personens pålitlighet, lojalitet och sårbarhet i säkerhetshänseende.*

Vägledande förklaring: Ett omprövat beslut i ärende om säkerhetsprövning gäller alltid tillsvidare, vilket innebär att även de villkor som ingår i beslutet gäller tillsvidare, om inte annat angivits.

6.10.2. Villkor vid beslut i ärende om säkerhetsprövning

Ett beslut i ärende om säkerhetsprövning kan förenas med villkor om ytterligare skyddsåtgärder. Av beslutet kan det även framgå vem som ska genomföra vissa skyddsåtgärder. De villkor som ingår i beslutet gäller tillsvidare om inget annat angivits. Villkoren kan omfatta skyddsåtgärder såsom särskild uppföljning (avsnitt 6.10.2.1, restriktioner (avsnitt 6.10.2.2), säkerhetssamtal (avsnitt 6.13.1), samt skyddssamtal (6.11.2).

Inom ramen för arbetsledningsrätten och inom ramen för övriga mandat kan chef för en organisationsenhet besluta om tillfälliga skyddsåtgärder kopplat till den som har varit föremål för säkerhetsprövning. Sådana tillfälliga skyddsåtgärder bör förenas med ett slutdatum och ska enligt moment 6:12 meddelas till säkerhetsprövningssektionen.

6.10.2.1 Särskild uppföljning

> *”Myndigheten ska förebygga och vidta rimliga skyddsåtgärder för att minska sårbarheter hos personer som deltar i myndighetens säkerhetskänsliga verksamhet.”*
>
> 6 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: En skyddsåtgärd, när brister i pålitlighet, lojalitet eller sårbarheter i säkerhetshänseende har identifierats hos en person, är att genomföra en särskild uppföljning av personen. Syftet med den särskilda uppföljningen är att kontrollera och följa en persons utveckling, samt att stötta personen med att komma tillrätta med den situation som har föranlett beslutet eller utredningen. Den särskilda uppföljningen kan innehålla åtgärder såsom att följa en rehabilitering eller en ekonomisk problematik, t.ex. genom kontakt med vårdgivare (efter medgivande från den enskilde) eller kontinuerliga ekonomiska kontroller.

Målet med den särskilda uppföljningen är att personen ska kunna placeras på en befattning i säkerhetsklass, placeras i en befattning i en högre säkerhetsklass, eller att den särskilda uppföljningen ska kunna avslutas. För att kunna inhämta ett tillräckligt underlag inför en ny bedömning av personen krävs det att uppföljningen fortgår under en längre tid.

Organisationsenheten ska utse vem som ska genomföra den särskilda uppföljningen och se till att personen är behörig (avsnitt 6.5). Av ett beslut i ärende om säkerhetsprövning kan det framgå vem som ska genomföra den särskilda uppföljningen (avsnitt 6.3).

Moment 6:57 *Den särskilda uppföljningen ska innefatta samtal. Samtalen ska dokumenteras och sparas vid organisationsenheten.*

Vägledande förklaring: Samtalen ska inriktas mot den omständighet som den särskilda uppföljningen grundas på, och ska även inkludera andra omständigheter som

ur ett säkerhetsperspektiv kan bli en följd av grundproblematiken, t.ex. kan ett missbruk leda till andra problem i form av ekonomiska svårigheter. Samtalen kan genomföras inom ramen för det ordinarie uppföljande samtalet (avsnitt 6.11.1). Om beslut i ärende om säkerhetsprövning anger en tätare periodicitet, kan ett av samtalet kombineras med det ordinarie uppföljande samtalet.

6.10.2.2 Restriktioner

En restriktion innebär begränsningar i deltagandet i den säkerhetskänsliga verksamheten, t.ex. att en person inte har tillgång till vissa säkerhetsskyddsvärden. Restriktioner genomförs som en skyddsåtgärd när brister i pålitlighet, lojalitet eller sårbarhet i säkerhetshänseende identifierats hos en person. Restriktionerna ska anpassas till de individuella omständigheterna och kan t.ex. omfatta tillgång till vapen, ammunition och sprängmedel, internationell verksamhet inom och utom Sverige samt tillgång till säkerhetsskyddsklassificerade uppgifter.

Chefen för en organisationsenhet ska utse vem som ansvarar för att följa upp att restriktionerna följs. Av ett beslut i ärende om säkerhetsprövning kan det framgå vem som tilldelats ansvaret (avsnitt 6.3).

6.10.3. Organisationsenhetens hantering av beslut i ärende om säkerhetsprövning

Moment 6:58 *Chefen för en organisationsenhet ska efter mottagandet av ett beslut i ärende om säkerhetsprövning meddela säkerhetsprövningssektionen vid Must om den som prövningen gäller ska delta i den säkerhetskänsliga verksamheten eller inte, samt skyndsamt vidta eventuella skyddsåtgärder enligt beslutet.*

Moment 6:59 *Ett meddelande enligt moment 6:58 ska skickas till säkerhetsprövningssektionen vid Must inom en månad efter att beslutet mottagits av organisationsenheten.*

Vägledande förklaring: I det fall säkerhetsprövningen är godkänd innebär det att den lokala säkerhetsorganisationen meddelar beslutet till den som vid organisationsenheten ansvarar för t.ex. rekrytering eller antagning av den prövade. Det kan t.ex. vara fråga om anställning i Försvarsmakten eller hemvärnsavtal. Den lokala säkerhetsorganisationen ska sedan i RK-rutinen i IS UNDSÄK meddela säkerhetsprövningssektionen om den prövade ska delta i den säkerhetskänsliga verksamheten eller inte. Åtgärderna ska även genomföras om en person enbart ska delta i säkerhetskänslig verksamhet utan placering i säkerhetsklass.

När beslut i ärende om säkerhetsprövning meddelats skriftligen ska det mottagningsbevis som medföljer beslutet sändas åter till säkerhetsprövningssektionen. På mottagningsbeviset ska chefen för en organisationsenhet notera att organisationsenheten har tagit del av beslutet, samt meddela om organisationsenheten har vidtagit egna skyddsåtgärder. Om beslutet är förenat med villkor som innebär att samtal ska genomföras med personen, ska dokumentationen från samtalet skickas till säkerhetsprövningssektionen senast i samband med att mottagningsbeviset återsänds. Det ex-

emplar av beslut i ärende om säkerhetsprövning som sänts till organisationsenheten förvaras vid organisationsenheten.

Moment 6:60 *Ett beslut i ärende om säkerhetsprövning får delges den prövade om beslutet inte anger annat. Som skäl för beslutet ska anges att det grundar sig på Försvarsmaktens säkerhetsprövning.*

Vägledande förklaring: I normalfallet ska den prövade endast meddelas om säkerhetsprövningen är godkänd eller inte. Om beslutet har kombinerats med villkor kan bakgrunden till dessa framgå i korthet av beslutet för att organisationsenheten ska ha möjlighet att vidta åtgärder. Uppgifter som kan komma att delges den prövade är omständigheter som personen redan känner till som t.ex. en dom, ett strafföreläggande eller skulder hos Kronofogdemyndigheten.

Observera!
I samband med delgivning ska den prövade informeras om att ett beslut i ärende om säkerhetsprövning omfattas av sekretess enligt 15 kap. 2 § OSL.

6.10.4. Skyddssamtal vid placering i säkerhetsklass

Ett skyddssamtal vid placering i säkerhetsklass syftar till att orientera om säkerhetshotande verksamhet som kan riktas mot personen eller den säkerhetskänsliga verksamhet som personen deltar i. Skyddssamtalet syftar även till att fördjupa personkännedomen genom att personen lämnar uppgifter om sig själv. Genom skyddssamtalet ska personen få förståelse för att denne kan bli ett mål för säkerhetshotande verksamhet och hur sådan verksamhet bedrivs. Skyddssamtalet ska även öka personens säkerhetsmedvetande. Ett skyddssamtal ska inte förväxlas med samtal för att informera om lokala säkerhetsbestämmelser.

Skyddssamtal kan även genomföras vid särskilda behov (avsnitt 6.11.2).

Moment 6:61 *När en person har placerats på en befattning i säkerhetsklass 1 ska ett skyddssamtal hållas snarast efter att personen tillträtt befattningen.*

Moment 6:62 *Vid säkerhetsprövningssektionen vid Must får man bestämma när ett skyddssamtal ska genomföras med en person som har en befattning som är placerad i säkerhetsklass 2 eller 3, eller en befattning som inte har placerats i säkerhetsklass.*

Vägledande förklaring: Det är den organisationsenhet som ansvarar för verksamheten som genomför skyddssamtalet och det genomförs vanligtvis inom några veckor efter personen har tillträtt befattningen och påbörjat deltagandet. När deltagandet inte avser säkerhetsklass 1, genomförs samtalet när det föreligger särskilda omständigheter, t.ex. om det under grundutredningen framkommit sårbarheter i säkerhetshänseende kopplat till en specifik befattning, eller när det föreligger en särskild hotbild mot befattningen. Om det finns ett särskilt behov får skyddssamtal genomföras vid organisationsenheten (moment 6:71). I vissa fall kan ett beslut i ärende om säker-

hetsprövning ställa krav på genomförande av skyddssamtal. I dessa fall ska samtalet genomföras enligt beslutets instruktioner.

Moment 6:63 *Ett skyddssamtal får inte genomföras med flera personer samtidigt, om man inte vid säkerhetsprövningssektionen vid Must har bestämt något annat.*

Vägledande förklaring: Eftersom ett skyddssamtal bl.a. syftar till att inhämta information om den prövade kan det som tas upp under samtalet vara personligt och ska därför inte delges någon annan än de som har beslutats vara behöriga enligt 5 kap. 11 och 13 §§ Försvarsmaktens interna bestämmelser om säkerhetsskydd (avsnitt 6.5). Av samma anledning är det viktigt att inte flera prövande samtidigt deltar i samtalet. Det finns inget hinder mot att man är flera samtalsledare.

Moment 6:64 *När ett skyddssamtal har genomförts ska organisationsenheten meddela säkerhetsprövningssektionen vid Must att det är genomfört.*

Vägledande förklaring: Ett sådant meddelande sänds via RK-rutinen i IS UNDSÄK.

Moment 6:65 *Vid ett skyddssamtal vid placering i säkerhetsklass ska anteckningar föras.*

Vägledande förklaring: Anteckningarna kan föras på dokumentmallen *Samtalsguide skyddssamtal – säkerhetsklass 1 och 2*, och utgör då den dokumentation som ska bevaras från skyddssamtalet. Om anteckningarna inte förts på *Samtalsguide skyddssamtal – säkerhetsklass 1 och 2* ska dokumentmallen fyllas i efter samtalet, och övriga anteckningar kan därefter förstöras. Dokumentmallen får kompletteras med extra sidor.

Uppgifterna som inhämtas vid intervjutillfället omfattas av försvarssekretess enlig 15 kap. 2 § OSL och därför måste informationssystem som är godkända för sådana uppgifter användas, om uppgifterna ska hanteras digitalt. Dokumenten kan även omfattas av annan sekretess till skydd för den enskilde, t.ex. 35 kap. 1 § OSL (enskilds personliga och ekonomiska förhållanden vid registerkontroll) och 38 kap. 4 § OSL (enskilds personliga och ekonomiska förhållanden i försvarsunderrättelseverksamhet och den militära säkerhetstjänsten).

KOM IHÅG!

- Organisationsenheten ska meddela säkerhetsprövningssektionen när ett skyddssamtal är genomfört.
- Skyddssamtalet ska dokumenteras.
- Om brister i pålitlighet, lojalitet eller sårbarhet i säkerhetshänseende framkommit under ett samtal ska det rapporteras till säkerhetsprövningssektionen.

6.11. Uppföljning av säkerhetsprövning

”Säkerhetsprövningen ska följas upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.”

3 kap. 3 § andra stycket säkerhetsskyddslagen

Vägledande förklaring: Säkerhetsprövning är en åtgärd som ska fortgå så länge deltagandet i den säkerhetskänsliga verksamheten pågår. Krav på uppföljning innebär bl.a. att uppgifterna i grundutredningen ska hållas uppdaterade. Under anställningstiden handlar det om att skaffa sig en fördjupad personkännedom genom t.ex. regelbundna kontakter och uppföljningssamtal för att fånga upp upplevt missnöje med arbetssituationen eller kontaktförsök från främmande makt. Förhållanden som kan påverka risk och mottaglighet för utpressning eller omständigheter som tyder på att personen är i riskzonen för olika former av missbruk ska också uppmärksammas. Det kan även finnas anledning att lägga särskild vikt vid tillfällen som innebär större förändringar av arbetsuppgifterna.[211]

”Myndigheten ska genomföra uppföljande säkerhetsprövning. Prövningen ska fördjupa personkännedomen och särskild vikt ska vid en bedömning läggas vid personliga förhållanden.

Den uppföljande säkerhetsprövningen ska dokumenteras.”

6 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd

[211] Prop. 2017/18:89 s. 144.

”I övriga fall än de som regleras i 8 § ansvarar chef för organisationsenhet för att grundutredning genomförs vid egen organisationsenhet, samt att säkerhetsprövningen följs upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.

I ansvaret ingår att

1. besluta vilka som får genomföra grundutredning och uppföljning,

2. besluta vilka personer som i övrigt är behöriga att ta del av uppgifter som förekommer i ärenden om säkerhetsprövning, och

3. se till att personal som arbetar med säkerhetsprövning har relevant utbildning och är lämpliga för uppgiften i enlighet med 6 kap. 2 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.

Om det under uppföljning av deltagandet i den säkerhetskänsliga verksamheten framkommer brister i pålitlighet, lojalitet eller omständigheter som i övrigt kan innebära sårbarheter i säkerhetshänseende ska uppgifterna rapporteras enligt rutinerna i 8 kap. 5 §.”

5 kap. 11 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Chefen för en organisationsenhet ansvarar för att följa upp säkerhetsprövningen vid den egna organisationsenheten. I ansvaret ingår att besluta vem som är behörig att genomföra uppföljning av säkerhetsprövningen. Ett sådant beslut kan vara generellt, och peka på en viss befattningskategori, men det kan även vara så att olika personer genomför olika delar av uppföljningen. Den som har som ansvar för att följa upp säkerhetsprövningen kan vara säkerhetsfunktionen vid organisationsenheten, men även den chef som har personalansvar för personen. Den som har utsetts att följa upp säkerhetsprövning ansvarar för att den dokumenteras (avsnitt 6.16.6).

Moment 6:66 *Säkerhetsprövningen ska följas upp kontinuerligt och bestå av:*

a) ett årligt uppföljande samtal,

b) ekonomisk kontroll vart femte år vid placering i säkerhetsklass 1 och 2, samt i övrigt när särskilda behov föreligger,

c) kontinuerlig kontakt i den dagliga verksamheten,

d) kontinuerlig uppdatering av personuppgifter i registerkontrollen, och

e) en årlig bedömning av den prövades pålitlighet och lojalitet samt om det föreligger någon sårbarhet i säkerhetshänseende.

Vägledande förklaring: Uppföljning av säkerhetsprövning ska t.ex. uppmärksamma förändringar i livssituation (t.ex. social situation), brottslig belastning, kontakter med utländsk underrättelse- och säkerhetstjänst, kontakter med organiserad brottslighet

samt organisationer som är involverade i författningshotande verksamhet (t.ex. terrorism eller annan verksamhet som genom ideologiskt motiverad brottslighet hotar våra grundläggande demokratiska funktioner, oavsett om de bakomliggande orsakerna är politiska eller religiösa), missnöje och besvikelse, hälsoaspekter (t.ex. beroendeproblematik), den ekonomiska situationen, eventuella kontakttagningsförsök, säkerhetsincidenter samt utbildningsbehov.

Tips!
Som stöd för den uppföljande säkerhetsprövningen i Försvarsmakten kan modellen BESKT användas. Läs mer i Försvarsmaktens handbok om säkerhetsprövning (H SÄK Säkprövn).

Om särskilda behov föreligger ska uppföljning av säkerhetsprövning omfattas av en ekonomisk kontroll. Ett särskilt behov kan finnas om den prövade har tillgång till Försvarsmaktens ekonomiska resurser och det finns en ekonomisk problematik hos personen. En ekonomisk kontroll kan alltid genomföras genom att kontakta Skatteverket och Kronofogdemyndigheten.

Moment 6:67 *Den årliga bedömningen av den prövades pålitlighet och lojalitet samt om det föreligger någon sårbarhet i säkerhetshänseende, ska dokumenteras med hjälp av dokumentmallen* Sammanfattande dokumentation uppföljning.

Vägledande förklaring: Den årliga bedömningen av en persons pålitlighet, lojalitet och sårbarhet i säkerhetshänseende genomförs lämpligen efter det årliga uppföljande samtalet. Bedömningen ska genomföras oavsett om det har framkommit något nytt eller inte sedan grundutredningen eller den föregående årliga bedömningen. Bedömningen genomförs även om befattningen inte är placerad i säkerhetsklass. På dokumentmallen noteras även vilka åtgärder som har genomförts (t.ex. referenstagning, säkerhetssamtal eller skyddssamtal). Dokumentet ska bevaras, enligt vad som beskrivs i avsnitt 6.16.6 om dokumentation.

Om det vid uppföljning av säkerhetsprövning har framkommit brister i den prövades lojalitet eller pålitlighet eller om det föreligger någon sårbarhet i säkerhetshänseende ska organisationsenheten påbörja en utredning (avsnitt 6.13). En sådan utredning ska alltid rapporteras till säkerhetsprövningssektionen enligt rutin i avsnitt 6.4.

6.11.1. Uppföljande samtal

Ett uppföljande samtal har sin utgångspunkt i grundutredningen och tidigare uppföljande samtal. Om grundutredningen inte har genomförts av personen som ska genomföra det uppföljande samtalet, är det viktigt att personen får kännedom om det finns områden som ska följas upp särskilt med den prövade.

Moment 6:68 *Det uppföljande samtalet ska minst ha den omfattning som man vid säkerhetsprövningssektionen vid Must har bestämt och i övrigt ha den omfattning som behövs för att bedöma den prövades pålitlighet och lojalitet samt om det föreligger några sårbarheter i säkerhetshänseende.*

Vägledande förklaring: Omfattningen av det uppföljande samtalet kan anpassas till den verksamhet som avses, men ska alltid innefatta de fastställda områdena. Frågeområdena framgår i dokumentmallen *Samtalsguide – uppföljande samtal.*

Den prövades lämplighet från säkerhetssynpunkt kan påverkas av förhållanden som inte direkt gäller den prövade själv utan en nära anhörig, som en make, maka, sambo eller partner. Det är därför viktigt att utreda den prövades lojalitetsband till en nära anhörig samt om det föreligger något beroendeförhållande till en maka, make, sambo eller partner som kan medföra en sårbarhet i säkerhetshänseende, eller påverka pålitligheten och lojalitet.

Moment 6:69 *Vid ett uppföljande samtal ska anteckningar föras.*

Vägledande förklaring: Anteckningarna kan föras på dokumentmallen *Samtalsguide uppföljande samtal* och utgör då den dokumentation som ska bevaras från det uppföljande samtalet. Om anteckningarna inte förts på *Samtalsguide uppföljande samtal* ska dokumentmallen fyllas i efter samtalet, och övriga anteckningar kan därefter förstöras. Dokumentmallen får kompletteras med extra sidor. Uppgifterna som inhämtas vid samtalet omfattas av försvarssekretess enligt 15 kap. 2 § OSL och därför måste informationssystem som är godkända för sådana uppgifter användas, om uppgifterna ska hanteras digitalt. Dokumenten kan även omfattas av annan sekretess till skydd för den enskilde, t.ex. 35 kap. 1 § OSL (enskilds personliga och ekonomiska förhållanden vid registerkontroll) och 38 kap. 4 § OSL (enskilds personliga och ekonomiska förhållanden i försvarsunderrättelseverksamhet och den militära säkerhetstjänsten). Det uppföljande samtalet för en person som inte har en befattning i säkerhetsklass, kan göras mindre omfattande, om det finns särskilda skäl.

Observera!
I Försvarsmakten ska det uppföljande samtalet och bedömningen genomföras en gång per år.

Moment 6:70 *Efter ett uppföljande samtal ska en bedömning göras av de uppgifter som har framkommit. Bedömningen ska dokumenteras med hjälp av dokumentmallen* Samtalsguide uppföljande samtal.

Vägledande förklaring: Bedömningen som genomförs efter samtalet ingår sedan i den sammanfattande bedömningen av individen. Om brister i pålitlighet, lojalitet eller sårbarhet i säkerhetshänseende identifierats ska organisationsenheten påbörja en utredning (avsnitt 6.13).

6.11.2. Skyddssamtal vid särskilda behov

Ett skyddssamtal syftar till att *orientera om säkerhetshotande verksamhet* som kan riktas mot personen eller den säkerhetskänsliga verksamhet som personen deltar i. Skyddssamtalet syftar även till att fördjupa personkännedomen genom att personen lämnar uppgifter om sig själv. Genom skyddssamtalet ska personen få förståelse för att den kan bli ett mål för säkerhetshotande verksamhet och hur sådan verksamhet

bedrivs. Skyddssamtalet ska även öka personens säkerhetsmedvetande. Ett skyddssamtal ska inte förväxlas med samtal för att informera om lokala säkerhetsbestämmelser.

Skyddssamtal kan även genomföras när en befattning är placerad i säkerhetsklass (avsnitt 6.10.4).

Moment 6:71 *Organisationsenheten ansvarar för att genomföra och dokumentera skyddssamtal vid särskilda behov.*

Vägledande förklaring: När särskilda behov föreligger kan organisationsenheten besluta att ett skyddssamtal ska genomföras. Ett särskilt behov kan vara: inför utlandstjänstgöring, resor, besök vid organisationsenheten och vid incidenter, förändrad hotbild eller omvärldsförhållande. Vid denna form av skyddssamtal finns inget hinder att de genomförs i grupp, om så bedöms lämpligt av organisationsenheten. I vissa fall kan ett beslut i ärende om säkerhetsprövning ställa krav på genomförande av skyddssamtal. I dessa fall ska samtalet genomföras enligt instruktion i beslutet.

Skyddssamtal kan även behöva genomföras när en person som kontinuerligt tjänstgör i Försvarsmakten har anmält resa till Ryssland, Kina eller Iran.[212]

6.12. Bedömning i samband med säkerhetsprövning

”Säkerhetsprövningen ska utgå från uppgifter som kommit fram när grundutredningen gjordes och den kännedom som i övrigt finns om den som ska prövas, uppgifter som har lämnats ut efter registerkontroll och särskild personutredning, arten av den verksamhet som prövningen gäller samt omständigheterna i övrigt.

Bedömningen görs av den som beslutar om anställning eller annat deltagande i den säkerhetskänsliga verksamheten. Om en myndighet har det bestämmande inflytandet över den prövades lämplighet att delta i säkerhetskänslig verksamhet hos en enskild verksamhetsutövare, är det i stället myndigheten som gör den slutliga bedömningen.

Om det finns anledning till det, ska en tidigare gjord bedömning av en persons lämplighet att delta i den säkerhetskänsliga verksamheten omprövas.”

3 kap. 4 § säkerhetsskyddslagen

[212] Utlandsresor för anställda i Försvarsmakten (FM2020-9915:1).

”Om det under eller efter genomförd grundutredning enligt 11 § står klart att den som prövningen gäller inte uppfyller kraven för en godkänd säkerhetsprövning ska chef för organisationsenhet, eller den chefen för organisationsenheten bestämmer, avsluta säkerhetsprövningen och rapportera bedömningen enligt rutinerna i 8 kap. 5 §.”

5 kap. 12 § första stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: En bedömning ska genomföras vid flera tillfällen under en säkerhetsprövning, dels efter en säkerhetsprövningsintervju (avsnitt 6.8.1) och dels innan grundutredningen avslutas (avsnitt 6.8.2). Bedömningen ska i dessa fall sammanfattas på dokumentmallen *Sammanfattande dokumentation grundutredning*.

En bedömning ska även genomföras vid uppföljning av säkerhetsprövning (avsnitt 6.11). I detta fall ska den sammanfattas på dokumentmallen *Sammanfattande dokumentation uppföljning*.

En bedömning ska även genomföras vid utredningar (avsnitt 6.13).

Dokumentationen ska bevaras (avsnitt 6.16.6).

Tips!
Stöd för hur en bedömning av en persons pålitlighet, lojalitet och sårbarhet genomförs finns i Försvarsmaktens handbok om säkerhetsprövning (H SÄK Säkprövn) .

6.13. Utredning

”Varje organisationsenhet ska rapportera brister i pålitlighet, lojalitet och omständigheter som kan innebära sårbarheter i säkerhetshänseende inför och under tiden för en persons anställning eller deltagande i säkerhetskänslig verksamhet.

Rapportering ska göras till Försvarsmaktens säkerhetsskyddschef eller den säkerhetsskyddschefen bestämmer.

Om brister eller omständigheter har rapporterats om en person ska varje organisationsenhet på begäran av Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, lämna ytterligare information om den person som rapporteringen rör.”

8 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 6:72 *Om det inom ramen för säkerhetsprövning, eller säkerhetsrapportering framkommer brister i en persons lojalitet och pålitlighet eller om det föreligger några sårbarheter i säkerhetshänseende ska organisationsenheten påbörja en utredning.*

Vägledande förklaring: Se även moment 6:90 om utredning om en person som har genomgått säkerhetsprövning mot särskilda befattningar.

Moment 6:73 *Om en organisationsenhet påbörjar en utredning ska det meddelas till säkerhetsprövningssektionen vid Must.*

Vägledande förklaring: Information om en persons pålitlighet, lojalitet och sårbarhet i säkerhetshänseende kan framkomma både innan deltagandet i den säkerhetskänsliga verksamheten påbörjas, men även under tiden för deltagandet. När det framkommer brister i pålitlighet och lojalitet eller sårbarhet i säkerhetshänseende, ska det rapporteras till säkerhetsprövningssektionen (avsnitt 6.4) Om bristerna framkommer under tiden för deltagandet, dvs. inom ramen för uppföljning av säkerhetsprövning ska organisationsenheten även starta en utredning. Vem som ansvarar för utredningen ska beslutas av organisationsenheten och de som deltar i utredningen ska vara bedömda som lämpliga enligt krav som finns i avsnitt 6.5.

Under utredningens gång kan säkerhetsprövningen kompletteras med åtgärder som referenstagning, inhämtning av information från öppna källor, säkerhetssamtal, skyddssamtal och ekonomisk kontroll. Organisationsenheten får under en utredning vidta tillfälliga skyddsåtgärder (moment 6:12 i avsnitt 6.3). En sådan åtgärd kan vara att begränsa åtkomst till säkerhetsskyddsklassificerade uppgifter eller tillträde till eller delar av ett skyddsobjekt. Om tillfälliga åtgärder vidtas rapporteras det enligt rutin i avsnitt 6.4.

Moment 6:74 *En utredning ska alltid innefatta en bedömning av lojalitet, pålitlighet samt sårbarhet i säkerhetshänseende.*

Moment 6:75 *Den organisationsenhet som genomför en utredning ansvarar för att utredningen dokumenteras.*

Vägledande förklaring: Dokumentation från en utredning ska som minst innehålla en fullständig bakgrund till varför utredningen påbörjades, vilka åtgärder som vidtagits och resultatet av dessa. Dokumentationen ska även innehålla de slutsatser som dragits av den information som har framkommit och slutligen en sammanfattande bedömning avseende personens pålitlighet, lojalitet och sårbarhet i säkerhetshänseende. Ett syfte med dokumentationen är att det ska finnas en spårbarhet inom organisationsenheten. Dokumentationen kan även komma att ligga till grund för en omprövning av ett beslut i ärende om säkerhetsprövning.

Läs mer om dokumentationskraven i avsnitt 6.16.6.

Tips!
Stöd för hur en utredning ska genomföras finns i Försvarsmaktens handbok om säkerhetsprövning (H SÄK Säkprövn).

6.13.1. Säkerhetssamtal

Under deltagandet i den säkerhetskänsliga verksamheten kan det framkomma att en person brister i pålitlighet, lojalitet eller att det föreligger någon sårbarhet i säkerhetshänseende. Det kan t.ex. röra sig om en händelse som personen har varit inblandad i. Säkerhetssamtal kan då vara lämpligt att genomföra med syfte att utreda omständigheterna och för att därefter kunna göra en ny bedömning av personens lojalitet, pålitlighet och sårbarhet i säkerhetshänseende. Ett beslut i ärende om säkerhetsprövning kan ställa krav på att ett säkerhetssamtal ska genomföras (avsnitt 6.10). Säkerhetsprövningssektionen kan besluta att ett säkerhetssamtal ska genomföras även i andra fall.

Moment 6:76 *När ett beslut om säkerhetssamtal har fattats vid säkerhetsprövningssektionen vid Must ska samtalet genomföras skyndsamt och senast inom en månad från beslutet.*

Vägledande förklaring: Den organisationsenhet som ansvarar för den säkerhetskänsliga verksamhet som en person deltar i får besluta om säkerhetssamtal inom ramen för en utredning (avsnitt 6.3). Organisationsenheten får då självständigt besluta vem som är bäst lämpad att genomföra samtalet. Enligt 5 kap. 13 § Försvarsmaktens interna bestämmelser om säkerhetsskydd kan säkerhetsprövningssektionen dock i enskilt fall besluta om vem som ska genomföra samtalet. Ett exempel är när en organisationsenhet på grund av jäv inte kan genomföra det.

Moment 6:77 *Ett säkerhetssamtal får inte genomföras om samtalet kan störa eller skada en brottsutredning.*

Vägledande förklaring: Bedömningen görs i samverkan med förundersökningsledare vid t.ex. Polismyndigheten.

Moment 6:78 *Vid ett säkerhetssamtal ska anteckningar föras.*

Vägledande förklaring: För säkerhetssamtal finns ingen samtalsguide som ska följas, utan varje samtal ska anpassas efter de rådande omständigheterna. Anteckningar ska dock föras vid samtalet. Uppgifterna som inhämtas vid samtalet omfattas av försvarssekretess enlig 15 kap. 2 § OSL och därför måste informationssystem som är godkända för sådana uppgifter användas, om uppgifterna ska hanteras digitalt. Dokumenten kan även omfattas av annan sekretess till skydd för den enskilde, t.ex. 35 kap. 1 § OSL (enskilds personliga och ekonomiska förhållanden vid registerkontroll) och 38 kap. 4 § OSL (enskilds personliga och ekonomiska förhållanden i försvarsunderrättelseverksamhet och den militära säkerhetstjänsten).

Moment 6:79 *Efter ett säkerhetssamtal ska en bedömning göras av de uppgifter som har framkommit. Bedömningen ska dokumenteras.*

Vägledande förklaring: Bedömningen av den prövades pålitlighet och lojalitet samt om sårbarheter i säkerhetshänseende, genomförs efter samtalet. Bedömningen ingår sedan, tillsammans med samtalsanteckningarna, i den dokumentation som ska finnas

i ärendet. Se även krav på dokumentation i åtgärder med anledning av beslut i ärende om säkerhetsprövning (avsnitt 6.16.5).

Moment 6:80 *När organisationsenheten har genomfört ett säkerhetssamtal ska detta meddelas säkerhetsprövningssektionen vid Must. Underlag från ett genomfört säkerhetssamtal skickas in till säkerhetsprövningssektionen vid Must.*

6.14. Säkerhetsprövning mot särskilda befattningar (SSB)

”Försvarsmaktens säkerhetsskyddschef ansvarar för att säkerhetsprövning genomförs inför

1. anställning i befattningsnivå OF 5, respektive befattningsnivå CF 5 för civila tjänstemän, eller högre,

2. befordran till befattningsnivå OF 5 eller högre,

3. byte av befattning inom befattningsnivå OF 5, respektive befattningsnivå CF 5 för civila tjänstemän, eller högre,

4. konstituering till befattningsnivå OF 5, eller högre, och

5. anställning som försvarsattaché.

Ansvaret omfattar inte de anställningar som nämns i 24 § förordningen (2007:1266) med instruktion för Försvarsmakten.

Försvarsmaktens säkerhetsskyddschef får besluta att säkerhetsskyddschefen ansvarar för säkerhetsprövning i fler fall än de som framgår i 1¬–5. .”

5 kap. 8 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Säkerhetsprövning enligt 5 kap. 8 § Försvarsmaktens interna bestämmelser om säkerhetsskydd benämns *säkerhetsprövning mot särskilda befattningar* (SSB). Säkerhetsprövningssektionen genomför säkerhetsprövning mot särskilda befattningar.

Personer som ska placeras i Försvarsmaktens chefskrets, alternativt avser tjänstgöra som försvarsattachéer eller i annan synnerligen känslig befattning, ska genomgå SSB. SSB säkerställer att det genomförs en omfattande grundutredning och syftar till att bedöma personens lojalitet, pålitlighet och sårbarhet i säkerhetshänseende.

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, beslutar om den som säkerhetsprövningen gäller uppfyller kraven för en godkänd säkerhetsprövning. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”

5 kap. 14 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: En SSB avslutas med ett beslut i ärende om säkerhetsprövning som anger om personen har en godkänd säkerhetsprövning vid SSB, och om personen kan tillträda tilltänkt befattning.

”I säkerhetsprövningar enligt 8 § ska det ingå en psykologisk personbedömning i de fall som Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, beslutar.”

5 kap. 9 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Vid SSB kompletteras grundutredningen med en psykologisk personbedömning som syftar till att klarlägga huruvida den prövade har de personliga förutsättningar som dessa befattningar kräver, såsom personlig mognad, integritet, emotionell stabilitet och ett högt säkerhetsmedvetande. Vid säkerhetsprövningssektionen bestäms vilka moment och bedömningskriterier som ingår i den psykologiska personbedömningen.

Moment 6:81 *Psykologisk personbedömning ska genomföras av en legitimerad psykolog.*

Moment 6:82 *Psykologisk testning ska genomföras och resultatet av testningen ska utgöra en del av det underlag som ligger till grund för den psykologiska personbedömningen.*

Moment 6:83 *Om en person som har genomgått säkerhetsprövning mot särskilda befattningar inte har fått anställning i befattningsnivå 5, ska resultatet gälla i tre år. Vid säkerhetsprövningssektionen vid Must får man dock besluta att en säkerhetsprövning mot särskilda befattningar ska genomföras på nytt innan tre år har förflutit.*

Moment 6:84 *Inför befordran till befattningsnivå 6 eller högre samt vid byte av befattning ska den tidigare genomförda grundutredningen förnyas.*

Vägledande förklaring: Av 3 kap. 3 § säkerhetsskyddslagen framgår att en grundutredning får göras mindre omfattade om det finns särskilda skäl. En grundutredning inom ramen för SSB ska i normalfallet förnyas om den genomfördes för mer än tre år sedan. Säkerhetsprövningssektionen får besluta att grundutredningen även ska göras om vid kortare intervall, samt vilka åtgärder som ska ingå i den förnyade grundutredningen.

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ansvarar för att säkerhetsprövningen enligt 8 § följs upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.”

5 kap. 10 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 6:85 *Säkerhetsprövningssektionen vid Must ska genomföra skyddssamtal senast tre år efter att den prövade har genomgått säkerhetsprövning mot särskilda befattningar.*

Moment 6:86 *Vid säkerhetsprövningssektionen vid Must ska man genomföra uppföljande samtal med personer som genomgått säkerhetsprövning mot särskilda befattningar.*

Moment 6:87 *I samband med uppföljning av säkerhetsprövning mot särskilda befattningar ska man vid säkerhetsprövningssektionen vid Must besluta om en förnyad psykologisk personbedömning ska genomföras.*

Moment 6:88 *Organisationsenheten ansvarar för att, i det dagliga arbetet vid organisationsenheten, följa upp personer som har genomgått säkerhetsprövning mot särskilda befattningar.*

Vägledande förklaring: Ansvaret för uppföljning av SSB är delat mellan säkerhetsprövningssektionen och den organisationsenhet där personen är placerad. Det delade ansvaret innebär även att organisationsenheten har ett rapporteringsansvar gentemot säkerhetsprövningssektionen i de fall där det framkommer brister avseende pålitlighet och lojalitet eller om sårbarheter i säkerhetshänseende identifieras.

Moment 6:89 *En utredning om en person som har genomgått säkerhetsprövning mot särskilda befattningar ska genomföras av personal vid säkerhetsprövningssektionen eller den som säkerhetsprövningssektionen bestämmer.*

> *”I 6 kap. 8 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd regleras när det ska genomföras avslutande samtal.*
>
> *Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ansvarar för att sådana samtal genomförs för de säkerhetsprövningar som regleras i 8 §.”*
>
> 5 kap. 19 § första och andra styckena
> Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Avslutande samtal med personer som har genomgått SSB genomförs vid säkerhetsprövningssektionen.

Moment 6:90 *Säkerhetsprövning mot särskilda befattningar ska dokumenteras på det sätt som man vid säkerhetsprövningssektionen vid Must beslutat.*

6.15. Avslutning av anställning eller annat deltagande i säkerhetskänslig verksamhet

”Säkerhetsprövningen ska följas upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.”

3 kap. 3 § andra stycket säkerhetsskyddslagen

Vägledande förklaring: I samband med att en anställning eller annat deltagande i säkerhetskänslig verksamhet upphör ska även uppföljningen av säkerhetsprövningen avslutas.

”Myndigheten ska genomföra ett avslutande samtal när personens deltagande i den säkerhetskänsliga verksamheten upphör. Det avslutande samtalet ska dokumenteras.

Om personen har tagit del av säkerhetsskyddsklassificerade uppgifter ska denne upplysas om räckvidden och innebörden av den sekretess och tystnadsplikt som följer av offentlighets- och sekretesslagen (2009:400) eller 5 kap. 2 § andra stycket säkerhetsskyddslagen (2018:585).

Ett sådant samtal behöver inte genomföras om det är uppenbart obehövligt.”

6 kap. 8 § Försvarsmaktens föreskrifter om säkerhetsskydd

”I 6 kap. 8 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd regleras när det ska genomföras avslutande samtal.

Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ansvarar för att sådana samtal genomförs för de säkerhetsprövningar som regleras i 8 §.

Chef för organisationsenhet ansvarar för att sådana samtal genomförs i övriga fall.”

5 kap. 19 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Ett avslutande samtal är en viktig del när deltagandet i den säkerhetskänsliga verksamheten upphör. Det har som syfte att stämma av hur tiden i verksamheten varit, vilka positiva och negativa erfarenheter personen tar med sig och om det finns någon besvikelse eller bitterhet som kan utgöra ett hot mot den säkerhetskänsliga verksamheten eller Sveriges säkerhet. Ett exempel på när ett avslutande samtal är uppenbart obehövligt är om deltagandet har varit kortvarigt eller om annat samtal inom ramen för uppföljning av säkerhetsprövning nyligen har genomförts.

Ett avslutande samtal ska inte enbart genomföras när en person lämnar Försvarsmakten utan även när en person byter organisationsenhet.

När en person slutar i verksamheten är det viktigt att personen upplyses om att uppgifterna som denne tagit del av kan omfattas av sekretess enligt OSL en längre tid, även efter det att personen har lämnat den säkerhetskänsliga verksamheten. Som bekräftelse på att personen har fått informationen kan sekretessbeviset undertecknas ytterligare en gång, det finns dock inget krav på att sekretessbeviset ska undertecknas på nytt.

Moment 6:91 *Det avslutande samtalet ska minst ha den omfattning som bestämts vid säkerhetsprövningssektionen vid Must och i övrigt ha den omfattning som behövs för att bedöma den prövades pålitlighet och lojalitet samt om det föreligger några sårbarheter i säkerhetshänseende.*

Vägledande förklaring: Omfattningen av det avslutande samtalet kan anpassas till den verksamhet som avses, men ska alltid innefatta de fastställda frågeområdena. Frågeområdena framgår i dokumentmallen *Samtalsguide – avslutande samtal.*

Moment 6:92 *Vid ett avslutande samtal ska anteckningar föras.*

Vägledande förklaring: Anteckningarna kan föras på dokumentmallen *Samtalsguide avslutande samtal* och utgör då den dokumentation som ska bevaras från det avslutande samtalet. Om anteckningar inte förts på *Samtalsguide avslutande samtal* ska dokumentmallen fyllas i efter samtalet, och övriga anteckningar kan därefter förstöras. Dokumentmallen får kompletteras med extra sidor.

Uppgifterna som inhämtas vid samtalstillfället omfattas av försvarssekretess enlig 15 kap. 2 § OSL och därför måste informationssystem som är godkända för sådana uppgifter användas, om uppgifterna ska hanteras digitalt. Dokumenten kan även omfattas av annan sekretess till skydd för den enskilde, t.ex. 35 kap. 1 § OSL (enskilds personliga och ekonomiska förhållanden vid registerkontroll) och 38 kap. 4 § OSL (enskilds personliga och ekonomiska förhållanden i försvarsunderrättelseverksamhet och den militära säkerhetstjänsten).

Moment 6:93 *Efter ett avslutande samtal ska en bedömning göras av de uppgifter som har framkommit. Bedömningen ska dokumenteras med hjälp av dokumentmallen* Samtalsguide avslutande samtal.

Vägledande förklaring: Bedömningen som genomförs efter samtalet ingår sedan i den sammanfattande bedömningen av individen. Om brister i pålitlighet, lojalitet eller sårbarhet i säkerhetshänseende identifierats ska detta rapporteras till säkerhetsprövningssektionen (avsnitt 6.4).

I avsnitt 6.16.7 finns krav på dokumentation för den avslutande delen av säkerhetsprövningen.

6.16. Dokumentation av säkerhetsprövning

”Resultatet av säkerhetsprövningen ska dokumenteras i de fall en person har bedömts vara pålitlig ur säkerhetssynpunkt och beslut har fattats om anställning eller annat deltagande i verksamheten.”

5 kap. 5 § säkerhetsskyddsförordningen

”Av 3 kap. 1 § säkerhetsskyddslagen (2018:585) framgår att den som genom en anställning eller på något annat sätt deltar i säkerhetskänslig verksamhet ska säkerhetsprövas. Säkerhetsprövningen ska dokumenteras.”

6 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Säkerhetsprövningsprocessen i sin helhet ska dokumenteras. Riksarkivet har föreskrivit vilka handlingar inom personalsäkerhet som ska bevaras och vilka som får gallras.[213] Bestämmelserna gäller såväl pappershandlingar som elektroniska handlingar. Det är den organisationsenhet som genomför säkerhetsprövning som ansvarar för att den dokumenteras, och att den bevaras. Om dokumentationen har sänts till säkerhetsprövningssektionen, kan det innebära att den bevaras där.

Dokumentmallar som anges i tabell 6.4 används för att dokumentera säkerhetsprövning.

Tabell 6.4. Dokumentmallar för att dokumentera säkerhetsprövning.

Dokumentmall	Innehåll
Förteckning befattningsanalys	Underlag för rapportering av förslag till befattningsanalys.
Intervjuguide säkerhetsprövningsintervju	Intervjuguide och sammanfattande bedömning.
Sammanfattande dokumentation grundutredning	Innehåller en sammanfattning av de åtgärder som vidtagits inom ramen för grundutredningen, samt en bedömning.
Samtalsguide skyddssamtal - säkerhetsklass 1 och 2	Samtalsguide för skyddssamtal vid placering i säkerhetsklass 1 och 2.
Blankett - Anmälan om förändringar av personliga förhållanden	En blankett som ska fyllas i av personen inför det uppföljande samtalet.

[213] Riksarkivets föreskrifter och allmänna råd (RA-MS 2018:42) om gallring hos Fortifikationsverket, Försvarets materielverk, Försvarsmakten, Totalförsvarets forskningsinstitut och Totalförsvarets rekryteringsmyndighet.

Dokumentmall	Innehåll
Samtalsguide uppföljande samtal	Samtalsguide och sammanfattande bedömning.
Sammanfattande dokumentation uppföljning	Innehåller en sammanfattning av de åtgärder som vidtagits inom ramen för uppföljning av säkerhetsprövning, samt en bedömning.
Samtalsguide avslutande samtal	Samtalsguide för avslutande samtal. Innehåller även information om vilka uppgifter som ska rapporteras till säkerhetsprövningssektionen.

6.16.1. Befattningsanalys

En befattningsanalys dokumenteras och ligger till grund för det förslag som skickas till säkerhetsprövningssektionen (avsnitt 6.2). Av RA-MS 2018:42 följer att befattningsanalysen och *Förteckning befattningsanalys* ska bevaras, avseende befattningar som har placerats i säkerhetsklass.

Moment 6:94 *Organisationsenheten ska bevara befattningsanalysen.* Förteckning befattningsanalys *ska bevaras vid säkerhetsprövningssektionen vid Must.*

6.16.2. Grundutredning

> *”Grundutredningen ska dokumenteras.”*
>
> 6 kap. 5 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Att grundutredningen ska dokumenteras innebär att anteckningar ska föras vid samtal, intervjuer och referenstagningar. Det innebär även att resultatet av kontroll av betyg, intyg, internet, sociala medier och ekonomisk kontroll ska dokumenteras. Av RA-MS 2018:42 följer att den dokumentation som ingår i grundutredningen ska bevaras om ett beslut om deltagande i den säkerhetskänsliga verksamheten har fattats för den prövade (avsnitt 6.10.3).

Moment 6:95 *Organisationsenheten ansvarar för att grundutredningar vid egen enhet bevaras. Om säkerhetsprövningen har avslutats, under eller efter genomförd grundutredning, och ärendet har rapporterats till säkerhetsprövningssektionen vid Must ska grundutredningen bevaras vid säkerhetsprövningssektionen.*

Vägledande förklaring: På dokumentmallen *Sammanfattande dokumentation grundutredning* sammanställs resultatet av grundutredningen och utgör tillsammans med *Intervjuguide säkerhetsprövningsintervju* dokumentationen från grundutredningen som ska bevaras. Dokumentationen ska kompletteras med kopior på betyg och intyg, men även med information från öppna källor såsom internet och sociala medier samt ekonomisk kontroll, i de fall där det behövs. Ett sådant fall kan vara om information har framkommit som påverkat bedömningen av pålitlighet, lojalitet och

sårbarhet i säkerhetshänseende. Det ska dock alltid framgå av *Sammanfattande dokumentation grundutredning* om åtgärden har genomförts eller inte. Dokumentmallen tillhandahålls av säkerhetsprövningssektionen.

När en organisationsenhet väljer att avsluta en grundutredning (avsnitt 6.8.5), ska dokumentationen sändas till säkerhetsprövningssektionen. Säkerhetsprövningssektionen ansvarar sedan för att dokumentationen bevaras enligt RA-MS 2018:42. Det samma gäller om det har framkommit brister i lojalitet, pålitlighet eller sårbarhet och den prövade tar tillbaka sin ansökan innan ett beslut i ärende om säkerhetsprövning har fattats (avsnitt 6.16.5).

Moment 6:96 *Om en person tar tillbaka sin ansökan och det inte har framkommit några uppgifter om brister i den prövades lojalitet, pålitlighet eller omständigheter som kan innebära sårbarheter i säkerhetshänseende, eller om organisationsenheten av annan anledning än säkerhetsskäl väljer att avbryta rekryteringen ska organisationsenheten bevara dokumentationen som ingår i grundutredningen.*

Vägledande förklaring: En anledning till att avbryta en rekrytering kan t.ex. vara att organisationsenheten inte längre ska tillsätta en befattning. Enligt RA-MS 2018:42 får uppgifterna gallras först när två år har förflutit.

Moment 6:97 *En säkerhetsprövningsintervju ska dokumenteras på dokumentmallen* Intervjuguide säkerhetsprövningsintervju.

Vägledande förklaring: Det finns inget krav på att dokumentmallen ska användas vid säkerhetsprövningsintervjun (avsnitt 6.8.1). Om dokumentationen inte har förts på dokumentmallen ska den fyllas i efter intervjun, och övriga anteckningar kan då förstöras. Dokumentmallen får kompletteras med extra sidor. Dokumentmallen utgör den dokumentation av grundutredningen som ska bevaras från intervjun. Dokumentmallen tillhandahålls av säkerhetsprövningssektionen.

6.16.3. Registerkontroll

> *”Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska dokumentera att samtycke till registerkontroll och särskild personutredning har lämnats av den som säkerhetsprövningen gäller.”*
>
> 6 kap. 11 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Vägledande förklaring: Enligt RA-MS 2018:42 ska ett samtycke till registerkontroll bevaras för den som har anställts eller på annat sätt ska delta i den säkerhetskänsliga verksamheten. I Försvarsmakten dokumenteras samtycket till registerkontroll i RK-rutinen i IS UNDSÄK för den som placeras på befattningen, samt att *Intervjuguide säkerhetsprövningsintervju* bevaras (avsnitt 6.16.2). Om en organisationsenhet väljer att dokumentera samtycket på annat sätt ska dokumentationen enligt RA-MS 2018:42 bevaras.

En ansökan om registerkontroll till Säkerhetspolisen får, enligt RA-MS 2018:42, gallras vid deltagandets slut, eller om personen efter en ansökan inte har ianspråktagits i Försvarsmaktens verksamhet.

Om en person fyllt i blanketten om särskild personutredning, men inte har antagits får blanketten, enligt RA-MS 2018:42, gallras när anställningsbeslutet för den som fått tjänsten har vunnit laga kraft eller efter beslut fattats om att personen inte ska ianspråktas.

Om en registerkontroll underlåts, enligt 3 kap. 3 § första stycket säkerhetsskyddslagen, ska skälen dokumenteras. Dokumentationen ska bevaras vid säkerhetsprövningssektionen.

6.16.4. Skyddssamtal vid placering i säkerhetsklass

Moment 6:98 *Skyddssamtal vid säkerhetsklass 1 och 2 ska dokumenteras på dokumentmallen* Samtalsguide skyddssamtal - säkerhetsklass 1 och 2.

Vägledande förklaring: Dokumentation från ett skyddssamtal som har genomförts vid säkerhetsklass 1 och 2 (avsnitt 6.10.4) bevaras vid den organisationsenhet som genomfört samtalet.

6.16.5. Beslut i ärende om säkerhetsprövning

Av 6 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd följer att ett beslut i ärende om säkerhetsprövning ska dokumenteras.

Moment 6:99 *Beslut i ärende om säkerhetsprövning ska bevaras vid säkerhetsprövningssektionen vid Must.*

Vägledande förklaring: I det fall en person uppfyller kraven för en godkänd säkerhetsprövning, och där det inte har framkommit några brister från säkerhetssynpunkt, meddelas ett beslut i ärende om säkerhetsprövning direkt i RK-rutinen i IS UNDSÄK och bevaras där.

När ett skriftligt beslut i ärende om säkerhetsprövning har fattats (tidigare kallat ”Säkerhetsskyddsbeslut i personärende”) ska beslutet samt den dokumentation som finns i ärendet bevaras enligt RA-MS 2018:42. Dokumentation som kan ligga till grund för ett skriftligt beslut i ärende om säkerhetsprövning är t.ex. minnesanteckningar, bedömningar från säkerhetssamtal (avsnitt 6.13.1) och samtal inom ramen för särskild uppföljning (avsnitt 6.10.2.1), men även beslut om restriktioner (avsnitt 6.10.2.2). Att dokumentationen ska bevaras vid säkerhetsprövningssektionen hindrar inte att en kopia finns vid organisationsenheten.

FARA!
Det saknas stöd i RA-MS 2018:42 för att gallra dokumentation som ligger till grund för beslut i ärenden om säkerhetsprövning, inklusive besluten. De ska därför bevaras!

6.16.6. Uppföljning av säkerhetsprövning

> *”Den uppföljande säkerhetsprövningen ska dokumenteras.”*
>
> 6 kap. 6 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Dokumentation inom ramen för uppföljning av säkerhetsprövning kan dels bestå av de underlag som skapas under tiden för uppföljning, men även i samband med en utredning. Av RA-MS 2018:42 följer att den dokumentation som ingår i uppföljning av säkerhetsprövning, samt utredning ska bevaras.

Moment 6:100 *Dokumentation från uppföljning av säkerhetsprövning ska bestå av* Samtalsguide uppföljande samtal *och* Sammanfattande dokumentation uppföljning *samt övrig i det enskilda fallet relevant information.*

Vägledande förklaring: Övrig relevant information kan vara t.ex. dokument från ekonomisk kontroll, skyddssamtal eller anteckningar från förnyad referenstagning. Det finns inget krav att S*amtalsguide uppföljande samtal* används vid det uppföljande samtalet (avsnitt 6.11.1). Om dokumentationen inte förts på dokumentmallen ska den fyllas i efter samtalet, och övriga anteckningar kan därefter förstöras. Dokumentmallarna får kompletteras med extra sidor. Dokumentmallen utgör sedan den dokumentation från uppföljning av säkerhetsprövning som ska bevaras. Dokumentmallen tillhandahålls av säkerhetsprövningssektionen.

Moment 6:101 *Dokumentation som ingår i en utredning ska bevaras vid säkerhetsprövningssektionen vid Must.*

Vägledande förklaring: En utredning består vanligtvis av en rapport med kompletterande information (som t.ex. kontroll av personens förekomst på internet och sociala medier, underlag från ekonomisk kontroll, bilder, domar och strafföreläggande), samtalsanteckningar från säkerhetssamtal och referenstagning samt en bedömning av pålitlighet, lojalitet och sårbarhet. Informationen kan även bestå av den dokumenterade säkerhetsprövningen i övrigt. Att dokumentationen ska bevaras vid säkerhetsprövningssektionen hindrar inte att en kopia finns vid organisationsenheten.

6.16.7. Avslutning av anställning eller annat deltagande i säkerhetskänslig verksamhet

När en person slutar i den säkerhetskänsliga verksamheten ska personen påminnas om tystnadsplikten (avsnitt 6.15), och kan även komma att underteckna sekretessbeviset på nytt. Oavsett om det undertecknas igen eller inte ska sekretessbeviset, enligt RA-MS 2018:42, sparas i minst 25 år innan det får gallras.

”Myndigheten ska genomföra ett avslutande samtal när personens deltagande i den säkerhetskänsliga verksamheten upphör. Det avslutande samtalet ska dokumenteras.”

6 kap. 8 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Moment 6:102 *Avslutande samtal ska dokumenteras på dokumentmallen* Samtalsguide avslutande samtal.

Vägledande förklaring: Dokumentationen består av dokumentmallen *Samtalsguide avslutande samtal* som ska innehålla minnesanteckningar från det avslutande samtalet samt en bedömning av personens pålitlighet, lojalitet och sårbarhet (avsnitt 6.15). Dokumentationen kan även bestå av andra underlag som t.ex. anteckningar från referenstagning eller kontroll av uppgifter. Dokumentmallen tillhandahålls av säkerhetsprövningssektionen.

Moment 6:103 *Dokumentation från det avslutande samtalet ska bevaras vid organisationsenheten. Om brister i pålitlighet, lojalitet och sårbarhet framkommit ska dokumentationen bevaras hos säkerhetsprövningssektionen vid Must.*

Vägledande förklaring: Av RA-MS 2018:42 följer att dokumentation om avslutande samtal, inklusive minnesanteckningar och avslutande bedömning, ska bevaras. Även om personen byter organisationsenhet ska dokumentationen bevaras vid den avlämnande organisationsenheten.

6.16.8. Säkerhetsskyddad upphandling

Säkerhetsprövning vid säkerhetsskyddad upphandling ska dokumenteras på samma sätt som vid anställning och annat deltagande i säkerhetskänslig verksamhet. När ett säkerhetsskyddsavtal upphör eller avslutas ska den dokumentation som finns hos leverantören, rörande säkerhetsprövning, överlämnas till Försvarsmakten. Det är den som ansvarar för säkerhetsskyddsavtalet som även ansvarar för att säkerhetsprövningen dokumenteras och bevaras enligt RA-MS 2018:42, i de fall där säkerhetsprövningssektionen inte har ett ansvar.

Moment 6:104 *Säkerhetsprövningssektionen vid Must ansvarar för att underlag för säkerhetsskyddad upphandling bevaras och sedan gallras, enligt RA-FS 2018:3, efter minst 5 år.*

Vägledande förklaring: Säkerhetspolisen ska underrättas när ett säkerhetsskyddsavtal ingås, och när det avslutas.[214] Säkerhetsprövningssektionen ansvarar för att en sådan anmälan genomförs, efter ansökan från den som har ingått avtalet.

[214] 2 kap. 7 § säkerhetsskyddsförordningen och 7 kap. 4 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

6.16.9. Säkerhetsintyg

I vissa fall kan Försvarsmakten utfärda ett säkerhetsintyg för en person som ska ta del av Nato säkerhetsskyddsklassificerade handlingar från NATO CONFIDENTIAL och högre. När Försvarsmakten utfärdar ett säkerhetsintyg ska detta bevaras, enligt RA-MS 2018:42, i minst 10 år.

Moment 6:105 *Säkerhetsprövningssektionen vid Must ansvarar för att uppgiften om vilka säkerhetsintyg som har utfärdats bevaras och sedan, enligt RA-MS 2018:42, gallras efter minst 10 år.*

6.16.10. Hantering av allmänna handlingar

Inom säkerhetsprövning förekommer allmänna handlingar som innehåller uppgifter som omfattas av sekretess (främst 15 kap. 2 § och 35 kap. 1 § OSL). Sådana handlingar ska enligt 5 kap. 1 § OSL registreras i ett register över allmänna handlingar. Säkerhetsprövningssektionen kan ge stöd i hur sådana handlingar ska diarieföras. Även inkommande e-post och brev avseende säkerhetsrapportering i personärende är allmänna handlingar.

6.17. Säkerhetsprövning vid säkerhetsskyddad upphandling

Säkerhetsskyddad upphandling beskrivs i kapitel 8.

I 3 kap. 1 § säkerhetsskyddslagen framgår att den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas. Detta innebär att den som deltar i Försvarsmaktens säkerhetskänsliga verksamhet genom säkerhetsskyddad upphandling ska säkerhetsprövas.

Säkerhetsprövning av de som deltar genom en säkerhetsskyddad upphandling ska genomföras på samma sätt som för annat deltagande i säkerhetskänslig verksamhet. Befattningsanalys, grundutredning, registerkontroll, uppföljning, avslutning och beslut i ärende om säkerhetsprövning är exempel på åtgärder som ska genomföras även för säkerhetsprövning av personer som genom säkerhetsskyddad upphandling deltar i säkerhetskänslig verksamhet. Säkerhetsprövningen dokumenteras enligt bestämmelser i detta reglemente (avsnitt 6.16).

Moment 6:106 *Om en leverantör ska genomföra grundutredning eller uppföljning av säkerhetsprövning av egen personal ska de som genomför detta eller i övrigt tar del av uppgifter inom ramen för säkerhetsprövning vara utbildade och bedömda som lämpliga. Den som ansvarar för ett säkerhetsskyddsavtal ska se till att lämplighetsbedömningen genomförs av Försvarsmakten, samt att utbildningen är godkänd.*

Vägledande förklaring: Lämplighetsbedömningar får inte överlåtas till leverantören, men kan genomföras tillsammans med leverantören. Utbildning i säkerhetsprövning ska i normalfallet genomföras av Försvarsmakten, men kan i vissa fall genomföras av leverantören, förutsatt att säkerhetsprövningssektionen beslutat att utbildningen är godkänd.

6.17.1. Befattningsanalys

Moment 6:107 *En befattningsanalys enligt 6 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd ska omfatta befattningar som avser deltagande i säkerhetskänslig verksamhet och som ingår i en säkerhetsskyddad upphandling, samt vilka i företagets styrelse och ledning som ska genomgå en säkerhetsprövning.*

Vägledande förklaring: En befattningsanalys ska vara genomförd innan ett säkerhetsskyddsavtal kan tecknas med leverantören. Om befattningsanalysen inte innehåller de befattningar som ingår i en säkerhetsskyddad upphandling måste analysen uppdateras. Det vill säga om befattningsanalysen är genomförd utifrån förutbestämda befattningar, som inte matchar leverantörens arbets- eller kompetensfördelning måste befattningsanalysen korrigeras så att varje befattning placeras i rätt säkerhetsklass, utifrån hur leverantören fördelat arbetsuppgifterna.

För att säkerhetsprövningssektionen ska kunna framställa om registerkontroll hos Säkerhetspolisen måste det finnas en godkänd förteckning över befattningar vid säkerhetsprövningssektionen. För befattningar som avses placeras i säkerhetsklass 1 är det regeringen som, efter hemställan från säkerhetsprövningssektionen, beslutar att befattningen ska placeras i säkerhetsklass 1 (avsnitt 6.2.2). Om en befattning avses placeras i säkerhetsklass 1 är det viktigt att befattningsanalysen inkommer i god tid till säkerhetsprövningssektionen, så att framställan till regeringen kan göras innan säkerhetsskyddsavtal tecknas.

6.17.2. Säkerhetsprövning av ledning, styrelse och säkerhetsskyddschef

Moment 6:108 *Den som ansvarar för ett säkerhetsskyddsavtal ska se till att säkerhetsprövning av en leverantörs ledning och styrelse samt säkerhetsskyddschef genomförs av Försvarsmakten.*

Vägledande förklaring: Försvarsmakten ansvarar i detta fall för samtliga moment som ingår i en säkerhetsprövning; grundutredning, registerkontroll, uppföljning samt avslutande samtal.

En företagsledning och dess styrelse, som kan bestå av verkställande direktör, styrelseordförande, styrelseledamöter eller andra representanter i en ledningsgrupp, t.ex. ekonomichef, och chefsjurist, kan alltid ha möjlighet att ta del av den verksamhet som företaget bedriver i Försvarsmaktens säkerhetskänsliga verksamhet. Detsamma kan gälla revisorer vid företaget. Ledningen och dess styrelse ska därför säkerhetsprövas på samma sätt som övriga deltagande.

Det är befattningsanalysen som svarar på vilka vid företaget som har insyn i den säkerhetskänsliga verksamheten. Beroende på företagets ledningsstruktur innebär detta i vissa fall att hela ledningen och styrelsen ska säkerhetsprövas och i andra fall kanske det endast är någon eller några personer som ska genomgå säkerhetsprövning.

Registerkontroll får inte genomföras förrän ett säkerhetsskyddsavtal är tecknat och information om detta har inkommit till Säkerhetspolisen (avsnitt 6.9.3).[215]

6.17.3. Grundutredning och uppföljning av leverantörs personal

Moment 6:109 *Den som ansvarar för ett säkerhetsskyddsavtal ska se till att grundutredning för leverantörens personal genomförs av Försvarsmakten när deltagandet är placerat i säkerhetsklass 1 eller 2. Vid säkerhetsprövningssektionen vid Must får man besluta att hela eller delar av en grundutredning ska genomföras av någon annan.*

Vägledande förklaring: Om en grundutredning ska få genomföras av någon annan än Försvarsmakten, t.ex. leverantören, måste det framgå av säkerhetsskyddsavtalet. I vissa fall kan delar av en grundutredning genomföras av leverantören vid säkerhetsklass 1 och 2, t.ex. om leverantören genomfört en godkänd kontroll av betyg och intyg för den prövade. I sådana fall kan Försvarsmaktens kontroll av betyg och intyg bestå av att leverantören bekräftar att kontrollen är genomförd. Om hela eller delar av en grundutredning vid säkerhetsklass 1 och 2 ska genomföras av en leverantör måste säkerhetsprövningssektionen först ha godkänt detta innan säkerhetsskyddsavtalet ingås.

Moment 6:110 *Den som ansvarar för ett säkerhetsskyddsavtal ansvarar för att uppföljning av säkerhetsprövning genomförs för leverantörens personal. Leverantören får i följande fall genomföra uppföljning av säkerhetsprövning av egen personal:*

a) Årliga uppföljande samtal och kontinuerlig kontakt i den dagliga verksamheten, när verksamheten bedrivs i leverantörens egna lokaler (nivå 1).

b) Årliga uppföljande samtal, när verksamheten bedrivs i Försvarsmaktens lokaler och befattningen är placerad i säkerhetsklass 3.

Vägledande förklaring: Försvarsmakten har alltid huvudansvaret för uppföljningen av säkerhetsprövning, och den kan aldrig delegeras i sin helhet till leverantören. Den sammanfattade bedömningen av en persons lojalitet, pålitlighet och sårbarhet i säkerhetshänseende ska alltid genomföras av Försvarsmakten, detsamma gäller beslut i ärende om säkerhetsprövning. Den som ansvarar för säkerhetsskyddsavtalet ansvarar även för att uppföljningen genomförs. Uppgiften kan dock, om det bedöms lämpligt, genomföras av någon annan än den som ansvarar för säkerhetsskyddsavtalet. Om leverantören ska ges ett ansvar för uppföljningen av säkerhetsprövningen måste detta vara klarlagt innan ett säkerhetsskyddsavtal ingås. Leverantörens uppgift att genomföra uppföljning måste då framgå i säkerhetsskyddsavtalet.

Läs mer om framställan och avslut av registerkontroll vid säkerhetsskyddad upphandling i avsnitt 6.9.3 och 6.9.7.

[215] 6 kap. 9 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

6.17.4. Bedömning och beslut i ärende om säkerhetsprövning

> *”Säkerhetsprövningen ska utgå från uppgifter som kommit fram när grundutredningen gjordes och den kännedom som i övrigt finns om den som ska prövas, uppgifter som har lämnats ut efter registerkontroll och särskild personutredning, arten av den verksamhet som prövningen gäller samt omständigheterna i övrigt.*
>
> *Bedömningen görs av den som beslutar om anställning eller annat deltagande i den säkerhetskänsliga verksamheten. Om en myndighet har det bestämmande inflytandet över den prövades lämplighet att delta i säkerhetskänslig verksamhet hos en enskild verksamhetsutövare, är det i stället myndigheten som gör den slutliga bedömningen.”*
>
> 3 kap. 4 § första och andra styckena säkerhetsskyddslagen

Vägledande förklaring: Med att en myndighet har *det bestämmande inflytandet över den prövades lämplighet* avses att det i ett säkerhetsskyddsavtal finns krav att ansvaret för säkerhetsprövningen delas upp mellan leverantören och myndigheten. Ofta avtalas om att leverantören ansvarar för säkerhetsprövningen men att ett godkännande efter registerkontroll krävs från den upphandlande myndigheten.[216]

Det framgår även av 3 kap. 4 § andra stycket säkerhetsskyddslagen att den slutliga bedömningen inte kan genomföras av leverantören. Om leverantören har genomfört grundutredningen måste den som ansvarar för säkerhetsskyddsavtalet ta del av de uppgifter som framkommit om den prövade för att genomföra den slutliga bedömningen. Vid uppföljning av säkerhetsprövning innebär detta att den som ansvarar för säkerhetsskyddsavtalet ska inhämta information från leverantören för att få en mer allsidig personkännedom som underlag för den sammanfattade bedömningen.

I moment 8:13 i avsnitt 8.11 finns krav på att säkerhetsskyddsavtalet ska innehålla bestämmelser om säkerhetsprövning av en leverantörs personal, samt krav på rapportering avseende brister i pålitlighet, lojalitet och sårbarhet i säkerhetshänseende.

Moment 6:111 *Om det under eller efter leverantörens genomförda grundutredning står klart att personen inte kommer att uppfylla kraven för en godkänd säkerhetsprövning, ska den som ansvarar för säkerhetsskyddsavtalet se till att grundutredningen avslutas.*

Vägledande förklaring: En leverantör kan inte på egen hand avsluta en grundutredning. Grundutredningen ska i detta fall dokumenteras och sedan rapporteras till organisationsenheten som i sin tur avslutar den. Den som ansvarar för säkerhetsskyddsavtalet rapporterar sedan avslut enligt ordinarie rutin (avsnitt 6.8.5).

[216] Prop. 2017/18:89 s.145.

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, beslutar om den som säkerhetsprövningen gäller uppfyller kraven för en godkänd säkerhetsprövning. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”

5 kap. 14 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

”Ett beslut om godkänd säkerhetsprövning ska omprövas om den prövningen gäller, inte längre uppfyller kraven för godkännandet. Ett sådant beslut får förenas med villkor enligt säkerhetsskyddschefens närmare bestämmande.”

5 kap. 15 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 6:112 *När Försvarsmaktens säkerhetsskyddchef har beslutat i ärende om säkerhetsprövning, ska den som ansvarar för säkerhetsskyddsavtalet:*

a) Meddela säkerhetsprövningssektionen vid Must om den person som prövningen gäller kommer att delta i den säkerhetskänsliga verksamheten eller inte.

b) Skyndsamt se till att eventuella skyddsåtgärder enligt beslutet vidtas.

c) Skyndsamt se till att leverantören meddelas beslutet.

Vägledande förklaring: Av 5 kap. 14 § Försvarsmaktens interna bestämmelser om säkerhetsskydd följer att en leverantör inte får besluta i ärenden om säkerhetsprövning. Skälen till ett beslut i ärende om säkerhetsprövning får inte delges leverantören. Det är tillräckligt att leverantören meddelas om personen får delta i Försvarsmaktens säkerhetskänsliga verksamhet eller inte. Leverantören ska genom säkerhetsskyddsavtalet ha en skyldighet att se till att en person som inte har en godkänd säkerhetsprövning inte deltar i den säkerhetskänsliga verksamheten (moment 8:13 i avsnitt 8.11).

Om ett beslut i ärende om säkerhetsprövning rör en person i företagets ledning eller styrelse, och beslutet innebär att personen inte har en godkänd säkerhetsprövning, kan detta medföra att säkerhetsskyddsavtal inte kan tecknas, eller att ett pågående uppdrag måste avbrytas.

6.17.5. Dokumentation

Moment 6:113 *Om leverantören inte har möjlighet att hantera säkerhetsskyddsklassificerade uppgifter i egna lokaler, ska all dokumentation om säkerhetsprövning av leverantörens personal förvaras av den som ansvarar för säkerhetsskyddsavtalet.*

Vägledande förklaring: Uppgifter som framkommer vid säkerhetsprövning omfattas av sekretess enligt 15 kap. 2 § OSL, vilket innebär att hänsyn måste tas till leverantörens möjlighet att hantera sådana uppgifter i egna lokaler.

Moment 6:114 *När ett säkerhetsskyddsavtal upphör eller avslutas ska den dokumentation som finns om den som har säkerhetsprövats hos leverantören, överlämnas till den som ansvarar för säkerhetsskyddsavtalet.*

Vägledande förklaring: Hur dokumentationen ska hanteras framgår i avsnitt 6.16.8. Se avsnitt 6.9.7 och avsnitt 8.15 om ytterligare åtgärder när säkerhetsskyddsavtal avslutas.

7. Utbildning och övning

7.1. Grunder

Utbildning och övning är en viktig del av säkerhetsskyddet där utgångspunkten ska vara att personal och andra får den kunskap (fakta, förståelse, färdighet och förtrogenhet) som deras arbetsuppgifter och ansvarsområden kräver. Att regelbundet utbilda personal eller andra som deltar i en säkerhetskänslig verksamhet bidrar till att motverka oaktsamhet och bristande kunskaper som kan leda till t.ex. informationsförluster. En ändamålsenlig utbildning medverkar även många gånger till ett engagemang och en delaktighet hos den enskilde, någonting som är speciellt viktigt i en säkerhetskänslig verksamhet.

> *”Personalsäkerhet ska*
>
> *2. säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd.”*
>
> 2 kap. 4 § första stycket 2 säkerhetsskyddslagen

Vägledande förklaring: Det är den som bedriver den säkerhetskänsliga verksamheten som har en skyldighet att säkerställa att de som deltar i verksamheten har tillräcklig kunskap om säkerhetsskydd, dvs. att det genomförs utbildning i säkerhetsskydd.

Utbildnings- och informationsinsatser för att höja kunskapen om verksamhetens säkerhetsskydd och för att öka förståelsen och acceptansen för det är en viktig del av säkerhetsskyddet.[217]

För att förebygga sådana sårbarheter som den s.k. mänskliga faktorn kan utgöra i en verksamhet är information och utbildning om säkerhetsskydd viktiga delar av säkerhetsskyddet. Sårbarheter vid t.ex. myndigheter kan inte sällan direkt kopplas samman med anställda som av okunskap, obetänksamhet eller bekvämlighet inte följer de krav på säkerhetsskydd som gäller för verksamheten. Säkerhetsskyddsåtgärder uppfattas inte sällan som krångliga, tidsödande och begränsande.[218]

[217] Prop. 2017/18:89 s. 139.
[218] Prop. 2017/18:89 s. 74.

”Behörig att ta del av säkerhetsskyddsklassificerade uppgifter eller i övrigt delta i säkerhetskänslig verksamhet är, om inte något annat följer av bestämmelser i lag, endast den som

1. har bedömts pålitlig från säkerhetssynpunkt,

2. har tillräckliga kunskaper om säkerhetsskydd, och

3. behöver uppgifterna eller annan tillgång till verksamheten för att kunna utföra sitt arbete eller på annat sätt delta i den säkerhetskänsliga verksamheten.”

2 kap. 3 § säkerhetsskyddsförordningen

Vägledande förklaring: Bestämmelsen gäller såväl för personer som ska ta del av säkerhetsskyddsklassificerade uppgifter som för personer som ska delta i en säkerhetskänslig verksamhet, även om de inte kommer ta del av säkerhetsskyddsklassificerade uppgifter.

”I 5 kap. 1 § säkerhetsskyddsförordningen (2018:658) finns föreskrifter om utbildning i säkerhetsskydd. Sådan utbildning ska genomföras innan personen får delta i säkerhetskänslig verksamhet.”

7 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

”Den som är ansvarig för en säkerhetskänslig verksamhet ska se till att den som anställs eller på annat sätt deltar i verksamheten får utbildning i säkerhetsskydd. Behovet av utbildning ska följas upp under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.”

5 kap. 1 § säkerhetsskyddsförordningen

”Myndigheten ska regelbundet utbilda och öva myndighetens personal och andra som deltar i den säkerhetskänsliga verksamheten i säkerhetsskydd. Omfattningen och innehållet ska utgå från myndighetens säkerhetsskyddsplan.”

7 kap. 2 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

”Chef för organisationsenhet ansvarar för att

1. personal vid den egna enheten utbildas och övas i säkerhetsskydd,

2. föra förteckning över de som har genomgått utbildning i säkerhetsskydd, och

3. dokumentera genomförda övningar.”

6 kap. 1 § andra stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: En övning med personal som deltar i en säkerhetskänslig verksamhet kan genomföras som ett moment i en större övning, t.ex. en brandövning där ett moment är att genomföra en utrymning och samtidigt säkerställa att säkerhetsskåp är stängda och låsta samt att säkerhetsskyddsklassificerade handlingar är inlåsta. En övning kan genomföras i liten skala.

Exempel
Vid X-förbandet finns en rutin för utrymning som omfattar säkerhetsskyddsklassificerade handlingar och lagringsmedier. Vid en brandövning med utrymning övas även rutinen.

Funktioner eller delar av verksamheten kan övas i att skydda informationstillgångar eller hantera incidenter, t.ex. åtgärder för att återställa kontinuitet efter brand i datorhall eller upptäcka och hantera intrång i informationssystem.

Säkerhetsskyddsåtgärder som innebär utbildning och övning ska framgå av säkerhetsskyddsplanen.[219] Det kan vara lämpligt att det även framgår vilken utbildning i säkerhetsskydd som olika personalkategorier och befattningar ska genomgå samt olika utbildnings- och övningsmål för olika målgrupper.

Med regelbunden utbildning menas att den ska vara återkommande och behovsanpassad med anledning av att:

- säkerhetsskyddsplaneringen reviderats vilket i sin tur kan ha påverkat säkerhetsskyddsplanen och behovet av utbildning och övning,
- en säkerhetshotande händelse eller incident som kräver utbildning och övning för att det inte ska återupprepas,
- nya eller reviderade regelverk ställer nya formella krav på en befattning, eller
- nya eller reviderade instruktioner och rutiner som angår säkerhetsskydd.

[219] 2 kap. 4 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd.

7.2. Krav på kunskaper om säkerhetsskydd

7.2.1. Grundläggande säkerhetsgenomgång i Försvarsmakten

Moment 7:1 *En grundläggande säkerhetsgenomgång ska genomföras för Försvarsmaktens personal och uppdragstagare.*

Vägledande förklaring: Även personal som inte kommer ta del av säkerhetsskyddsklassificerade uppgifter men som på något annat sätt avses delta i säkerhetskänslig verksamhet, ska delta i genomgången. Med *uppdragstagare* avses t.ex. konsulter som arbetar i Försvarsmaktens lokaler. Genomgången bör genomföras senast tre månader efter att en anställning eller ett uppdrag har påbörjats. Den bör kunna genomföras under en lektionstimme utan förkunskapskrav.

Med *personal* avses personal enligt 1-2 §§ förordningen (1996:927) om Försvarsmaktens personal, d.v.s. militär och civil personal. Den militära personalen består av yrkesofficerare, reservofficerare, anställda gruppbefäl, soldater och sjömän, officersaspiranter, rekryter, totalförsvarspliktig personal, krigsfrivillig personal, hemvärnssoldater, frivillig personal, tjänstepliktig personal samt personal i Försvarsmaktens internationella militära insatser.

Moment 7:2 *Den grundläggande säkerhetsgenomgången ska vara lärarledd.*

Moment 7:3 *Den grundläggande säkerhetsgenomgången ska ge personalen förståelse för:*

a) Säkerhetshotande verksamhet som riktas mot Försvarsmakten och aktuell lokal säkerhetshotbild.

b) Skyddsvärden (funktioner, system och anläggningar) som är skyddsvärda ur ett försvarsmakts- respektive lokalt perspektiv.

c) Aktuella risker kopplat till användning av internet, såsom e-post, surfning och sociala medier.

Vägledande förklaring till b): I avsnitt 2.5.2 beskrivs skyddsvärden.

Moment 7:4 *Den grundläggande säkerhetsgenomgången ska ge personalen kunskap om:*

a) Lokal säkerhetsorganisation (t.ex. vem som är säkerhetschef, it-säkerhetschef och signalskyddschef samt eventuella säkerhetsmän).

b) Hur man kontaktar den lokala säkerhetsorganisationen.

c) Lokala säkerhetsbestämmelser (t.ex. rutiner för tillträde och besök).

d) Personalens skyldighet att rapportera säkerhetshotande händelser och verksamhet eller brister i säkerhetsskyddet samt hur rapportering genomförs lokalt.

e) Var man kan få mer information (t.ex. den lokala säkerhetsorganisationen på emilia och samarbetsytan Säkerhetstjänst i FM).

7.2.2. Utbildning för att vara behörig att ta del av säkerhetsskyddsklassificerade uppgifter

Moment 7:5 *En utbildning i säkerhetsskydd för Försvarsmaktens personal eller uppdragstagare som ska ta del av säkerhetsskyddsklassificerade uppgifter, ska minst omfatta:*

a) säkerhetshotande verksamhet,

b) informationssäkerhet,

c) it-säkerhet och

d) fysisk säkerhet.

Vägledande förklaring: Personal och uppdragstagare har redan genomfört den grundläggande säkerhetsgenomgången innan de genomför utbildning enligt moment 7:5.

Moment 7:6 *Om personal eller uppdragstagare endast vid enstaka tillfällen ska ta del av eller på annat sätt hantera säkerhetsskyddsklassificerade uppgifter upp till och med säkerhetsskyddsklass hemlig, får utbildningen i moment 7:5 anpassas så att den som utbildats inte av okunskap röjer säkerhetsskyddsklassificerade uppgifter.*

Vägledande förklaring: Syftet med momentet är att inte ställa alltför omfattande krav på utbildning av t.ex. hemvärnsmän, soldater och sjömän som under övning eller insats tar del av säkerhetsskyddsklassificerade uppgifter om skyddsobjekt och krigsplanläggning.

Innehåll i en sådan anpassad utbildning måste planeras i organisationsenhetens säkerhetsskyddsplan eller i en särskild säkerhetsskyddsplan.

Moment 7:7 *Utbildningen i moment 7:5 ska ge deltagare följande kunskaper.*

a) Säkerhetshotande verksamhet:

1) Indelningen av säkerhetshotande verksamhet i främmande underrättelseverksamhet, kriminalitet, terrorism, sabotage och subversion.

2) Generell omfattning (typ av aktörer och dess intention, kapacitet och tillfälle) av respektive säkerhetshot (främmande underrättelseverksamhet, kriminalitet, terrorism, sabotage och subversion).

3) *Metoder för främmande underrättelseverksamhet (modus operandi) inklusive exempel på genomförande av kontaktförsök.*

4) *Exempel på hur internet och annan it kan användas i säkerhetshotande syfte.*

5) *Belysa risken från insiders och vilka krav det ställer på all personal vad avser uppmärksamhet och rapportering.*

6) *Personalens skyldighet att rapportera säkerhetshotande verksamhet.*

   i. *Hur rapportering av säkerhetshotande verksamhet eller brister i säkerhetsskyddet genomförs på organisationsenheten.*

   ii. *Hur sådan rapportering genomförs i samband med utlandsresor eller utländska besök.*

7) *Lokal och regional säkerhetshotbild med tyngdpunkt på främmande underrättelseverksamhet och kriminalitet.*

b) *Informationssäkerhet:*

1) *Försvarsmaktens modell för informationsklassificering.*

2) *Försvarssekretess (15 kap. 2 § OSL), utrikessekretess (15 kap. 1 § OSL) och säkerhets- och bevakningssekretess (18 kap. 8 § OSL).*

3) *Indelning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklasser och klassernas betydelser.*

4) *Exempel på uppgifter som:*

   i. *omfattas av sekretess och som är säkerhetsskyddsklassificerade,*

   ii. *omfattas av sekretess men som inte är säkerhetsskyddsklassificerade samt*

   iii. *inte omfattas av någon sekretess.*

5) *Hur säkerhetsskyddsklassificerade handlingar ska hanteras:*

   i. *Behörighet.*

   ii. *Registrering.*

   iii. *Märkning med sekretessmarkering.*

   iv. *Märkning med säkerhetsskyddsklass.*

v. *Kopiering.*

vi. *Intern och extern distribution.*

vii. *Kvittering vid mottagande.*

viii. *Inventering.*

ix. *Muntlig delgivning eller visning.*

x. *Medförande.*

xi. *Förvaring.*

xii. *Återlämning.*

xiii. *Förstöring.*

c) *It-säkerhet:*

1) *Endast informationssystem som är godkända från säkerhetssynpunkt får användas för behandling av säkerhetsskyddsklassificerade uppgifter.*

i. *Vilka system som får användas.*

ii. *Vilka system som inte får användas. Det ska framgå att FM AP inte får användas för säkerhetsskyddsklassificerade uppgifter.*

2) *Användning av privata informationssystem inklusive datorer, mobiltelefoner, surfplattor m.m.*

3) *Skydda kort och kod samt lösenord för informationssystem.*

4) *Placering av bildskärmar.*

5) *Utskrifter.*

6) *Kopieringsmaskiner för kopiering av säkerhetsskyddsklassificerade uppgifter.*

7) *Risker med lagringsmedier.*

8) *Hur säkerhetsskyddsklassificerade lagringsmedier ska hanteras:*

i. *Anskaffning.*

ii. *Registrering.*

iii. *Märkning med sekretessmarkering.*

iv. *Märkning med säkerhetsskyddsklass.*

v. *Intern och extern distribution.*

vi. *Kvittering vid mottagande.*

vii. *Inventering.*

viii. *Medförande.*

ix. *Förvaring.*

x. *Återlämning.*

xi. *Förstöring.*

9) *Överföring av information mellan system som är godkända från säkerhetssynpunkt för olika säkerhetsskyddsklasser.*

10) *Organisationsenhetens bestämmelser för informationssystem.*

11) *Rapportering av it-incidenter.*

d) *Fysisk säkerhet:*

1) *Vad den fysiska säkerheten ska skydda mot.*

2) *Organisationsenhetens bestämmelser för:*

i. *Tillträdesrätt, passerkontroll och eventuell indelning i zoner.*

ii. *Besök.*

iii. *Kort, nycklar och koder.*

iv. *Skydd mot farliga ämnen, vapen samt avlyssnings- och störutrustning.*

3) *Utrymmen vid organisationsenheten som är godkända för regelbunden muntlig delgivning.*

4) *Inre bevakning.*

5) *Organisationsenhetens bestämmelser för larm.*

6) *Var deltagarna kan hitta organisationsenhetens instruktion om den fysiska säkerheten för organisationsenheten.*

7.2.3. Specialiserad utbildning i säkerhetsskydd

Grundläggande säkerhetsgenomgång och utbildning för att vara behörig att ta del av säkerhetsskyddsklassificerade uppgifter utgör en grund för Försvarsmaktens personal. För många kan genomgången och utbildningen vara tillräckliga. För andra behövs mer specialiserade utbildningar, t.ex. säkerhetschefer, it-säkerhetschefer, signalskyddspersonal, personal som arbetar med dokumenthantering och personal som arbetar med it. Innehållet i sådana utbildningar ska utgå från verksamhetens säkerhetsskyddsplan och återfinns inte i detta reglemente.

I avsnitt 6.5.1 finns krav på utbildning av personer som ska genomföra säkerhetsprövning.

I Försvarsmaktens säkerhetsskyddsplan ska behovet av utbildning särskilt framgå.[220] Sådan utbildning kan avse utbildning som behövs med anledning av inträffade snarlika händelser med negativa konsekvenser för säkerhetsskyddet eller nya regler. Planen kan även ange vilken specialiserad utbildning i säkerhetsskydd som vissa personalkategorier behöver.

Även i organisationsenhetens säkerhetsskyddsplan ska behovet av utbildning särskilt framgå (avsnitt 2.6). Sådant behov bör främst handla om vilken utbildning i säkerhetsskydd som behövs med anledning av lokala förhållanden.

> *”Den som innehar en befattning som säkerhetschef ska genomgå en centralt anordnad utbildning för säkerhetschefer och nå godkänt resultat, eller ha förvärvat motsvarande kunskap på annat sätt.”*
>
> 6 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: För att anses ha fått motsvarande kunskaper på annat sätt behöver personen ha utbildats i, eller ha tillämpat, bestämmelser om säkerhetsskydd som gäller i Försvarsmakten. Det är inte tillräckligt att enbart ha erfarenhet från säkerhetsskyddsarbete utanför Försvarsmakten.

Det är den som ansvarar för anställningen som bedömer om en person har förvärvat motsvarande kunskaper. Säkerhetsskyddsavdelningen vid Must kan ge stöd i bedömningen.

[220] 2 kap. 4 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd.

7.3. Dokumentation av genomförd utbildning och övning

”Myndigheten ska föra en förteckning över de anställda och andra som har genomgått utbildning i säkerhetsskydd, samt vilken utbildning som genomförts och när. En genomförd övning ska dokumenteras.”

7 kap. 2 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Genom att förteckna *vem* som genomgått *vilken utbildning och övning* i säkerhetsskydd samt *när* kan Försvarsmakten även följa upp en enskilds utbildningsbehov. En förteckning ger även stöd för en långsiktig planering av utbildnings- och övningsinsatser. Förteckningen kan även användas för att skriftligen bekräfta att man tagit del av utbildning eller genomfört en övning i säkerhetsskydd; därmed hålls den enskilde medansvarig för sin egen utbildning.

Förteckningen förs lämpligen genom dokumentation vid den organisationsenhet som personen hör till.

8. Säkerhetsskyddad upphandling

8.1. Säkerhetsskyddsavtal

”Den som bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska dokumenteras.

Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.

Verksamhetsutövaren ska även kontrollera säkerhetsskyddet i den egna verksamheten, anmäla och rapportera sådant som är av vikt för säkerhetsskyddet och i övrigt vidta de åtgärder som krävs enligt denna lag.

Så långt det är möjligt ska säkerhetsskyddsåtgärderna utformas så att de inte medför någon skada eller annan olägenhet för andra allmänna eller enskilda intressen.”

2 kap. 1 § säkerhetsskyddslagen

”Statliga myndigheter, kommuner och regioner som avser att genomföra en upphandling och ingå ett avtal om varor, tjänster eller byggentreprenader ska se till att det i ett säkerhetsskyddsavtal anges hur kraven på säkerhetsskydd enligt 1 § ska tillgodoses av leverantören om

1. det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller

2. upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.”

2 kap. 6 § första stycket säkerhetsskyddslagen

Vägledande förklaring: Statliga myndigheter, kommuner och regioner är under vissa förutsättningar skyldiga att se till att den leverantör som man efter en upphandling avser att ingå ett avtal med ska teckna ett säkerhetsskyddsavtal. Med leverantör avses även anbudssökande och anbudsgivare.[221]

Hänvisningen till 2 kap. 1 § säkerhetsskyddslagen tydliggör grundtanken i säkerhetsskyddet att de intressen som lagen slår vakt om ska ha samma skydd oavsett om verksamheten bedrivs av det allmänna eller av enskilda. I det här sammanhanget innebär det att när en utomstående aktör genom en upphandling engageras i säkerhetskänslig verksamhet ska behovet av säkerhetsskyddsåtgärder enligt 2 kap. 1 § säkerhetsskyddslagen utredas och kraven på sådana åtgärder uppställas i ett säkerhetsskyddsavtal mellan parterna.

[221] Prop. 2017/18:89 s. 141.

För säkerhetsprövning gäller bestämmelserna i 3 kap. säkerhetsskyddslagen. Hänvisningen till 2 kap. 1 § säkerhetsskyddslagen innebär vidare att säkerhetsskyddet inte får göras mindre långtgående än vad som följer av den bestämmelsen. En enskild aktör som omfattas av lagstiftningen kan alltså inte genom ett säkerhetsskyddsavtal åläggas mindre omfattande säkerhetsskyddsåtgärder än de som redan gäller för verksamheten enligt denna lag. Däremot kan ett säkerhetsskyddsavtal fylla funktionen att det preciserar säkerhetsskyddet hos leverantören för att passa den aktuella upphandlingen.

Ledning för tolkning av ordet *upphandling* kan hämtas från upphandlingslagstiftningen. Paragrafen gäller all typ av upphandling, även sådan upphandling som med stöd av upphandlingslagstiftningen kan undantas från lagstiftningens regelverk. Med leverantör avses även anbudssökande och anbudsgivare.[222] Med upphandling avses de åtgärder som vidtas i syfte att anskaffa varor, tjänster eller byggentreprenader genom tilldelning av kontrakt.[223] Bestämmelsen gäller även vid tecknande av ramavtal (affärsavtal).

Enligt andra punkten gäller kravet på säkerhetsskyddsavtal även om upphandlingen och avtalet inte berör säkerhetsskyddsklassificerade uppgifter om avtalsingåendet i övrigt ger en leverantör tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet. Det kan t.ex. vara fråga om upphandling av informationssystem eller andra elektroniska kommunikationslösningar som avser vitala funktioner för samhället och som medför höga krav på tillgänglighet och riktighet. Det kan även gälla situationer där leverantören ska delta i säkerhetskänslig verksamhet i övrigt. Detta kan vara fallet på t.ex. kärnkraftverk och flygplatser där den säkerhetskänsliga verksamheten enbart i begränsad omfattning avser säkerhetsskyddsklassificerade uppgifter.[224]

Av författningskommentaren ovan följer att ett säkerhetsskyddsavtal är en förutsättning för att en upphandling i vissa situationer kan genomföras och avtal ingås. Därför måste också varje enskild upphandling ha ett eget säkerhetsskyddsavtal. De upphandlande myndigheterna har olika krav på säkerhetsskydd som genom säkerhetsskyddsavtal överförs till leverantörer. Ett säkerhetsskyddsavtal som en annan myndighet har ingått med en leverantör kan inte användas av en annan myndighet. Dessutom kan de säkerhetshotande verksamheter som påverkar uppdraget variera.

Se även avsnitt 6.17 för mer information om hur säkerhetsprövning ska genomföras vid säkerhetsskyddad upphandling.

[222] Prop. 2017/18:89 s. 141.
[223] 1 kap. 2 § lagen (2016:1145) om offentlig upphandling.
[224] Prop. 2017/18:89 s. 141.

8.1.1. Begränsat hemlig och säkerhetskänslig verksamhet av motsvarande betydelse

”En myndighet som avser att genomföra en upphandling som rör säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet ska säkerställa att säkerhetsskyddet upprätthålls.”

8 kap. 3 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Att krav inte ställs på säkerhetsskyddsavtal för alla upphandlingar eller kontraktssituationer vid säkerhetskänslig verksamhet innebär inget hinder mot att sådana avtal ändå ingås när det t.ex. gäller en upphandling där det förekommer säkerhetsskyddsklassificerade uppgifter i den lägsta säkerhetsskyddsklassen.[225] Genom att ingå ett säkerhetsskyddsavtal kan Försvarsmakten ställa krav i syfte att säkerhetsskyddet ska upprätthållas.

”I 8 kap. 3 § andra stycket Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd finns bestämmelser att en myndighet ska säkerställa att säkerhetsskyddet upprätthålls om en upphandling rör säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Den i Försvarsmakten som avser att genomföra en sådan upphandling ska se till att säkerhetsskyddet regleras i ett säkerhetsskyddsavtal.”

7 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Krav på skyddsåtgärder i ett sådant säkerhetsskyddsavtal måste anpassas så att tillräcklig skyddsnivå uppnås utan att oönskade kostnader uppstår.

8.2. Internationell säkerhetsskyddad upphandling

Även upphandlingar med leverantörer som har sitt säte i ett annat land än Sverige ska genomföras som en säkerhetsskyddad upphandling. Något undantag i säkerhetsskyddslagen finns inte för sådana leverantörer. Detta innebär att sådana internationella upphandlingar ska hanteras på samma sätt som med en leverantör som har sitt säte i Sverige.

[225] Prop. 2017/18:89 s. 141.

”Säkerhetsskyddsklassificerade uppgifter får inte lämnas till en utländsk leverantör om inte Sverige har ingått ett internationellt säkerhetsskyddsåtagande med den andra staten och leverantören har godkänts genom en kontroll enligt den andra statens säkerhetsskyddslagstiftning.”

3 kap. 9 § andra stycket säkerhetsskyddsförordningen

Enligt punkten 6 i övergångsbestämmelserna i säkerhetsskyddsförordningen behöver bestämmelsen inte följas förrän den 1 januari 2022.

Vägledande förklaring: Med utländsk leverantör avses en leverantör som har sitt säte i ett annat land än Sverige. Ett godkännande avser säkerhetsintyg för leverantör (på engelska Facility Security Clearance Certificate, vilket förkortas FSCC eller ibland enbart FSC). Ett sådant godkännande lämnas från den behöriga säkerhetsmyndigheten i den andra staten. I internationella säkerhetsskyddsåtaganden (t.ex. ett generellt säkerhetsskyddsavtal mellan Sverige och den andra staten) framgår vilken myndighet hos den andra staten som är behörig säkerhetsmyndighet.

8.3. Analys före upphandling

”Myndigheten ska innan en upphandling påbörjas analysera om uppdraget rör säkerhetskänslig verksamhet.”

8 kap. 1 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Analys i bestämmelsen är inte en säkerhetsskyddsanalys, utan endast en analys för att komma fram till om uppdraget rör säkerhetskänslig verksamhet. Det är fråga om en ”ja eller nej”-analys. Säkerhetsskyddsanalyser i Försvarsmakten är ett stöd för en sådan analys.

Den säkerhetskänsliga verksamheten som avses i bestämmelsen innefattar även säkerhetsskyddsklassificerade uppgifter. Om analysen visar att uppdraget rör säkerhetskänslig verksamhet ska analysen innehålla identifiering och prioritering av skyddsvärda tillgångar, bedömning av säkerhetshot, bedömning av sårbarheter, bedömning av risker samt prioritering och hantering av risker. Vilka säkerhetsåtgärder som ska finnas anges i en plan för hur säkerhetsskyddet ska regleras i uppdraget.

Även upphandlingar som rör säkerhetskänslig verksamhet som omfattar begränsat hemliga uppgifter eller annan säkerhetskänslig verksamhet där skadan för Sveriges säkerhet endast kan bli ringa, ska identifieras.

Enligt tredje stycket i bestämmelsen ska analysen dokumenteras.

Om en analys visar att uppdraget inte rör säkerhetskänslig verksamhet enligt 1 kap. 1 § säkerhetsskyddslagen ska upphandlingen genomföras utan säkerhetsskydd.

8.3.1. Analys före upphandling och avrop

Moment 8:1 *När organisationsenheten avser att avropa från ett ramavtal ska organisationsenheten först genomföra en analys enligt 8 kap. 1 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd.*

Moment 8:2 *Om ett uppdrag som avses upphandlas eller avropas rör säkerhetskänslig verksamhet ska analysen enligt 8 kap. 1 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd minst omfatta:*

a) En bedömning av lämpligheten från säkerhetsskyddssynpunkt att genomföra upphandlingen.

b) Vilken säkerhetshotande verksamhet som kan riktas mot uppdraget.

c) Identifiering av vilka organisationsenheter som kan påverkas av uppdraget.

d) Vilken omfattning en leverantör kommer att få ta del av eller hantera säkerhetsskyddsklassificerade uppgifter eller delta i säkerhetskänslig verksamhet.

Moment 8:3 *Om analysen enligt 8 kap. 1 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd visar att någon annan organisationsenhet påverkas av uppdraget ska den som är ansvarig för upphandlingen samverka med berörd organisationsenhet om vilken säkerhetskänslig verksamhet som berörs och behovet av säkerhetsskydd.*

8.4. Plan när ett uppdrag rör säkerhetskänslig verksamhet

> *”Om upphandlingen rör säkerhetskänslig verksamhet ska myndigheten ta fram en plan för hur säkerhetsskyddet ska regleras i uppdraget. Vid behov ska myndighetens säkerhetsskyddsplanering revideras.”*
>
> 8 kap. 1 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Syftet med planen är att det ska skapas en struktur för regleringen av säkerhetsskyddet i uppdraget. I det enkla fallet är det endast ett uppdrag och en leverantör. Den plan som då ska upprättas blir mycket kortfattad och enkel eftersom den enbart innehåller krav på säkerhetsskyddsavtal, vem som ska ta fram avtalet, vem som ska teckna avtalet och när i upphandlingsprocessen avtalet ska tecknas.

I mer komplicerade uppdrag med flera leverantörer, flera uppdrag mot en leverantör eller flera underleverantörer till en huvudleverantör kommer planen att skapa en struktur som ger översikt över säkerhetsskyddet i upphandlingen.

8.5. Analys av deltagande i säkerhetskänslig verksamhet

”Innan en myndighet lämnar ut säkerhetsskyddsklassificerade uppgifter till en leverantör eller när leverantören ska delta i säkerhetskänslig verksamhet ska myndigheten göra en analys enligt 6 kap. 3 §. Analysen ska omfatta leverantörens ledning och övriga hos leverantören som avses delta i den säkerhetskänsliga verksamheten.”

8 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Av 6 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd följer att analysen ska ange:

- vilka befattningar hos leverantören som ska vara placerade i säkerhetsklass och i sådant fall vilken säkerhetsklass samt
- vilka befattningar som endast ska vara föremål för säkerhetsprövning utan registerkontroll.

Enligt samma bestämmelse ska analysen utgå från säkerhetsskyddsanalyser i Försvarsmakten och särskilt beakta förekomsten av internationella åtaganden om säkerhetsskydd. Enligt bestämmelsen ska analysen dokumenteras.

Analysen ska säkerställa att någon som inte är säkerhetsprövad inte kommer att delta i den säkerhetskänsliga verksamheten eller få ta del av säkerhetsskyddsklassificerade uppgifter.

Med leverantörens ledning ska här förstås verkställande direktör, styrelse och andra i ledningen förutsatt att de kommer att ha, eller kan få, tillgång till eller insyn i den säkerhetskänsliga verksamheten. I avsnitt 6.17 finns moment om säkerhetsprövning vid säkerhetsskyddad upphandling, inklusive analys av befattningar.

8.6. Särskild säkerhetsskyddsbedömning (SSB)

”En statlig myndighet som avser att genomföra en upphandling som innebär krav på säkerhetsskyddsavtal enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585) ska vidta de åtgärder som anges i andra stycket, om

1. leverantören kan få tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller högre utanför myndighetens lokaler, eller

2. leverantören kan få tillgång till säkerhetskänsliga informationssystem utanför myndighetens lokaler och obehörig åtkomst till systemen kan medföra allvarlig skada för Sveriges säkerhet.”

2 kap. 6 § första stycket säkerhetsskyddsförordningen

”En statlig myndighet som avser att genomföra en sådan upphandling ska innan förfarandet inleds
1. genom en särskild säkerhetsskyddsbedömning identifiera och dokumentera vilka säkerhetsskyddsklassificerade uppgifter eller säkerhetskänsliga informationssystem som leverantören kan få del av och som kräver säkerhetsskydd, och
2. samråda med den myndighet som enligt 7 kap. 1 § första stycket 1 eller 2 utövar tillsyn över den aktuella verksamheten.”

2 kap. 6 § andra stycket säkerhetsskyddsförordningen

Moment 8:4 *En särskild säkerhetsskyddsbedömning ska även genomföras om en upphandling ger leverantören tillgång till säkerhetskänslig verksamhet där den som deltar har möjlighet att orsaka allvarlig skada.*

Vägledande förklaring: I Försvarsmakten utgör en särskild säkerhetsskyddsbedömning (SSB) de två första stegen i en säkerhetsskyddsanalys. Dessa steg består av verksamhetsbeskrivning (avsnitt 2.5.1) och identifiering av säkerhetsskyddsvärden (avsnitt 2.5.2) i den säkerhetskänsliga verksamheten. Metodstöd för att genomföra särskild säkerhetsskyddsbedömning finns i kapitel 2.

8.7. Samråd

I 2 kap. 6 § säkerhetsskyddsförordningen finns krav på samråd om:

- leverantören kan få tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller högre utanför myndighetens lokaler, eller
- leverantören kan få tillgång till säkerhetskänsliga informationssystem utanför myndighetens lokaler och obehörig åtkomst till systemen kan medföra allvarlig skada för Sveriges säkerhet.

Myndigheter som ska följa Försvarsmaktens föreskrifter om säkerhetsskydd ska samråda med Försvarsmakten.

”En begäran om samråd enligt 2 kap. 6 § andra stycket 2 säkerhetsskyddsförordningen (2018:658) ska ställas till Försvarsmaktens högkvarter. Till ett sådant samrådsförfarande ska de uppgifter som Försvarsmakten efterfrågar tillhandahållas.”

8 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd

”Chefen för militära underrättelse och säkerhetstjänsten bemyndigas att besluta i ärenden som avses i 2 kap. 6 § säkerhetsskyddsförordningen (2018:658).

Beslut om förelägganden enligt 2 kap. 6 § säkerhetsskyddsförordningen får delegeras till lägst kontorschef vid militära underrättelse- och säkerhetstjänsten.

Beslut att stoppa en upphandling får inte delegeras.”

11 kap. 14 § FIB FM ArbO

8.7.1. Samråd i Försvarsmakten

Produktionschefen, FM CIO, chefen för Must och chefen för specialförbanden har bemyndigats att genomföra upphandling.[226] Enligt FM ArbO ska produktionschefen, FM CIO och chefen för specialförbanden samråda med chefen för Must.[227] Om bemyndigandet att genomföra upphandling delegeras måste även samrådsskyldigheten uppmärksammas.

Moment 8:5 *En begäran om samråd ska innehålla:*

a) Motivering till varför verksamheten behöver bedrivas utanför myndighetens lokaler.

b) Särskild säkerhetsskyddsbedömning.

c) Särskild säkerhetsskyddsplan.

d) Utkast till signalskyddskrav, om signalskydd ska användas.

e) Anbudsförfrågan.

f) Analys av vilka befattningar hos leverantören som ska placeras i säkerhetsklass samt vilket övrigt deltagande i den säkerhetskänsliga verksamheten som endast vara föremål för säkerhetsprövning utan registerkontroll.

g) Utkast till säkerhetsskyddsavtal.

h) Övriga dokument och krav som påverkar säkerhetsskyddet.

Moment 8:6 *En begäran om samråd ska skickas till säkerhetsskyddsavdelningen vid Must.*

[226] 8 kap. 40 §, 9 kap. 3 §, 11 kap. 13 § 3 och 12 kap. 6 § FM ArbO.
[227] 8 kap. 40 §, 9 kap. 9 a § och 12 kap. 6 § FM ArbO.

8.8. Bedömning av en leverantörs lämplighet

”En bedömning av en leverantörs lämplighet ur säkerhetsskyddssynpunkt ska göras innan ett säkerhetsskyddsavtal tecknas. Bedömningen ska dokumenteras.”

8 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Myndighetens bedömning avser leverantören som juridisk person. Om en leverantör har stora ekonomiska skulder som kan innebära en sårbarhet, eller om ägarförhållandena innebär att individer som inte är pålitliga från säkerhetssynpunkt har inflytande över leverantören, kan bedömningen vara att leverantören inte är lämplig.

8.8.1. Bedömning av en leverantörs lämplighet

Moment 8:7 *I en bedömning av en leverantörs lämplighet ska ägarförhållanden, ekonomiska förhållanden och kopplingar till säkerhetshotande verksamhet framgå.*

Moment 8:8 *En underleverantörs lämplighet ska bedömas om underleverantören*

a) kan få tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter utanför Försvarsmaktens lokaler, eller

b) kan få tillgång till säkerhetskänsliga informationssystem utanför Försvarsmaktens lokaler och obehörig åtkomst till systemen kan medföra ringa skada eller högre för Sveriges säkerhet, eller

c) kan få tillgång till säkerhetskänslig verksamhet där den som deltar har möjlighet att orsaka ringa skada eller högre för Sveriges säkerhet.

Vägledande förklaring: Ur ett säkerhetsskyddsperspektiv måste bedömningen innehålla en undersökning av bolagsstrukturen, utländska ägarförhållanden och var den egentliga verksamheten bedrivs, t.ex. om verksamheten kommer att genomföras av underleverantör eller om verksamheten kommer att genomföras utanför Sverige.

Moment 8:9 *Om en leverantör har bedömts vara olämplig får inte affärsavtal och säkerhetsskyddsavtal ingås.*

8.9. Parter i säkerhetsskyddsavtal

Moment 8:10 *Om Försvarsmakten avser att genomföra en upphandling av varor, tjänster eller byggentreprenader eller avropar från ett tecknat ramavtal (affärsavtal) ska Försvarsmakten vara part i säkerhetsskyddsavtalet.*

Vägledande förklaring: Syftet med säkerhetsskyddsavtalet är att överföra de säkerhetsskyddsbestämmelser som gäller för Försvarsmakten på en part som normalt inte omfattas av regelverket. Därför är det viktigt att säkerhetsskyddsavtalet är särskilt anpassat till Försvarsmaktens verksamhet, de säkerhetsskyddsbestämmelser som

reglerar Försvarsmaktens verksamhet och det säkerhetsskydd som behövs hos leverantören.

Moment 8:11 *Varje uppdrag, upphandling eller avrop från ramavtal (affärsavtal) ska omfattas av ett eget säkerhetsskyddsavtal.*

Vägledande förklaring: Detta innebär att en leverantör kan ha flera säkerhetsskyddsavtal. Ett säkerhetsskyddsavtal per uppdrag, upphandling eller avrop från ramavtal (affärsavtal) medför att det blir möjligt att ha en överblick över vilka uppgifter, informationssystem och säkerhetskänslig verksamhet som en leverantör har tillgång till. Det krävs även för att kunna genomföra och följa de krav som ställs avseende säkerhetsprövning i kapitel 6.

8.10. Behörighet att ingå säkerhetsskyddsavtal

”Av 4 § myndighetsförordningen (2007:515) följer att myndigheten ska utse vem som är behörig att ingå ett säkerhetsskyddsavtal.”

8 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: I FM ArbO framgår vem som för Försvarsmaktens räkning har rätt att ingå avtal, bl.a. FM CIO, produktionschefen, chefen för Must och chefen för specialförbanden. Denna rätt omfattar även säkerhetsskyddsavtal. Chef för organisationsenhet har i FM ArbO inte bemyndigats att ingå avtal. För att chef för organisationsenhet ska få ingå säkerhetsskyddsavtal måste chefen vara bemyndigad.

Säkerhetsskyddsavtal som har ingåtts tidigare fortsätter att gälla.

”Den som med stöd av denna författning har fått ett bemyndigande att ingå avtal eller överenskommelser med myndigheter, regioner, kommuner, organisationer eller enskilda, får göra det under förutsättning att juridiska avdelningen i Högkvarteret har deltagit i beredningen.

Chefsjuristen beslutar vilka avtal och överenskommelser som inte måste beredas med juridiska avdelningen i Högkvarteret. Bemyndigandet får inte delegeras.”

5 kap. 2 § första och andra styckena FM ArbO

Vägledande förklaring: Bestämmelsen gäller även säkerhetsskyddsavtal.

8.11. Säkerhetsskyddsavtalets innehåll

Moment 8:12 *Ett säkerhetsskyddsavtal ska innehålla bestämmelser som ger Försvarsmakten rätt att:*

a) ensidigt säga upp eller häva säkerhetsskyddsavtalet,

b) begära ersättning för Försvarsmaktens skada samt vite om leverantören bryter mot säkerhetsskyddsavtalet, samt

c) genomföra föranmälda och oanmälda säkerhetsskyddskontroller hos leverantören.

Moment 8:13 *Ett säkerhetsskyddsavtal ska innehålla bestämmelser om säkerhetsprövning av en leverantörs personal. Det ska framgå:*

a) vem som ansvarar för genomförandet,

b) att brister i pålitlighet, lojalitet och sårbarhet i säkerhänseende ska rapporteras till Försvarsmakten, och

c) att leverantören ska följa Försvarsmaktens beslut i ärende om säkerhetsprövning samt Försvarsmaktens omprövning av sådana beslut.

Moment 8:14 *Ett säkerhetsskyddsavtal ska innehålla bestämmelser som reglerar leverantörens skyldighet att till Försvarsmakten redovisa:*

a) förändringar avseende personer med betydande inflytande (PBI) hos leverantören, samt

b) förändringar i uppdraget som påverkar säkerhetsskyddet eller behov av säkerhetsskydd.

Moment 8:15 *Ett säkerhetsskyddsavtal ska utöver de krav som anges i lagar, förordningar, föreskrifter och andra bestämmelser omfatta de krav som tagits fram i den särskilda säkerhetsskyddsplanen.*

8.12. Utanför Försvarsmaktens lokaler

”Om leverantören utanför myndighetens lokaler ska hantera eller förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller när leverantören utanför myndighetens lokaler ska delta i säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, ska myndigheten om det inte är uppenbart obehövligt vidta följande åtgärder.

1. Kontrollera att lokalerna och övriga förhållanden är lämpliga ur säkerhetsskyddssynpunkt,

2. dokumentera kontrollen, och

3. se till att det av säkerhetsskyddsavtalet framgår att leverantören ska upprätta en säkerhetsskyddsinstruktion som ska granskas och godkännas av myndigheten.”

8 kap. 8 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Om brister i säkerhetsskyddet har identifierats i en kontroll av lokaler och övriga förhållanden, t.ex. den fysiska miljön runt lokalerna, måste det

särskilt framgå i dokumentationen. En sådan dokumentation kan tjäna som underlag för ett eventuellt återbesök. Det kan vara uppenbart obehövligt att göra en sådan kontroll som föreskrivs i bestämmelsen om leverantören redan i lokalerna bedriver sådan verksamhet som kräver ett säkerhetsskydd för Försvarsmaktens räkning.

Säkerhetsskyddsinstruktionen måste innehålla bestämmelser som motsvarar de bestämmelser för hantering och förvaring som gäller i Försvarsmakten. Uppgifter eller verksamhet får inte ges ett sämre skydd för att de förvaras i lokaler som inte är under Försvarsmaktens kontroll. Samma krav för säkerhetsskyddsåtgärder måste finnas hos leverantören som hos Försvarsmakten.

8.12.1. Säkerhetsskyddsinstruktion

Moment 8:16 *Säkerhetsskyddsinstruktionen ska granskas och godkännas av organisationsenheten. Ett godkännande får inte lämnas före ett samråd enligt 2 kap. 6 § andra stycket 2 säkerhetsskyddsförordningen har ägt rum med säkerhetsskyddsavdelningen vid Must.*

Moment 8:17 *Ett säkerhetsskyddsavtal får inte ingås innan kontroll av leverantörens lokaler och övriga förhållanden är genomförda. En sådan kontroll ska inte genomföras om den bedöms vara uppenbart obehövlig. En sådan bedömning ska då dokumenteras.*

8.13. Anmälan om säkerhetsskyddsavtal

> *”Den som har ingått ett säkerhetsskyddsavtal enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585) ska anmäla det till Säkerhetspolisen. En sådan anmälan ska också göras när ett säkerhetsskyddsavtal upphör att gälla.”*
>
> 2 kap. 7 § säkerhetsskyddsförordningen

> *”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ska anmäla säkerhetsskyddsavtal till Säkerhetspolisen enligt vad som föreskrivs i 2 kap. 7 § säkerhetsskyddsförordningen (2018:658).”*
>
> 7 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 8:18 *Den som har tecknat ett säkerhetsskyddsavtal ska genom SUA-rutinen i IS UNDSÄK meddela säkerhetsskyddsavdelningen vid Must om avtalet. Uppgifter om diarienummer för säkerhetsskyddsavtalet och affärsavtalet ska ingå.*

Vägledande förklaring: Uppgifter diarienummer kan antecknas i kommentarsfältet i SUA-uppdraget i SUA-rutinen.

Endast säkerhetsskyddsavtal som avser säkerhetsskyddsklassen konfidentiell eller högre samt säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges sä-

kerhet ska anmälas till Säkerhetspolisen.[228] Säkerhetsskyddsavdelningen vid Must behöver dock ha information om alla säkerhetsskyddsavtal, oavsett vilken säkerhetsskyddsklass eller vilken verksamhet som ett säkerhetsskyddsavtal avser.

8.14. Uppdatering av särskild säkerhetsskyddsbedömning och särskild säkerhetsskyddsplan

> *”Myndigheten ska se till att den särskilda säkerhetsskyddsbedömningen som anges i 2 kap. 6 § andra stycket 1 säkerhetsskyddsförordningen (2018:658) och sådana analyser och planer som anges i 1 § hålls uppdaterade till dess att säkerhetsskyddsavtalet upphör att gälla.”*
>
> 8 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Om den särskilda säkerhetsskyddsbedömningen, analyserna eller planerna uppdateras, kan det finnas ett behov av att säga upp och ingå ett nytt reviderat säkerhetsskyddsavtal.

2 kap. 6 § säkerhetsskyddsförordningen återges i avsnitt 8.6. Analys enligt 8 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd beskrivs i avsnitt 8.3. Plan enligt 8 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd beskrivs i avsnitt 8.4.

Moment 8:19 *Den särskilda säkerhetsskyddsbedömningen, den särskilda säkerhetsskyddsanalysen och den särskilda säkerhetsskyddsplanen ska uppdateras när:*

a) ägarförhållanden förändras som leder till förändringar i vilka som har inflytande över leverantören,

b) leverantören kommer ta del av säkerhetsskyddsklassificerade uppgifter i en högre säkerhetsskyddsklass än vad som ursprungligen var bedömt,

c) leverantörens personal kommer att delta i en säkerhetskänslig verksamhet och till följd av sitt deltagande har möjlighet att orsaka större skada för Sveriges säkerhet än vad som ursprungligen var bedömt, eller

d) en kontroll av leverantörens säkerhetsskydd visar att leverantören inte har följt säkerhetsskyddsavtalet.

Vägledande förklaring: Det kan även finnas andra omständigheter som medför att en bedömning, analys och plan behöver uppdateras. Därför är det viktigt att den som har tecknat ett säkerhetsskyddsavtal har en kontinuerlig dialog med den som ansvarar för affärsavtalet samt med leverantörens säkerhetsskyddsföreträdare.

[228] 2 kap. 6 § första stycket säkerhetsskyddslagen.

8.15. Avslut av säkerhetsskyddsavtal

”Den som har ingått ett säkerhetsskyddsavtal enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585) ska anmäla det till Säkerhetspolisen. En sådan anmälan ska också göras när ett säkerhetsskyddsavtal upphör att gälla.”

2 kap. 7 § säkerhetsskyddsförordningen

”Försvarsmaktens säkerhetsskyddschef bemyndigas att anmäla säkerhetsskyddsavtal till Säkerhetspolisen enligt vad som föreskrivs i 2 kap. 7 § säkerhetsskyddsförordningen.”

11 kap. 25 § 4 FM ArbO

Moment 8:20 *Den som har ingått ett säkerhetsskyddsavtal ska underrätta säkerhetsskyddsavdelningen vid Must när ett säkerhetsskyddsavtal har upphört att gälla.*

Vägledande förklaring: Se även avsnitt 6.9.7 om avanmälan av registerkontroll.

8.16. Bevarande av handlingar om säkerhetsskyddad upphandling

Riksarkivet har meddelat föreskrifter om bevarande och gallringsfrister för allmänna handlingar om säkerhetsskyddad upphandling.[229]

[229] Riksarkivets föreskrifter (RA-FS 2018:3) och allmänna råd om återlämnande eller gallring av handlingar vid upphandling.

9. Kontroll av säkerhetsskydd

9.1. Grunder

”Verksamhetsutövaren ska även kontrollera säkerhetsskyddet i den egna verksamheten, anmäla och rapportera sådant som är av vikt för säkerhetsskyddet och i övrigt vidta åtgärder som krävs enligt denna lag.”

2 kap. 1 § tredje stycket säkerhetsskyddslagen

Vägledande förklaring: Verksamhetsutövaren ska se till att det finns intern kontroll av säkerhetsskyddet.[230]

”Vid verksamhet som förordningen gäller för ska det, om det inte är uppenbart obehövligt, finnas en säkerhetsskyddschef som kontrollerar att verksamheten bedrivs i enlighet med vad som föreskrivs i säkerhetsskyddslagen (2018:585) och denna förordning.”

2 kap. 2 § första stycket säkerhetsskyddsförordningen

Vägledande förklaring: Kontroll av säkerhetsskyddet genomförs genom säkerhetsskyddskontroller och syftet är att identifiera eventuella brister i säkerhetsskyddet med stöd av bestämmelser för säkerhetsskydd. Resultatet från säkerhetsskyddskontrollen utgör ett stöd för verksamhetsutövaren, och leverantör vid kontroll av säkerhetsskyddsavtal, för att vid behov vidta säkerhetsskyddsåtgärder.

9.2. Myndigheternas kontroll av det egna säkerhetsskyddet

”Myndigheten ska årligen och vid behov kontrollera att regler för säkerhetsskyddet vid myndigheten följs och att säkerhetsskyddet är anpassat till aktuell säkerhetsskyddsplanering.

Kontrollen ska dokumenteras.”

9 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Med regler för säkerhetsskyddet avses bl.a. säkerhetsskyddslagen, säkerhetsskyddsförordningen, Försvarsmaktens föreskrifter om säkerhetsskydd, Försvarsmaktens interna bestämmelser, lokala instruktioner och rutiner. Det är viktigt att kontrollen även innefattar interna bestämmelser och lokala instruktioner.

Om det vid en intern kontroll upptäcks brister i säkerhetsskyddet bör det av dokumentationen tydligt framgå: vilken regel som inte följs, vad bristen består av, behov

[230] Prop. 2017/18:89 s. 137.

av åtgärd som behöver vidtas, vem som är ansvarig för att vidta åtgärden samt när bristen ska vara åtgärdad. Uppföljning av brister beskrivs i avsnitt 9.5.

Resultatet från kontroller behöver fortlöpande utvärderas för att ge ingångsvärden till planering av kontroller.

En intern kontroll av säkerhetsskyddet kan genomföras som en föranmäld kontroll, vilket ska framgå av en plan, se 9 kap. 3 § nedan. Genom att utan förvarning, eller med kort förvarning, genomföra en kontroll av säkerhetsskyddet kan brister i säkerhetsskyddet identifieras som annars inte är möjligt genom en föranmäld kontroll. En säkerhetshotande händelse eller säkerhetshotande verksamhet som har rapporterats, kan föranleda en intern kontroll som inte föranmäls.

”Myndigheten ska ha en plan för kontroll av den egna verksamhetens säkerhetsskydd. En sådan plan ska i förekommande fall även omfatta sådan kontroll som framgår av 2 kap. 6 § andra stycket säkerhetsskyddslagen (2018:585). Planen ska uppdateras löpande och i planen ska det anges vem som är ansvarig för att kontroll och uppföljning genomförs.”

9 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: En plan ska fungera som ett stöd för den som är ansvarig för att leda och dokumentera interna kontroller i den egna verksamheten och av leverantörer. Planen ska fortlöpande göras aktuell mot bakgrund av bl.a. resultat från genomförda interna kontroller, säkerhetshotande händelser eller när en reviderad säkerhetsskyddsplanering resulterat i nya eller förändrade säkerhetsskyddskrav i säkerhetsskyddsplanen.

Den som har ingått ett säkerhetsskyddsavtal med en leverantör ska även kontrollera att leverantören följer säkerhetsskyddsavtalet. Se avsnitt 9.3 om kontroll av säkerhetsskydd vid säkerhetsskyddad upphandling.

9.2.1. Intern kontroll av säkerhetsskyddet vid organisationsenheter och enheter i Högkvarteret

Observera!
En *intern kontroll* är en kontroll av det egna säkerhetsskyddet som genomförs inom en organisationsenhet eller en enhet i Högkvarteret.

Enhet i Högkvarteret avser enheter som ska ha en säkerhetschef, dvs. ledningsstaben, produktionsledningen, insatsledningen respektive Must.

Moment 9:1 *Säkerhetschefen vid en organisationsenhet eller enhet i Högkvarteret ska leda interna kontroller av säkerhetsskyddet inom den egna verksamheten.*

Moment 9:2 *Vid en intern kontroll av säkerhetsskyddet ska rutiner prövas för hur incidenter och störningar i den säkerhetskänsliga verksamheten ska hanteras.*

9.2.2. Extern kontroll av säkerhetsskyddet vid organisationsenheter och enheter i Högkvarteret

Observera!
En *extern kontroll* av säkerhetsskyddet är en kontroll som utförs av någon utanför den kontrollerade organisationsenheten eller enheten i Högkvarteret.

”Chefen för militära underrättelse- och säkerhetstjänsten är Försvarsmaktens säkerhetsskyddschef och ska som sådan enligt 2 kap. 2 § säkerhetsskyddsförordningen (2018:658) kontrollera att Försvarsmaktens verksamhet bedrivs i enlighet med vad som föreskrivs i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen.

I uppgiften ingår även att kontrollera Försvarsmaktens informationssäkerhet och it-säkerhet som inte omfattas av säkerhetsskyddslagen.”

11 kap. 19 § första och andra styckena FM ArbO

Vägledande förklaring: Även författningar som meddelats med stöd i säkerhetsskyddsförordningen, t.ex. Försvarsmaktens föreskrifter om säkerhetsskydd, samt andra bestämmelser som reglerar säkerhetsskydd inom Försvarsmakten, t.ex. detta reglemente, ingår i en kontroll.

”Försvarsmaktens säkerhetsskyddschef ska leda och samordna säkerhetsskyddsarbetet vid myndigheten. I uppgiften ingår att:

3. utarbeta Försvarsmaktens plan för kontroll av säkerhetsskyddet enligt 9 kap. 3 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd,

4. årligen redovisa resultatet från kontroller av säkerhetsskyddet för överbefälhavaren och generaldirektören,

5. varje halvår redovisa resultatet från kontroller av säkerhetsskyddet för chefen för ledningsstaben, produktionschefen, insatschefen samt chefen för militära underrättelse- och säkerhetstjänsten,”

11 kap. 20 § 3-5 FM ArbO

”Insatschefen ska stödja Försvarsmaktens säkerhetsskyddschef i dennes kontroll av säkerhetsskyddet enligt 2 kap. 2 § säkerhetsskyddsförordningen (2018:658).”

10 kap. 7 a § FM ArbO

Vägledande förklaring: En extern kontroll av säkerhetsskyddet leds av säkerhetsskyddsavdelningen vid Must och underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2), samt regionalt av respektive militärregion. An-

svaret för att kontrollera respektive organisationsenhet regleras i Försvarsmaktens årliga plan för kontroller.

”Försvarsmaktens säkerhetsskyddschef beslutar

6. Försvarsmaktens årliga plan för kontroll av säkerhetsskyddet, ”

11 kap. 24 § 6 FM ArbO

Moment 9:3 *Säkerhetsskyddsavdelningen vid Must ska ta fram den årliga planen för extern kontroll av säkerhetsskyddet i Försvarsmakten. Planens innehåll ska samordnas med underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2).*

Moment 9:4 *Försvarsmaktens årliga plan för extern kontroll av säkerhetsskyddet ska upprättas i samverkan med den som ska kontrolleras.*

Moment 9:5 *Om det för en viss verksamhet har utsetts en säkerhetschef, en signalskyddschef eller en it-säkerhetschef ska den verksamheten kontrolleras. Vem som ska genomföra den externa kontrollen ska framgå av den reglering som beskriver verksamhetens säkerhetsorganisation och lydnadsförhållanden.*

Vägledande förklaring: Med viss verksamhet avses t.ex. en övning som involverar flera organisationsenheter eller ett internationellt deltagande. Det kan också vara ett projekt där nya informationssystem eller förmågor utvecklas och prövas.

9.3. Kontroll vid säkerhetsskyddad upphandling

”Statliga myndigheter, kommuner och landsting som avser att genomföra en upphandling och ingå ett avtal om varor, tjänster eller byggentreprenader ska se till att det i ett säkerhetsskyddsavtal anges hur kraven på säkerhetsskydd enligt 1 § ska tillgodoses av leverantören om

1. det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller

2. upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Verksamhetsutövaren ska kontrollera att leverantören följer säkerhetsskyddsavtalet.”

2 kap. 6 § första och andra styckena säkerhetsskyddslagen

”Av 2 kap. 6 § andra stycket säkerhetsskyddslagen (2018:585) framgår att en verksamhetsutövare ska kontrollera att en leverantör följer säkerhetsskyddsavtalet. En sådan kontroll ska genomföras regelbundet. Om säkerhetsskyddsavtalet avser kvalificerat hemliga uppgifter eller säkerhetskänslig verksamhet som är av synnerlig betydelse för Sverige säkerhet, ska kontrollen genomföras varje år.

Kontrollen ska dokumenteras.”

9 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

FM CIO, produktionschefen och chefen för Must ska kontrollera att en leverantör följer ett ingånget säkerhetsskyddsavtal som någon av dessa har tecknat. Resultat av dessa kontroller ska årligen redovisas för Försvarsmaktens säkerhetsskyddschef.[231]

Moment 9:6 *I de fall som den som är bemyndigad att teckna avtal för sin egen verksamhet har tecknat ett säkerhetsskyddsavtal är den även ansvarig för att säkerhetsskyddet hos leverantören kontrolleras.*

Moment 9:7 *Om ett säkerhetsskyddsavtal med en leverantör har tecknats av någon annan än organisationsenheten och det finns ett behov av att genomföra en kontroll av säkerhetsskyddet hos leverantören, ska behovet anmälas till den som har tecknat avtalet.*

Vägledande förklaring: Affärsavtal kan vara tecknade så att verksamheten berör flera verksamhetsansvariga inom Försvarsmakten som inte själva har ingått säkerhetsskyddsavtalet.

9.4. Protokoll

Moment 9:8 *Protokoll från interna kontroller av säkerhetsskyddet ska förvaras samlade hos den som har genomfört kontrollen.*

Moment 9:9 *Ett protokoll från en extern kontroll av säkerhetsskyddet ska inom tre månader vara den kontrollerade tillhanda, om inte annat är överenskommet. En kopia på protokollet ska även ställas till säkerhetsskyddsavdelningen vid Must, J2 vid INSS och den militärregionstab i den militärregion som organisationsenheten är placerad i.*

Moment 9:10 *Ett protokoll från en extern kontroll av säkerhetsskyddet ska minst omfatta:*

a) Behov av omedelbara säkerhetsskyddsåtgärder.

b) Brister i säkerhetsskyddet som ska åtgärdas med hänvisning till regelverk eller säkerhetsskyddsavtal.

[231] 8 kap. 40 a §, 9 kap. 6 a § och 11 kap. 16 § FM ArbO.

c) *Ansvaret för att vidta tvingande säkerhetsskyddsåtgärder (om det finns flera verksamhetsansvariga).*

d) *Datum när den kontrollerade ska uppvisa en åtgärdsplan som reglerar hur identifierade brister i säkerhetsskyddet ska omhändertas.*

Vägledande förklaring: Om en extern kontroll visar att en bestämmelse eller moment inte kan följas kan det vara nödvändigt att i protokollet beskriva att den kontrollerade ska begära ett undantag från bestämmelser (avsnitt 1.10.2) eller avvikelse från moment (avsnitt 1.10.4).

9.5. Uppföljning av brister

Moment 9:11 *Den som vid en kontroll av säkerhetsskyddet har brister i säkerhetsskyddet ska upprätta en åtgärdsplan. Planen ska redovisas för den som har genomfört kontrollen.*

Hur lång tid efter en kontroll som åtgärdsplanen senast ska överlämnas till den som genomfört kontrollen bör ske i en dialog. Om möjligt fastställs tidpunkten redan i samband med kontrolltillfället, och om det inte är möjligt regleras tidpunkt i protokollet.

Moment 9:12 *Den som genomfört en kontroll av säkerhetsskyddet ska även följa upp att brister åtgärdas enligt en upprättad åtgärdsplan. Uppföljningen genomförs på det sätt som den som har genomfört kontrollen bestämmer.*

Redovisning av åtgärdsplanen och uppföljning av planerade eller vidtagna säkerhetsskyddsåtgärder genomförs lämpligen vid ett och samma tillfälle.

För brister i säkerhetsskyddet, som inte är kritiska eller inte behöver redovisas, räcker det med att åtgärdsplanen sänds till den som har utfört kontrollen.

9.6. Försvarsmaktens tillsynsområde

”Tillsyn över säkerhetsskyddet ska utövas av

1. Försvarsmakten när det gäller Fortifikationsverket och Försvarshögskolan samt de myndigheter som hör till Försvarsdepartementet,

De myndigheter som anges i första stycket får inom sitt tillsynsområde utöva tillsyn över säkerhetsskyddet hos leverantörer som omfattas av ett säkerhetsskyddsavtal enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585). Sådan tillsyn får också utövas över underleverantörer som leverantören har anlitat inom ramen för säkerhetsskyddsavtalet.”

7 kap. 1 § första stycket 1 och andra stycket säkerhetsskyddsförordningen

Vägledande förklaring: Av bestämmelsen följer att Försvarsmakten utövar tillsyn över Försvarsmaktens säkerhetsskydd.

9.6.1. Försvarsmaktens tillsyn över enskilda verksamhetsutövare och leverantörer

”Säkerhetspolisen och Försvarsmakten får utöva tillsyn inom de ansvarsområden som anges i 1 § första stycket 3–6 och andra stycket. När sådan tillsyn har utövats ska den som har ansvar för tillsynen enligt 1 § underrättas.

Säkerhetspolisen och Försvarsmakten får även utöva tillsyn över leverantörer som har uppdrag för flera verksamhetsutövare om leverantörens samlade uppdrag är av stor betydelse för Sveriges säkerhet.”

7 kap. 2 § säkerhetsskyddsförordningen

Vägledande förklaring till första stycket: Försvarsmakten får utöva tillsyn över sådana enskildas säkerhetsskydd som Svenska kraftnät, Transportstyrelsen, Post- och telestyrelsen och länsstyrelserna ansvarar för. Försvarsmakten, får inom sitt tillsynsområde, även utöva tillsyn över säkerhetsskyddet hos leverantörer som omfattas av ett säkerhetsskyddsavtal enligt 2 kap. 6 § säkerhetsskyddslagen. Försvarsmakten får även utöva tillsyn hos underleverantörer som leverantören anlitat inom ramen för säkerhetsskyddsavtalet.

”Chefen för militära underrättelse- och säkerhetstjänsten bemyndigas att utöva tillsyn över säkerhetsskyddet vid myndigheter och leverantörer enligt 7 kap. 1 och 2 §§ säkerhetsskyddsförordningen (2018:658). I uppgiften ingår att:

3. vid utövande av tillsyn enligt 7 kap. 2 § säkerhetsskyddsförordningen underrätta ansvarig tillsynsmyndighet.”

11 kap. 17 § 3 FM ArbO

”Insatschefen ska stödja chefen för militära underrättelse- och säkerhetstjänsten vid dennes tillsyn av säkerhetsskyddet vid myndigheter, enskilda verk samhetsutövare och leverantörer enligt 7 kap. 1 och 2 §§ säkerhetsskyddsförordningen (2018:658).”

10 kap. 7 b § FM ArbO

”Produktionschefen ska stödja chefen för militära underrättelse- och säkerhetstjänsten vid dennes tillsyn av säkerhetsskyddet vid myndigheter, enskilda verksamhetsutövare och leverantörer enligt 7 kap. 1 och 2 §§ säkerhetsskyddsförordningen (2018:658).”

9 kap. 6 b § FM ArbO

9.6.2. Plan för Försvarsmaktens tillsyn

”Chefen för militära underrättelse- och säkerhetstjänsten bemyndigas att utöva tillsyn över säkerhetsskyddet vid myndigheter och leverantörer enligt 7 kap. 1 och 2 §§ säkerhetsskyddsförordningen (2018:658). I uppgiften ingår att:

5. besluta Försvarsmaktens årliga plan för tillsyn av säkerhetsskyddet enligt 7 kap. 1 och 2 §§ säkerhetsskyddsförordningen.”

11 kap. 17 § 5 FM ArbO

9.6.3. Tillgång till dokumentation vid Försvarsmaktens tillsyn

”När Försvarsmakten genomför tillsyn enligt 7 kap. 1 § första stycket 1 och andra stycket säkerhetsskyddsförordningen (2018:658) ska Försvarsmakten få tillgång till sådan dokumentation som krävs för att kunna utöva tillsyn över säkerhetsskyddet.”

9 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: För Försvarsmaktens tillsyn av myndigheter kan dokumentationen bl.a. vara (hänvisningar inom parentes avser, om inget annat anges, Försvarsmaktens föreskrifter om säkerhetsskydd.):

- Säkerhetsskyddsanalyser, säkerhetsskyddsplaner, signalskyddsinstruktion och andra styrdokument som rör myndighetens säkerhetsskydd såsom föreskrifter, interna bestämmelser, arbetsordning och delegationsordning.
- Rutiner för att upptäcka, bedöma och hantera incidenter och avvikelser samt fel eller brister (1 kap. 3 §).
- Behörighetsförteckning (3 kap. 1 §).
- Rutiner för ändring respektive borttagning av märkning av säkerhetsskyddsklass (3 kap. 9 §).
- Rutiner för kopiering av eller utdrag ur säkerhetsskyddsklassificerade handlingar (3 kap. 14 §).
- Rutiner för kvittering vid muntlig delgivning eller visning (3 kap. 17 §).
- Beslut om medförande (3 kap. 20 §).
- Rutiner för distribution internt och utom myndigheten (3 kap. 25 §).
- Godkända distributörer (3 kap. 25 §).
- Beslut om hur transporter ska genomföras (3 kap. 26 §).
- Särskilda säkerhetsskyddsbedömningar inför driftsättning av informationssystem (4 kap. 5 §).
- Granskningar och godkännanden av skyddsåtgärder för informationssystem (4 kap. 6 §).
- Godkännande av informationssystem från säkerhetsskyddssynpunkt (3 kap. 3 § säkerhetsskyddsförordningen).

REGLEMENTE

- Beslut om vilka rutiner, resurser och kompetenser för drift, förvaltning, underhåll, övervakning av informationssystem och hantering av incidenter (4 kap. 10 §).
- Beskrivningar av informationssystemen (4 kap. 11 §).
- Beslut om säkerhetskrav för skydd mot röjande signaler (4 kap. 25 §).
- Rutiner för tillträde (5 kap. 2 §).
- Utredning om behov av säkerhetsskydd för att säkerställa bevakningssystemens funktionalitet (5 kap. 5 §).
- Beslut om vilka skyddsåtgärder som ska vidtas vid larm (5 kap. 6 §).
- Förteckning över nycklar, kort och koder (5 kap. 10 §).
- Beslut om administrativa zoner och säkerhetszoner (5 kap. 13 §).
- Beslut om vilka utrymmen som är godkända för regelbunden muntlig delgivning (5 kap. 20 §).
- Analys av vilka anställningar och deltagande som ska placeras i säkerhetsklass, samt vilket övrigt deltagande som endast ska vara föremål för säkerhetsprövning (6 kap. 3 §).
- Förteckning över utbildning och övning i säkerhetsskydd (7 kap. 2 §).
- Analyser och planer för säkerhetsskyddad upphandling med säkerhetsskyddsavtal (8 kap. 1 §).
- Bedömningar av leverantörers lämplighet ur säkerhetsskyddssynpunkt (8 kap. 2 §).
- Särskilda säkerhetsskyddsbedömningar inför upphandling (2 kap. 6 § säkerhetsskyddsförordningen).
- Kontroller av att leverantörers lokaler och övriga förhållanden är lämpliga ur säkerhetsskyddssynpunkt (8 kap. 8 §).
- Kontroller av myndighetens säkerhetsskydd (9 kap. 1 §).
- Kontroller av att leverantörer följer säkerhetsskyddsavtal (9 kap. 2 §).
- Plan för kontroll av den egna verksamhetens säkerhetsskydd (9 kap. 3 §).
- Beslut om undantag (12 kap. 1 §).

”Sekretess hindrar inte att en uppgift lämnas till en myndighet, om uppgiften behövs där för tillsyn över eller revision hos den myndighet där uppgiften förekommer.”

10 kap. 17 § OSL

”Den som med stöd av denna författning har fått mandat att genomföra tillsyn ska få de uppgifter som krävs för tillsynen, samt omedelbart få tillträde till de områden, byggnader och andra anläggningar eller objekt, ledningsstödsystem och transportmedel som är nödvändiga för att kunna genomföra tillsynen.”

4 kap. 13 § FM ArbO

Vägledande förklaring: Bestämmelsen är tillämplig när chefen för Must utövar tillsyn över Försvarsmaktens säkerhetsskydd.

9.6.4. Information till Regeringskansliet

Se även avsnitt 10.5 om anmälan till regeringen.

”Chefen för militära underrättelse- och säkerhetstjänsten bemyndigas att utöva tillsyn över säkerhetsskyddet vid myndigheter och leverantörer enligt 7 kap. 1 och 2 §§ säkerhetsskyddsförordningen (2018:658). I uppgiften ingår att:

4. på förfrågan informera Regeringskansliet i frågor som rör Försvarsmaktens tillsyn.”

11 kap. 17 § 4 FM ArbO

10. Säkerhetsrapportering

10.1. Allmänt om säkerhetsrapportering

”Verksamhetsutövaren ska även kontrollera säkerhetsskyddet i den egna verksamheten, anmäla och rapportera sådant som är av vikt för säkerhetsskyddet och i övrigt vidta de åtgärder som krävs enligt denna lag.”

2 kap. 1 § tredje stycket säkerhetsskyddslagen

Vägledande förklaring: För att tillsynsmyndigheterna ska kunna utöva sin tillsyn på ett effektivt sätt och för att utfärdade tillämpningsföreskrifter ska bli så ändamålsenliga som möjligt är det av stor vikt att de får kännedom om händelser och företeelser som är av betydelse för säkerhetsskyddet.[232]

”En verksamhetsutövare ska skyndsamt anmäla till Säkerhetspolisen om

1. en säkerhetsskyddsklassificerad uppgift kan ha röjts,

2. det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller

3. verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.

Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1, ska anmälan göras också till Försvarsmakten.”

2 kap. 10 § säkerhetsskyddsförordning (2018:658)

Vägledande förklaring: Myndigheter som hör till Försvarsmaktens tillsynsområde ska enligt bestämmelsen anmäla till både Säkerhetspolisen och Försvarsmakten. Eftersom Försvarsmakten hör till Försvarsmaktens tillsynsområde[233] ska även Försvarsmakten anmäla till Säkerhetspolisen. Försvarsmaktens anmälan till Säkerhetspolisen beskrivs i avsnitt 10.3.

”Sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse för Sveriges säkerhet ska snarast åtgärdas och anmälas till Försvarsmaktens högkvarter.”

10 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Skälet till att information avseende fel och brister i säkerhetsskyddet behövs är för att t.ex. följa upp bristerna vid den aktuella verksamheten

[232] SOU 2015:25 s. 495.
[233] 7 kap. 1 § första stycket 1 säkerhetsskyddsförordningen.

eller för att vidta andra åtgärder. Om bristerna gäller verksamhet som omfattas av ett internationellt säkerhetsskyddsåtagande (t.ex. ett generellt säkerhetsskyddsavtal, GSA) är det av ännu större vikt att bristerna rapporteras, eftersom Försvarsmakten i många fall i avtalen är utpekad att vara nationell säkerhetsmyndighet. Som nationell säkerhetsmyndighet ansvarar Försvarsmakten för att informera den andra parten om händelsen.

Med ringa betydelse för Sveriges säkerhet avses bl.a. att konsekvenserna är begränsade till att endast i mindre omfattning påverka, försvåra, hindra, undergräva, misskreditera eller störa verksamheten för de särskilda skyddsintressen som omfattas av säkerhetsskyddslagen.

Observera!
Såväl säkerhetshotande händelser och verksamhet som fel och brister i säkerhetsskyddet ska rapporteras skyndsamt.

”Av en anmälan ska det framgå typ av händelse, tidpunkt och plats för det inträffade, vilka sårbarheter och brister som har identifierats samt vilken säkerhetskänslig verksamhet som har berörts.”

10 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

10.2. Säkerhetsrapportering i Försvarsmakten

Den militära säkerhetstjänstens uppgift är att skydda de säkerhetsintressen som berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen.[234]

En förutsättning för att Försvarsmakten ska kunna lösa uppgiften är att hotbilden mot säkerhetsintressena är klarlagd samt att Försvarsmaktens sårbarheter är identifierade. Således behöver såväl säkerhetshotande verksamhet som sårbarheter rapporteras till den militära säkerhetstjänsten. Säkerhetsrapportering är därför en viktig del i arbetet med att skydda Försvarsmaktens säkerhetsintressen.

”Försvarsmaktens säkerhetsskyddschef får besluta närmare bestämmelser om säkerhetsrapportering.”

8 kap. 1 § tredje stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Bemyndigandet får inte delegeras.

[234] Regleringsbrev för budgetåret 2020 avseende Försvarsmakten, bilaga 4.

Vägledande förklaring: Bestämmelserna kan t.ex. handla om vilka uppgifter som ska ingå i en rapport eller vilka mottagare som ska delges en rapport. Bestämmelserna kan även handla om rapportering i säkerhetskänslig verksamhet där insynen särskilt behöver begränsas.

10.2.1. Säkerhetshotande händelser och verksamhet samt fel och brister i säkerhetsskyddet

”Var och en som får kännedom om säkerhetshotande händelser eller verksamhet eller misstänker sådan händelse eller verksamhet ska snarast rapportera förhållandet till organisationsenhetens säkerhetsorganisation eller närmaste chef. Detsamma gäller om fel eller brister i säkerhetsskyddet upptäcks.”

8 kap. 1 § första stycket
Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Bestämmelsen reglerar skyldigheten för alla i Försvarsmakten att rapportera *säkerhetshotande händelser eller verksamhet eller misstanke om sådan händelse eller verksamhet*. Kännedom om säkerhetshotande verksamhet är en väsentlig förutsättning för att kunna ta fram en korrekt och aktuell hotbeskrivning, ge råd och stöd till verksamheter och genomföra kontroll. Det är därför angeläget att den militära säkerhetstjänsten får information om säkerhetshotande händelser och verksamhet.

Inom Försvarsmakten rapporteras även säkerhetshotande händelser och verksamhet som inte bedöms som allvarliga. Detta eftersom det kan vara svårt för enskild organisationsenhet eller individ att avgöra huruvida en händelse är allvarlig eller inte.

En händelse är något som är avgränsat till tid och rum medan en verksamhet kan pågå över tiden på flera geografiska platser samtidigt. Vad som är vad har egentligen ingen praktisk betydelse för rapportering – säkerhetshotande verksamhet och händelser rapporteras på samma sätt till samma mottagare enligt avsnitt 10.2.6.

Exempel på händelser som ska rapporteras är:

- en säkerhetsskyddsklassificerad uppgift kan ha röjts eller
- när en säkerhetsskyddsklassificerad handling, en tryckt skrift, ett lagringsmedium eller materiel trots eftersökning inte kan återfinnas vid inventering (avsnitt 3.13.1).

Förutom säkerhetshotande händelser och verksamhet ska även *fel och brister i säkerhetsskyddet* rapporteras. Anmälan görs i form av en säkerhetsrapport inom Försvarsmakten. Med fel och brister avses t.ex. avsaknad av beslutade säkerhetsskyddsåtgärder, tekniska system som inte fungerar och som därmed påverkar säkerhetsskyddet, säkerhetsrutiner som inte fungerar eller inte tillämpas eller logiska fel i genomförd säkerhetsskyddsanalys. Den militära säkerhetstjänsten behöver information avseende fel och brister i säkerhetsskyddet för att t.ex. följa upp bristerna vid den aktuella

verksamheten eller för att vidta andra åtgärder. Fel och brister utgör sårbarheter som behöver omhändertas.

Moment 10:1 *När säkerhetsorganisationen vid en organisationsenhet har tagit emot en säkerhetsrapport ska rapporten lämnas till militärregionstaben i den militärregion som organisationsenheten är placerad i. Militärregionstaben ansvarar för att åtgärder vidtas. Militärregionstaben ska se till att säkerhetsrapporten vidarebefordras till:*

a) insatsledningen i Högkvarteret, och

b) säkerhetskontoret vid Must.

Vägledande förklaring: En del av militärregionens ansvar är att se till att säkerhetsrapporten är korrekt ifylld samt att rapporten delges de som behöver den genom att lägga på rätt läsbehörigheter i IS UNDSÄK.

Moment 10:2 *När säkerhetsorganisationen vid en kontingent i en internationell militär insats har tagit emot en säkerhetsrapport ska rapporten lämnas till den försvarsgrensstab som ansvarar för kontingenten. Försvarsgrensstaben ska se till att säkerhetsrapporten vidarebefordras till:*

a) insatsledningen i Högkvarteret, och

b) *säkerhetskontoret vid Must.*

Vägledande förklaring: Alla nivåer i Försvarsmaktens säkerhetsorganisation behöver ta del av säkerhetsrapporter om säkerhetshotande händelser eller verksamhet vid en organisationsenhet.

Oavsett i vilken verksamhet eller vilket förband som den säkerhetshotande händelsen eller verksamheten upptäcktes i eller berör ska en säkerhetsrapport alltid delges säkerhetskontoret vid Must.

10.2.1.1 Rapportering som rör organisationsenhetens säkerhetsorganisation

> *”Försvarsmaktens säkerhetsskyddschef får besluta att en säkerhetsrapport som rör organisationsenhetens säkerhetsorganisation ska rapporteras på annat sätt.”*
>
> 8 kap. 1 § andra stycket
> Försvarsmaktens interna bestämmelser om säkerhetsskydd

Moment 10:3 *En säkerhetsrapport som rör organisationsenhetens säkerhetsorganisation ska lämnas direkt till staben för den militärregion som organisationsenheten är placerad i. Militärregionstaben ska vidarebefordra rapporten till insatsledningen i Högkvarteret och säkerhetskontoret vid Must.*

Vägledande förklaring: Syftet är att den enskilde som upptäcker eller misstänker en säkerhetshotande händelse eller verksamhet som rör den egna organisationsenhetens säkerhetsorganisation endast ska rapportera detta till militärregionstaben.

Moment 10:4 *En säkerhetsrapport som rör säkerhetsorganisationen vid en militärregionstab ska endast lämnas till insatsledningen i Högkvarteret. Insatsledningen ska vidarebefordra rapporten till säkerhetskontoret vid Must.*

Moment 10:5 *En säkerhetsrapport som rör säkerhetsorganisationen vid FMTIS stab, Högkvarteret eller SOG ska endast lämnas till säkerhetskontoret vid Must.*

10.2.2. It-säkerhetsrapportering

”Händelser som kan påverka säkerheten negativt i och kring Försvarsmaktens it-system ska omedelbart rapporteras till lokal säkerhetsorganisation eller närmaste chef.

Den som har tagit emot en sådan it-säkerhetsrapport ska se till att den vidarebefordras till:

- den regionala stab som den rapporterande organisationsenheten tillhör,
- it-säkerhetsansvarig för aktuellt it-system,
- it-försvarsförbandet vid Försvarsmaktens telekommunikations- och informationssystemförband,
- ledningsstaben i Högkvarteret,
- produktionsledningen i Högkvarteret,
- insatsledningen i Högkvarteret, och
- den militära underrättelse- och säkerhetstjänsten i Högkvarteret.”

2 kap. 1 § Försvarsmaktens interna bestämmelser om it-säkerhet

Vägledande förklaring: Rapporteringsbestämmelser för it-säkerhetsrelaterade händelser regleras även inom försvarsplaneringen genom ÖB beredskapsorder (FMO Beredskap) och dess underliggande orderverk som t.ex. stående order för nationella operationer (SOFO NAT). Därutöver regleras it-verksamheten särskilt genom bl.a. direktiv och processbeskrivningar.

Andra myndigheters rapportering av it-incidenter till Försvarsmakten beskrivs i avsnitt 10.4.

Observera!
Skyndsam rapportering av it-säkerhetsincidenter är nödvändigt för att snabbt kunna identifiera och avbryta skadlig verksamhet i Försvarsmaktens informationssystem. Sådan rapportering fyller därför flera behov och omfattas av ytterligare regleringar och styrningar utöver Försvarsmaktens föreskrifter som säkerhetsskydd.

10.2.3. Signalskyddsincident

Signalskyddsincident avser:[235]

- När en signalskyddsnyckel saknas eller har, eller kan antas ha, kommit till obehörigs kännedom (*nyckelincident*).
- När signalskyddsmateriel saknas eller kan antas ha manipulerats eller utsatts för annan åverkan (*materielincident*).
- När ett aktivt kort eller lagringsmedium för mjukt certifikat saknas, kan antas ha manipulerats eller att obehörig kan antas ha haft tillgång till kortet eller det mjuka certifikatet (*incident med aktivt kort eller certifikat*).

> *”Vid en inträffad nyckelincident ska anmälan omedelbart göras till en nyckelansvarig verksamhetsutövare och egen signalskydds- samt säkerhetsskyddsorganisation.”*
>
> 2 kap. 25 § första stycket Försvarsmaktens föreskrifter om signalskyddstjänsten

> *”Den som har förlorat eller inte kan återfinna signalskyddsmateriel, eller misstänker manipulation av eller åverkan på signalskyddsmateriel eller dess försegling, ska omedelbart anmäla detta. Anmälan ska göras till en verksamhetsutövares eller enhets signalskydds- samt säkerhetsskyddsorganisation och till den som tilldelat materielen samt till Försvarsmaktens högkvarter.”*
>
> 3 kap. 17 § första stycket Försvarsmaktens föreskrifter om signalskyddstjänsten

> *”Den som har förlorat eller inte kan återfinna ett aktivt kort eller mjukt certifikat, eller misstänker manipulation av aktivt kort eller mjukt certifikat, ska omedelbart anmäla detta. Anmälan ska göras till en verksamhetsutövares eller enhets signalskydds- samt säkerhetsskyddsorganisation och till den som tilldelat det aktiva kortet eller mjuka certifikatet, samt till Försvarsmaktens högkvarter.”*
>
> 4 kap. 16 § första stycket Försvarsmaktens föreskrifter om signalskyddstjänsten

Vägledande förklaring: En incident kan komma att negativt påverka säkerhetskänslig verksamhet. Det är därför av betydelse att incidenten anmäls till säkerhetsskyddsorganisationen.

[235] 1 kap. 3 § Försvarsmaktens föreskrifter om signalskyddstjänsten.

10.2.4. Exponering av skyddsvärden

”Varje organisationsenhet ska ha rutiner för att identifiera och rapportera säkerhetskänslig verksamhet eller annan verksamhet av betydelse för Försvarsmakten där myndighetens skyddsvärden kan komma att exponeras.”

8 kap. 3 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Rutiner för att identifiera och rapportera verksamhet behöver inte finnas förrän den 1 februari 2021.[236] Det hindrar inte att rutiner tas fram före den dagen.

Vägledande förklaring: Rutinerna behöver anpassas efter de lokala förutsättningar och vilken verksamhet som genomförs vid enheten. Exempel på verksamhet som ska rapporteras är prov och försök med ett nytt robotsystem eller en övning där skyddsvärden exponeras. Sådan verksamhet kan också ställa krav på anpassade säkerhetsskyddsåtgärder (avsnitt 2.3.4).

Rapportering av exponering av skyddsvärden skapar förutsättningar för att kunna förvarna om en känd säkerhetshotande verksamhet kan påverka det skyddsvärda som exponeras. Ett exempel är om en främmande makts signalspaningsflygplan kommer inom räckvidd för det exponerade skyddsvärdet.

Rapporteringen syftar även till att i efterhand bättre kunna förstå den säkerhetshotande verksamheten och aktörer som bedriver den. Jämförelser görs mellan observationer av säkerhetshotande verksamhet och med den egna skyddsvärda verksamheten.

”En organisationsenhet ska rapportera förekomst av säkerhetskänslig verksamhet eller annan verksamhet av betydelse för Försvarsmakten där myndighetens skyddsvärden kan komma att exponeras.

Försvarsmaktens säkerhetsskyddschef får besluta närmare bestämmelser om sådan rapportering.”

8 kap. 4 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Bestämmelsen reglerar rapportering av det som tidigare benämndes *skyddsvärd verksamhet*. Sådan rapportering genomförs i dag enligt insatschefens stående order för nationella operationer (C INSATS SOFO NAT).

Försvarsmaktens säkerhetsskyddschef bemyndigas att besluta närmare bestämmelser om rapportering, t.ex. för säkerhetskänslig verksamhet där insynen särskilt behöver begränsas. Bemyndigandet får inte delegeras.

[236] Punkten 5 i ikraftträdande- och övergångsbestämmelser till Försvarsmaktens interna bestämmelser om säkerhetsskydd.

10.2.5. Säkerhetsrapportering i personärende

I avsnitt 6.4 beskrivs säkerhetsrapportering i personärende, dvs. rapportering av uppgifter som kan komma att påverka en bedömning av en persons pålitlighet, lojalitet eller sårbarhet i säkerhetshänseende.

10.2.6. Säkerhetsrapportens innehåll och delgivning

En säkerhetsrapport består av två delar där rapportören svarar för den första delen, medan säkerhetsorganisationen svarar för den andra delen. Den första delen består av en beskrivning av den observerade händelsen med tillhörande kommentarer.

Tips!
Använd minnesregeln 7S när du beskriver händelsen i en säkerhetsrapport!

Beskrivningen enligt 7S omfattar:

1) **Stund** (tidpunkt, datum och klockslag för händelsen).
2) **Ställe** (plats för iakttagelse).
3) **Styrka** (antal inblandade eller iakttagna objekt).
4) **Slag** (typ av objekt).
5) **Sysselsättning** (objektets verksamhet, beskrivning av händelseförloppet).
6) **Symbol** (observerade kännetecken eller andra detaljer som kan vara behjälpliga för identifikation).
7) **Sagesman** (källa när upphovet är någon annan än de som upprättat rapporten).

Tips!
Tänk på att rapporten ska förstås av läsaren, även om denne saknar lokalkännedom eller inte har djup fackkompetens om det som har rapporterats. Undvik därför lokala benämningar eller fackuttryck, alternativt förklara dessa. Det ska tydligt framgå av rapporten varför den skrevs, det vill säga vad det var som gjorde att du bedömde det observerade som intressant att rapportera.

Vid rapportering av fel och brister i säkerhetsskyddet är inte alla rubriker alltid tillämpbara. Rubrikerna enligt 7S ska ses som en minnesregel för att säkerställa att samtlig relevant information är med.

Komplettera rapporten med uppgifter om eventuella vidtagna åtgärder som t.ex. genomförd avspärrning eller att ett visst system tillfälligt tagits ur drift. Minnesordet för detta är *sedan*. Dessutom antecknas uppgifter som underlättar värderingen av rappor-

ten, som under vilka förhållanden (t.ex. rådande siktförhållanden) observationen gjordes.

Den andra delen av säkerhetsrapporten som säkerhetsorganisationen (t.ex. organisationsenhetens säkerhetschef) ansvarar för kompletterar rapporten med information om:

- vilken säkerhetskänslig verksamhet som har drabbats,
- vilka sårbarheter och brister som har identifierats,
- vilka konsekvenser det inträffade har fått, samt
- eventuella vidtagna åtgärder.

Observera!
Skilj mellan den observerade händelsen och bedömningar eller antaganden.

För att skapa förutsättningar för bearbetning av en säkerhetsrapport är det viktigt att det i rapporten tydligt framgår vad som är en observation (händelse eller verksamhet) och vad som är en bedömning eller ett antagande.

Kompletterande information som t.ex. bakgrundsinformation som behövs för att sätta informationen i sitt rätta sammanhang anges som kommentarer. Innebörd och de slutsatser som kan dras av det som har rapporterats anges som en bedömning. För bedömningar används konfidensgrader som beskrivs i avsnitt 1.6.1.

Säkerhetsrapportering ska ske skyndsamt för att möjliggöra att adekvata åtgärder vidtas innan skyddsvärdena påverkas negativt.

Om det inte är möjligt att rapportera i IS UNDSÄK måste säkerhetsrapporten överföras på något annat säkert sätt till en annan enhet så att säkerhetsrapporten kan skrivas in i IS UNDSÄK.

Om en initial säkerhetsrapport ska skickas för att uppmärksamma en händelse måste rapporten kompletteras senare.

För att snabbt nå ut till den militära säkerhetstjänsten på lokal, regional och central nivå görs säkerhetsrapporter normalt tillgängliga för alla samtidigt. Rapporteringsbestämmelser (t.ex. rapportformat och rapporteringsvägar) beskrivs i bl.a. stående order för nationella operationer (SOFO NAT) och stående order för internationella insatser (SOFI INT).

Mottagare av en säkerhetsrapport bör eftersträva att återkoppla till rapportören för att tydliggöra att rapporten är mottagen. Återkopplingen bör om möjligt beskriva vad rapporten resulterade i.

10.2.7. Diarieföring av säkerhetsrapporter

Moment 10:6 *En säkerhetsrapport, förutom säkerhetsrapport i personärende enligt 8 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd, ska diarieföras i underrättelse- och säkerhetsdiariet vid Must.*

Vägledande förklaring: En säkerhetsrapport som hanteras inom Försvarsmakten är en allmän handling när den har nått sin slutliga form.[237] Säkerhetsrapporter innehåller normalt uppgifter som omfattas av sekretess (t.ex. 15 kap. 2 §, 18 kap. 8 § eller 35 kap. 1 § 3 OSL) och ska därför diarieföras.[238] En säkerhetsrapport är en underrättelse inom försvarets underrättelse- och säkerhetstjänst[239] och ska därför diarieföras i ett register som är skilt från VIDAR. Register som är undantagna allmänhetens insyn beskrivs i avsnitt 3.8.3. Must har tagit fram en rutin för diarieföring av säkerhetsrapporter. Momentet gäller även för säkerhetsrapporter med begränsad delgivning.

Tips!
Rutin för diarieföring finns i IS UNDSÄK i handlingen:
201110 HKV MUST RUTIN DIARIEFÖRING SÄKR

Säkerhetsrapportering i personärende beskrivs i avsnitt 6.4. Hantering av allmänna handlingar inom säkerhetsprövning beskrivs i avsnitt 6.16.10.

10.3. Försvarsmaktens anmälan till Säkerhetspolisen

”Försvarsmaktens säkerhetsskyddschef, eller den säkerhetsskyddschefen bestämmer, ska anmäla säkerhetshotande händelser och verksamhet enligt vad som föreskrivs i 2 kap. 10 § säkerhetsskyddsförordningen (2018:658).”

8 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd

Vägledande förklaring: Av 2 kap. 10 § säkerhetsskyddsförordningen följer att en anmälan ska göras om:

- en säkerhetsskyddsklassificerad uppgift kan ha röjts,
- det har inträffat en it-incident i ett informationssystem som Försvarsmakten är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller
- Försvarsmakten får kännedom eller misstanke om någon annan för Försvarsmakten allvarlig säkerhetshotande verksamhet.

[237] 2 kap. 10 § tryckfrihetsförordningen.
[238] 5 kap. 1 § första och tredje styckena OSL.
[239] 3 § OSF.

Stöd för att bedöma om en säkerhetsskyddsklassificerad uppgift kan ha röjts samt ta fram underlag som ska lämnas till Säkerhetspolisen finns i Handbok Försvarsmaktens säkerhetstjänst Menbedömning (H SÄK MEN 2017).

10.4. Andra myndigheters anmälan till Försvarsmakten

”En verksamhetsutövare ska skyndsamt anmäla till Säkerhetspolisen om

1. en säkerhetsskyddsklassificerad uppgift kan ha röjts,

2. det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller

3. verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.

Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1, ska anmälan göras också till Försvarsmakten.”

2 kap. 10 § säkerhetsskyddsförordning (2018:658)

Vägledande förklaring: Av bestämmelsen följer att myndigheter inom Försvarsmaktens tillsynsområde ska genomföra anmälan till både Säkerhetspolisen och Försvarsmakten.

”Vid tveksamhet om en säkerhetshotande verksamhet är allvarlig enligt 2 kap. 10 § första stycket 3 säkerhetsskyddsförordningen ska myndigheten samverka med Försvarsmaktens högkvarter.”

10 kap. 1 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Kännedom om säkerhetshotande verksamhet är en väsentlig förutsättning för att kunna ta fram en korrekt och aktuell hotbeskrivning och även i övrigt ge råd och stöd till enskilda verksamheter samt utföra tillsyn på ett ändamålsenligt sätt. Det är därför angeläget att de myndigheter som utför tillsyn får information om säkerhetshotande händelser och verksamhet inom sitt tillsynsområde.

Därför ska den myndighet som får kännedom om säkerhetshotande verksamhet eller misstänker sådan verksamhet anmäla förhållandet till Försvarsmakten.

För att en rapporteringsskyldighet ska vara ändamålsenlig och inte mer betungande än nödvändigt behöver den innehålla en kvalificeringsregel. Skyldigheten är därför begränsad till säkerhetshotande verksamhet av *allvarlig* karaktär. Exempel på säkerhetshotande verksamhet som är av allvarlig karaktär är sådan där angreppen är av kvalificerad art eller som tyder på en systematisk och målinriktad strategi från en aktör. Vidare torde angrepp som samtidigt riktas mot flera verksamheter inom en samhällssektor ofta anses vara allvarliga. Nya och tidigare okända angreppssätt och metoder är exempel på när en säkerhetshotande verksamhet är allvarlig. Säkerhetsho-

tande verksamhet av mindre betydelse som t.ex. överträdelser mot tillträdesförbud eller smärre it-incidenter ger i regel inte Försvarsmakten sådan information som kan motivera en rapporteringsskyldighet. Skyndsamhetskrav i säkerhetsskyddsförordningen finns för att säkerställa att Försvarsmakten ska kunna ge stöd i fråga om säkerhetsskyddsåtgärder i ett tidigt skede i syfte att minska effekter och spridning av den säkerhetshotande verksamheten.[240]

”Sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse för Sveriges säkerhet ska snarast åtgärdas och anmälas till Försvarsmaktens högkvarter.”

10 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: Skälet till att Försvarsmakten kan behöva information avseende fel och brister i säkerhetsskyddet är för att t.ex. följa upp bristerna vid den aktuella verksamheten eller för att vidta andra åtgärder. Om bristerna gäller verksamhet som omfattas av ett internationellt säkerhetsskyddsåtagande (t.ex. ett generellt säkerhetsskyddsavtal, GSA) är det av ännu större vikt att bristerna rapporteras, eftersom Försvarsmakten i många fall är utpekad att fullgöra uppgiften som nationell säkerhetsmyndighet. Som nationell säkerhetsmyndighet ansvarar Försvarsmakten för att informera den andra parten om händelsen.

Med ringa betydelse för Sveriges säkerhet avses bl.a. att eventuella konsekvenser är begränsade till att endast i mindre omfattning påverka, försvåra, hindra, undergräva, eller störa verksamheten för de intressen som skyddas genom säkerhetsskyddslagen.

”Chefen för militära underrättelse- och säkerhetstjänsten bemyndigas att utöva tillsyn över säkerhetsskyddet vid myndigheter och leverantörer enligt 7 kap. 1 och 2 §§ säkerhetsskyddsförordningen (2018:658). I uppgiften ingår att:

1. bereda anmälningar från andra myndigheter om säkerhetshotande händelser och verksamhet enligt vad som föreskrivs i 2 kap. 10 § säkerhetsskyddsförordningen (2018:658),

2. bereda anmälningar från andra myndigheter om fel och brister i säkerhetsskyddet enligt vad som föreskrivs i 10 kap. 2 § Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd,”

11 kap. 17 § 1 och 2 FM ArbO

Vägledande förklaring: Must har tagit fram en rutin för andra myndigheters it-incidentrapportering till Försvarsmakten.[241]

[240] SOU 2015:25 s. 497-498.
[241] Rutin för it-incidentrapportering till Försvarsmakten (FM2016-20774:1).

10.5. Försvarsmaktens anmälningar till regeringen

”Om det vid tillsynen över säkerhetsskyddet konstateras allvarliga brister som trots påpekanden inte rättas till, ska Säkerhetspolisen eller Försvarsmakten anmäla förhållandet till regeringen. Det gäller dock inte brister hos sådana leverantörer där villkoren för säkerhetsskyddet angetts i ett säkerhetsskyddsavtal.”

7 kap. 3 § första stycket säkerhetsskyddsförordningen

”Chefen för militära underrättelse- och säkerhetstjänsten bemyndigas att anmäla brister i säkerhetsskyddet till regeringen enligt 7 kap. 3 § säkerhetsskyddsförordningen.”

11 kap. 18 § 2 FM ArbO

11. Incidenter och avvikelser

”Myndigheten ska ha rutiner för att upptäcka, bedöma och hantera incidenter och avvikelser som rör säkerhetskänslig verksamhet samt sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse. Rutinerna ska dokumenteras.”

1 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vägledande förklaring: En incident kan t.ex. vara ett brott som innebär konsekvenser för Sveriges säkerhet även om det inte var brottets primära syfte. En stöld av t.ex. datorer i ett luftövervakningssystem kan ge konsekvenser för Sveriges säkerhet, även om detta inte varit brottets primära syfte.[242] Ett fel kan t.ex. vara när någon upptäcker ett hål i ett stängsel till ett skyddsobjekt. Försvarsmakten behöver därför rutiner för att kunna upptäcka, bedöma och hantera sådana situationer.

Rutiner bör t.ex. tas fram för vilka åtgärder som ska vidtas vid upptäckt att ett säkerhetsskåp som innehåller säkerhetsskyddsklassificerade uppgifter står olåst eller när ett okänt USB-minne påträffas i en dator. Förebyggande rutiner kan t.ex. vara regelbundna administrativa och tekniska kontroller såsom manuella kontroller av arbetsstationer som används i ett informationssystem. De tekniska kontrollerna kan göras automatiserade genom t.ex. automatisk upptäckt och frånkoppling av icke auktoriserade enheter (s.k. eng. DUD – disable unauthorized device).

Bestämmelsen innefattar även incidenthantering för it-incidenter i informationssystem som används i säkerhetskänslig verksamhet. Incidenthanteringen innebär både att vidta sådana åtgärder som omedelbart behövs för att den säkerhetskänsliga verksamheten ska kunna bedrivas och säkerhetsskyddet upprätthållas, men också att ta reda på orsakerna till incidenten eller avvikelsen och om möjligt vidta åtgärder för att undvika att den upprepas. En förutsättning för att kunna hantera it-säkerhetsincidenter är att de upptäcks och skyndsamt rapporteras till den eller de verksamheter som har till uppgift att möta och avvärja hotet. I Försvarsmakten finns bestämmelser om rapportering av it-incidenter (avsnitt 10.2.2).

[242] Prop. 2017/18:89 s. 50.

Begreppsförklaringar

I den här publikationen används nedanstående begrepp som inte definieras i den löpande texten.

Begrepp	Innebörd
Aktör	En organisation, gruppering eller person som bedöms kunna påverka operationsmiljön.
Aktörsdrivet hot	Hot som kommer från en aktör. Benämns även antagonistiskt hot.
Befattning	Avses i säkerhetsprövningssammanhang anställningar samt annat deltagande i Försvarsmaktens säkerhetskänsliga verksamhet.
Kryptografiska funktioner som är avsedda för att skydda säkerhetskänslig verksamhet	Signalskyddstjänst
Modus operandi	En aktörs tillvägagångssätt för viss verksamhet. Används såväl för att ange en konkret metod som en strategi.
Prop.	Proposition
Påverkansoperation	Samordnad och ofta förnekbar verksamhet som initieras av en statsaktör och som har som målsättning att påverka beslut, uppfattningar och beteenden hos en statsledning, befolkning eller särskilt utpekade målgrupper i syfte att främja egna säkerhetspolitiska mål. Bedrivs huvudsakligen genom spridande av vilseledande eller oriktig information kompletterad med annat för ändamålet särskilt anpassat agerande.
SOU	Statens offentliga utredningar
Säkerhetshot	Med säkerhetshot avses aktörsdrivna hot, dvs. hot från en eller flera aktörer i form av individer, grupper, nätverk, organisationer eller stater.
ÖB	Överbefälhavaren

Bilaga 1 – Momentsamling

Bilagan innehåller samtliga moment i reglementet. Momentsamlingen innehåller inte andra bestämmelser, t.ex. i Försvarsmaktens interna bestämmelser om säkerhetsskydd. Enbart momentsamlingen kan därför inte användas som stöd i utbildning eller kontroll. Om ett moment i momentsamlingen avviker från momentet i kapitel 1-11, har momentet i kapitlet företräde.

Kapitel 1 – Militär säkerhetstjänst

Moment 1:1 *Följande hotnivåer för säkerhetshotande verksamhet ska användas.* s. 21

Momentet innehåller en tabell som inte återges här.

Moment 1:2 *I en hotbedömning av säkerhetshot ska hotkomponenterna intention, kapacitet och tillfälle analyseras.* s. 22

Moment 1:3 *Följande konfidensgrader ska användas för att uttrycka säkerheten i en hotbedömningen avseende säkerhetshot.* s. 22

Momentet innehåller en tabell som inte återges här.

Moment 1:4 *I en begäran om undantag från en bestämmelse i författning eller reglemente ska det i begäran anges:* s. 38

a) Vilken bestämmelse som undantaget rör.

b) Vad anledningen är till varför bestämmelsen inte går att följa.

c) En bedömning av konsekvenser för verksamheten om ett undantag inte medges.

d) En bedömning av sårbarheter till följd av att bestämmelsen inte kan följas.

e) En bedömning om risken för Sveriges säkerhet är acceptabel.

f) När bestämmelsen bedöms vara uppfylld, eller om den inte går att uppfylla.

Moment 1:5 *Samråd och underrättelse enligt 1 kap. 9 § andra stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd ska ske med säkerhetsskyddsavdelningen vid Must.* s. 39

Moment 1:6 *Insatschefen får, i fråga om verksamhet som syftar till hävdande av Sveriges suveränitet och territoriella integritet, fatta beslut som avviker från moment i detta reglemente, om det är oundgängligen nödvändigt för verksamheten.* s. 39

Ett sådant beslut ska dokumenteras och, om möjligt, föregås av samråd med säkerhetsskyddsavdelningen vid Must. Har sådant samråd inte skett ska säkerhetsskyddsavdelningen vid Must snarast underrättas om beslutet.

Kapitel 2 – Analys och planering

Moment 2:1 *Försvarsmaktens metod för säkerhetsskyddsanalys ska användas vid genomförande av säkerhetsskyddsanalys i Försvarsmakten.* s. 49

Moment 2:2 *Innan chefen för organisationsenheten eller en enhet i Högkvarteret beslutar en säkerhetsskyddsanalys eller en säkerhetsskyddsplan ska organisationsenhetens eller enhetens ledningsgrupp, eller motsvarande, orienteras.* s. 52

Moment 2:3 *Alla säkerhetsskyddsanalyser, säkerhetsskyddsplaner, särskilda säkerhetsskyddsanalyser och särskilda säkerhetsskyddsplaner ska delges säkerhetskontoret vid Must.* s. 52

Moment 2:4 *Organisationsenhetens, samt enheternas i Högkvarteret, säkerhetsskyddsplanering ska identifiera behovet av fysiska säkerhetsskyddsåtgärder. Säkerhetsskyddsplaneringen ska minst innehålla:* s. 52

a) Identifiering av platser där säkerhetsskyddsklassificerade handlingar, lagringsmedier och säkerhetskänslig materiel förvaras. Hur förvaringen ska utformas med hänsyn till platsernas belägenhet, möjligheterna att upptäcka intrång och den tid det tar för en särskilt avdelad styrka att försvåra intrång i förvaringsutrymmena.

b) Identifiering av platser där det i övrigt bedrivs säkerhetskänslig verksamhet och hur den fysiska säkerheten ska utformas vid dessa platser, för att förebygga skadlig inverkan på verksamheten.

c) Identifiering av utrymmen som ska användas för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell eller högre.

d) Rutiner som ska följas eller andra fysiska säkerhetsskyddsåtgärder som ska vidtas vid förhöjd beredskap eller förändrad hotbild.

Moment 2:5 *En särskild säkerhetsskyddsanalys ska samordnas med Försvarsmaktens säkerhetsskyddsanalys samt med övriga relevanta säkerhetsskyddsanalyser.* s. 54

Moment 2:6 *Organisationsenhet samt enhet i Högkvarteret ska vartannat år och vid behov utvärdera säkerhetsskyddsplaneringen. Utvärderingen ska dokumenteras.* s. 56

Moment 2:7 *De identifierade och värderade säkerhetsskyddsvärdena ska godkännas av verksamhetsansvarig chef innan säkerhetsskyddsanalysen fortsätter.* s. 71

Moment 2:8 *Säkerhetsskyddsanalysen ska dokumenteras enligt följande disposition.* s. 77

1. Sammanfattning.

2. Inledning

2.1. Syfte och omfattning

3. *Verksamhetsbeskrivning*

4. *Identifierade och värderade säkerhetsskyddsvärden*

   4.1. Funktioner

   4.2. System

   4.3. Anläggningar

5. *Kritiska beroenden*

6. *Hotbild mot verksamheten*

7. *Sårbarheter*

8. *Gapanalys till gällande bestämmelser*

9. *Analys.*

10. *Slutsatser, förslag på generella säkerhetsskyddsåtgärder och rekommenderad prioritering.*

Moment 2:9 *Om en säkerhetsskyddsåtgärd inte kan vidtas ska följande anges för åtgärden.* s. 79

a) Skäl för att åtgärden inte kan vidtas.

b) En bedömning av konsekvensen för säkerhetsskyddet och den säkerhetskänsliga verksamheten.

c) Om något rättsligt krav eller moment i reglemente inte kan följas.

Moment 2:10 *Om en säkerhetsskyddsåtgärd inte kan vidtas får verksamhetsansvarig chef fatta beslut om att säkerhetsskyddsåtgärden inte ska vidtas. Ett sådant beslut får endast fattas under förutsättning att rättsliga krav eller moment i detta reglemente följs. Beslutet ska dokumenteras.* s. 79

Kapitel 3 – Informationssäkerhet

Moment 3:1 *En märkning med säkerhetsskyddsklass på en allmän handling ska placeras i övre delen på den säkerhetsskyddsklassificerade allmänna handlingens första sida. Säkerhetsskyddsklassen anges med versaler. Märkningen ska vara rektangulär. Upp till och med säkerhetsskyddsklassen hemlig ska ramen vara enkel. För säkerhetsskyddsklassen kvalificerat hemlig ska ramen vara dubbel.*	s. 105
Moment 3:2 *En märkning med säkerhetsskyddsklass på en allmän handling ska innehålla en hänvisning till vilken eller vilka sekretessbestämmelser i OSL som de säkerhetsskyddsklassificerade uppgifterna i den allmänna handlingen omfattas av. I märkningen ska framgå datum för när märkningen gjordes och att det är Försvarsmakten som har gjort märkningen. Försvarsmakten ska anges även på engelska (Swedish Armed Forces).*	s. 105
Moment 3:3 *Om märkningen avser en säkerhetsskyddsklassificerad allmän handling som är av synnerlig betydelse för rikets säkerhet ska märkningen även ange vilken myndighet som enligt 1 § offentlighets- och sekretessförordningen (2009:641) ska pröva begäran om utlämnande av allmän handling.*	s. 107
Moment 3:4 *På övriga sidor i en säkerhetsskyddsklassificerad allmän handling ska märkningen bestå av säkerhetsskyddsklassen i versaler med en hänvisning till handlingens första sida. Märkningen ska vara rektangulär. Upp till och med säkerhetsskyddsklassen hemlig ska ramen vara enkel. För säkerhetsskyddsklassen kvalificerat hemlig ska ramen vara dubbel.*	s. 108
Moment 3:5 *En inkommande handling från en annan stat eller en mellanfolklig organisation som är märkt med den statens eller organisationens motsvarighet till säkerhetsskyddsklass, ska placeras i säkerhetsskyddsklass även om Sverige inte omfattas av ett internationellt åtagande om säkerhetsskydd med den andra staten eller organisationen.*	s. 108
Moment 3:6 *En märkning med säkerhetsskyddsklass på en handling som inte är allmän ska placeras i övre delen på den säkerhetsskyddsklassificerade handlingens första sida. I märkningen ska det framgå den säkerhetsskyddsklass som avses.*	s. 108
Moment 3:7 *Delar av en säkerhetsskyddsklassificerad handling får märkas med säkerhetsskyddsklass. Varje del ska då märkas med den högsta säkerhetsskyddsklassen för uppgifterna som ingår i delen. Delar av handling får även förses med märkning som talar om att delen inte innehåller någon säkerhetsskyddsklassificerad uppgift.*	s. 109
Moment 3:8 *En ändring eller borttagning av säkerhetsskyddsklass på en tryckt skrift ska beslutas av den chef som, enligt FM ArbO, ansvarar för den aktuella bokpublikationen.*	s. 115
Moment 3:9 *Organisationsenheten ska i en lokal instruktion reglera vem som får besluta om ändring respektive borttagning av en säkerhetsskyddsklass på en allmän handling, ett lagringsmedium eller annan materiel som förvaras vid organisationsenheten. Instruktionen ska även beskriva hur ändringen eller borttagningen dokumenteras i det diarium som handlingen är diarieförd i eller i det register som*	s. 115

används för uppföljning av exemplar av handlingen, lagringsmediet eller materielen.

Moment 3:10 *Om det vid en organisationsenhet bedöms att en säkerhetsskyddsklassificerad allmän handling, som har upprättats vid någon annan organisationsenhet eller en annan myndighet, inte längre är säkerhetsskyddsklassificerad alternativt ska placeras i en annan säkerhetsskyddsklass än den ursprungliga, ska den organisationsenhet respektive den myndighet som har upprättat handlingen underrättas.*	s. 115
Moment 3:11 *Ändring på en säkerhetsskyddsklassificerad allmän handling i pappersform utförs genom att beslutet antecknas i anslutning till märkningen, den del av märkning som ska ändras överkorsas. I anteckningen ska det framgå vem som har fattat beslutet och datum när ändringen görs. Därefter anges den nya märkningen i anslutning till överkorsningen.*	s. 116
Moment 3:12 *Borttagning på en säkerhetsskyddsklassificerad allmän handling i pappersform utförs genom att beslutet antecknas i anslutning till märkningen. I anteckningen ska det framgå vem som har fattat beslutet och datum när ändringen görs. Därefter överkorsas märkningen.*	s. 116
Moment 3:13 *Den som förvarar en säkerhetsskyddsklassificerad handling som inte är allmän får besluta om ändring eller borttagning av säkerhetsskyddsklass på handlingen.*	s. 116
Moment 3:14 *En ändring av eller borttagning av säkerhetsskyddsklassen kvalificerat hemlig på en säkerhetsskyddsklassificerad handling som har upprättas av Försvarsmakten, får ske först efter att den organisationsenhet som har upprättat handlingen godkänt ändringen eller borttagningen.*	s. 117
Moment 3:15 *Om en säkerhetsskyddsklassificerad handling i ett internationellt samarbete får delges till en annan stat eller en mellanfolklig organisation, ska handlingen märkas med en anteckning om vilka stater och organisationer som den får delges till.*	s. 121
Moment 3:16 *Om en säkerhetsskyddsklassificerad handling innehåller uppgifter som enligt 8 kap. 3 § OSL* inte får *delges någon annan stat eller mellanfolklig organisation får handlingen märkas med anteckningen FÅR EJ DELGES UTLÄNDSK MYNDIGHET.*	s. 121
Moment 3:17 *Har en utländsk myndighet eller en mellanfolklig organisation försett en säkerhetsskyddsklassificerad handling med en anteckning som innebär begränsningar i att delge eller använda handlingen ska anteckningen följas om hinder inte möter enligt svensk rätt.*	s. 122
Moment 3:18 *Organisationsenheten ska ta fram rutiner för hur kopiering av eller utdrag ur fysiska säkerhetsskyddsklassificerade handlingar ska genomföras vid enheten.*	s. 127
Moment 3:19 *För säkerhetsskyddsklassificerade allmänna handlingar i säkerhetsskyddsklass konfidentiell eller högre ska rutinerna dessutom beskriva:*	s. 127

a) Vem som beslutar att en handling får kopieras (kopieringstillstånd).

b) Hur en kopia eller utdrag ska hanteras så att det nya exemplaret registreras innan det lämnas till den person som ska ta emot det. Rutinerna ska säkerställa att en person som förvarar en handling inte själv får kopiera den

---

Moment 3:20 *Om organisationsenheten utför distribution av fysiska säkerhetsskyddsklassificerade handlingar, lagringsmedier och materiel som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, ska enheten ta fram rutiner för distributionen.* s. 129

Moment 3:21 *Rutiner för distribution ska minst innehålla:* s. 129

a) Åtgärder för iordningsställande, avsändning, mottagning och kontroll av emballage och försändelser.

b) Åtgärder för uppföljning av att försändelser har kommit fram samt upptäckt av förseningar och förlust.

c) Åtgärder för spårbarhet av vilka handlingar, tryckta skrifter, lagringsmedier och materiel som finns i en försändelse.

d) Åtgärder när:

1) försändelser har försenats eller förlorats,

2) innehåll i försändelser inte överensstämmer med det förväntade, samt

3) försändelser eller emballage har påverkats.

Moment 3:22 *När uppgifter i en säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig, lämnas muntligt eller genom visning, ska kvittering genom namnteckning och namnförtydligande ske på delgivningskvitto eller lista. På delgivningskvittot eller listan anges det datum när uppgifterna lämnades eller visades. Kvittot eller listan ska om möjligt förvaras tillsammans med handlingen.* s. 134

Moment 3:23 *Kvitton och listor ska hållas ordnade vid expeditioner eller arkiv så att det är möjligt att undersöka vilka personer som har kvitterat att de, muntligen eller genom visning, har tagit del av uppgifterna.* s. 135

Moment 3:24 *Organisationsenheten ska ha dokumenterade rutiner för hur inventering av säkerhetsskyddsklassificerade handlingar, tryckta skrifter, lagringsmedier och materiel ska gå till.* s. 137

Moment 3:25 *Inventering ska protokollföras av en inventeringsförrättare. Ett inventeringsprotokoll upprättas för varje person som har inventerats. I protokollet ska det framgå vilka exemplar av handlingar, tryckta skrifter, lagringsmedier och materiel som är i behåll och vilka som saknas.* s. 138

Moment 3:35 *Om det av något beslut om verksamhetens genomförande följer att en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium ska medföras utanför Försvarsmaktens lokaler eller områden, behövs inte något särskilt beslut om medförande enligt den lokala instruktionen.* s. 144

Moment 3:36 *Innan säkerhetsskyddsklassificerade handlingar och lagringsmedier som har placerats i säkerhetsskyddsklassen konfidentiell eller högre medförs utanför Sverige ska organisationsenheten upprätta en förteckning över handlingarna och lagringsmedierna. I förteckningen ska anges om någon av handlingarna eller lagringsmedierna ska överlämnas utomlands. När det gäller de handlingar som ska återföras till Sverige ska organisationsenheten, när handlingarna har återförts, kontrollera att dessa är desamma som de som enligt förteckningen ska återföras.* s. 146

Moment 3:37 *Inför en skyddad transport ska säkerhetsskyddsklassificerade handlingar och lagringsmedier förpackas i emballage som förseglas så att mottagaren kan upptäcka att emballage har öppnats eller ersatts under transporten.* s. 147

Moment 3:38 *Inför en skyddad transport ska åtgärder vidtas så att det finns spårbarhet för vilka säkerhetsskyddsklassificerade handlingar och lagringsmedier som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre som ska transporteras.* s. 147

Moment 3:39 *Den person som med stöd av ett beslut om gemensam användning har kvitterat mottagandet av en handling eller ett lagringsmedium som ska användas gemensamt, ska tillsammans med var och en av dem som ingår i gruppen, svara för att säkerhetsskyddet upprätthålls vid hantering av den säkerhetsskyddsklassificerade handlingen eller lagringsmediet.* s. 147

Moment 3:40 *Om gemensam användning tillämpas ska organisationsenheten ta fram rutiner för gemensam användning. Rutinerna ska minst innehålla:* s. 148

a) Vilka befattningar vid enheten som får besluta om inrättande eller avveckling av en grupp, att en person ska ingå, eller inte längre ska ingå, i en grupp samt att en viss säkerhetsskyddsklassificerad handling eller lagringsmedium ska användas gemensamt av en viss grupp.

b) Åtgärder för beslut om inrättande eller avveckling av en grupp för gemensam användning.

c) Åtgärder för beslut att en person ska ingå, eller inte längre ska ingå, i en grupp. Åtgärderna ska säkerställa att det i efterhand går att avgöra vilka personer som har ingått i en grupp och tidpunkter för in- och utträde ur gruppen.

d) Åtgärder för samråd med en annan organisationsenhet eller myndighet om en person som avses ingå i en grupp inte är anställd vid enheten.

e) Åtgärder för beslut att en viss säkerhetsskyddsklassificerad handling eller lagringsmedium ska användas gemensamt av en viss grupp. Åtgärderna ska säkerställa att det i efterhand går att avgöra vilka handlingar och lagringsmedier som kunnat användas av personer i en grupp och tidpunkt för

beslut.

f) Åtgärder för hur en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium ska tas emot av en grupp.

g) Åtgärder för förvaring av säkerhetsskyddsklassificerade handlingar och lagringsmedier. Åtgärderna ska säkerställa att endast personer som ingår i en grupp kan komma in i förvaringsutrymmen för handlingar och lagringsmedier som gruppen gemensamt använder. Åtgärderna ska även säkerställa dokumentation över vilka förvaringsutrymmen som en grupp förvarar handlingar och lagringsmedier i.

h) Åtgärder för inventering av säkerhetsskyddsklassificerade handlingar och lagringsmedier som används gemensamt.

i) Åtgärder för hur en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium ska lämnas tillbaka från en grupp.

j) Åtgärder när någon som ingår i en grupp upptäcker:

1) att en säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium saknas, kan ha röjts eller obehörigen har ändrats, samt

2) *någon annan brist i säkerhetsskyddet för den gemensamma användningen.*

Moment 3:41 *Om en säkerhetsskyddsklassificerad allmän handling lånas ut till en myndighet eller ett företag ska det i diariet där handlingen är diarieförd anges vem som har lånat handlingen och om handlingen har återlämnats. Uppgifterna får istället för i diariet antecknas i ett register för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.* s. 150

Moment 3:42 *Om ett säkerhetsskyddsklassificerat lagringsmedium lånas ut till en myndighet eller ett företag ska det i register över Försvarsmaktens säkerhetsskyddsklassificerade lagringsmedier framgå vem som har lånat mediet och om mediet har återlämnats.* s. 150

Kapitel 4 – Informationssäkerhet i och kring informationssystem

Kapitlet saknar moment.

Kapitel 5 – Fysisk säkerhet

Moment 5:1 *Beslut om tillträde enligt 4 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd ska innefatta it-utrymmen vid organisationsenheten där det behandlas säkerhetsskyddsklassificerade uppgifter eller bedrivs annan säkerhetskänslig verksamhet.* s. 176

Moment 5:2 *Tabell 5.1 ska användas för att fastställa den tid en särskild avdelad styrka har till sitt förfogande innan ett intrång har skett i ett nivåreglerat förvaringsutrymme.* s. 181

Momentet innehåller en tabell som inte återges här.

Moment 5:3 *Säkerhetskänslig materiel ska förvaras i ett förvaringsutrymme som ska placeras i någon av följande skyddsnivåer.* s. 183

Skyddsnivå 1 gäller för förvaring av en ringa mängd säkerhetskänslig materiel.
Skyddsnivå 2 gäller för förvaring av en mindre mängd säkerhetskänslig materiel.
Skyddsnivå 3 gäller för förvaring av en större mängd säkerhetskänslig materiel.
Skyddsnivå 4 gäller för förvaring av mycket stora mängder säkerhetskänslig materiel.

Moment 5:4 *Vid organisationsenheten ska en förteckning föras över nycklar, kort och koder till områden, byggnader eller utrymmen som används för säkerhetskänslig verksamhet där en inträffad skada lägst kan vara inte obetydlig för Sveriges säkerhet.* s. 185

Moment 5:5 *Sådana nycklar, kort och koder som anges i 5 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd och moment 5:4 ska inventeras en gång per år.* s. 185

Moment 5:6 *En nyckel som ännu inte har lämnats till den som ska ansvara för ett förvaringsutrymme ska förvaras av säkerhetschefen, eller av den han eller hon bestämmer.* s. 186

Moment 5:7 *En anteckning om en kod till ett kombinationslås eller en anteckning om en kod som används tillsammans med ett passerbevis ska förvaras i ett förseglat emballage. Emballaget ska vara så beskaffat att det är omöjligt att ta del av anteckningen utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget. Anteckningen med emballage ska förvaras på samma sätt som gäller för säkerhetsskyddsklassificerade handlingar eller säkerhetskänslig materiel som förvaras i det utrymme som koden går till.* s. 186

Moment 5:8 *Om en person ska vara borta från organisationsenheten en längre tid ska han eller hon överlämna nyckeln till förvaringsutrymmet till säkerhetschefen, eller till den säkerhetschefen bestämmer. Nyckeln ska förvaras på samma sätt som anges i moment 5:7.* s. 186

Moment 5:9 *En kod eller en reservnyckel får endast i vittnes närvaro användas av någon annan än den som har ansvar för förvaringsutrymmet. I organisationsenhetens bestämmelser för fysisk säkerhet ska förutsättningar för en sådan användning anges.* s. 186

Moment 5:10 *I ett avtal om inköp av ett flyttbart förvaringsutrymme, en dörr till ett förvaringsutrymme eller ett lås ska det säkerställas att nyckeln till utrymmet eller låset levereras separat och direkt till organisationsenheten samt att leveransen sker enligt vad som gäller för säkerhetsskyddsklassificerade handlingar i lägst den säkerhetsskyddsklassen som förvaringsutrymmet är avsett för.* s. 186

Moment 5:11 *Ett sådant förhållande som anges i 5 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd ska vid organisationsenheten rapporteras som en säkerhetshotande händelse.* s. 186

Moment 5:12 *En reservnyckel till ett förvaringsutrymme ska förvaras i ett förseglat emballage. Emballaget ska vara så beskaffat att det är omöjligt att avläsa nyckelaxet utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget.* s. 187

Moment 5:13 *Ett emballage som innehåller en reservnyckel ska förvaras på samma sätt som gäller för de handlingar, lagringsmedier eller den materiel som förvaras i det utrymme som nyckeln går till.* s. 187

Moment 5:14 *Organisationsenhetens tekniska bevakningssystem för platser där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan vara inte obetydlig för Sveriges säkerhet, ska säkerhetsskyddet av de centrala delarna i det tekniska bevakningssystemet uppfylla de krav på förvaring som gäller för lägst skyddsnivå 2.* s. 190

Moment 5:15 *Organisationsenheten ska vidta de skyddsåtgärder som behövs för att* s. 190

a) säkerställa att ett tekniskt bevakningssystem inte kan manipuleras i syfte att någon obehörig ska kunna ta komma in i utrymmen, samt

b) kontinuitet för det tekniska bevakningssystemets funktion.

Moment 5:16 *Vilka åtgärder som behöver vidtas för att ett utrymme ska kunna godkännas ska identifieras i en sårbarhetsanalys. Identifierade åtgärder ska genomföras innan utrymmet godkänns.* s. 193

Moment 5:17 *Om ett utrymme för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre avses användas vid organisationsenheten, ska en sårbarhetsbedömning genomföras. En begäran om sårbarhetsbedömning ska göras till underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2).* s. 194

Moment 5:18 *Efter att en sårbarhetsbedömning enligt moment 5:17 har genomförts ska organisationsenheten begära samråd med säkerhetsskyddsavdelningen vid Must. Ett samråd ska inhämtas:* s. 194

a) Innan ett konstruktionsarbete påbörjas av ett befintligt eller ett nytt utrymme.

b) Innan ett godkännande av ett befintligt eller ett nytt utrymme, i det fall ett

konstruktionsarbete inte kommer att genomföras.

Moment 5:19 *En begäran om samråd ska innehålla:* s. 194

a) Beskrivning av den säkerhetskänsliga verksamhet som ska använda utrymmet.

b) Vilka typer av säkerhetsskyddsklassificerade uppgifter som ska behandlas i utrymmet.

c) Den verksamhetsansvariges hotbild för den egna säkerhetskänsliga verksamheten.

d) Bedömda sårbarheter för utrymmet och dess omgivning. Resultat från sårbarhetsbedömning beställd av underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2) ska bifogas.

e) Vilka åtgärder som har identifierats i sårbarhetsanalysen enligt moment 5:16 och hur dessa kommer att uppfyllas.

f) Situationsplan för byggnaden och dess omgivning.

g) Vilken teknisk utrustning och inventarier som ska finnas i utrymmet.

Moment 5:20 *Ett utrymme som är avsett att användas för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell eller högre, ska uppfylla följande krav.* s. 195

a) Utrymmet ska vara placerat i en administrativ zon. Om utrymmet är avsett för delgivning av kvalificerat hemliga uppgifter ska utrymmet vara en säkerhetszon.

b) Utrymmet ska vara larmat.

c) För att reducera möjligheter till obehörig avlyssning ska administrativa-, fysiska- och tekniska åtgärder vidtas. Åtgärderna ska dokumenteras.

d) En förteckning över vilka personer som är behöriga till utrymmet ska upprättas.

e) Utrymmet ska vara försett med loggning på personnivå över vilken behörig personal som har haft tillträde till utrymmet.

f) Det ska i utrymmet finnas en förteckning över vilken teknisk utrustning som får finnas i, eller som får medföras in i utrymmet.

g) Det ska i utrymmet finnas en förteckning över vilken inredning som får finnas i, eller som får medföras in i utrymmet.

h) Personal som ska vara behörig till utrymmet ska vara utbildade i bestämmelser och rutiner kring användning av utrymmet och dess säkerhetsskydd.

Moment 5:21 *Efter beslut om godkännande har fattats ska hemställan om tekniskt säkerhetsskyddsundersökning tillställas underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2).* s. 196

Moment 5:22 *Utrymmen som har godkänts för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell och högre, ska regelbundet kontrolleras. Sådana kontroller ska även genomföras efter ett obehörigt intrång eller misstanke om sådant intrång.* s. 196

Moment 5:23 *Innan ett utrymme används för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter i högst säkerhetsskyddsklass begränsat hemlig ska följande beaktas.* s. 197

d) Utrymmets utformning och placering.

e) Vilken teknisk utrustning som finns i, eller får medföras in i utrymmet.

f) Den tekniska utrustningens möjlighet till kommunikation med omvärlden.

Moment 5:24 *Ett it-utrymme där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan medföra en skada för Sveriges säkerhet som inte är obetydlig, ska uppfylla de krav som gäller för skyddsnivå 3 samt förses med larm.* s. 199

Moment 5:25 *Ett it-utrymme där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan vara ringa för Sveriges säkerhet ska uppfylla de krav som gäller för skyddsnivå 2.* s. 199

Moment 5:26 En *organisationsenhet som avser att sända säkerhetsskyddsklassificerade handlingar, lagringsmedier eller säkerhetskänslig materiel ska göra en särskild säkerhetsskyddsanalys för att fastställa transportnivå för den aktuella transporten. Innan en sådan transport genomförs ska säkerhetsskyddsanalysen granskas och godkännas av organisationsenhetens säkerhetschef eller den säkerhetschefen bestämmer.* s. 200

Moment 5:27 *En skyddad transport för säkerhetsskyddsklassificerade handlingar, lagringsmedier och säkerhetskänslig materiel ska placeras i någon av följande transportnivåer.* s. 200

Momentet är omfattande och återges inte i sin helhet här, se s. 200.

Moment 5:28 *Inför en skyddad transport i transportnivå 2-4 ska den organisationsenhet som ansvarar för att planera transporten upprätta en särskild säkerhetsskyddsplan.* s. 202

Moment 5:29 *Innan en skyddad transport i transportnivå 2-4 påbörjas, ska den organisationsenhet som organiserar transporten informera mottagaren av godset, berörda polisregioner och berörda regionala staber om att transporten ska genomföras.* s. 202

Moment 5:30 *Vid en skyddad transport ska om möjligt nycklar eller koder till förvaringsutrymmen som ingår i transporten skickas till mottagaren i en separat försändelse. Om nycklar eller koder inte kan skickas till mottagaren i en separat försändelse, ska de under transporten vara under kontroll av personal i följebil,* s. 202

transportskyddsstyrkan eller transportfordonet.

Moment 5:31 *Vid uppehåll under transporten ska det skydd som gäller för transporten upprätthållas.* s. 202

Kapitel 6 – Säkerhetsprövning

ser om säkerhetsskydd ska göras till säkerhetsprövningssektionen vid Must.

Moment 6:14 *Organisationsenheten ska på begäran av säkerhetsprövningssektionen vid Must lämna den information som finns om en person vid organisationsenheten, om hinder inte möter på grund av bestämmelse om sekretess i offentlighets- och sekretesslagen.* s. 225

Moment 6:15 *Information om brister i pålitlighet, lojalitet och omständigheter som kan innebära sårbarheter i säkerhetshänseende, samt annan information som begärs av säkerhetsprövningssektionen vid Must, ska hanteras på ett sådant sätt att endast de som är behöriga att ta del av informationen kan få tillgång till den.* s. 226

Moment 6:16 *En person är behörig att vidta åtgärder inom ramen för säkerhetsprövning först efter att den har genomgått relevant utbildning samt bedömts som lämplig.* s. 227

Moment 6:17 *Vid varje organisationsenhet ska det minst finnas en befattning som är utsedd att ansvara för registerkontrollhantering. Innan en person får tillgång till RK-rutinen i IS UNDSÄK ska säkerhetsprövningssektionen vid Must ha godkänt personen.* s. 228

Moment 6:18 *Personer som* s. 229

a) administrerar registerkontroller,

b) genomför samtal och intervjuer,

c) genomför grundutredning,

d) genomför uppföljning av säkerhetsprövning,

e) genomför utredningar eller tar del av utredningsinformation,

f) handlägger den dokumentation som finns om den som säkerhetsprövningen gäller,

g) genomför bedömningar inför beslut i ärenden om säkerhetsprövning,

h) beslutar i ärenden om säkerhetsprövning, eller

i) utbildar i säkerhetsprövning

ska ha genomgått en av Försvarsmaktens säkerhetsskyddschefs godkända utbildningar innan de deltar i ärenden som rör säkerhetsprövning.

Moment 6:19 *Chefen för en organisationsenhet ska besluta vilka som ska utbilda i säkerhetsprövning vid organisationsenheten.* s. 229

Moment 6:20 *Organisationsenheten ska förteckna vilka som har genomgått utbildning i säkerhetsprövning, vilken utbildning som genomförts och när den genomfördes. Förteckningen ska meddelas till säkerhetsprövningssektionen vid Must i IS UNDSÄK.* s. 230

Moment 6:21 *En förteckning enligt moment 6:20 ska även innefatta vilka vid organisationsenheten som är behöriga att genomföra grundutredning och uppföljning, samt vilka personer som i övrigt är behöriga att ta del av uppgifter som förekommer i ärenden om säkerhetsprövning.*	s. 230
Moment 6:22 *En person som ska säkerhetsprövas ska få information om att säkerhetsprövning ska genomföras och vad den omfattar. Personen ska även informeras om nödvändigheten av att anmäla förändringar i personliga förhållanden.*	s. 231
Moment 6:23 *Den organisationsenhet som genomför säkerhetsprövningen ska informera den prövade om vad registerkontroll innebär och ansvarar för att den prövade lämnar sitt samtycke inför registerkontroll. Om den prövade inte lämnar sitt samtycke ska grundutredningen avslutas.*	s. 231
Moment 6:24 *En organisationsenhet ska registrera samtycket i RK-rutinen i IS UNDSÄK samt på dokumentmallen* Intervjuguide säkerhetsprövningsintervju *inför ansökan om registerkontroll.*	s. 232
Moment 6:25 *Om den prövade under grundutredningens genomförande återtar ett tidigare lämnat samtycke, ska grundutredningen avslutas.*	s. 232
Moment 6:26 *Om den prövade, efter genomförd registerkontroll, återtar sitt samtycke ska säkerhetsprövningen avslutas och ett avslutande samtal ska genomföras med den prövade. Säkerhetsprövningssektionen vid Must ska informeras innan registerkontrollen avslutas.*	s. 232
Moment 6:27 *Om befattningen är placerad i säkerhetsklass 1 eller 2 ska grundutredningen även omfatta:* *a) personens ekonomiska förhållanden, och* *b) personens förekomst på internet och sociala medier som är allmänt tillgängliga och som har betydelse för säkerhetsprövningen*	s. 234
Moment 6:28 *När en person, som redan deltar i Försvarsmaktens säkerhetskänsliga verksamhet, byter organisationsenhet ska den mottagande organisationsenheten inhämta information om säkerhetsprövningen från den avlämnande organisationsenheten.*	s. 235
Moment 6:29 *Vid säkerhetsprövningssektionen vid Must får det beslutas om ytterligare säkerhetsprövningsintervjuer inom ramen för en grundutredning.*	s. 236
Moment 6:30 *En säkerhetsprövningsintervju ska ha minst den omfattning som man vid säkerhetsprövningssektionen vid Must har bestämt. Säkerhetsprövningsintervjun ska i övrigt ha den omfattning som behövs för att bedöma den prövades pålitlighet och lojalitet samt om det föreligger några sårbarheter i säkerhetshänseende.*	s. 236
Moment 6:31 *Vid en säkerhetsprövningsintervju ska anteckningar föras.*	s. 237

Moment 6:32 *Efter en säkerhetsprövningsintervju ska en bedömning göras av de uppgifter som har framkommit. Bedömningen ska dokumenteras med hjälp av dokumentmallen* Intervjuguide säkerhetsprövningsintervju. s. 237

Moment 6:33 *Resultatet av grundutredningen ska sammanställas på dokumentmallen* Sammanfattande dokumentation grundutredning. s. 237

Moment 6:34 *En grundutredning ska avslutas med en sammanfattande bedömning. Bedömningen ska genomföras innan framställan om registerkontroll och ska dokumenteras på dokumentmallen* Sammanfattande dokumentation grundutredning. s. 237

Moment 6:35 *Dokumentmallen* Sammanfattande dokumentation grundutredning *ska sändas till säkerhetsprövningssektionen vid Must. Bedömningen ska kompletteras med en säkerhetsrapport i personärende med uppgifter om:* s. 239

a) vilka åtgärder som vidtagits inom ramen för säkerhetsprövningen,

b) brister i den prövades lojalitet, pålitlighet eller omständigheter som kan innebära sårbarheter i säkerhetshänseende, och

c) kompletterande skyddsåtgärder som kan uppväga den prövades brister eller sårbarheter.

Moment 6:36 *Om organisationsenheten avslutar säkerhetsprövningen av säkerhetsrelaterade skäl, ska dokumentationen av grundutredningen sändas till säkerhetsprövningssektionen vid Must, tillsammans med* Sammanfattande dokumentation grundutredning. *Dokumentationen ska kompletteras med en säkerhetsrapport i personärende med uppgifter om:* s. 240

a) vilka åtgärder som vidtagits inom ramen för säkerhetsprövningen, och

b) brister i den prövades lojalitet, pålitlighet eller omständigheter som kan innebära sårbarheter i säkerhetshänseende.

Moment 6:37 *Om en totalförsvarspliktig som är inskriven för värnplikt ska placeras på en befattning i säkerhetsklass 1 eller 2 ska grundutredningen genomföras av den organisationsenhet där den värnpliktige ska placeras. Grundutredningen och registerkontrollen ska vara genomförda innan den värnpliktige får delta i säkerhetskänslig verksamhet som kräver placering i säkerhetsklass 1 eller 2.* s. 241

Moment 6:38 *En grundutredning ska göras om vid följande tillfällen.* s. 241

a) När en person placeras på en ny befattning med andra arbetsuppgifter, oavsett om befattningarna är placerade i samma säkerhetsklass.

b) När en person får förändrade arbetsuppgifter i sin nuvarande befattning som, efter en befattningsanalys, påverkar placeringen i säkerhetsklass.

c) När en registerkontroll ska förnyas för en person som redan är placerad på en befattning i säkerhetsklass 1 eller 2, och där registerkontrollen är

genomförd före den 1 april 2019.

d) När en person byter organisationsenhet (oavsett befattning).

e) När en värnpliktig ska placeras på en befattning efter avslutad grundutbildning. Kravet gäller dock inte i det fall den värnpliktige endast krigsplaceras.

Moment 6:39 *Om en organisationsenhet bedömer att en grundutredning ska göras mindre omfattande ska det anmälas till säkerhetsprövningssektionen vid Must.* s. 243

Moment 6:40 *Om befattningen inte är placerad i säkerhetsklass ska en ansökan om deltagande i säkerhetskänslig verksamhet skickas till säkerhetsprövningssektionen vid Must*. s. 243

Moment 6:41 *En ansökan om deltagande i säkerhetskänslig verksamhet ska innehålla personuppgifter, kontrollorsak och kontrollorsakstext. Vid ansökan ska nivå ”Ej RK” väljas.* s. 243

Moment 6:42 *Organisationsenheten ska minst en gång om året, samt vid behov, genomföra översyn och säkerställa att endast de som deltar i verksamheten på en säkerhetsklassad befattning är registerkontrollerade samt att de har en registerkontroll i rätt säkerhetsklass.* s. 245

Moment 6:43 *Organisationsenheten ska framställa om registerkontroll hos säkerhetsprövningssektionen vid Must.* s. 246

Moment 6:44 *En ansökan om registerkontroll ska innehålla:* s. 246

a) De personuppgifter som Säkerhetspolisen efterfrågar.

b) Säkerhetsklass.

c) Kontrollorsak och kontrollorsakstext.

d) Vid säkerhetsskyddad upphandling ska uppdrag, företag och befattning i företaget anges.

Moment 6:45 *Vid säkerhetsklass 1 och 2 ska ansökan kompletteras med* Bilaga – Särskild personutredning för säkerhetsklass 1 och 2. *Bilagan ska skickas till säkerhetsprövningssektionen vid Must, efter att ansökan om registerkontroll har lagts in i RK-rutinen i IS UNDSÄK.* s. 246

Moment 6:46 *Om ett deltagande i en säkerhetskänslig verksamhet är tidsbegränsat ska detta framgå vid ansökan om registerkontroll och en sluttid ska anges i RK-rutinen i IS UNDSÄK.* s. 246

Moment 6:47 *Endast följande kontrollorsaker för registerkontroll får användas.* s. 247

Momentet innehåller en punktlista som inte återges här.

Moment 6:48 *Kontrollorsaken ska kompletteras med en beskrivning av orsaken till placering i säkerhetsklass, samt vilken befattning som avses. En sådan beskrivning av orsaken till placering i säkerhetsklass får endast begränsas i omfattning efter beslut vid säkerhetsprövningssektion vid Must.* s. 249

Moment 6:49 *Den som har tecknat ett säkerhetsskyddsavtal ska ansöka om registerkontroll av leverantörens personal hos säkerhetsprövningssektionen vid Must. Underlag för säkerhetsskyddad upphandling ska vara säkerhetsprövningssektionen vid Must tillhanda senast två veckor innan ansökan om registerkontroll.* s. 250

Moment 6:50 *Om en befattnings placering i säkerhetsklass har ändrats till en annan säkerhetsklass får inte den befintliga registerkontrollen avslutas förrän den nya registerkontrollen har godkänts vid säkerhetsprövningssektionen vid Must.* s. 251

Moment 6:51 *En organisationsenhet kan begära flytt av en registerkontroll:* s. 251

a) Om den befintliga befattningen flyttas till en annan organisationsenhet p.g.a. en organisationsförändring och befattningsanalysen inte förändras.

b) Om en person byter arbetsplats till en annan organisationsenhet och befattningsanalysen, kontrollorsak och arbetsuppgifter är desamma.

Moment 6:52 *Den mottagande organisationsenheten ska hemställa om flytt av registerkontroll hos säkerhetsprövningssektionen vid Must samt meddela den avlämnade organisationsenheten om att flytt av registerkontroll kommer att genomföras.* s. 252

Moment 6:53 *Den som har ingått ett säkerhetsskyddavtal ansvarar för att registerkontrollen avslutas när uppdraget avslutas eller upphör.* s. 253

Moment 6:54 *Om en organisationsenhet bedömer att en registerkontroll inte behöver göras enligt 3 kap. 3 § första stycket säkerhetsskyddslagen, ska det anmälas till säkerhetsprövningssektionen vid Must som bestämmer om registerkontroll inte behöver göras.* s. 255

Moment 6:55 *Organisationsenheten ska skyndsamt ansöka om deltagande i säkerhetskänslig verksamhet, om:* s. 257

a) en person som är anställd i Försvarsmakten inte uppfyller kraven för en godkänd säkerhetsprövning för en befattning placerad i säkerhetsklass, och

b) personen ändå ska delta i Försvarsmaktens säkerhetskänsliga verksamhet.

Moment 6:56 *Om ett beslut om godkänd säkerhetsprövning ska omprövas, ska chef för organisationsenheten hemställa om omprövning hos säkerhetsprövningssektionen vid Must. Hemställan ska innehålla den dokumentation som finns om den prövade, samt en bedömning av personens pålitlighet, lojalitet och sårbarhet i säkerhetshänseende.* s. 258

Moment 6:57 *Den särskilda uppföljningen ska innefatta samtal. Samtalen ska dokumenteras och sparas vid organisationsenheten.* s. 259

Moment 6:58 *Chefen för en organisationsenhet ska efter mottagandet av ett beslut i ärende om säkerhetsprövning meddela säkerhetsprövningssektionen vid Must om den som prövningen gäller ska delta i den säkerhetskänsliga verksamheten eller inte, samt skyndsamt vidta eventuella skyddsåtgärder enligt beslutet.* s. 260

Moment 6:59 *Ett meddelande enligt moment 6:58 ska skickas till säkerhetsprövningssektionen vid Must inom en månad efter att beslutet mottagits av organisationsenheten.* s. 260

Moment 6:60 *Ett beslut i ärende om säkerhetsprövning får delges den prövade om beslutet inte anger annat. Som skäl för beslutet ska anges att det grundar sig på Försvarsmaktens säkerhetsprövning.* s. 261

Moment 6:61 *När en person har placerats på en befattning i säkerhetsklass 1 ska ett skyddssamtal hållas snarast efter att personen tillträtt befattningen.* s. 261

Moment 6:62 *Vid säkerhetsprövningssektionen vid Must får man bestämma när ett skyddssamtal ska genomföras med en person som har en befattning som är placerad i säkerhetsklass 2 eller 3, eller en befattning som inte har placerats i säkerhetsklass.* s. 261

Moment 6:63 *Ett skyddssamtal får inte genomföras med flera personer samtidigt, om man inte vid säkerhetsprövningssektionen vid Must har bestämt något annat.* s. 262

Moment 6:64 *När ett skyddssamtal har genomförts ska organisationsenheten meddela säkerhetsprövningssektionen vid Must att det är genomfört.* s. 262

Moment 6:65 *Vid ett skyddssamtal vid placering i säkerhetsklass ska anteckningar föras.* s. 262

Moment 6:66 *Säkerhetsprövningen ska följas upp kontinuerligt och bestå av:* s. 264

a) ett årligt uppföljande samtal,

b) ekonomisk kontroll vart femte år vid placering i säkerhetsklass 1 och 2, samt i övrigt när särskilda behov föreligger,

c) kontinuerlig kontakt i den dagliga verksamheten,

d) kontinuerlig uppdatering av personuppgifter i registerkontrollen, och

e) en årlig bedömning av den prövades pålitlighet och lojalitet samt om det föreligger någon sårbarhet i säkerhetshänseende.

Moment 6:67 *Den årliga bedömningen av den prövades pålitlighet och lojalitet samt om det föreligger någon sårbarhet i säkerhetshänseende, ska dokumenteras med hjälp av dokumentmallen* Sammanfattande dokumentation uppföljning. s. 265

Moment 6:68 *Det uppföljande samtalet ska minst ha den omfattning som man vid säkerhetsprövningssektionen vid Must har bestämt och i övrigt ha den omfattning som behövs för att bedöma den prövades pålitlighet och lojalitet samt om det föreligger några sårbarheter i säkerhetshänseende.*	s. 265
Moment 6:69 *Vid ett uppföljande samtal ska anteckningar föras.*	s. 266
Moment 6:70 *Efter ett uppföljande samtal ska en bedömning göras av de uppgifter som har framkommit. Bedömningen ska dokumenteras med hjälp av dokumentmallen* Samtalsguide uppföljande samtal.	s. 266
Moment 6:71 *Organisationsenheten ansvarar för att genomföra och dokumentera skyddssamtal vid särskilda behov.*	s. 267
Moment 6:72 *Om det inom ramen för säkerhetsprövning, eller säkerhetsrapportering framkommer brister i en persons lojalitet och pålitlighet eller om det föreligger några sårbarheter i säkerhetshänseende ska organisationsenheten påbörja en utredning.*	s. 268
Moment 6:73 *Om en organisationsenhet påbörjar en utredning ska det meddelas till säkerhetsprövningssektionen vid Must.*	s. 269
Moment 6:74 *En utredning ska alltid innefatta en bedömning av lojalitet, pålitlighet samt sårbarhet i säkerhetshänseende.*	s. 269
Moment 6:75 *Den organisationsenhet som genomför en utredning ansvarar för att utredningen dokumenteras.*	s. 269
Moment 6:76 *När ett beslut om säkerhetssamtal har fattats vid säkerhetsprövningssektionen vid Must ska samtalet genomföras skyndsamt och senast inom en månad från beslutet.*	s. 270
Moment 6:77 *Ett säkerhetssamtal får inte genomföras om samtalet kan störa eller skada en brottsutredning.*	s. 270
Moment 6:78 *Vid ett säkerhetssamtal ska anteckningar föras.*	s. 270
Moment 6:79 *Efter ett säkerhetssamtal ska en bedömning göras av de uppgifter som har framkommit. Bedömningen ska dokumenteras.*	s. 270
Moment 6:80 *När organisationsenheten har genomfört ett säkerhetssamtal ska detta meddelas säkerhetsprövningssektionen vid Must. Underlag från ett genomfört säkerhetssamtal skickas in till säkerhetsprövningssektionen vid Must.*	s. 271
Moment 6:81 *Psykologisk personbedömning ska genomföras av en legitimerad psykolog.*	s. 272
Moment 6:82 *Psykologisk testning ska genomföras och resultatet av testningen ska utgöra en del av det underlag som ligger till grund för den psykologiska personbedömningen.*	s. 272

Moment 6:83 *Om en person som har genomgått säkerhetsprövning mot särskilda befattningar inte har fått anställning i befattningsnivå 5, ska resultatet gälla i tre år. Vid säkerhetsprövningssektionen vid Must får man dock besluta att en säkerhetsprövning mot särskilda befattningar ska genomföras på nytt innan tre år har förflutit.*	s. 272
Moment 6:84 *Inför befordran till befattningsnivå 6 eller högre samt vid byte av befattning ska den tidigare genomförda grundutredningen förnyas.*	s. 272
Moment 6:85 *Säkerhetsprövningssektionen vid Must ska genomföra skyddssamtal senast tre år efter att den prövade har genomgått säkerhetsprövning mot särskilda befattningar.*	s. 273
Moment 6:86 *Vid säkerhetsprövningssektionen vid Must ska man genomföra uppföljande samtal med personer som genomgått säkerhetsprövning mot särskilda befattningar.*	s. 273
Moment 6:87 *I samband med uppföljning av säkerhetsprövning mot särskilda befattningar ska man vid säkerhetsprövningssektionen vid Must besluta om en förnyad psykologisk personbedömning ska genomföras.*	s. 273
Moment 6:88 *Organisationsenheten ansvarar för att, i det dagliga arbetet vid organisationsenheten, följa upp personer som har genomgått säkerhetsprövning mot särskilda befattningar.*	s. 273
Moment 6:90 *Säkerhetsprövning mot särskilda befattningar ska dokumenteras på det sätt som man vid säkerhetsprövningssektionen vid Must beslutat.*	s. 273
Moment 6:90 *Säkerhetsprövning mot särskilda befattningar ska dokumenteras på det sätt som man vid säkerhetsprövningssektionen vid Must beslutat.*	s. 273
Moment 6:91 *Det avslutande samtalet ska minst ha den omfattning som bestämts vid säkerhetsprövningssektionen vid Must och i övrigt ha den omfattning som behövs för att bedöma den prövades pålitlighet och lojalitet samt om det föreligger några sårbarheter i säkerhetshänseende.*	s. 275
Moment 6:92 *Vid ett avslutande samtal ska anteckningar föras.*	s. 275
Moment 6:93 *Efter ett avslutande samtal ska en bedömning göras av de uppgifter som har framkommit. Bedömningen ska dokumenteras med hjälp av dokumentmallen* Samtalsguide avslutande samtal.	s. 275
Moment 6:94 *Organisationsenheten ska bevara befattningsanalysen.* Förteckning befattningsanalys *ska bevaras vid säkerhetsprövningssektionen vid Must.*	s. 277
Moment 6:95 *Organisationsenheten ansvarar för att grundutredningar vid egen enhet bevaras. Om säkerhetsprövningen har avslutats, under eller efter genomförd grundutredning, och ärendet har rapporterats till säkerhetsprövningssektionen vid Must ska grundutredningen bevaras vid säkerhetsprövningssektionen.*	s. 277

nomförs av Försvarsmakten.

Moment 6:109 *Den som ansvarar för ett säkerhetsskyddsavtal ska se till att grundutredning för leverantörens personal genomförs av Försvarsmakten när deltagandet är placerat i säkerhetsklass 1 eller 2. Vid säkerhetsprövningssektionen vid Must får man besluta att hela eller delar av en grundutredning ska genomföras av någon annan.* s. 284

Moment 6:110 *Den som ansvarar för ett säkerhetsskyddsavtal ansvarar för att uppföljning av säkerhetsprövning genomförs för leverantörens personal. Leverantören får i följande fall genomföra uppföljning av säkerhetsprövning av egen personal:* s. 284

a) Årliga uppföljande samtal och kontinuerlig kontakt i den dagliga verksamheten, när verksamheten bedrivs i leverantörens egna lokaler (nivå 1).

b) Årliga uppföljande samtal, när verksamheten bedrivs i Försvarsmaktens lokaler och befattningen är placerad i säkerhetsklass 3.

Moment 6:111 *Om det under eller efter leverantörens genomförda grundutredning står klart att personen inte kommer att uppfylla kraven för en godkänd säkerhetsprövning, ska den som ansvarar för säkerhetsskyddsavtalet se till att grundutredningen avslutas.* s. 285

Moment 6:112 *När Försvarsmaktens säkerhetsskyddchef har beslutat i ärende om säkerhetsprövning, ska den som ansvarar för säkerhetsskyddsavtalet:* s. 286

a) Meddela säkerhetsprövningssektionen vid Must om den person som prövningen gäller kommer att delta i den säkerhetskänsliga verksamheten eller inte.

b) Skyndsamt se till att eventuella skyddsåtgärder enligt beslutet vidtas.

c) Skyndsamt se till att leverantören meddelas beslutet.

Moment 6:113 *Om leverantören inte har möjlighet att hantera säkerhetsskyddsklassificerade uppgifter i egna lokaler, ska all dokumentation om säkerhetsprövning av leverantörens personal förvaras av den som ansvarar för säkerhetsskyddsavtalet.* s. 286

Moment 6:114 *När ett säkerhetsskyddsavtal upphör eller avslutas ska den dokumentation som finns om den som har säkerhetsprövats hos leverantören, överlämnas till den som* ansvarar för säkerhetsskyddsavtalet. s. 287

Kapitel 7 – Utbildning och övning

Moment 7:1 *En grundläggande säkerhetsgenomgång ska genomföras för Försvarsmaktens personal och uppdragstagare.* s. 291

Moment 7:2 *Den grundläggande säkerhetsgenomgången ska vara lärarledd.* s. 291

Moment 7:3 *Den grundläggande säkerhetsgenomgången ska ge personalen förståelse för:* s. 291

a) Säkerhetshotande verksamhet som riktas mot Försvarsmakten och aktuell lokal säkerhetshotbild.

b) Skyddsvärden (funktioner, system och anläggningar) som är skyddsvärda ur ett försvarsmakts- respektive lokalt perspektiv.

c) Aktuella risker kopplat till användning av internet, såsom e-post, surfning och sociala medier.

Moment 7:4 *Den grundläggande säkerhetsgenomgången ska ge personalen kunskap om:* s. 291

a) Lokal säkerhetsorganisation (t.ex. vem som är säkerhetschef, it-säkerhetschef och signalskyddschef samt eventuella säkerhetsmän).

b) Hur man kontaktar den lokala säkerhetsorganisationen.

c) Lokala säkerhetsbestämmelser (t.ex. rutiner för tillträde och besök).

d) Personalens skyldighet att rapportera säkerhetshotande händelser och verksamhet eller brister i säkerhetsskyddet samt hur rapportering genomförs lokalt.

e) Var man kan få mer information (t.ex. den lokala säkerhetsorganisationen på emilia och samarbetsytan Säkerhetstjänst i FM).

Moment 7:5 *En utbildning i säkerhetsskydd för Försvarsmaktens personal eller uppdragstagare som ska ta del av säkerhetsskyddsklassificerade uppgifter, ska minst omfatta:* s. 292

a) säkerhetshotande verksamhet,

b) informationssäkerhet,

c) it-säkerhet och

d) fysisk säkerhet.

Moment 7:6 *Om personal eller uppdragstagare endast vid enstaka tillfällen ska ta del av eller på annat sätt hantera säkerhetsskyddsklassificerade uppgifter upp till och med säkerhetsskyddsklass hemlig, får utbildningen i moment 7:5 anpassas så att den som utbildats inte av okunskap röjer säkerhetsskyddsklassificerade uppgifter.* s. 292

Moment 7:7 *Utbildningen i moment 7:5 ska ge deltagare följande kunskaper.* s. 292

Momentet är omfattande och återges inte i sin helhet här, se s. 292.

Kapitel 8 – Säkerhetsskyddad upphandling

Moment 8:1 *När organisationsenheten avser att avropa från ett ramavtal ska organisationsenheten först genomföra en analys enligt 8 kap. 1 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd.* s. 302

Moment 8:2 *Om ett uppdrag som avses upphandlas eller avropas rör säkerhetskänslig verksamhet ska analysen enligt 8 kap. 1 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd minst omfatta:* s. 302

a) En bedömning av lämpligheten från säkerhetsskyddssynpunkt att genomföra upphandlingen.

b) Vilken säkerhetshotande verksamhet som kan riktas mot uppdraget.

c) Identifiering av vilka organisationsenheter som kan påverkas av uppdraget.

d) Vilken omfattning en leverantör kommer att få ta del av eller hantera säkerhetsskyddsklassificerade uppgifter eller delta i säkerhetskänslig verksamhet.

Moment 8:3 *Om analysen enligt 8 kap. 1 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd visar att någon annan organisationsenhet påverkas av uppdraget ska den som är ansvarig för upphandlingen samverka med berörd organisationsenhet om vilken säkerhetskänslig verksamhet som berörs och behovet av säkerhetsskydd.* s. 302

Moment 8:4 *En särskild säkerhetsskyddsbedömning ska även genomföras om en upphandling ger leverantören tillgång till säkerhetskänslig verksamhet där den som deltar har möjlighet att orsaka allvarlig skada.* s. 304

Moment 8:5 *En begäran om samråd ska innehålla:* s. 305

a) Motivering till varför verksamheten behöver bedrivas utanför myndighetens lokaler.

b) Särskild säkerhetsskyddsbedömning.

c) Särskild säkerhetsskyddsplan.

d) Utkast till signalskyddskrav, om signalskydd ska användas.

e) Anbudsförfrågan.

f) Analys av vilka befattningar hos leverantören som ska placeras i säkerhetsklass samt vilket övrigt deltagande i den säkerhetskänsliga verksamheten som endast vara föremål för säkerhetsprövning utan registerkontroll.

g) Utkast till säkerhetsskyddsavtal.

h) Övriga dokument och krav som påverkar säkerhetsskyddet.

Moment 8:6 *En begäran om samråd ska skickas till säkerhetsskyddsavdelningen vid Must.* s. 305

Moment 8:7 *I en bedömning av en leverantörs lämplighet ska ägarförhållanden, ekonomiska förhållanden och kopplingar till säkerhetshotande verksamhet framgå.* s. 306

Moment 8:8 *En underleverantörs lämplighet ska bedömas om underleverantören* s. 306

a) kan få tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter utanför Försvarsmaktens lokaler, eller

b) kan få tillgång till säkerhetskänsliga informationssystem utanför Försvarsmaktens lokaler och obehörig åtkomst till systemen kan medföra ringa skada eller högre för Sveriges säkerhet, eller

c) kan få tillgång till säkerhetskänslig verksamhet där den som deltar har möjlighet att orsaka ringa skada eller högre för Sveriges säkerhet.

Moment 8:9 *Om en leverantör har bedömts vara olämplig får inte affärsavtal och säkerhetsskyddsavtal ingås.* s. 306

Moment 8:10 *Om Försvarsmakten avser att genomföra en upphandling av varor, tjänster eller byggentreprenader eller avropar från ett tecknat ramavtal (affärsavtal) ska Försvarsmakten vara part i säkerhetsskyddsavtalet.* s. 306

Moment 8:11 *Varje uppdrag, upphandling eller avrop från ramavtal (affärsavtal) ska omfattas av ett eget säkerhetsskyddsavtal.* s. 307

Moment 8:12 *Ett säkerhetsskyddsavtal ska innehålla bestämmelser som ger Försvarsmakten rätt att:* s. 307

a) ensidigt säga upp eller häva säkerhetsskyddsavtalet,

b) begära ersättning för Försvarsmaktens skada samt vite om leverantören bryter mot säkerhetsskyddsavtalet, samt

c) genomföra föranmälda och oanmälda säkerhetsskyddskontroller hos leverantören.

Moment 8:13 *Ett säkerhetsskyddsavtal ska innehålla bestämmelser om säkerhetsprövning av en leverantörs personal. Det ska framgå:* s. 308

a) vem som ansvarar för genomförandet,

b) att brister i pålitlighet, lojalitet och sårbarhet i säkerhänseende ska rapporteras till Försvarsmakten, och

c) att leverantören ska följa Försvarsmaktens beslut i ärende om säkerhetsprövning samt Försvarsmaktens omprövning av sådana beslut.

Moment 8:14 *Ett säkerhetsskyddsavtal ska innehålla bestämmelser som reglerar leverantörens skyldighet att till Försvarsmakten redovisa:* s. 308

a) förändringar avseende personer med betydande inflytande (PBI) hos leverantören, samt

b) förändringar i uppdraget som påverkar säkerhetsskyddet eller behov av säkerhetsskydd.

Moment 8:15 *Ett säkerhetsskyddsavtal ska utöver de krav som anges i lagar, förordningar, föreskrifter och andra bestämmelser omfatta de krav som tagits fram i den särskilda säkerhetsskyddsplanen.* s. 308

Moment 8:16 *Säkerhetsskyddsinstruktionen ska granskas och godkännas av organisationsenheten. Ett godkännande får inte lämnas före ett samråd enligt 2 kap. 6 § andra stycket 2 säkerhetsskyddsförordningen har ägt rum med säkerhetsskyddsavdelningen vid Must*. s. 309

Moment 8:17 *Ett säkerhetsskyddsavtal får inte ingås innan kontroll av leverantörens lokaler och övriga förhållanden är genomförda. En sådan kontroll ska inte genomföras om den bedöms vara uppenbart obehövlig. En sådan bedömning ska då dokumenteras.* s. 309

Moment 8:18 *Den som har tecknat ett säkerhetsskyddsavtal ska genom SUA-rutinen i IS UNDSÄK meddela säkerhetsskyddsavdelningen vid Must om avtalet. Uppgifter om diarienummer för säkerhetsskyddsavtalet och affärsavtalet ska ingå.* s. 309

Moment 8:19 *Den särskilda säkerhetsskyddsbedömningen, den särskilda säkerhetsskyddsanalysen och den särskilda säkerhetsskyddsplanen ska uppdateras när:* s. 310

e) ägarförhållanden förändras som leder till förändringar i vilka som har inflytande över leverantören,

f) leverantören kommer ta del av säkerhetsskyddsklassificerade uppgifter i en högre säkerhetsskyddsklass än vad som ursprungligen var bedömt,

g) leverantörens personal kommer att delta i en säkerhetskänslig verksamhet och till följd av sitt deltagande har möjlighet att orsaka större skada för Sveriges säkerhet än vad som ursprungligen var bedömt, eller

a) en kontroll av leverantörens säkerhetsskydd visar att leverantören inte har följt säkerhetsskyddsavtalet.

Moment 8:20 *Den som har ingått ett säkerhetsskyddsavtal ska underrätta säkerhetsskyddsavdelningen vid Must när ett säkerhetsskyddsavtal har upphört att gälla.* s. 311

Kapitel 9 – Kontroll av säkerhetsskydd

Moment 9:1 *Säkerhetschefen vid en organisationsenhet eller enhet i Högkvarteret ska leda interna kontroller av säkerhetsskyddet inom den egna verksamheten.*	s. 313
Moment 9:2 *Vid en intern kontroll av säkerhetsskyddet ska rutiner prövas för hur incidenter och störningar i den säkerhetskänsliga verksamheten ska hanteras.*	s. 313
Moment 9:3 *Säkerhetsskyddsavdelningen vid Must ska ta fram den årliga planen för extern kontroll av säkerhetsskyddet i Försvarsmakten. Planens innehåll ska samordnas med underrättelse- och säkerhetsavdelningen vid insatsledningen i Högkvarteret (INSS J2).*	s. 315
Moment 9:4 *Försvarsmaktens årliga plan för extern kontroll av säkerhetsskyddet ska upprättas i samverkan med den som ska kontrolleras.*	s. 315
Moment 9:5 *Om det för en viss verksamhet har utsetts en säkerhetschef, en signalskyddschef eller en it-säkerhetschef ska den verksamheten kontrolleras. Vem som ska genomföra den externa kontrollen ska framgå av den reglering som beskriver verksamhetens säkerhetsorganisation och lydnadsförhållanden.*	s. 315
Moment 9:6 *I de fall som den som är bemyndigad att teckna avtal för sin egen verksamhet har tecknat ett säkerhetsskyddsavtal är den även ansvarig för att säkerhetsskyddet hos leverantören kontrolleras.*	s. 316
Moment 9:7 *Om ett säkerhetsskyddsavtal med en leverantör har tecknats av någon annan än organisationsenheten och det finns ett behov av att genomföra en kontroll av säkerhetsskyddet hos leverantören, ska behovet anmälas till den som har tecknat avtalet.*	s. 316
Moment 9:8 *Protokoll från interna kontroller av säkerhetsskyddet ska förvaras samlade hos den som har genomfört kontrollen.*	s. 316
Moment 9:9 *Ett protokoll från en extern kontroll av säkerhetsskyddet ska inom tre månader vara den kontrollerade tillhanda, om inte annat är överenskommet. En kopia på protokollet ska även ställas till säkerhetsskyddsavdelningen vid Must, J2 vid INSS och den militärregionstab i den militärregion som organisationsenheten är placerad i.*	s. 316
Moment 9:10 *Ett protokoll från en extern kontroll av säkerhetsskyddet ska minst omfatta:* *a) Behov av omedelbara säkerhetsskyddsåtgärder.* *b) Brister i säkerhetsskyddet som ska åtgärdas med hänvisning till regelverk eller säkerhetsskyddsavtal.* *c) Ansvaret för att vidta tvingande säkerhetsskyddsåtgärder (om det finns flera verksamhetsansvariga).* *a) Datum när den kontrollerade ska uppvisa en åtgärdsplan som reglerar hur identifierade brister i säkerhetsskyddet ska omhändertas.*	s. 316

Moment 9:11 *Den som vid en kontroll av säkerhetsskyddet har brister i säkerhetsskyddet ska upprätta en åtgärdsplan. Planen ska redovisas för den som har genomfört kontrollen.* s. 317

Moment 9:12 *Den som genomfört en kontroll av säkerhetsskyddet ska även följa upp att brister åtgärdas enligt en upprättad åtgärdsplan. Uppföljningen genomförs på det sätt som den som har genomfört kontrollen bestämmer.* s. 317

Kapitel 10 – Säkerhetsrapportering

Moment 10:1 *När säkerhetsorganisationen vid en organisationsenhet har tagit emot en säkerhetsrapport ska rapporten lämnas till militärregionstaben i den militärregion som organisationsenheten är placerad i. Militärregionstaben ansvarar för att åtgärder vidtas. Militärregionstaben ska se till att säkerhetsrapporten vidarebefordras till:* s. 325

a) insatsledningen i Högkvarteret, och

b) säkerhetskontoret vid Must.

Moment 10:2 *När säkerhetsorganisationen vid en kontingent i en internationell militär insats har tagit emot en säkerhetsrapport ska rapporten lämnas till den försvarsgrensstab som ansvarar för kontingenten. Försvarsgrensstaben ska se till att säkerhetsrapporten vidarebefordras till:* s. 325

a) insatsledningen i Högkvarteret, och

b) *säkerhetskontoret vid Must.*

Moment 10:3 *En säkerhetsrapport som rör organisationsenhetens säkerhetsorganisation ska lämnas direkt till staben för den militärregion som organisationsenheten är placerad i. Militärregionstaben ska vidarebefordra rapporten till insatsledningen i Högkvarteret och säkerhetskontoret vid Must.* s. 325

Moment 10:4 *En säkerhetsrapport som rör säkerhetsorganisationen vid en militärregionstab ska endast lämnas till insatsledningen i Högkvarteret. Insatsledningen ska vidarebefordra rapporten till säkerhetskontoret vid Must.* s. 326

Moment 10:5 *En säkerhetsrapport som rör säkerhetsorganisationen vid FMTIS stab, Högkvarteret eller SOG ska endast lämnas till säkerhetskontoret vid Must.* s. 326

Moment 10:6 *En säkerhetsrapport, förutom säkerhetsrapport i personärende enligt 8 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd, ska diarieföras i underrättelse- och säkerhetsdiariet vid Must.* s. 331

Kapitel 11 – Incidenter och avvikelser

Kapitlet saknar moment.

Bilaga 2 – Undantag

Tabellen är en sammanställning över vem som ansöker om, vem som leder beredning samt vem som beslutar i ärenden om undantag från bestämmelser i författningar samt detta reglemente. I avsnitt 1.10.1 och 1.10.5 beskrivs undantag från bestämmelser i författningar. I avsnitt 1.10.1 och 1.10.4 beskrivs undantag från bestämmelser i detta reglemente.

Från vilken bestämmelse som undantaget avser	Vem som ansöker	Vem som leder beredningen	Vem som beslutar i ärendet
3 kap. 4 § första stycket säkerhetsskyddsförordningen (avsnitt 4.9)	Myndigheter inom Försvarsmaktens tillsynsområde, inklusive Försvarsmakten.	C Must[243]	ÖB[244]
3 kap. 5 § andra stycket säkerhetsskyddsförordningen (avsnitt 4.8.9)	Alla verksamhetsutövare, inklusive Försvarsmakten.	C Must[245]	C Must[246]
Försvarsmaktens föreskrifter om signalskyddstjänsten	Alla verksamhetsutövare, inklusive Försvarsmakten.	C Must[247]	ÖB[248]
Försvarsmaktens föreskrifter om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar	Myndigheter inom Försvarsmaktens tillsynsområde, inklusive Försvarsmakten.	C Must[249]	ÖB
Försvarsmaktens föreskrifter om säkerhetsskydd	Myndigheter inom Försvarsmaktens tillsynsområde, men inte Försvarsmakten.	C Must[250]	ÖB[251]
Försvarsmaktens föreskrifter om säkerhetsskydd, men inte avseende it-säkerhet	Försvarsmakten	C Must[252]	ÖB[253]

[243] 11 kap. 5 § första stycket FM ArbO.
[244] 6 kap. 1 § 24 FM ArbO.
[245] 11 kap. 5 § första stycket FM ArbO.
[246] 11 kap. 12 § 11 FM ArbO.
[247] 11 kap. 5 § andra stycket 2 FM ArbO.
[248] 6 kap. 1 § Försvarsmaktens föreskrifter om signalskyddstjänsten.
[249] 11 kap. 5 § andra stycket 3 FM ArbO.
[250] 11 kap. 5 § andra stycket 1 FM ArbO.
[251] 12 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd.
[252] 11 kap. 5 § andra stycket 1 FM ArbO.
[253] 12 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Från vilken bestämmelse som undantaget avser	Vem som ansöker	Vem som leder beredningen	Vem som beslutar i ärendet
Försvarsmaktens föreskrifter om säkerhetsskydd, avseende it-säkerhet	Försvarsmakten	FM CIO[254]	ÖB[255]
Försvarsmaktens interna bestämmelser om it-säkerhet	Försvarsmakten	FM CIO[256]	ÖB[257]
Försvarsmaktens interna bestämmelser om säkerhetsskydd	Försvarsmakten	FM säkerhetsskyddschef[258]	ÖB[259]
Försvarsmaktens interna bestämmelser om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar	Försvarsmakten	FM säkerhetsskyddschef[260]	ÖB
Försvarsmaktens interna bestämmelser om signalskyddstjänsten	Försvarsmakten	FM säkerhetsskyddschef[261]	ÖB[262]
Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar	Försvarsmakten	Ej reglerat	ÖB[263]
Reglemente säkerhetstjänst	Organisationsenhet Enhet i Högkvarteret Kontingent i en internationell militär insats	Säkerhetsskyddsavdelningen vid Must[264]	Försvarsmaktens säkerhetsskyddschef[265]

[254] 8 kap. 35 § FM ArbO.
[255] 12 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd.
[256] 8 kap. 35 § FM ArbO.
[257] 16 kap. 1 § Försvarsmaktens interna bestämmelser om it-säkerhet.
[258] 11 kap. 23 § tredje stycket FM ArbO.
[259] 9 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd.
[260] 11 kap. 23 § tredje stycket FM ArbO.
[261] 11 kap. 23 § tredje stycket FM ArbO.
[262] 37 § Försvarsmaktens interna bestämmelser om signalskyddstjänsten.
[263] 4 kap. 1 § Försvarsmaktens interna bestämmelser (FIB 2015:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
[264] Moment 1:9.
[265] Moment 1:10.

Redaktionell information

Efter att ny säkerhetsskyddslag, säkerhetsskyddsförordning och Försvarsmaktens föreskrifter om säkerhetsskydd trädde i kraft den 1 april 2019 har det funnits ett behov av att se över Försvarsmaktens interna styrdokument. Krav i lag, förordning och föreskrifter behöver ofta brytas ner i detaljerade krav och anpassas så att administrativa och tekniska åtgärder blir ändamålsenliga och ger ett effektivt säkerhetsskydd.

Det har även funnits ett behov av att se över strukturen av styrdokument. Detaljerade bestämmelser om åtgärder som tidigare funnits i FIB har förts över till reglementet. Ett reglemente för säkerhetstjänst har inte funnits tidigare. FM ArbO och Försvarsmaktens interna bestämmelser om säkerhetsskydd är nu tydligare i vilka uppgifter och bemyndiganden som chefer i Högkvarteret respektive chefer för organisationsenheterna har.

Reglementet har tagits fram av en expertgrupp vid säkerhetskontoret på Must. Det har internberetts inom säkerhetskontoret 2020-03-12--16 samt inom Försvarsmakten 2020-03-23--04-20. LEDS JUR har granskat förslaget till reglemente och lämnat synpunkter samt varit ett stöd för momentens utformning. Förslaget har även publicerats på samarbetsytan Säkerhetstjänst i FM. Inkomna synpunkter har behandlats av berörda ämnesexperter i expertgruppen. Ett reviderat förslag publicerades på samarbetsytan 2020-07-09--09-07.

För de delar av reglementet som rör informationssäkerhet inklusive it-säkerhet, samt it-säkerhet som inte omfattas av säkerhetsskyddslagen ska FM CIO ha lämnat samråd innan Försvarsmaktens säkerhetsskyddschef beslutar reglementet. FM CIO lämnade samråd 2020-10-05.

Ämnesexperter som har medverkat i skrivarbetet: Anders Bengtsson, Ebba Skygge, Jörgen Nilsson, Kim Hakkarainen, Kristoffer Månsson, Maria Lind, Mårten Karlsson, Rolf Dahlman, Sanna Jonsson, Therése Palmqvist, Tomas Borg, Tseciay Tewelde och Zenobia Rosander.

Projektledare: Kim Hakkarainen och Zenobia Rosander

Redaktör: Kim Hakkarainen

Bildförteckning

I denna publikation förkommer följande bilder med verkshöjd.

Illustratör anges med namn och organisatorisk tillhörighet.

Bild nr	Fotograf/Illustratör	Hur FM säkrat rätten att använda bilden
0.1 2.8 3.3 3.18-3.23	Kim Hakkarainen, Must	Avtal om nyttjanderätt av illustrationer FM2016-24552:5
6.1-2	Maria Lind, Must	Avtal om nyttjanderätt av illustrationer FM2020-22717:1
	Sanna Jonsson, Must	Avtal om nyttjanderätt av illustrationer FM2020-22712:1

Källförteckning

I den här utgåvan av reglementet har följande källor använts.

- Arkivförordningen (1991:446).
- Arkivlagen (1990:782).
- Brottsbalken.
- Europeiska unionens råd. 2013/488/EU. *Rådets beslut av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter.*
- Förordning (1982:756) om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet, m.m. (IKFN-förordning).
- Förordningen (2007:1266) med instruktion för Försvarsmakten.
- Förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.
- Förordningen (1999:1134) om belastningsregister.
- Förordningen (1994:524) om frivillig försvarsverksamhet.
- Förordningen (FFS 1987:8) om frivillig tjänstgöring vid Försvarsmakten.
- Förordningen (1996:927) om Försvarsmaktens personal.
- Förordningen (1998:896) om hushållning med mark och vattenområden.
- Förordningen (2015:613) om militär grundutbildning.
- Förordningen (1999:1135) om misstankeregister.
- Förordningen (2005:801) om restriktioner för luftfart inom vissa områden.
- Förordningen (2016:320) om skydd för geografisk information.
- Förordningen (1996:31) om statliga myndigheters skjutvapen m.m.
- Förordningen (1958:272) om tjänstekort.
- Förordningen (2010:649) om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet.
- Förordningen (1996:442) om utländska besök vid vissa myndigheter inom Försvarsdepartementets verksamhetsområde.
- Försvarsdepartementet. Regeringsbeslut 5 2019-12-19, Bilaga 4 till Regleringsbrev för budgetåret 2020 avseende Försvarsmakten. *Riktlinjer för den militära säkerhetstjänsten.*
- Förenta nationerna. ST/SGB/2007/6. Secretary-General's bulletin. *Information sensitivity, classification and handling.*
- Förvaltningslagen (2019:900).
- Hemvärnsförordningen (1997:146).
- Justitiedepartementet. Broschyr 2019. *Offentlighetsprincipen och sekretess – Kortfattat om lagstiftningen.*
- Kamerabevakningslagen (2018:1200).
- Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
- Lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

REGLEMENTE

- Lagen (2000:130) om försvarsunderrättelseverksamhet.
- Lagen (2016:319) om skydd för geografisk information.
- Lagen (2003:148) om straff för terroristbrott.
- Lagen (1994:1809) om totalförsvarsplikt.
- Lagen (1992:1402) om undanförsel och förstöring.
- Lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet.
- Lantmäteriets föreskrifter (LMFS 2016:1) om spridningstillstånd för sammanställningar av landgeografisk information.
- Miljöbalken.
- Myndighetsförordningen (2007:515).
- Offentlighets- och sekretessförordningen (2009:641).
- Offentlighets- och sekretesslagen (2009:400).
- Officersförordningen (2007:1268).
- Personuppgiftslagen (1998:204).
- Plan- och bygglagen (2010:900).
- Polislagen (1984:387).
- Proposition 2017/18:89. *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag.*
- Proposition 1975/76:160. *Om nya grundlagsbestämmelser angående allmänna handlingars offentlighet.*
- Proposition 1992/93:78. *Om undanförsel och förstöring.*
- Proposition 2016/17:180. *En modern och rättssäker förvaltning – ny förvaltningslag.*
- Proposition 2018/19:127. *Skyddsobjekt och obemannade farkoster.*
- Regeringsformen.
- Riksarkivets föreskrifter (RA-MS 2018:42) och allmänna råd om gallring hos Fortifikationsverket, Försvarets materielverk, Försvarsmakten, Totalförsvarets forskningsinstitut och Totalförsvarets rekryteringsmyndighet.
- Riksarkivets föreskrifter (RA-MS 2014:38) om bevarande i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten hos Försvarsmakten.
- Sambolagen (2003:376).
- Skyddslagen (2010:305).
- SOU 2015:25. Utredningen om säkerhetsskyddslagen. *En ny säkerhetsskyddslag.*
- SOU 2013:51. Utredningen om skydd för geografisk information. *Skydd för geografisk information.*
- Säkerhetspolisen. Juni 2019. *Säkerhetspolisens vägledning i säkerhetsskydd – Personalsäkerhet.*
- Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.
- Säkerhetsskyddsförordningen (2018:658).
- Säkerhetsskyddslagen (2018:585).
- Tryckfrihetsförordningen.

<u>Källor inom Försvarsmakten</u>

- Doktrintillägg underrättelse- och säkerhetstjänst (DTLG UNDSÄK 19) (M7739-354029).

- Upphävt beslut: Godkännande av distributör för postdistribution av hemliga handlingar (FM2015-8736:1).
- Upphävd instruktion: Instruktion avseende kunskapskrav säkerhetstjänst (2012-03-16 HKV 10 700:50011).
- Upphävd instruktion: Instruktion avseende säkerhetsprövning (2013-06-18 HKV 10 730:58639).
- Upphävd publikation: Handbok för Försvarsmaktens säkerhetstjänst, Hotbedömning (H Säk Hot), 2006 års utgåva (M7745-734022).
- Handbok för Försvarsmaktens säkerhetstjänst, Informationssäkerhet (H SÄK Infosäk), 2013 års utgåva (M7739-352056).
- Handbok för Försvarsmaktens säkerhetstjänst, Sekretessbedömning Del A (H Säk Sekrbed A), 2011 års utgåva (M7739-352028).
- Upphävt meddelande: Kommentarer till Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd (FM2019-11683:1).
- Upphävd specifikation: Utformning av sekretessmarkering och säkerhetsskyddsklasser i Försvarsmakten (FM2019-14769:1 och FM2019-14769:2).

Regler, bestämmelser och handböcker som påverkat innehållet i detta reglemente

FFS 2019:7	Försvarsmaktens föreskrifter om befordran och konstituering
FFS 2007:1	Försvarsmaktens föreskrifter om hantering, förvaring och transport av skjutvapen och ammunition
FFS 2019:6	Försvarsmaktens föreskrifter om personaltjänst
FFS 2019:9	Försvarsmaktens föreskrifter om signalskyddstjänsten
FFS 2019:2	Försvarsmaktens föreskrifter om säkerhetsskydd
	Försvarsmaktens föreskrifter om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar
FIB 2020:3	Försvarsmaktens interna bestämmelser med arbetsordning för Försvarsmakten (FM Arbo)
FIB 2013:5	Försvarsmaktens interna bestämmelser om hantering, förvaring och transport av skjutvapen och ammunition
FIB 2017:8	Försvarsmaktens interna bestämmelser om it-säkerhet
FIB 2017:11	Försvarsmaktens interna bestämmelser om it-verksamhet
FIB 2008:3	Försvarsmaktens interna bestämmelser om signalskyddstjänsten
FIB 2015:1	Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

REGLEMENTE

FIB 2020:4	Försvarsmaktens interna bestämmelser om säkerhetsskydd
	Försvarsmaktens interna bestämmelser om säkerhetsskydd för särskilda underrättelseuppgifter och -handlingar
FIB 2017:7	Försvarsmaktens interna bestämmelser om tjänstekort och vissa behörighetshandlingar
FFS 2010:5	Försvarsmaktens skyddsföreskrifter

Reglementet innehåller bestämmelser för hur militär säkerhetstjänst ska genomföras i Försvarsmakten avseende säkerhetsskyddsplanering (inklusive identifiering av hot och sårbarheter), informationssäkerhet, fysisk säkerhet, personalsäkerhet, utbildning och övning, säkerhetsskyddad upphandling, kontroll och tillsyn samt säkerhetsrapportering.

Reglementet förklarar författningskrav inom den militära säkerhetstjänstens område, främst bestämmelser om säkerhetsskydd.

FÖRSVARSMAKTEN

107 85 Stockholm
www.forsvarsmakten.se

R SÄK 2021
M7739-353149