Ert tjänsteställe, handläggare | Ert datum | Er beteckning

Vårt tjänsteställe, handläggare | Vårt föregående datum | Vår föregående beteckning

Zenobia Rosander, zenobia.rosander@mil.se
Ebba Skygge, ebba.skygge@mil.se

Kommentarer till Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd

Den 1 april 2019 trädde säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2018:685) i kraft. Av lagstiftningen följer att Försvarsmakten får meddela föreskrifter för Fortifikationsverket och Försvarshögskolan och de myndigheter som hör till Försvarsdepartementet. Överbefälhavaren beslutade Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd den 27 februari 2019. Föreskrifterna trädde ikraft samma dag som säkerhetsskyddslagen och dess förordning.

För att ge en bättre förståelse för föreskrifternas innebörd har säkerhetskontoret vid den militära underrättelse- och säkerhetstjänsten utarbetat kommentarer till dessa. Kommentarerna är endast av vägledande karaktär. Endast vissa bestämmelser kommenteras. Det är därför viktigt att även ha tillgång till lag och förordning samt Försvarsmaktens föreskrifter om säkerhetsskydd när ärenden som rör säkerhetsskydd ska beredas.

Den primära målgruppen för kommentarerna är personal inom Försvarsmakten som arbetar i säkerhetstjänsten. Kommentarerna får dock även användas av myndigheten i övrigt samt av de myndigheter som Försvarsmakten utövar tillsyn över.

Kommentarerna kommer även att tillgängliggöras på Försvarsmaktens webbplats, forsvarsmakten.se/must.

Postadress	Besöksadress	Telefon	Telefax	E-post, Internet
Högkvarteret	Lidingövägen 24	08-788 75 00	08-788 77 78	exp-hkv@mil.se
107 85 Stockholm				www.forsvarsmakten.se/hkv

1 kap. Allmänna bestämmelser

1 § Denna författning gäller för Fortifikationsverket, Försvarshögskolan samt de myndigheter som hör till Försvarsdepartementet.

Kommentar: I 7 kap. 5 § punkterna 2 och 3 säkerhetsskyddsförordningen bemyndigas Försvarsmakten att meddela ytterligare föreskrifter om säkerhetsskyddsanalys, anmälnings- och rapporteringsskyldighet, säkerhetsskyddsåtgärder, säkerhetsskyddsklassificering och säkerhetsskyddsavtal samt verkställigheten av säkerhetsskyddslagen för sitt tillsynsområde.

Försvarsmakten utövar tillsyn över Försvarets radioanstalt, Försvarets materielverk, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet, Statens inspektion för försvarsunderrättelseverksamheten, Försvarsunderrättelsedomstolen, Fortifikationsverket och Försvarshögskolan.[1]

2 § I denna författning används följande begrepp med nedan angiven betydelse.

Begrepp	**Betydelse**
Elektronisk handling	Upptagning enligt 2 kap. 3 § tryckfrihetsförordningen som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel (upptagning för automatiserad behandling).
Elektroniskt kommunikationsnät	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.
Handling	Detsamma som anges i 2 kap. 3 § tryckfrihetsförordningen.
It-utrymme	Utrymme som innehåller växlar, korskopplingar och servrar samt datorhallar.
Lagringsmedium	Permanent minnesmedium som används för att kunna lagra och läsa uppgifter.
Skadlig kod	Otillåten programkod som är till för att ändra,

[1] 7 kap. 1 § första stycket 1 säkerhetsskyddsförordningen.

	röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett informationssystem.
Säkerhetskänslig verksamhet	Detsamma som anges i 1 kap. 1 § säkerhetsskyddslagen (2018:585).
Säkerhetsskyddsklassificerad handling	Detsamma som anges i 1 kap. 4 § säkerhetsskyddsförordningen (2018:658).
Säkerhetsskyddsklassificerat lagringsmedium	Lagringsmedium som innehåller eller är avsett att innehålla säkerhetsskyddsklassificerade uppgifter, om uppgifterna inte är krypterade med kryptografiska funktioner som har godkänts av Försvarsmakten.
Säkerhetsskyddsklassificerade uppgifter	Detsamma som anges i 1 kap. 2 § säkerhetsskyddslagen (2018:585).

Kommentar:

Handling: Enligt 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.

Lagringsmedium: Ett permanent minnesmedium används för att kunna lagra och läsa uppgifter. Ett permanent minnesmedium är ”icke-flyktigt”, dvs. det behöver inte vara anslutet till ström för att behålla lagrade data. Exempel på permanent minnesmedium är lagringsmedium 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.

Säkerhetskänslig verksamhet: Verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

För att säkerhetsskyddslagen ska vara tillämplig krävs inte att hela verksamheten ska utgöra säkerhetskänslig verksamhet, utan det är tillräckligt att någon del av verksamheten utgör säkerhetskänslig verksamhet för att lagen ska vara tillämplig på den verksamheten.

Begreppet Sveriges säkerhet har ersatt rikets säkerhet men det utgör i huvudsak endast en språklig korrigering. Sveriges säkerhet tar sikte på förhållande av grund-

läggande betydelse för Sverige[2]. Säkerhetsskyddslagen gäller för såväl militär som civil verksamhet.

Några exempel på uppgifter vid civila verksamheter som rör den nationella säkerheten är t.ex. uppgifter om viktig civil infrastruktur såsom flygplatser, energianläggningar och konstruktion av produkter inom telekommunikationsområdet.[3]

Alla delar i en verksamhet som har betydelse för Sveriges säkerhet är säkerhetskänslig verksamhet. Det kan t.ex. röra sig om uppgifter som är säkerhetsskyddsklassificerade (se förklaring av begreppet säkerhetsskyddsklassificerad uppgift nedan) 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.[4]

Med uttrycket ”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. Sverige har ingått ett flertal generella säkerhetsskyddsavtal, s.k. GSA, både bilateralt med andra länder och mellanfolkliga organisationer (t.ex. Nato), och multilateralt med flera länder (t.ex. de nordiska länderna).

Säkerhetsskyddsklassificerad handling: En handling som innehåller en säkerhetsskyddsklassificerad uppgift enligt 1 kap. 2 § säkerhetsskyddslagen. Se vidare kommentarer till säkerhetsskyddsklassificerade uppgifter nedan.

Säkerhetsskyddsklassificerade uppgifter: 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. Särskilt relevant för vägledning i fråga om vilka uppgifter som till sin natur medför krav på säkerhetsskydd är den s.k. försvarssekretessen i 15 kap. 2 § OSL. Sådana uppgifter är alltid säkerhetsskyddsklassificerade uppgifter. Uppgifter som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande omfattas i regel av bestämmelser om sekretess i förhållande till annan stat eller mellanfolklig organisation, den s.k. utrikessekretessen i 15 kap. 1 § OSL. Även andra sekretessbestämmelser kan komma i fråga.[5]

[2] Prop. 2017/18:89, s. 133, Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag, och prop. 2013/14:51 s. 36, Förstärkt skydd mot främmande makts underrättelseverksamhet.
[3] Prop. 2017/18:89 s. 133.
[4] Prop. 2017/18:89 s. 134.
[5] Prop. 2017/18:89 s. 52.

3 § 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.

Kommentar: 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[6]. Ett fel kan t.ex. vara när någon upptäcker att ett hål i ett stängsel till ett skyddsobjekt. Myndigheten behöver därför rutiner för att kunna upptäcka, bedöma och hantera sådana situationer.

Myndigheten bör ta fram rutiner för t.ex. vad som ska åtgärdas då det upptäcks att ett säkerhetsskåp som innehåller säkerhetsskyddsklassificerade uppgifter har stått olåst eller då t.ex. ett USB-minne påträffas i en dator i ett gemensamt informationssystem. 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.

4 § För signalskyddstjänsten inklusive kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet ska Försvarsmaktens föreskrifter om signalskyddstjänsten tillämpas istället för denna författning.

Kommentar: Det finns inga kommentarer till denna föreskrift.

Särskilda underrättelseuppgifter och särskilda underrättelsehandlingar

5 § För särskilda underrättelseuppgifter och särskilda underrättelsehandlingar gäller även Försvarsmaktens föreskrifter om säkerhetsskydd för särskilda underrättelseuppgifter och särskilda underrättelsehandlingar.

Kommentar: Bestämmelsen är en upplysning om att särskilda underrättelseuppgifter och särskilda underrättelsehandlingar även omfattas av ett regelverk om

[6] Prop. 2017/18:89 s. 50.

särskilt säkerhetsskydd.[7] Innehållet i regelverket omfattas av sekretess enligt 15 kap. 2 § OSL.

[7] Bilaga 1 till HKV 2011-10-28 H/C 10 810:81980.

2 kap. Säkerhetsskyddsplanering

1 § I 2 kap. 1 § säkerhetsskyddslagen (2018:585) och 2 kap. 1 § säkerhetsskyddsförordningen (2018:658) finns föreskrifter om säkerhetsskyddsanalys och att säkerhetsskyddsanalysen ska omfatta vilka hot och sårbarheter som finns kopplade till myndighetens skyddsvärden.

Kommentar: Paragrafen innehåller en upplysning om vad som gäller enligt lag och förordning.

Bestämmelserna i lagen och förordningen innebär att myndigheten har en skyldighet att utreda behovet av säkerhetsskydd i en säkerhetsskyddsanalys. Avgörande för behovet av säkerhetsskydd är bl.a. vilka hot, skyddsvärden och sårbarheter som kan finnas i verksamheten. Av lagen framgår att säkerhetsskyddsanalysen ska dokumenteras.

Analysen ska enligt förordningen identifiera vilka säkerhetsskyddsklassificerade uppgifter som förekommer i verksamheten och vad som i övrigt behöver ett säkerhetsskydd i verksamheten. Analysen ska alltså även identifiera vilken säkerhetskänslig verksamhet som myndigheten bedriver.

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

Kommentar: 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.[8] 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 tydligt 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.[9]

[8] Prop. 2017/18:89, s. 56.
[9] Prop. 2017/18:89, s. 50.

I 9 kap. 1 § finns föreskrifter om myndighetens kontroll av säkerhetsskyddet. Detta krav innefattar även att säkerhetsskyddet ska vara anpassat till aktuell säkerhetsskyddsplanering.

3 § En säkerhetsskyddsanalys ska innehålla en beskrivning av myndighetens verksamhet och organisation samt dess skyddsvärden (verksamhetsbeskrivning).

Myndigheten ska beakta Försvarsmaktens dimensionerande hotbeskrivning och ta fram en hotbild som är relevant, anpassad och aktuell i förhållande till den säkerhetskänsliga verksamheten.

Kommentar: *Första stycket:* För att göra det möjligt att urskilja vilka delar av verksamheten som utgör säkerhetskänslig verksamhet, och som därmed ska ges ett säkerhetsskydd, behöver verksamhets- och organisationsbeskrivningen omfatta hela myndigheten. Bestämmelsen utgör dock inget hinder mot att komplettera myndighetens övergripande säkerhetsskyddsanalys med nedbrutna säkerhetsskyddsanalyser och säkerhetsskyddsplaner för specifika verksamheter eller lokala förhållanden. I sådana fall bör det dock finnas en spårbarhet mellan dokumenten och de behöver också vara koordinerade för att myndighetens ledning kan ta ansvar för en sammanhållen säkerhetsskyddsplanering och ge identifierade skyddsvärden ett likvärdigt säkerhetsskydd oavsett var i myndigheten de finns.

Andra stycket: Försvarsmaktens dimensionerande hotbeskrivning utgörs av rapporten Säkerhetsunderrättelseårsbedömande (SÅB). SÅB ges ut årligen, normalt i maj, av den militära underrättelse- och säkerhetstjänstens säkerhetsunderrättelseavdelning i Högkvarteret.

Hotbilden ska främst ge långsiktiga planeringsförutsättningar. Hotbilden kan vidare med fördel utgå från dimensionerande hotaktörers förmåga, samt tydliggöras med rimliga typfall som säkerhetsskyddet ska vara dimensionerat att hantera - utifrån perspektivet acceptabla konsekvenser för Sveriges säkerhet. Hotbilden kan vid behov kompletteras med aktualiserade specifika hot som kräver kompletterande säkerhetsskyddsåtgärder tillfälligt eller permanent.

4 § 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.

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.

Kommentar: *Första stycket:* Säkerhetsskyddsåtgärder kan vara kostsamma, effektivitetshämmande och integritetskränkande. Enligt 2 kap. 1 § säkerhetsskyddslagen ska åtgärderna så långt det är möjligt utformas så att de inte medför någon

skada eller annan olägenhet för andra allmänna eller enskilda intressen. Det är alltså 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.

Andra stycket: Trots att säkerhetsskyddslagen främst är avsedd att skydda mot antagonistiska hot, så påverkas den säkerhetskänsliga verksamheten även av avbrott och störningar som inte är aktörsdrivna. Exempel är olyckshändelser eller naturkatastrofer. Sådana händelser påverkar särskilt tillgänglighet till verksamheten. Bestämmelsen ger därför möjlighet att även ta hänsyn till sådana störningar, om den potentiella skadan är mer än ringa.

5 § Innan myndighetens säkerhetsskyddsanalys och säkerhetsskyddsplan beslutas ska myndighetens ledning orienteras.

Kommentar: Myndighetens ledning ska orienteras därför att det är den som kan tilldela budget och resurser för de säkerhetsåtgärder som ska implementeras. Myndighetens ledning har också ansvaret för om säkerhetsskyddet brister. Därför kan det även vara lämpligt att överbefälhavaren fastställer Försvarsmaktens säkerhetsskyddsanalys och säkerhetsskyddsplan.

3 kap. Informationssäkerhet

Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter

1 § 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.

Kommentar: *Första stycket:* I 2 kap. 3 § säkerhetsskyddsförordningen finns tre villkor som ska vara uppfyllda för att en person ska få ta del av säkerhetsskyddsklassificerade uppgifter. Om inte något annat följer av bestämmelser i lag, ska personen ha bedömts vara pålitlig från säkerhetssynpunkt (dvs. säkerhetsprövad), ha tillräckliga kunskaper om säkerhetsskydd, och behöva uppgifterna för att kunna utföra sitt arbete.

Andra stycket: 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. då behörigheter läggs in i ett informationssystem, då en person tar emot en sådan säkerhetsskyddsklassificerad handling eller lagringsmedium från myndighetens registratur eller deltar i ett möte där sådana uppgifter kommer att delges.

Myndigheten kan ha 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 då personer avslutat sin anställning eller deltagande i myndighetens verksamhet. Det är därför lämpligt att använda namn och personnummer i förteckningen.

Det är lämpligt att det på behörighetsförteckningen framgår vem som har beslutat att en person ska tas med på förteckningen.

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.

2 § Om inget annat anges, avses med säkerhetsskyddsklassificerad handling även säkerhetsskyddsklassificerad elektronisk handling.

Med begreppet säkerhetsskyddsklassificerad handling avses både allmänna och icke allmänna handlingar.

Kommentar: 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.

Materiel och tryckta skrifter

3 § Materiel som innehåller säkerhetsskyddsklassificerade uppgifter ska ges ett säkerhetsskydd som motsvarar vad som gäller för säkerhetsskyddsklassificerade lagringsmedier.

Bestämmelser om säkerhetsskyddsklassificerade lagringsmedier finns även i 4 kapitlet.

Kommentar: 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.

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

Kommentar: Handlingar som ingår i en myndighets bibliotek är undantagna från att vara allmänna handlingar, enligt det så kallade biblioteksundantaget i 2 kap. 11 § första stycket 3 tryckfrihetsförordningen. Bestämmelsen syftar till att ge publikationer och andra tryckta skrifter som innehåller säkerhetsskyddsklassificerade uppgifter 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 materielpublikationer, reglementen, manualer och handböcker som innehåller säkerhetsskyddsklassificerade uppgifter. Ett annat exempel är kartor och sjökort som innehåller säkerhetsskyddsklassificerade uppgifter.

Lån av säkerhetsskyddsklassificerade handlingar

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

Kommentar: 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.

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.

Anteckning om säkerhetsskyddsklass

6 § 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).

Kommentar: *Första meningen:* Paragrafen innehåller en upplysning om vad som gäller enligt lag och förordning.

I 5 kap. 5 § första stycket OSL framgår att 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 en särskild anteckning (sekretessmarkering) på handlingen. Om handlingen är elektronisk införs sekretessmarkeringen i handlingen eller i det system där den elektroniska handlingen hanteras.

I 5 kap. 5 § första stycket OSL finns krav på vad som ska anges i en sekretessmarkering. Det är upp till myndigheten att avgöra vad en sekretessmarkering ska innehålla förutom de obligatoriska uppgifter som ska anges. Avsikten är att Försvarsmaktens utformning av sekretessmarkering ska överensstämma med Säkerhetspolisens utformning.

I 5 kap. 5 § andra stycket OSL framgår att om utlämnande till en enskild av 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 i ett sådant fall även framgå vilken myndighet som ska pröva frågan om utlämnande.

Sekretessmarkeringen är en varningssignal om att det kan finnas uppgifter i handlingen som omfattas av någon sekretessbestämmelse i OSL. Sekretessmarkering-

en innebär inte något bindande avgörande av sekretessfrågan. Innan en handling lämnas ut till någon, som begärt att få ta del av en allmän handling, måste därför en sekretessprövning av innehållet göras oavsett om handlingen är sekretessmarkerad eller inte.

Förutom säkerhetsskyddsklassificerade allmänna handlingar som är av synnerlig betydelse för rikets säkerhet finns det inget krav på att handlingar ska sekretessmarkeras.

Andra meningen: Oavsett om en säkerhetsskyddsklassificerad handling är en allmän handling eller inte, ska handlingen förses med anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har.

En handling får endast förses med en anteckning om säkerhetsskyddsklass om uppgifterna i handlingen har bedömts röra säkerhetskänslig verksamhet och uppgifterna av den anledningen omfattas av sekretess enligt offentlighets- och sekretesslagen hos myndigheten.

En säkerhetsskyddsklassificerad handling kan placeras i säkerhetsskyddsklass p.g.a. att:

1. Ett röjande av de säkerhetsskyddsklassificerade uppgifterna i handlingen kan medföra skada för Sveriges säkerhet.[10]
2. De säkerhetsskyddsklassificerade uppgifterna omfattas av ett internationellt åtagande om säkerhetsskydd:
    a. Uppgifterna *har* klassificerats av en annan stat eller en mellanfolklig organisation.[11] En gjord klassificering ska då godtas och läggas till grund för bestämmande av skyddsnivå.[12]
    b. Uppgifterna *har inte* klassificerats av en annan stat eller en mellanfolklig organisation. Indelning i säkerhetsskyddsklass görs då utifrån skada ett röjande kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation.[13] Det regelverk som är tillämpligt i det aktuella samarbetet kan utgöra ett stöd vid bedömningen.[14]

Det finns en övergångsbestämmelse som rör anteckning om säkerhetsskyddsklass. Se övergångsbestämmelse 3 nedan.

7 § 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

[10] 2 kap. 5 § första stycket säkerhetsskyddslagen.
[11] 2 kap. 5 § andra stycket första meningen säkerhetsskyddslagen.
[12] Prop. 2017/18:89, s. 140.
[13] 2 kap. 5 § andra stycket säkerhetsskyddslagen.
[14] Prop. 2017/18:89, s. 140.

första sidan förses med den högsta säkerhetsskyddsklassen som uppgifterna i bilagan är placerade i.

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.

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.

Kommentar: 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. Försvarsmaktens utformning av märkning överensstämmer i stort med Säkerhetspolisens utformning.

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

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

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.

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.

Det finns en övergångsbestämmelse som rör anteckning om säkerhetsskyddsklass. Se kommentaren till övergångsbestämmelse 3 nedan.

8 § Ett säkerhetsskyddsklassificerat lagringsmedium ska på höljet förses med en anteckning (märkning) om den högsta säkerhetsskyddsklass lagringsmediet är avsett för.

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.

Kommentar: *Första stycket:* 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. då 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.

Andra stycket: 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 märknigen 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 märkas.

9 § 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.

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

Rutinerna bör utformas så att den som beslutar om ändring eller borttagning har sakkunskap om de förhållanden uppgifterna rör, för att kunna avgöra om ändringen eller borttagningen är lämplig och får genomföras.

Ändring av märkning kan ske genom att den ursprungliga märkningen överkorsas och ny märkning tillförs tillsammans med en anteckning om datum för när änd-

ringen görs. Det är även lämpligt att det framgår vem som har genomfört ändringen.

Borttagning bör göras genom att märkningen överkorsas och datum för när borttagningen görs antecknas. Det bör även framgå vem som har genomfört borttagningen.

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.

10 § 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.

Kommentar: *Första stycket:* Med kvalificerat hemlig handling avses i bestämmelsen alla säkerhetsskyddsklassificerade handlingar som är placerade i säkerhetsskyddsklassen kvalificerat hemlig.

Uppgifter som är placerade i säkerhetsskyddsklassen kvalificerat hemlig är uppgifter som om de röjs kan medföra synnerligen allvarlig skada för Sveriges säkerhet.[15] *Kvalificerat hemlig* är den högsta säkerhetsskyddsklassen. Den myndighet 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.

Andra stycket: Den myndighet 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 kommentaren till säkerhetsskyddsklassificering i 3 kap. 6 § ovan. 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 § offentlighets-

[15] 2 kap. 5 § säkerhetsskyddslagen.

och sekretessförordningen (2009:641) (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.

Åtgärder med säkerhetsskyddsklassificerade handlingar och lagringsmedier

11 § 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.

Kommentar: Exemplar av allmänna handlingar i säkerhetsskyddsklassen konfidentiell och högre ska kunna följas upp så att myndigheten vet 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. Syftet är att uppnå spårbarhet för varje exemplar av sådana handlingar.

12 § 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.

Kommentar: Bestämmelsen gäller såväl handlingar som ska distribueras till mottagare utanför myndigheten 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.

13 § Ett säkerhetsskyddsklassificerat lagringsmedium som är placerat i säkerhetsskyddsklassen konfidentiell eller högre ska märkas med identifieringsuppgift på höljet.

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.

Kommentar: Identifieringsuppgiften behövs för att kunna upprätthålla spårbarhet i hanteringen, t.ex. kvittering vid mottagande, inventering och dokumenterad förstöring. Se även kommentaren till 3 kap. 8 §.

14 § 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.

Kommentar: Rutinerna ska förebygga att s.k. svartkopior uppstår. Svartkopior är oregistrerade kopior av eller utdrag ur säkerhetsskyddsklassificerade allmänna handlingar som ska registreras, dvs. kopior som myndigheten 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 då uppgift om kopian (exemplaret) saknas i registret över myndighetens säkerhetsskyddsklassificerade handlingar. Rutinerna om kopiering och utdrag har därför en stark koppling till krav på registrering och exemplarhantering.

Kvittering av säkerhetsskyddsklassificerade handlingar och lagringsmedier

15 § 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 säkerhetsskyddad elektronisk handling behöver dock inte kvitteras om mottagandet sker i ett informationssystem där det i en säkerhetslogg noteras vem som tagit del av handlingen.

Kommentar: *Första stycket:* 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.

För handlingar gäller krav på kvittering endast säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklass konfidentiell eller högre.

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.

Andra stycket: 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.

Tredje stycket: En underskrift kan vara elektronisk.

Språklig korrigering: ska stå säkerhetsskyddsklassificerad elektronisk handling.

16 § 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.

Kommentar: 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.

17 § 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.

Kommentar: Bestämmelsen gäller muntlig överföring av uppgifter och visning och ska alltså tillämpas i mötessammanhang där en presentation uppfyller villkoren i tryckfrihetsförordningen för att vara en allmän handling, t.ex. om en presentation har färdigställts, och därmed upprättats, före mötet.

Kvittering bör göras genom namnteckning och namnförtydligande på ett delgivningskvitto eller en lista. Det är även lämpligt att ange datum för kvittering på delgivningskvittot eller listan samt att myndighetens registratur förser handlingarna med ett delgivningskvitto. På så sätt behöver inte innehavaren av en handling tänka på att finna en sådan blankett i samband med att delgivning av uppgifter ur handlingen ska ske.

18 § 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 säkerhetsskyddsklassificerade elektroniska allmänna handlingar får det istället anges i vilket informationssystem handlingen behandlas.

Kommentar: Registreringen är av stor betydelse för informationssäkerheten då 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.

Myndigheten 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.

19 § 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 säkerhetsskyddsklassificerade uppgifter mellan två

informationssystem och som därefter omedelbart förstörs behöver inte föras in i registret.

Kommentar: *Första stycket:* Se kommentaren till 3 kap. 18 § ovan.

Det är lämpligt att registret 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.

Medförande av säkerhetsskyddsklassificerade handlingar och lagringsmedier utanför myndighetens lokaler

20 § 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.

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.

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.

Kommentar: *Första stycket:* Med medförande avses när en person för sitt arbete behöver transportera och förvara handlingar eller lagringsmedier utanför myndighetens lokaler eller områden.

Bestämmelsen 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, då skyddet alltid blir sämre utanför myndighetens lokaler och områden. Verksamheten kan dock ha behov av att medföra handlingar och lagringsmedier.

Rutinen bör innehålla vilka hänsyn som ska tas till vilket ändamål handlingar och lagringsmedier medförs och till vilka platser medförandet sker. Det kan vara fråga om för vilket ändamål och till vilka platser som handlingarna och lagringsmedierna ska medföras. Rutinen bör utformas så att det i efterhand är möjligt att kunna avgöra om ett medförande har varit tillåten.

Att myndigheten inte behöver besluta rutiner för säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen begrän-

sat hemlig, innebär att sådana handlingar och lagringsmedier får medföras – om inte myndigheten bestämt något annat.

Andra stycket: Att 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.

Exempel på när handlingarna eller lagringsmedierna *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 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 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 handlingarna eller lagringsmedierna *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 eller på ett hotellrum.
- 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 handlingar och lagringsmedier i ett förseglat emballage (kuvert eller säkerhetskuvert). Ett eventuellt försök till intrång i emballaget kan därmed lättare uppmärksammas.

Andra och *tredje styckena* gäller även för säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen begränsad.

Inventering av säkerhetsskyddsklassificerade handlingar och lagringsmedier

21 § I 3 kap. 8 § säkerhetsskyddsförordningen (2018:658) finns föreskrifter om att säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklassen kvalificerat hemlig ska inventeras minst en gång per år.

Säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig ska inventeras en gång per år.

Säkerhetsskyddsklassificerade elektroniska handlingar behöver inte inventeras.

Kommentar: 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.

Uppgifter om vilka exemplar som ska inventeras finns i det diarium eller register där exemplaren är registrerade enligt 3 kap. 18 §.

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. då sidor lossnat.

Första stycket: Paragrafen innehåller en upplysning om vad som gäller enligt förordning.

I 3 kap. 8 § säkerhetsskyddsförordningen framgår att *även arkiverade* säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklassen kvalificerat hemlig ska inventeras.

Andra stycket: I 3 kap. 8 § säkerhetsskyddsförordningen framgår att kravet på inventering *inte gäller arkiverade* säkerhetsskyddsklassificerade allmänna handlingar som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig.

Tredje stycket: Fysiska föremål (såsom handlingar i pappersform och lagringsmedier och materiel) 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 §.

22 § Ett säkerhetsskyddsklassificerat lagringsmedium som är placerat i säkerhetsskyddsklassen konfidentiell eller högre ska inventeras en gång per år.

Kommentar: 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 TF är undantagna från att vara allmänna handlingar.

Lagringsmedier som personal har kvitterat vid mottagandet 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.

Gallring och förstöring av säkerhetsskyddsklassificerade handlingar och lagringsmedier

23 § För gallring av säkerhetsskyddsklassificerade allmänna handlingar gäller särskilda bestämmelser som meddelas av Riksarkivet.

Kommentar: Det finns inga kommentarer till denna föreskrift.

24 § Förstöring av säkerhetsskyddsklassificerade handlingar och lagringsmedier ska ske så att återskapande av uppgifterna omöjliggörs.

Förstöring av säkerhetsskyddsklassificerade allmänna handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre ska dokumenteras.

Kommentar: *Första stycket:* Bestämmelsen gäller såväl allmänna handlingar som handlingar som inte är allmänna. Hur förstöringen sker är upp till myndigheten att avgöra. Förstöring av handlingar i pappersform kan t.ex. göras med dokumentförstörare eller bränning. Det är lämpligt att myndigheten tar fram rutiner 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 §§.

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.

När handlingar i pappersform förstörs i en dokumentförstörare bör restprodukterna vara högst 1,2 mm breda och ha en längd av högst 15 mm.

Andra stycket: Bestämmelsen gäller alla exemplar av en handling. När en handling eller ett lagringsmedium har förstörts upphör behovet av 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.

Särskilt om 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 då Sverige är i krig. Bestämmelserna i lagen omfattar även manuella eller informationssystembaserade informationstillgångar.[16] Lagen gäller före arkivlagens föreskrifter om vilka handlingar som får gallras.[17] När planläggning för undanförsel och förstöring genomförs är det nödvändigt att den även omfattar säkerhetsskyddsklassificerade handlingar och lagringsmedier.

I stridssituationer, t.ex. då 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.[18] Det är sannolikt av större vikt att uppgifter som kan hjälpa en motståndare inte röjs till denne.

Åtgärder vid distribution av säkerhetsskyddsklassificerade handlingar och lagringsmedier

25 § 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.

En försändelse med säkerhetsskyddsklassificerade handlingar eller lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre ska

[16] Prop. 1992/93:78 s. 1.
[17] 10 § tredje stycket arkivlagen (1990:782).
[18] Prop. 1992/93:78 s. 6.

sändas med en distributör som har godkänts av myndigheten. En sådan distributör ska kunna verifiera att försändelsen har levererats till mottagaren.

Första och andra styckena gäller inte för säkerhetsskyddsklassificerade elektroniska handlingar.

Kommentar: 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 myndighet. Om det inte är möjligt får uppgifterna skrivas ut eller lagras på ett lagringsmedium som distribueras fysiskt.

Bestämmelsen gäller enligt 3 kap. 3-4 §§ även för tryckta skrifter och materiel.

Första stycket: Rutinerna bör utformas så att handlingarna och lagringsmedierna skyddas så att obehöriga inte kan ta del av uppgifterna i handlingarna och lagringsmedierna när de distribueras. För distribution utanför myndigheten 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, då sådana ökar sannolikheten för att handlingar och lagringsmedier inte kommer att registreras.

Om skyddet för handlingarna och lagringsmedierna blir lägre under distribution utanför myndigheten, 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 och ersatts med ett nytt emballage.

En mindre myndighet som endast finns på en plats kan ha en enklare rutin för distribution inom myndigheten, jämfört med en större myndighet som har verksamhet på flera platser.

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.

Andra stycket: 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 av myndigheten. Det finns inte heller något hinder mot att sådana handlingar och lagringsmedier skickas med en distributör som myndigheten god-

känt för handlingar och lagringsmedier som är placerade i högre säkerhetsskyddsklasser.

26 § En myndighet ska besluta hur transporter av säkerhetsskyddsklassificerade handlingar och lagringsmedier ska genomföras. Beslutet ska dokumenteras.

Kommentar: Skyddsåtgärderna behöver anpassas efter hur stor mängd handlingar och lagringsmedier som ska transporteras, deras placering i säkerhetsskyddsklass, var transporten går och förhållanden under transporten.

Delgivning och distribution till utländsk myndighet och mellanfolklig organisation

27 § I 3 kap. 7 § säkerhetsskyddsförordningen (2018:658) föreskrivs att 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.

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.

En säkerhetsskyddsklassificerad elektronisk handling får istället märkas enligt första och andra stycket på lämpligt sätt med hänsyn till de informationssystem som handlingen behandlas i.

Kommentar: I 8 kap. 3 § OSL finns villkor för när uppgifter som omfattas av sekretess får lämnas till en utländsk myndighet eller en mellanfolklig organisation. I förordningen (2010:649) om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet, finns bestämmelser med villkor som gäller för Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut. I 3 kap. 9 § säkerhetsskyddsförordningen anges att säkerhetsskyddsklassificerade uppgifter som lämnas till en utländsk myndighet eller en mellanfolklig organisation ska omfattas av ett internationellt säkerhetsskyddsåtagande, om inte särskilda skäl finns för att ändå lämna sådana uppgifter.

Första stycket: Grundregeln är att handlingar som ska lämnas över ska förses med anteckning om ursprungsland (Sverige).

Andra stycket: 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. Se vidare kommentaren till 1 kap. 2 § ovan avseende begreppet säkerhetskänslig verksamhet.

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).

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.

28 § Om ett säkerhetsskyddsklassificerat 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.

Kommentar: Se kommentaren till 27 § första och andra styckena.

29 § I 3 kap. 10 § första stycket säkerhetsskyddsförordningen (2018:658) finns föreskrifter om försändelser med säkerhetsskyddsklassificerade handlingar till utlandet.

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.

Kommentar: *Första stycket:* I 3 kap. 10 § säkerhetsskyddsförordningen anges att Utrikesdepartementets kurirförbindelser ska anlitas för försändelser med säkerhetsskyddsklassificerade handlingar till och från utlandet. Försändelserna ges då ett skydd mot obehörig åtkomst genom att kuriren har uppsikt över försändelsen och att den inte får genomsökas.

Andra stycket: Det är inte alltid möjligt att använda Utrikesdepartementets kurirförbindelser. Enligt vissa säkerhetsskyddsavtal kan de nationella säkerhetsmyndigheterna komma överens om andra rutiner som är ändamålsenliga i det specifika fallet. Det kan t.ex. röra sig om distribution mellan Sverige och ett annat land av säkerhetsskyddsklassificerade handlingar som rör ett specifikt samarbete och där transportvägen mellan länderna anses tillräckligt säker även utan det skydd som Utrikesdepartementets kurirförbindelser ger.

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. Distributionen underlättas av att transporten genomförs av Försvarsmaktens personal i militärt fartyg, luftfartyg eller fordon.

4 kap. Informationssäkerhet i och kring informationssystem

1 § Vad som anges om informationssystem gäller även för sådana informationssystem som utgörs endast av ett elektroniskt kommunikationsnät.

Kommentar: 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.

Hantering av säkerhetsskyddsklassificerade lagringsmedier

2 § 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.

Kommentar: 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.

3 § 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.

Kommentar: 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.

4 § 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.

Kommentar: Lagringsmediet får även återanvändas i sådana informationssystem som inte är avsedda för behandling av säkerhetsskyddsklassificerade uppgifter

under förutsättning att myndigheten har vidtagit åtgärder för att säkerställa att inga säkerhetsskyddsklassificerade uppgifter kan utläsas ur lagringsmediet.

Åtgärder inför driftsättning

5 § I 3 kap. 1 § säkerhetsskyddsförordningen (2018:658) finns bestämmelser om särskild säkerhetsskyddsbedömning inför driftsättning av informationssystem.

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.

Kommentar: Föreskriften gäller alla informationssystem som har betydelse för säkerhetskänslig verksamhet, även om de inte hanterar säkerhetsskyddsklassificerade 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 föreskriften. Sådana system som är avsedda att hantera säkerhetsskyddsklassificerade uppgifter ska alltid anses ha betydelse för säkerhetskänslig verksamhet och omfattas alltså av föreskriften.

Även fristående datorer som endast används av en användare, och som inte har någon koppling till omvärlden genom t.ex. USB, 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.

Myndigheten kan ta fram grundkrav eller grundkravprofiler för system som har olika betydelse för den säkerhetskänsliga verksamheten och som hanterar uppgifter i olika säkerhetsskyddsklasser. Dessa grundkrav kan refereras till i den särskilda säkerhetsskyddsbedömningen för ett visst system. Krav som tillkommer för det specifika systemet dokumenteras i den särskilda säkerhetsskyddsbedömningen.

6 § 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.

De personer som ansvarar för utvecklingen av systemet får inte ansvara för granskningen och godkännandet av skyddsåtgärderna.

Kommentar: *Första stycket:* De skyddsåtgärder som beskrivs i 15–27 §§ är inte uttömmande men beskriver en uppsättning åtgärder som normalt täcker de flesta behov. Resultatet av den särskilda säkerhetsskyddsbedömningen kan vara att ytterligare åtgärder bedöms vara nödvändiga, t.ex. åtgärder för fysisk säkerhet och personalsäkerhet. Det är vidare särskilt viktigt att fastställa att samverkande informationssystem inte skyddar uppgifter enligt för låga kravnivåer.

Skyddsåtgärderna innehåller ofta tekniska säkerhetsfunktioner i informationssystemen men kan också vara administrativa eller organisatoriska, särskilt i kombination med fysiskt skydd och begränsat tillträde till de platser där informationssystemet finns.

Med test avses främst provning av det aktuella informationssystemet och de tekniska skyddsåtgärderna i detta. Det är alltså inte tillräckligt med enbart en granskning av dokumentation som beskriver informationssystemet.

För fristående datorer kan testning innebära t.ex. funktionstester av behörighetskontroll, antivirus eller liknande. Om åtgärderna är fysiska eller administrativa så får man tänka sig mer simulerade tester (table-top) etc. men även (icke-förstörande) pen-tester av ett sådant skydd kan göras.

Andra stycket: Syftet med föreskriften är att säkerställa ett visst oberoende mellan utvecklare och granskare. Att låta den som utvecklat en skyddsåtgärd också granska den innebär en stor risk att sårbarheter förbises.

7 § 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.

Kommentar: Det är inte möjligt att helt förvissa sig om att en produkt är tillförlitlig, det är däremot viktigt att göra en helhetsbedömning av om tillförlitligheten är tillräcklig för att man ska kunna använda produkten i ett informationssystem som är av betydelse för säkerhetskänslig verksamhet. Åtgärder för att skaffa sig förtroende för en leverantör kan innefatta granskning av leverantören och dess rutiner och åtgärder för säkerhet i utveckling, tillverkning och leverans. Åtgärderna kan också inbegripa skydd under leverans. För hårdvara handlar detta främst om fysiskt skydd, för mjukvara kan det också vara logiska skydd, t.ex. med kryptografiska metoder.

8 § Ett informationssystem får inte godkännas från säkerhetssynpunkt (ackrediteras) innan åtgärderna enligt 6 § har godkänts.

Kommentar: Det finns ingen kommentar till denna föreskrift.

Begäran om samråd

9 § 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.

Kommentar: Försvarsmakten kan bl.a. efterfråga den särskilda säkerhetsskyddsbedömningen, granskningsrapporter, m.m.

Drift och förvaltning av informationssystem

10 § 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.

Myndigheten ska fortlöpande förvalta och underhålla de informationssystem som har betydelse för säkerhetskänslig verksamhet så att säkerhetsskyddet i och kring systemen kan upprätthållas.

Kommentar: Myndigheten 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.

11 § Myndigheten ska dokumentera de informationssystem som har betydelse för säkerhetskänslig verksamhet. System som är av särskild betydelse vid höjd beredskap ska dokumenteras särskilt.

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.

Kommentar: *Första stycket:* 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.

Andra stycket: 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.

Övervakning

12 § 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.

Kommentar: Övervakningen är en del i incidenthanteringen som krävs enligt 1 kap. 3 §; det som upptäcks genom övervakningen ska tas om hand i enlighet med de rutiner som myndigheten har beslutat.

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 då det antagligen inte är praktiskt genomförbart. Sådana system bör istället regelbundet kontrolleras på annat sätt.

Åtgärder vid förändringar i och kring informationssystem

13 § 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.

Kommentar: 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.

14 § 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 §§.

Kommentar: Mindre ändringar, som t.ex. säkerhetsuppdateringar av programvara, som kan göras utan någon påtaglig risk för att skyddet försämras kan normalt göras utan ny granskning och godkännande. 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.

Även om inga större förändringar gjorts bör den särskilda säkerhetsskyddsbedömningen uppdateras och en ny granskning göras med viss regelbundenhet, t.ex. minst vart tredje år, för att säkerställa att säkerhetsskyddet fortfarande motsvarar vad som krävs.

Autentisering och behörighetskontroll

15 § För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att verifiera användares 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.

Kommentar: *Första stycket:* 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 då alla användare av systemet faktiskt är behöriga till alla uppgifter och funktioner).

Andra stycket: 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.

16 § 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.

Kommentar: 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.

Säkerhetsloggning

17 § 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.

Kommentar: 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.

Föreskriften behandlar endast säkerhetsloggar vilket innebär att myndigheten själv kan och bör 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.

18 § Säkerhetsloggar och säkerhetskopior av dessa ska skyddas så att de finns tillgängliga när de behövs, att deras riktighet bevaras och att obehörig åtkomst försvåras.

Kommentar: Med skydd avses även fysiska skyddsåtgärder.

Intrångsskydd och intrångsdetektering

19 § 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.

Kommentar: 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.

20 § Myndigheten ska se till att informationssystem som har betydelse för säkerhetskänslig verksamhet separeras från övriga informationssystem som inte omfattas av krav på säkerhetsskydd.

Kommentar: Separationen mellan informationssystem kan vara antingen fysisk eller logisk. Med fysisk separation menas att informationssystemen använder helt olika fysiska infrastrukturer, dvs. olika datorer, servrar, lagring, 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. Denna typ av risker kan vara mycket svåra att upptäcka vid en granskning.

Skydd mot skadlig kod

21 § 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.

Kommentar: 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.

Bevarande av riktighet

22 § 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.

Kommentar: 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.

Säkerhetskopiering

23 § 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.

Kommentar: 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.

24 § 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.

Kommentar: Säkerhetskopior av informationssystem som används i säkerhetskänslig verksamhet innehåller i de flesta fall säkerhetsskyddsklassificerade uppgifter och därför ska ges ett skydd utifrån detta.

Skydd mot röjande signaler och obehörig avlyssning

25 § 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.

Kommentar: Röjande signaler (RÖS) är icke önskvärda elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs. Kravet på skydd mot röjande signaler gäller bara informationssystem som avses behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre och informationssystem där en obehörig åtkomst till systemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig.[19]

Skydd mot RÖS kan åstadkommas genom att byggnaden i sig har ett skydd som dämpar de röjande signalerna och då behövs inga ytterligare skydd i informationssystemen. Det finns dock inget som hindrar att kombinationer mellan skydd i byggnader och i informationssystem vidtas vilket också kan vara önskvärt. I Försvarsmakten anses myndighetens RÖS-strategi och RÖS-policy utgöra grund för att kunna godkänna en skyddsåtgärd för skydd mot RÖS. Strategin och policyn är föremål för översyn.

26 § 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.

Kommentar: Det finns ingen kommentar till denna föreskrift.

Säkerhetskonfiguration

27 § 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.

[19] 3 kap. 4 § säkerhetsskyddsförordningen.

Kommentar: 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. Myndigheten bör fastställa vilka rekommendationer som ska följas för sådana operativsystem, applikationsprogramvaror m.m. som myndigheten använder i sina informationssystem.

Undantag från krav på skyddsåtgärder

28 § Myndigheten får ansöka om undantag från 3 kap. 4 § första stycket säkerhetsskyddsförordningen (2018:658) enligt det förfaringssätt som Försvarsmakten bestämmer.

Kommentar: En ansökan ska ställas till den militära underrättelse- och säkerhetstjänsten vid Försvarsmaktens högkvarter. Av ansökan ska det minst framgå vilka föreskrifter som undantaget rör, vad anledningen är till varför de inte går att följa samt en uppgift om när myndigheten bedömer att föreskrifterna går att följa.

5 kap. Fysisk säkerhet

1 § 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.

Kommentar: Fysiska säkerhetsskyddsåtgärder omfattar byggnadstekniska åtgärder, teknisk och personell bevakning samt möjlighet att ingripa.

Myndighetens behov av detektering anpassas till fred, kris och krig.

Med farliga ämnen, vapen samt avlyssnings- och störutrustning avses sjukdomsalstrande substanser eller toxiska ämnen, samt olika former av CBRNE-ämnen (kemiska, biologiska inkl. toxiner, radiologiska, nukleära och explosivämnen), spräng- och tändmedel, ammunition, elektroniska störvapen såsom EMP och HPM varianter av akustisk, elektronisk och visuell avlyssning samt radiosändare.

Språklig korrigering: ska stå säkerhetsskyddsklassificerade uppgifter.

Tillträde och bevakning

2 § Myndigheten ska ha rutiner för tillträde till myndighetens områden, byggnader och andra anläggningar eller objekt. Rutinerna ska dokumenteras.

Kommentar: Rutinerna kan förtecknas i myndighetens säkerhetsbestämmelser eller motsvarande bestämmelser.

3 § 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.

Kommentar: *Första stycket:* Identitet fastställs med stöd av godkänd identitetshandling I 3 kap. 2 § Försvarsmaktens interna bestämmelser (FIB 2017:7) om tjänstekort och vissa behörighetshandlingar finns föreskrifter om godkända identitetshandlingar i Försvarsmakten.

I 13 § Försvarsmaktens skyddsföreskrifter (FFS 2010:5) finns föreskrifter 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 finns föreskrifter om när en skyddsvakt får medge tillträde till ett skyddsobjekt.

Andra stycket: När en person vill ta del av myndighetens allmänna handlingar behöver personen inte uppge sitt namn, varje person har rätt att vara anonym i en sådan situation.[20]

4 § Bevakning med personal eller tekniska bevakningssystem ska finnas vid alla passerställen till platser där det bedrivs säkerhetskänslig verksamhet.

Kommentar: Vid platser dit besökare kan förväntas komma bör bevakningen företrädesvis vara personell.

Tekniska bevakningssystem (passagekontrollsystem) kan med fördel användas vid passerställen som används av myndighetens personal.

5 § 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.

Kommentar: Med de centrala delarna av det tekniska bevakningssystemet avses styrdator, inte detektorer, kontakter, kortläsare eller ringklockor. Det tekniska bevakningssystemet ska inte kunna manipuleras eller på annat sätt påverkas.

6 § 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.

Kommentar: Syftet med bestämmelsen är att myndigheten ska analysera vilka åtgärder som bedöms lämpliga vid larm. Beroende på avstånd till objektet kan annan åtgärd än insats vara aktuell.

[20] 2 kap. 18 § tryckfrihetsförordningen.

Nycklar, kort och koder

7 § 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.

Kommentar: 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 så ingen obehörig kan komma åt dessa. Begreppet kan även innebära att innehavaren alltid bär nyckel och kort med sig och på sig, att anteckning om kod inte förvaras tillsammans med kortet eller att den personliga koden döljs vid användandet. Se även kommentaren till 3 kap. 20 § när det gäller att ha nycklar, kort och koder under kontroll i samband med medförande.

En nyckel som enskilt ger tillträde till ett nivåreglerat utrymme ska således förvaras i ett utrymme med motsvarande skyddsnivå då den 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.

8 § En kod ska bestämmas och ställas in av den som har tilldelats ett utrymme där säkerhetsskyddsklassificerade uppgifter förvaras eller där säkerhetskänslig verksamhet bedrivs.

Kommentar: Bestämmelsen innebär att det ska vara den person som ansvarar för utrymmet som ska bestämma och ställa in koden eller vad avser omställbara nyckellås ställa in låset.

9 § En nyckel, ett kort eller en kod får innehas endast av den som har ansvaret för utrymmet, om inte myndigheten har beslutat annat.

Kommentar: Syftet med bestämmelsen är att förhindra obehöriga att få tillgång till utrymmena. Myndigheten kan dock t.ex. besluta om att flera personer får tillträde till ett sådant utrymme. Beslutet ska dokumenteras, vilket framgår av myndighetsförordningen (2007:515).

10 § 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.

Kommentar: Syftet är att ha motsvarande ordning på nycklar, kort och koder som på säkerhetsskyddsklassificerade handlingar och lagringsmedier.

11 § 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.

Kommentar: Det finns inga kommentarer till denna föreskrift.

Förvaring

12 § I bilaga 1 till denna författning anges de krav som gäller för respektive skyddsnivå. Ett förvaringsutrymme för säkerhetsskyddsklassificerade handlingar ska uppfylla de krav som gäller för skyddsnivå 1, 2, 3 eller 4.

Kommentar: Beroende på säkerhetsskyddsklass för uppgifter eller verksamhet, ska den fysiska säkerheten kunna motstå försök till intrång under viss tid. Utrymmen delas därför in i skyddsnivå 1-4. Ju kraftigare konstruerat utrymmet är, och därmed dess sammanhängande förmåga att motstå angrepp, desto högre skyddsnivå har det. Ju högre säkerhetsskyddsklass desto kraftigare konstruerat förvaringsutrymme, d.v.s. en högre skyddsnivå.

De specifika kraven som gäller för skyddsnivå 1-4 framgår av bilaga 1.

13 § Myndigheten får besluta att områden, byggnader och andra anläggningar eller objekt ska vara en administrativ zon och en säkerhetszon. Beslutet ska dokumenteras.

Kommentar: Bestämmelsen är avsedd att ge myndigheten ett alternativt sätt att konstruera det fysiska skyddet. Beslutet måste dock föregås av en säkerhetsskyddsplanering.

Införandet av 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 zon. I byggnaden kompletteras skyddet med olika säkerhetszoner, med begränsat tillträde, t.ex. olika ledningscentraler. Med säkerhetzon avses t.ex. utrymmen som kräver särskild behörighet för tillträde, där säkerhetskänslig verksamhet bedrivs. I en säkerhets-

zon kan myndigheten besluta att t.ex. servicepersonal för bl.a. it-drift och lokalvård inte får lämnas ensamma.

14 § I bilaga 2 till denna författning anges de krav som gäller för administrativ zon respektive säkerhetszon.

Kommentar: De specifika kraven som gäller för zonerna framgår av bilaga 2.

15 § En säkerhetsskyddsklassificerad handling som är placerad i säkerhetsskyddsklassen begränsat hemlig ska vara under kontroll eller förvaras inlåst eller i en låst lokal som endast den som är behörig att ta del av handlingen 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.

Kommentar: Se kommentar till 3 kap. 20 § ovan.

16 § En säkerhetsskyddsklassificerad handling som är placerad i säkerhetsskyddsklassen konfidentiell eller hemlig ska vara under kontroll eller förvaras inlåst 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 inte förvaras i någon zon ska handlingen förvaras i ett larmat utrymme i lägst skyddsnivå 3.

Kommentar: Se kommentar till 3 kap. 20 § ovan.

17 § En säkerhetsskyddsklassificerad handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig ska vara under kontroll eller förvaras inlåst i ett larmat utrymme i skyddsnivå 4 vid förvaring i eller utanför en administrativ zon eller en säkerhetszon.

Kommentar: Se kommentar till 3 kap. 20 § ovan.

18 § Myndigheten får fatta beslut som avviker från 15–17 §§ under förutsättning att motsvarande skydd kan upprätthållas. Beslutet ska dokumenteras.

Kommentar: Beslutet ska grunda sig på en säkerhetsskyddsanalys och därtill kopplad säkerhetsskyddsplan. I säkerhetsskyddsplanen anges vilka åtgärder som ska vidtas för att uppnå en motsvarande skyddsnivå.

19 § Om myndigheten har beslutat att personalen under kortare tid får lämna säkerhetsskyddsklassificerade handlingar framme i ett låst arbetsrum, ska huvudnycklar och reservnycklar förvaras så att någon obehörig inte kan komma åt dem.

Kommentar: Om myndigheten ska bevilja att personalen under kortare tid, t.ex. lunch, får lämna säkerhetsskyddsklassificerade handlingar framme i arbetsrummet

och inte behöva låsa in dem i ett säkerhetsskåp måste man säkerställa 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 förseglade säkerhetspåse eller liknande.

Bevakningspersonal som inte är behörig att ta del av information eller verksamhet, kan ändå beslutas vara behöriga till utrymmen då det ingår i deras arbetsuppgifter att kontrollera och stödja vid behov.

Utrymmen för muntlig delgivning

20 § 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.

Kommentar: Innan ett utrymme kan godkännas för muntlig delgivning av säkerhetsskyddsklassificerade uppgifter ska en säkerhetsskyddsanalys genomföras. Av säkerhetsskyddsanalysen 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 vara också vara en möteslokal som återkommande över tiden används för planerade, och icke planerade, mötesgenomgångar av säkerhetsskyddsklassificerade uppgifter. Det kan också röra sig om ledningsrum eller ledningscentraler som JOC (Joint Operations Center) eller JIOC (Joint Intelligence Operations Center).

Skydd för it-utrymmen

21 § 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.

Kommentar: 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.

Se även kommentaren till 5 kap. 22 § nedan.

22 § 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.

Kommentar: Se kommentaren till 5 kap. 6 § avseende åtgärder för larm.

23 § 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.

Kommentar: Syftet med bestämmelsen är att myndigheten ska ha kontroll över tillträde till, och därmed även verksamhet i, utrymmen och lokaler som innehåller tele- och dataväxlar, korskopplingar, dataservar och motsvarande tekniska 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 myndigheten analyserar sina säkerhetsloggar.

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.

24 § 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.

Kommentar: Bestämmelsen tar sikte på it-utrymmen där det inte behandlas säkerhetsskyddsklassificerade uppgifter, men där det bedrivs säkerhetskänslig verksamhet. Det handlar alltså om skydd för säkerhetskänsliga informationssystem, dvs. system som har ett högt skyddsvärde av andra skäl, t.ex. digital infrastruktur eller system för styrning av kraftförsörjning.[21]

Se kommentaren till 5 kap. 6 § avseende åtgärder för larm.

25 § Myndigheten får fatta beslut som avviker från 21–22 och 24 §§ under förutsättning att motsvarande skyddsnivå kan upprätthållas. Beslutet ska dokumenteras.

Kommentar: Beslutet ska grunda sig på en säkerhetsskyddsanalys och därtill kopplad säkerhetsskyddsplan. I säkerhetsskyddsplanen anges vilka åtgärder som ska vidtas för att få en motsvarande skyddsnivå.

[21] Prop. 2017/18:89, s. 70.

6 kap. Säkerhetsprövning

1 § 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.

Kommentar: Bestämmelsen innehåller en upplysning om vad som gäller enligt lag.

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, SUA, utbildning, utbytes- eller växeltjänstgöring, praktik, eller militära befattningar såsom värnpliktig och hemvärnsoldat). Se vidare kommentaren till 6 kap. 3 § nedan.

Vid säkerhetsprövningen ska en helhetsbedömning göras, baserat på ett allsidigt underlag och personkännedom. Bedömningen ska utgå från personens lojalitet, pålitlighet och sårbarhet. Myndigheten ska även ta hänsyn till den prövades personliga integritet. Den prövade ska vidare lämna sitt samtycke till registerkontroll.[22]

I 5 kap. 5 § säkerhetsskyddsförordningen framgår att en säkerhetsprövning ska dokumenteras i de fall en person bedömts vara pålitlig ur säkerhetssynpunkt. Riksarkivet har föreskrivit att viss dokumentation inom ramen för personalsäkerhet ska bevaras.[23] Ett exempel är resultatet av en persons säkerhetsprövning.

2 § Myndigheten ska se till att den som genomför säkerhetsprövning har relevant utbildning och är lämplig för uppgiften.

Kommentar: Säkerhetsprövning innebär ett kontinuerligt intrång i den personliga integriteten, vilket ställer särskilda krav på myndigheten och på de som för myndighetens verksamhet genomför säkerhetsprövning. Därför är det viktigt att de personer som arbetar med säkerhetsprövning, oavsett i vilken roll, har en relevant utbildning. Det kan röra sig om personer som administrerar registerkontroller, personer som genomför samtal och intervjuer, personer som ska genomföra den uppföljande säkerhetsprövningen, t.ex. personalansvarig chef, eller personer som ska fatta beslut i säkerhetsprövning eller handlägga den dokumentation som finns om individen.

En relevant utbildning bör ge kunskap om följande områden: vad säkerhetsprövning är, hur den ska genomföras, det regelverk som styr säkerhetsprövning, hur en

[22] 3 kap. 18 § säkerhetsskyddslagen.
[23] Riksarkivets föreskrifter och allmänna råd (RA-MS 2018:42) om gallring hos Fortifikationsverket, Försvarets materielverk, Försvarsmakten, Totalförsvarets forskningsinstitut och Totalförsvarets rekryteringsmyndighet.

helhetsbedömning genomförs, och vem som har rätt att fatta beslut, samt vad som ska dokumenteras. Om personen i fråga ska genomföra samtal och intervjuer bör personen ha en sådan utbildning. Utbildningen ska[24] genomföras innan personen arbetar med eller tar del av uppgifter inom ramen för säkerhetsprövning, och ska även uppdateras fortlöpande så att individens kompetens upprätthålls. Det är upp till myndigheten att besluta om vad som är en relevant utbildning inom ramen för den egna verksamheten.

Eftersom det finns ett krav på att en person som genomför säkerhetsprövning ska vara lämplig, behöver myndigheten bedöma och besluta att personen ska arbeta med säkerhetsprövning utifrån ett lämplighetsperspektiv.

Placering i säkerhetsklass

3 § 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.

Kommentar: *Första stycket:* En analys av den säkerhetskänsliga verksamheten utifrån ett befattningsperspektiv är grunden till säkerhetsprövning. Befattningsanalysen ska genomföras inför varje deltagande i den säkerhetskänsliga verksamheten. Den har sin utgångspunkt i säkerhetsskyddsanalysen och ska därmed uppdateras då säkerhetsskyddsanalysen förändras. Då nya befattningar tillkommer, utan att säkerhetsskyddsanalysen förändrats, ska en befattningsanalys genomföras för minst de befattningar som tillkommit, innan säkerhetsprövning påbörjas. Befattningsanalysen genomförs för att dels komma fram till om och vilken säkerhetsklass som är aktuell, men även för att komma fram till om verksamheten ska skyddas på något annat sätt än genom placering i säkerhetsklass.[25] Ett sådant skydd kan exempelvis vara åtgärder inom fysiskt skydd och informationssäkerhet.

En befattningsanalys bör bl.a. ta hänsyn till om befattningen innebär krigsplacering. Om en krigsplacering ställer särskilda krav, t.ex. att befattningen bör placeras i en högre säkerhetsklass, bör analysen svara på om en sådan placering kan genomföras vid t.ex. höjd beredskap, eller om särskilda befattningar bör placeras i en högre säkerhetsklass även i fredstid.

[24] 2 kap. 3 § och 5 kap. 1 § säkerhetsskyddsförordningen.
[25] 3 kap. 10 § säkerhetsskyddslagen.

Strävan vid placering i säkerhetsklass bör vara att placera en befattning i så låg säkerhetsklass som möjligt. När det gäller säkerhetsskyddsklassificerade uppgifter ska hänsyn tas till mängden uppgifter, vilket i särskilda fall kan innebära att en befattning bör placeras i säkerhetsklass 3, även om befattningen endast innebär tillgång till säkerhetsskyddsklassificerade uppgifter i nivån begränsat hemlig. Det kan även innebära att visst tillträde till skyddsobjekt, som i tidigare lagstiftning omfattats av säkerhetsprövning och registerkontroll för skyddet mot terrorism och därmed normalt omfattas av säkerhetsklass 3, medför behov av placering i säkerhetsklass 2 om anläggningen är av kritisk betydelse.

Tredje stycket: Befattningsanalysen ska dokumenteras på ett sådant sätt så att grunden till placering i säkerhetsklass framkommer.

4 § 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).

Kommentar: Förteckningen bör revideras löpande. En lämplig frekvens kan vara åtminstone en gång per år. En sådan förteckning kan utgöra en allmän handling, och ska då diarieföras. Ett syfte med förteckningen är spårbarhet över vilka som tar del av den säkerhetskänsliga verksamheten och på vilket sätt. Förteckningen bör därför knytas till de individer som är placerade i säkerhetsklass, och därmed har en registerkontroll för befattningen, samt de individer som registerkontrollerats med stöd av 3 kap. 15 § säkerhetsskyddslagen.

En registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen avser en situation där befattningen inte placerats i säkerhetsklass men där registerkontroll ändå ska genomföras.

Grundutredning

5 § Bestämmelser om grundutredning finns i 5 kap. 2 § säkerhetsskyddsförordningen (2018:658).

En grundutredning inför en anställning eller annat deltagande i säkerhetskänslig verksamhet som är placerad i säkerhetsklass ska innefatta en säkerhetsprövningsintervju.

Grundutredningen ska dokumenteras.

Kommentar: *Första stycket:* En grundutredning ska bestå av en utredning om personliga förhållanden som omfattar betyg, intyg, referenser och uppgifter om den som prövningen gäller har lämnat, samt andra uppgifter i den utsträckning det är relevant för prövningen.[26]

[26] 5 kap. 2 § säkerhetsskyddsförordningen.

Andra stycket: Säkerhetsprövningsintervjun ska alltid genomföras innan registerkontroll, men det finns inget hinder mot att efter registerkontroll genomföra ytterligare intervjuer med personen för att klargöra omständigheter som framkommit vid registerkontrollen.[27] Registerkontroll ska dock inte genomföras om det efter säkerhetsprövningsintervjun står klart att den som prövningen gäller inte uppfyller kraven för en godkänd säkerhetsprövning.[28]

En intervju bör åtminstone innehålla följande områden: umgänge (den sökandes vänner och eventuella ovänner), tidigare verksamhet (erfarenheter från tidigare anställningar), ekonomi (inkomst, skulder, förmögenhet och boendeform), bisysslor (eventuella andra åttagande samt uppgifter om företag och verksamhet), personliga egenskaper (den sökandes ambition, samarbetsförmåga, etik säkerhetssmedvetande och dylikt) samt intressekonflikter (om den sökande kan hamna i en intressekonflikt vid eventuell anställning). Förutom dessa områden är det viktigt att vid bedömningen ta hänsyn till ytterligare aspekter som har betydelse vid deltagande i säkerhetskänslig verksamhet, t.ex. kontakter med utländsk underrättelse- och säkerhetstjänst, organiserad brottslighet och organisationer involverade i samhällsomstörtande verksamhet samt terrorism, levnadsbakgrund, beroendeproblematik samt lag- och regelefterlevnad.[29]

En säkerhetsprövning kan göras mindre omfattande om det finns särskilda skäl. Ett sådant skäl kan vara att personen är prövad på likvärdigt sätt, och en upprepad underlagsinhämtning inte tillför något nytt. En ny registerkontroll bör dock alltid göras. I sådana fall kan säkerhetsprövningsintervjun ersättas med ett skyddssamtal. Ett skyddssamtal syftar bl.a. till att orientera om säkerhetshotande verksamhet som kan riktas mot personen eller den verksamhet som personen ska delta i och att öka personens säkerhetsmedvetande. Skyddssamtalet syftar även till att fördjupa personkännedomen genom att personen lämnar uppgifter om sig själv. Om så bedöms kan delar av skyddssamtalet ersättas eller kompletteras med ett frågeformulär som personen fyller i.

Uppföljande säkerhetsprövning

6 § 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.

Kommentar: Den uppföljande säkerhetsprövningen ska genomföras kontinuerligt under hela deltagandet, och bör bestå av regelbundna kontakter och uppföljande samtal. Uppföljningens omfattning bör anpassas efter typ av deltagande och

[27] 5 kap. 2-3 §§ säkerhetsskyddsförordningen.
[28] 5 kap. 14 § säkerhetsskyddsförordningen.
[29] Prop. 2017/18:89, s. 80-81.

säkerhetskänslig verksamhet, men ska alltid innefatta en bedömning avseende lojalitet, pålitlighet och sårbarhet.[30]
Uppföljningen bör uppmärksamma förändringar i livssituation, avseende exempelvis social situation, kontakter med utländsk underrättelse- och säkerhetstjänst, organiserad brottslighet samt organisationer involverade i samhällsomstörtande verksamhet och terrorism. Vidare bör missnöje och besvikelse samt hälsoaspekter som exempelvis beroendeproblematik fångas upp. Uppföljningen bör även innefatta en ekonomisk genomgång med ekonomisk kontroll, samt eventuella kontakttagningsförsök, säkerhetsincidenter och utbildningsbehov.

Den uppföljande säkerhetsprövningen för personer som inte är placerade i säkerhetsklass, kan göras mindre omfattande. Dock bör åtminstone utbildningsbehov, säkerhetsincidenter, kontakttagningsförsök, missnöje och kontakter samt eventuella andra sårbarheter tas upp.

7 § Myndigheten ska förebygga och vidta rimliga skyddsåtgärder för att minska sårbarheter hos personer som deltar i myndighetens säkerhetskänsliga verksamhet.

Kommentar: Vid en uppföljande säkerhetsprövning kan uppgifter framkomma som innebär att det finns anledning att uppmärksamma en persons sårbarhet. I sådana fall kan ett nytt beslut om placering i säkerhetsklass eller deltagande i den säkerhetskänsliga verksamheten vara aktuellt, för att skydda myndigheten från förluster av skyddsvärden. Beslutet kan i vissa fall även fattas till skydd för individen, för att t.ex. inte öka eller överföra sårbarhet, och skydda individen från exponering och utsatthet för påtryckningar och utpressning. Beslutet kan även omfatta säkerhetsskyddsåtgärder som exempelvis begränsat tillträde till vissa lokaler eller tillgång till viss information.

Vid ett beslut som innebär begränsningar av vilka skyddsvärden en person får ta del av bör det genomföras en mer djupgående uppföljning, för att fördjupa personkännedomen och följa hur t.ex. en rehabilitering fortlöper. Syftet är att skaffa en djupgående bild av problematiken och personen, för att få en bred grund inför nya beslut om deltagandet i den säkerhetskänsliga verksamheten. En sådan uppföljning ska dokumenteras som en del av den uppföljande säkerhetsprövningen.

Avslutande samtal

8 § 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 tystnads-plikt som följer av offentlighets- och sekretesslagen (2009:400) eller 5 kap. 2 § andra stycket säkerhetsskyddslagen (2018:585).

[30] 3 kap. 2 § säkerhetsskyddslagen.

Ett sådant samtal behöver inte genomföras om det är uppenbart obehövligt.

Kommentar: *Första stycket:* Det avslutande samtalet 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 bitterhet eller besvikelse som kan utgöra ett hot mot den säkerhetskänsliga verksamheten eller Sveriges säkerhet.

Den avslutande delen av säkerhetsprövningen kan även bestå av ytterligare åtgärder, som exempelvis att myndigheten håller fortsatt kontakt med personen efter deltagandet slut. En sådan uppföljning kan vara särskilt viktig om personen tvingas lämna myndigheten t.ex. genom ett beslut om personens placering i säkerhetsklass.

Andra stycket: Den som ska ta del av säkerhetsskyddsklassificerad information har tystnadsplikt enligt 5 kap. 2 § säkerhetsskyddslagen. I samband med att upplysning om tystnadsplikten lämnas, bör individen underteckna ett sekretessbevis. När en person slutar i verksamheten är det viktigt att personen upplyses om att uppgifterna som denne tagit del av kan omfattas av sekretess en längre tid, även efter det att personen lämnat den säkerhetskänsliga verksamheten. Som bekräftelse på att personen har fått informationen kan sekretessbeviset undertecknas ytterligare en gång.

Tredje stycket: Ett exempel på när ett avslutande samtal är uppenbart obehövligt är om deltagandet varit kortvarigt eller om annat samtal inom ramen för den uppföljande säkerhetsprövningen nyligen genomförts.

7 kap. Utbildning och övning

1 § I 5 kap. 1 § säkerhetsskyddsförordningen (2018:658) finns föreskrifter om utbildning i säkerhetsskydd. Sådan utbildning ska genomföras innan personen får delta i säkerhetskänslig verksamhet.

Kommentar: Det finns inga kommentarer till denna föreskrift.

2 § 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.

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.

Kommentar: *Första stycket:* Utbildning och övning är en viktig del av säkerhetsskyddet, där utgångspunkten ska vara att personal och andra får den utbildning och övning 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. En övning kan genomföras som ett moment i en större övning, t.ex. en brandövning där ett moment är att säkerställa att säkerhetsskåp är stängda och låsta samt att säkerhetsskyddsklassificerade handlingar är inlåsta.

Funktioner eller delar av myndigheten 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 bör även omsättas till en utbildningsplan i säkerhetsskydd. Av utbildningsplanen bör det framgå om det finns målgrupper med olika utbildnings- och övningsmål.

Med regelbunden utbildning menas att den ska vara återkommande och behovsanpassad bl.a. med anledning av att:

- säkerhetsskyddsplaneringen reviderats vilket i sin tur påverkat säkerhetsskyddsplanen och behovet av utbildning och övning,
- nya eller reviderade regelverk ställer nya formella krav på en befattning, eller
- nya eller reviderade instruktioner och rutiner som angår säkerhetsskydd.

Andra stycket: Genom att förteckna vem som genomgått vilken utbildning och övning i säkerhetsskydd samt när kan myndigheten 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.

8 kap. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal

1 § Myndigheten ska innan en upphandling påbörjas analysera om uppdraget 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.

Analysen och planen ska dokumenteras.

Kommentar: 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 samt beslut om skyddsåtgärder.

2 § En bedömning av en leverantörs lämplighet ur säkerhetsskyddssynpunkt ska göras innan ett säkerhetsskyddsavtal tecknas. Bedömningen ska dokumenteras.

Kommentar: Bedömningen ska ske av den juridiska personen. 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.

3 § I 2 kap. 6 § säkerhetsskyddslagen (2018:585) föreskrivs om krav på säkerhetsskyddsavtal vid upphandlingar där det förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

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.

Kommentar: *Första stycket:* Paragrafen innehåller en upplysning om vad som gäller enligt lag.

Andra stycket: 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 säkerhetsskyddsklassen begränsat hemlig.[31] Genom att ingå ett säkerhetsskyddsavtal eller affärsavtal med säkerhetsskyddsbestämmelser kan myndigheten säkerställa att säkerhetsskyddet upprätthålls.

[31] Prop. 2017/18:89, s. 141.

4 § Av 4 § myndighetsförordningen (2007:515) följer att myndigheten ska utse vem som är behörig att ingå ett säkerhetsskyddsavtal.

Kommentar: Det finns inga kommentarer till denna föreskrift.

5 § 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.

Kommentar: Uppgifter som efterfrågas kan vara säkerhetsskyddsplan, utkast till säkerhetsskyddsavtal och förfrågningsunderlag.

6 § 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.

Kommentar: Det finns inga kommentarer till denna föreskrift.

7 § 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.

Kommentar: Om den särskilda säkerhetsskyddsbedömningen, analyser eller planer uppdateras, ska säkerhetsskyddsavtalet vid behov revideras.

8 § 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.

Kommentar: Om brister i säkerhetsskyddet har identifierats bör det särskilt framgå i protokollet, som underlag för ett eventuellt återbesök.

Säkerhetsskyddsinstruktionen måste innehålla bestämmelser som motsvarar de bestämmelser för hantering och förvaring som gäller hos myndigheten.

Överlåtelse av säkerhetskänslig verksamhet

9 § En anmälan enligt 2 kap. 9 § säkerhetsskyddsförordningen (2018:658) ska ställas till Försvarsmaktens högkvarter. Anmälan ska göras snarast, dock senast 6 månader innan den säkerhetskänsliga verksamheten ska överlåtas. Anmälan ska omfatta en beskrivning av den verksamhet som myndigheten avser att överlåta, när överlåtelsen planeras att genomföras och på vilket sätt överlåtelsen är avsedd att genomföras.

Kommentar: Det finns inga kommentarer till denna föreskrift.

9 kap. Kontroll och tillsyn av säkerhetsskyddet

1 § 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.

Kommentar: Med regler för säkerhetsskyddet avses säkerhetsskyddslagstiftningen tillsammans med dessa föreskrifter och myndighetens egna föreskrifter, instruktioner och rutiner. Myndigheten ska därmed även kontrollera att egna fastställda regler är aktuella och att de följs.

Om det vid kontrollen upptäcks brister i säkerhetsskyddet bör det av dokumentationen tydligt framgå: vilken regel som inte följs, vad bristen består av, behov av åtgärd som behöver vidtas, vem som är ansvarig för att vidta åtgärden samt när bristen ska vara åtgärdad.

En allvarlig brist, som inte kan åtgärdas omedelbart eller en brist som tar lång tid att åtgärda, kan innebära att myndigheten måste utfärda tillfälliga regler intill dess att bristen är åtgärdad. Sådana tillfälliga regler måste naturligtvis ligga inom myndighetens föreskriftsrätt och får inte innebära att undantag görs från gällande lagstiftning och övriga föreskrifter. Även efterlevnaden av sådana tillfälliga regler ska kontrolleras. Resultatet från kontroller utvärderas fortlöpande för att ge ingångsvärden till myndighetens plan för kontroller.

Kontroll av säkerhetsskyddet kan genomföras som en föranmäld kontroll, vilket ska framgå av en plan, se vidare kommentaren till 9 kap. 3 § nedan. Genom att genomföra en kontroll utan förvarning, eller med kort förvarning, kan brister i säkerhetsskyddet identifieras som annars inte är möjligt genom en föranmäld kontroll. En säkerhetshotande händelse eller verksamhet, kan föranleda en kontroll som inte föranmäls.

2 § 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.

Kommentar: *Första stycket:* Om säkerhetsskyddsavtalet inte avser kvalificerat hemliga uppgifter eller säkerhetskänslig verksamhet som är av synnerlig betydelse för Sverige säkerhet bör regelbundenheten vara minst var tredje år. Är uppdraget som omfattas av säkerhetsskyddsavtal kortare än tre år bör kontrollen genomföras vid minst ett tillfälle, om det inte är uppenbarligt obehövligt, till exempel om uppdraget pågår under mycket kort tid.

Kontroll bör även genomföras så snart det finns kännedom eller misstanke om brister i leverantörens säkerhetsskydd. Även i det fall säkerhetsskyddet regleras på annat sätt än säkerhetsskyddsavtal, kan det finnas anledning för verksamhetsutövaren att kontrollera leverantörens säkerhetsskydd.

Andra stycket: Av dokumentationen ska det, om det upptäcks brister i säkerhetsskyddet, tydligt framgå: vilken del i säkerhetsskyddsavtalet som inte följs, vad bristen består av samt när bristen ska vara åtgärdad.

3 § 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.

Kommentar: En plan ska fungera som ett stöd för den som är ansvarig för att planera, genomföra och dokumentera kontroller i den egna verksamheten och av leverantörer. Planen ska fortlöpande göras aktuell mot bakgrund av bl.a. resultat från genomförda kontroller eller då en reviderad säkerhetsskyddsplanering resulterat i nya eller förändrade säkerhetsskyddskrav i säkerhetsskyddsplanen.

4 § 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.

Kommentar: Tillsyn av säkerhetsskyddet innebär bl.a. tillsyn av att myndigheten följer reglerna om säkerhetsskydd och att säkerhetsskyddet är tillräckligt för den verksamhet som bedrivs. Den dokumentation som avses kan bl.a. vara:

- 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 en 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 säkerhetssynpunkt (3 kap. 3 § säkerhetsskyddsförordningen).
- 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 det 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 §).

Hänvisningar inom parentes avser, om inget annat anges, Försvarsmaktens föreskrifter om säkerhetsskydd.

Även annan dokumentation kan avses för att undersöka om regler om säkerhetsskydd har följts.

10 kap. Anmälan

1 § I 2 kap. 10 § säkerhetsskyddsförordningen (2018:658) framgår när en myndighet ska anmäla säkerhetshotande händelser och verksamhet till Försvarsmakten.
Vid tveksamhet om en säkerhetshotande verksamhet är allvarlig enligt 2 kap. 10 § första stycket 3 säkerhetsskyddsförordningen ska myndigheten samverka med Försvarsmaktens högkvarter.

Kommentar: Att en säkerhetsskyddsklassificerad uppgift röjts, eller befarats röjts, är ett slag av säkerhetshotande verksamhet. 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 medför att allvarlighetskriteriet kan vara uppfyllt. Säkerhetshotande 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 förordningen 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.[32]

2 § Sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse för Sveriges säkerhet ska snarast åtgärdas och anmälas till Försvarsmaktens högkvarter.

Kommentar: 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 utepekad att fullgöra uppgiften som nat-

[32] En ny säkerhetsskyddslag, SOU 2015:25, s. 497-8.

ionell 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.

3 § 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.

Kommentar: Det finns inga kommentarer till denna föreskrift.

11 kap. Internationell verksamhet

1 § 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.

Kommentar: 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 dessa föreskrifter. 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 säkerhetsskyddslavtal (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. ISAF eller MINUSMA).

12 kap. Undantag

1 § Försvarsmakten får medge undantag från föreskrifterna i denna författning.

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

Kommentar: Med hänsyn till att det kan finnas olika oförutsedda situationer som kan medföra att det inte är möjligt att följa en föreskrift är det rimligt att det finns en möjlighet att medge undantag från bestämmelserna i författningen. 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 undantag. Således kan ingen annan person besluta om undantag från en föreskrift utan att först ha blivit bemyndigad av överbefälhavaren. Ett sådant bemyndigande ges t.ex. i 5 kap. 25 § denna författning.

I frågor som rör informationssäkerhet i informationssystem är det FM CIO som bereder undantag med stöd av militära underrättelse- och säkerhetstjänstens säkerhetskontor (MUST SÄKK) och juridiska avdelningen vid ledningsstaben (LEDS JUR) i Högkvarteret. I övriga ärenden om undantag enligt denna författning bereder MUST SÄKK med stöd av LEDS JUR dessa ärenden.

Ikraftträdande- och övergångsbestämmelser

Punkten 1 Denna författning träder i kraft den 1 april 2019.

Kommentar: Det finns ingen kommentar till denna föreskrift.

Punkten 2 Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd med undantag för 2 kap. 2 § som ska gälla till och med den 31 mars 2020.

Kommentar: Se kommentar till punkten 3 nedan.

Punkten 3 Intill den 31 mars 2020 behöver en säkerhetsskyddsklassificerad handling inte förses med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har. Istället ska 2 kap. 2 § Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd tillämpas på en sådan handling.

Kommentar: Av 2 kap. 2 § FFS 2015:2 följer att en hemlig handling ska placeras i en av fyra angivna informationssäkerhetsklasser och att det på en handlings första sida ska finnas en uppgift om i vilken informationssäkerhetsklass uppgiften har placerats i. Samtliga myndigheter som har att följa författningen kommer sannolikt inte att ha hunnit införa t.ex. automatiserade funktioner i informationssystem som kan förse en säkerhetsskyddsklassificerad handling med en anteckning om vilken säkerhetsskyddsklass som uppgifterna i handlingen har, till den 1 april. Det är dessutom inte sannolikt att det har gått att få fram manuella stämplar till den 1 april 2019.

Punkten 4 Handlingar som har märkts enligt 2 kap. 2 § Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd och som inte har arkiverats behöver inte förses med en anteckning om vilken säkerhetsskyddsklass uppgifter i handlingen har.

Kommentar: En handling som inte har arkiverats och som har märkts med en uppgift om i vilken informationssäkerhetsklass uppgifterna i handlingen har placerats i behöver inte ommärkas med en säkerhetsskyddsklass. Inte heller arkiverade handlingar som är märkta med informationssäkerhetsklass behöver märkas om med säkerhetsskyddsklass. Anledningen till övergångsbestämmelsen är att arbetsinsatsen inte står i proportion till det mervärde som en ommärkning skulle ha.

Punkten 5 Har en säkerhetsanalys eller en säkerhetsplan beslutats före den 1 april 2019 gäller dessa som säkerhetsskyddsanalys respektive säkerhetsskyddsplan fram till och med den 31 mars 2020.

Kommentar: För att en myndighet eller en organisationsenhet ska ha möjlighet att ta fram en ny säkerhetsskyddsanalys och säkerhetsskyddsplan får befintliga

analyser och planer gälla som säkerhetsskyddsanalys respektive säkerhetsskyddsplan fram t.o.m. den 31 mars 2020.

Punkten 6 Beslut enligt 2 kap. 9 § första stycket, 2 kap. 12, 18, 20 och 24 §§ samt 3 kap. 1, 6 och 12 §§ Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd får gälla till och med den 31 mars 2020.

Kommentar: Nedan återges huvuddragen i nämnda föreskrifter.

2 kap. 9 § rör beslut om rutiner för kopiering och utdrag ur en hemlig handling i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre.

2 kap. 12 § rör beslut om rutiner för kvittering av muntlig delgivning eller visning av en hemlig handling i informationssäkerhetsklassen HEMLIG/TOP SECRET.

2 kap. 18 § rör beslut om förvaring av hemliga handlingar under kortare tid.

2 kap. 20 § rör beslut om medförande av hemlig handling i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre utanför myndighetens lokaler.

2 kap. 24 § rör beslut om rutiner för distribution av hemlig handling i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre.

3 kap. 1 § rör beslut om tillträdesrätt.

3 kap. 6 § rör beslut om innehav av nycklar, koder och kort.

3 kap. 12 § rör beslut om avvikelse från skyddsnivåer för vissa utrymmen.

Punkten 7 Har en ackreditering beslutats före den 1 april 2019 gäller inte 4 kap. 15, 17, 19-25 §§ i den nya författningen.

Kommentar: Det finns ingen kommentar till denna föreskrift.

Punkten 8 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.

Kommentar: Det finns ingen kommentar till denna föreskrift.

Punkten 9 En analys enligt 7 kap. 7 § Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd får gälla som en särskild säkerhetsskyddsbedömning enligt 3 kap. 1 § säkerhetsskyddsförordningen (2018:658).

Kommentar: I Försvarsmakten benämns en analys enligt 7 kap. 7 § FFS 2015:2 säkerhetsmålsättning. Övergångsbestämmelsen innebär att en sådan målsättning får gälla som en särskild säkerhetsskyddsbedömning. Det innebär t.ex. att ett projekt som rör införande av ett nytt informationssystem och där det redan finns en framtagen säkerhetsmålsättning inte behöver göra om den till en särskild säkerhetsbedömning.

Bilaga 1

Utrymmens indelning i skyddsnivåer

Skyddsnivå 1	Byggnad eller lokal där väggar, golv och tak samt dörrar består av trämaterial, gipsskivor eller korrugerad plåt. Dörrar ska vara låsbara. Flyttbara förvaringsutrymmen med omslutningsytor av tunnplåt eller träkonstruktion.
Skyddsnivå 2	Byggnad eller lokal med certifierad dörr i lägst klass 2 enligt norm SSF 1078, dörr enligt standard SS–EN 1627 RC/MK 3 eller 4, branddörr i plåt, arkivdörr eller D-dörr. Väggar, golv och tak ska bestå av betong med 75 mm, sten med 120 mm eller lättbetong med 150 mm tjocklek. Fönster enligt norm SS 22 44 25 i lägst klass B 3, fönster i kategori P8B enligt standard SS–EN 356 eller galler certifierade enligt Sveriges Försäkringsförbunds normer för galler i gallerklass 3. Omslutningsytorna får bestå av annat material med motsvarande motståndskraft. Flyttbara förvaringsutrymmen såsom vapenkista med beteckning 1-3 eller sprängämneskista.
Skyddsnivå 3	Byggnad eller lokal med certifierad dörr i klass 3 eller 4 enligt norm SSF 1078, dörr enligt standard SS–EN 1627 RC/MK 4, 5 eller 6, splitterskyddad dörr av stål, förstärkt D-dörr (D+), stötvågsdörr och lucka eller gastät ståldörr och lucka med minst 30 mm tjocklek. Väggar, golv och tak ska bestå av armerad betong med en tjocklek av minst 100 mm. Armeringen får inte medge genomkrypning. Armeringen ska vara minst 10 mm i diameter och avståndet från centrum till centrum mellan armeringsstålen får vara högst 250 mm. Fönster enligt norm SS 22 44 25 i lägst klass B 3, fönster i kategori P8B enligt standard SS–EN 356 eller galler certifierade enligt Sveriges Försäkringsförbunds normer för galler i gallerklass 3. Omslutningsytorna får bestå av annat material med motsvarande motståndskraft. Ammunitionsbox som är fast monterad i truppserviceförråd samt flyttbara förvaringsutrymmen såsom värdeskåp enligt norm SS 3150 och med lägre än 100 skyddsvärdespoäng, säkerhetsskåp enligt norm SSF 3492 (SS 3492), standard SS-EN 1143-1 grade 0-III, kassaskåp en-

	ligt norm SS 3493, vapenkista med beteckning 1 B, 2 B, 3 B eller 1 TP, vapenkassun som inte är förankrad på bottenplatta eller motsvarande underlag eller tillträdesskyddad container.
Skyddsnivå 4	Byggnad eller lokal med valvdörr, vapenkassundörr, AD-dörr, VDS-dörr, TD-dörr eller VDB-dörr. Väggar, golv och tak ska bestå av betong med dubbel, förskjuten armering med en tjocklek av minst 180 mm. Armeringen får inte medge genomkrypning. Armeringen ska vara minst 12 mm i diameter och avståndet från centrum till centrum mellan armeringsstålen får vara högst 180 mm. Förskjutning av armering krävs inte vid högst 130 mm avstånd från centrum till centrum mellan armeringsstålen. Väggar, golv, tak och dörrar får bestå av annat material med motsvarande motståndskraft. Byggnad eller lokal får inte ha fönster. Flyttbara förvaringsutrymmen såsom värdeskåp enligt norm SS 3150 med minst 100 skyddsvärdespoäng, standard SS-EN 1143-1 lägst grade IV, säkerhetsbox med beteckning 301 eller 302 samt vapenkassun som är förankrad på bottenplatta eller motsvarande underlag. Utrymme i skyddsnivå 3 som är larmat med seismiska detektorer (vibrationsdetektor) och magnetdetektorer eller placerats i ett volymlarmat utrymme. Om larm har utlösts eller angreppsförsök har konstaterats ska en särskild avdelad styrka vara på plats, inom sådan tid att ett intrång i utrymmet kan försvåras. It-utrymme i skyddsnivå 3 som är larmat med seismiska detektorer (vibrationsdetektorer) och magnetdetektorer eller som är ett volymlarmat utrymme. Om larm har utlösts eller angreppsförsök har konstaterats ska en skyddsåtgärd vidtas så att förlust av information kan försvåras.

Kommentar: Det finns inga kommentarer till denna föreskrift.

Bilaga 2

Utrymmens indelning i zoner

Administrativ zon	En administrativ zon ska utgöras av eller ingå i ett skyddsobjekt enligt skyddslagen (2010:305). En administrativ zon ska vid passerställen vara försedda med ett tekniskt bevakningssystem (system för inpassering) eller personell bevakning eller annan förmåga som säkerställer att endast behöriga har tillträde. Myndigheten ska vid passerställen till administrativ zon kunna kontrollera personer eller fordon. Myndigheten ska besluta vilka som är behöriga till administrativ zon. Myndigheten ska besluta om rutiner och bestämmelser hur besökare till administrativ zon ska hanteras.
Säkerhetszon	En säkerhetszon ska vara belägen i en administrativ zon. En säkerhetszon ska uppfylla de krav som gäller för skyddsnivå 2. Tillträde till en säkerhetszon ska ske med minst tvåfaktors autentisering, t.ex. kort och kod. En säkerhetszon ska vara larmad. Myndigheten ska överväga behovet av att skydda en säkerhetszon från insyn. En säkerhetszon ska vid passerställen vara försedda med ett tekniskt bevakningssystem (system för inpassering) eller personell bevakning eller annan förmåga som säkerställer att endast behöriga har tillträde. Myndigheten ska vid passerställen till en säkerhetszon kunna kontrollera personer eller fordon. Myndigheten ska besluta vilka som är behöriga till en säkerhetszon.

Kommentar: Det finns inga kommentarer till denna föreskrift.

I beredningen av ärendet har deltagit major Mårten Karlsson, chefsanalytiker säkerhetsskydd Karin Widström, informationssäkerhetsspecialist Kim Hakkarainen, it-säkerhetsstrateg Jan Wünsche, kapten Rolf Dahlman, utredare Maria Lind, Martin Lagerström, major Anders Bengtsson.

Detta meddelande har beslutats av överstelöjtnant Patrik Lind. I den slutliga handläggningen har dessutom deltagit säkerhetsskyddsanalytiker Ebba Skygge och, som föredragande, avdelningsdirektör Zenobia Rosander.

Lind, Patrik

C MUST SÄKK SÄKS

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

Sändlista
AST, MS, FS
LG, I 19, K 3, P 4, P 7, P 18, A 9, Lv 6, Ing 2, LedR, TrängR,
1. ubflj, 3. sjöstriflj, 4. sjöstriflj, Amf 1, MarinB,
F 7, F 17, F 21, Hkpflj,
FMLOG, FMTIS, SOG,
MHS K, MHS H, MSS, SSS, LSS, HvSS, FMTS, SWEDEC, SkyddC, FMUndSäkC, FM HRC, FömedC

Inom HKV
REV
SÄKINSP
LEDS
PROD
INS
MUST
HKV AVD
FIHM
FLYGI
SFL

Som orientering utanför myndigheten

Försvarets materielverk	FMV
Försvarets radioanstalt	FRA
Försvarsunderrättelsedomstolen	
Rekryteringsmyndigheten	
Statens inspektion för försvarsunderrättelseverksamhet	SIUN
Totalförsvarets forskningsinstitut	FOI

Fortifikationsverket
Försvarshögskolan
Säkerhetspolisen
Riksarkivet