Kommentarer till Försvarsmaktens föreskrifter (2025:3) om säkerhetsskydd

(OSW)

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

1 kap. Allmänna bestämmelser

1 § Denna författning innehåller kompletterande bestämmelser till säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955). Föreskrifterna gäller för Fortifikationsverket, Försvarshögskolan, de myndigheter som hör till Försvarsdepartementet samt enskilda verksamhetsutövare inom området försvarsmateriel.

Kommentar:

Bemyndigande att meddela föreskrifter inom myndighetens eget samt Försvarets materielverks tillsynsområde framgår av 3 kap. 6, 10 §§ och 8 kap. 7 § säkerhetsskyddsförordningen. Tillsynsområdena beskrivs i 8 kap. 1 § säkerhetsskyddsförordningen. Tillämpningsområdet för Försvarsmaktens föreskrifter (FFS 2025:3) om säkerhetsskydd (”föreskrifterna”) omfattar både myndigheter och andra, enskilda verksamhetsutövare i enlighet med vad som anges här. Tidigare föreskrifter (FFS 2019:2) gällde endast de i bestämmelsen nämnda myndigheterna. En konsekvens av detta är att det i föreskrifterna genomgående används ”verksamhetsutövare” istället för ”myndigheter”. En del bestämmelser som reglerar handlingar samt deras bevarande och gallring har anpassats till det utvidgade tillämpningsområdet där handlingar finns både hos offentliga och enskilda verksamhetsutövare.

Kommentarerna innehåller frekventa jämförelser med, och hänvisningar till, Försvarsmaktens tidigare föreskrifter (FFS 2019:2) om säkerhetsskydd samt Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd. För att öka läsbarheten sker detta genom förkortade omnämnanden, ”Försvarsmaktens tidigare föreskrifter” och ”Säkerhetspolisens föreskrifter”. Om inget annat anges i sammanhanget avses alltså nyss nämnda föreskrifter.

2 § Författningen innehåller kapitel med följande innehåll.

1 kap. – Allmänna bestämmelser

2 kap. – Grundläggande bestämmelser om säkerhetsskydd

3 kap. – Informationssäkerhet

4 kap. – Informationssäkerhet i och kring informationssystem

5 kap. – Fysisk säkerhet

6 kap. – Personalsäkerhet

7 kap. – Skyldigheter när en annan aktör kan få tillgång till säkerhetskänslig verksamhet

8 kap. – Hantering av brister samt säkerhetshotande händelser och verksamhet

9 kap. – Undantag

Kommentar:

Föreskrifternas disposition och indelning i kapitel har justerats jämfört med tidigare föreskrifter. Kapitelindelning följer i hög grad motsvarande indelning i Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd, vilket kan underlätta vid tolkning och jämförelse. Även på paragrafnivå har bestämmelserna i de nya föreskrifterna i högre grad sin motsvarighet i Säkerhetspolisens föreskrifter. En större enhetlighet i Försvarsmaktens och Säkerhetspolisens föreskrifter om säkerhetsskydd, i den mån den är motiverad i sak, bedöms ligga i linje med myndigheternas samordnande roll inom säkerhetsskyddsområdet. Författningstekniska skillnader och det faktum att föreskrifterna ingår i olika föreskriftssamlingar medför dock att det kan förekomma att bestämmelsernas ordval och disposition skiljer sig åt.

3 § Ord och uttryck som används i denna författning har samma innebörd som i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955). I övrigt används följande begrepp med nedan angiven betydelse.

Begrepp	**Betydelse**
Dimensionerande antagonistiska förmågor	Antagonistiska förmågor som vissa säkerhetsskyddsåtgärder ska dimensioneras utifrån, oavsett om de motsvaras av något identifierat säkerhetshot mot den säkerhetskänsliga verksamheten eller inte.
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.

Lagringsmedium	Permanent minnesmedium som används för att kunna lagra och läsa uppgifter.
Röjande signaler	Elektromagnetiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs.
Skadlig kod	Oönskad programkod som är till för att ändra, röja, förstöra, förhindra åtkomst till eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett informationssystem.
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.

Kommentar:

Denna förteckning med förklaringar till de begrepp som används i föreskrifterna har justerats något jämfört med motsvarande förteckning i tidigare föreskrifter. Begrepp som används med samma betydelse som i säkerhetsskyddslagen (2018:585) eller säkerhetsskyddsförordningen har utgått ur förteckningen och har ersatts av en inledande bestämmelse (första stycket) om att ord och uttryck har samma innebörd som i lagen och förordningen. Begreppen *dimensionerande antagonistiska förmågor* och *röjande signaler* har tillkommit och används här på samma sätt som i Säkerhetspolisens föreskrifter.

Företräde för bestämmelser i vissa internationella överenskommelser

4 § Om det i en sådan internationell överenskommelse som avses i 10 kap. 1 eller 2 § regeringsformen förekommer bestämmelser om säkerhetsskydd som avviker från denna författning ska bestämmelserna i överenskommelsen ha företräde, under förutsättning att de inte strider mot en bestämmelse i lag eller förordning.

Kommentar:

En bestämmelse med samma innebörd fanns i 11 kap. 1 § i Försvarsmaktens tidigare föreskrifter och har här flyttats fram till föreskrifternas allmänna bestämmelser, med viss språklig justering. Motsvarande bestämmelse finns i 1 kap. 3 § i Säkerhetspolisens föreskrifter.

Syftet med bestämmelsen är att tydliggöra att andra bestämmelser om säkerhetsskydd kan vara tillämpliga i vissa fall, till följd av internationella överenskommelser. Det finns ett omfattande antal sådana överenskommelser rörande säkerhetsskydd som Sverige har ingått med andra länder eller mellanfolkliga organisationer. Överenskommelserna kallas i internationella sammanhang *General Security Agreement* (förkortas GSA). De flesta överenskommelser som Sverige har ingått har publicerats av regeringen i den s.k. SÖ-serien och går att hitta på regeringens webbplats.

Krav på dokumentation

5 § Bedömningar, analyser, beslut, planer, åtgärder, förstöring, rutiner och uppföljning enligt denna författning ska dokumenteras.

Kommentar:

Bestämmelsen är ny. I Försvarsmaktens tidigare föreskrifter förekom många bestämmelser om att rutiner, beslut m.m. skulle dokumenteras, något som nu har ersatts med detta generella krav på dokumentation.

Bestämmelsen har en motsvarighet i 1 kap. 4 § Säkerhetspolisens föreskrifter. Jämfört med bestämmelsen i Säkerhetspolisens föreskrifter har Försvarsmakten valt att även nämna analyser, förstöring och rutiner i bestämmelsen, vilket förtydligar att dokumentation är ett genomgående krav i arbete med säkerhetsskydd.

Signalskydd

6 § För signalskyddstjänsten, inklusive kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet, finns särskilda bestämmelser i Försvarsmaktens föreskrifter (FFS 2021:1) om signalskyddstjänsten.

Kommentar:

Paragrafen upplyser om att det även finns andra föreskrifter med bestämmelser som kan vara tillämpliga i säkerhetskänslig verksamhet. Motsvarande bestämmelse fanns även i tidigare föreskrifter. Hänvisningen till Försvarsmaktens föreskrifter om signalskyddstjänsten har uppdaterats då nya sådana föreskrifter (FFS 2021:1) har trätt i kraft.

Särskilda underrättelseuppgifter och särskilda underrättelsehandlingar

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

Kommentar:

Bestämmelsen är oförändrad jämfört med Försvarsmaktens tidigare föreskrifter och upplyser om att även andra föreskrifter är tillämpliga i de i bestämmelsen angivna sammanhangen.

2 kap. Grundläggande bestämmelser om säkerhetsskydd

Säkerhetsskyddsanalys

Innehåll

1 § Av 2 kap. 1 § säkerhetsskyddslagen (2018:585) och 2 kap. 1 § säkerhetsskyddsförordningen (2021:955) framgår att den som bedriver säkerhetskänslig verksamhet ska göra en säkerhetsskyddsanalys.

Säkerhetsskyddsanalysen ska innehålla de moment som följer av 2–5 §§.

Säkerhetsskyddsanalysen ska beslutas av verksamhetsutövarens högsta chef eller motsvarande organ.

Kommentar:

Bestämmelsen innehåller, såsom i Försvarsmaktens tidigare föreskrifter, en påminnelse om säkerhetshetsskyddslagens och säkerhetsskyddsförordningens krav på säkerhetsskyddsanalys. Vidare hänvisas till kapitlets övriga paragrafer. Tredje stycket innehåller krav på att högsta chef eller motsvarande ska besluta om säkerhetsskyddsanalysen, ett krav som är nytt och som kan läsas mot bakgrund av 2 kap. 7 § säkerhetsskyddslagen, där det anges att säkerhetsskyddschefen, som ska leda och samordna säkerhetsskyddsarbetet, ska vara direkt underställd verksamhetsutövarens chef/ledning. Kravet om beslut av högsta chef eller motsvarande organ finns även i Säkerhetspolisens föreskrifter (2 kap. 10 §).

Verksamhetsbeskrivning

2 § Säkerhetsskyddsanalysen ska innehålla en beskrivning av verksamheten och organisationen (verksamhetsbeskrivning). I verksamhetsbeskrivningen ska anges vilka delar av verksamheten som är av betydelse för Sveriges säkerhet.

Om den säkerhetskänsliga verksamhet som ska bedrivas skiljer sig åt mellan olika konfliktnivåer ska detta beskrivas. Verksamhetsutövaren ska även dokumentera vilka informationssystem som ska användas vid höjd beredskap.

Kommentar:

I bestämmelsen anges att en verksamhetsbeskrivning ska ingå i säkerhetsskyddsanalysen och vad den ska innehålla. Med olika konfliktnivåer avses (höjd eller högsta) beredskap och krig. Om verksamheten förändras på grund av höjd beredskap ska detta ingå i verksamhetsbeskrivningen. Ett liknande men mindre preciserat krav fanns i 2 kap. 3 § Försvarsmaktens tidigare föreskrifter. I Säkerhetspolisens föreskrifter finns en bestämmelse med krav på verksamhetsbeskrivning i 2 kap. 2 §.

Skyddsvärden

3 § Enligt 2 kap. 5 § säkerhetsskyddslagen (2018:585) ska säkerhetsskyddsklassificerade uppgifter delas in i säkerhetsskyddsklasser. Identifierade skyddsvärden i övrigt ska delas in i konsekvensnivåer utifrån den skada som en antagonistisk handling mot skyddsvärdet kan medföra för Sveriges säkerhet.

Indelningen i konsekvensnivåer ska göras enligt följande:

- Konsekvensnivå A vid synnerligen allvarlig skada för Sveriges säkerhet.
- Konsekvensnivå B vid allvarlig skada för Sveriges säkerhet.
- Konsekvensnivå C vid inte obetydlig skada för Sveriges säkerhet.
- Konsekvensnivå D vid endast ringa skada för Sveriges säkerhet.

Verksamhetsutövaren ska bedöma från vilket eller vilka av perspektiven konfidentialitet, riktighet och tillgänglighet som respektive skyddsvärde är skyddsvärt.

Kommentar:

Bestämmelsen om indelning i konsekvensnivåer är ny; motsvarande finns i Säkerhetspolisens föreskrifter (2 kap. 4 och 5 §§). Att identifiera och värdera även andra skyddsvärden än säkerhetsskyddsklassificerade uppgifter är dock inte någon ny företeelse utan ingår förutom i Säkerhetspolisens föreskrifter även i Försvarsmaktens interna reglering av säkerhetsskydd. Exempel på sådana skyddsvärden är anläggningar, materiel eller system som används i verksamheten.

Konfidentialitet, riktighet och tillgänglighet är perspektiv som används i informationssäkerhetsarbete men som även kan tillämpas för att identifiera och bedöma andra skyddsvärden.

Säkerhetshot och sårbarheter

4 § Om Försvarsmakten har tillhandahållit en beskrivning av dimensionerande antagonistiska förmågor ska verksamhetsutövaren utgå från denna vid den identifiering av säkerhetshot och sårbarheter som ska göras enligt 2 kap. 1 § andra stycket säkerhetsskyddsförordningen (2021:955).

Kommentar:

Bestämmelsen är ny. Motsvarande krav finns i 2 kap. 7–8 §§ Säkerhetspolisens föreskrifter men gäller då Säkerhetspolisens beskrivningar av dimensionerande antagonistiska förmågor (DAF). Krav på att verksamhetsutövare ska ta hänsyn till Försvarsmaktens DAF-beskrivningar förekommer i flera bestämmelser i föreskrifterna. Försvarsmakten kommer att tillhandahålla dessa beskrivningar i syfte att ge verksamhetsutövare bättre förutsättningar för att bedöma relevanta hot som man behöver förhålla sig till. Utifrån DAF-beskrivningar kan också sårbarheter identifieras.

Säkerhetsskyddsåtgärder

5 § Som grund för bedömningen av vilka säkerhetsskyddsåtgärder som är nödvändiga ska verksamhetsutövaren utgå från

1. de identifierade skyddsvärdenas egenskaper och konsekvensnivå, och
2. de säkerhetshot och sårbarheter som finns kopplade till dessa skyddsvärden.

Om Försvarsmakten har tillhandahållit en beskrivning av dimensionerande antagonistiska förmågor ska bedömningen även utgå från den beskrivningen.

Kommentar:

En motsvarande bestämmelse finns i 2 kap. 9 § Säkerhetspolisens föreskrifter i kombination med de andra paragrafer som den hänvisar till.

Ett skyddsvärdes relevanta egenskaper kan exempelvis vara dess geografiska placering, hur det används i verksamheten eller mängd/antal.

Krav ställs på att verksamhetsutövaren, i bedömningen om säkerhetsskyddsåtgärder, även ska utgå från Försvarsmaktens beskrivning av dimensionerande antagonistiska förmågor om en sådan har tillhandahållits. I Försvarsmaktens tidigare föreskrifter (2 kap. 3 §) användes istället begreppet ”dimensionerande hotbeskrivning”.

Säkerhetsskyddsplan

6 § Med säkerhetsskyddsanalysen som grund ska verksamhetsutövaren upprätta en säkerhetsskyddsplan. Av planen ska framgå vilka säkerhetsskyddsåtgärder som ska vidtas, vilken funktion som har ansvaret, vilka resurser som krävs och när respektive åtgärd ska vara genomförd.

Säkerhetsskyddsplanen ska beslutas av verksamhetsutövarens högsta chef eller motsvarande organ.

Kommentar:

Det som anges i bestämmelsens första stycke fanns även i Försvarsmaktens tidigare föreskrifter (2 kap. 4 §) och uttrycks här lite mer kortfattat. Att det ska framgå *vilken funktion* som har ansvaret, inte *vem* som har ansvaret, syftar till att tydliggöra att ansvar knyts till funktioner som kan innehas av olika personer över tid, och inte till personerna själva.

Andra stycket är nytt och innebär att högsta ledningen har ansvar att besluta både säkerhetsskyddsanalysen och säkerhetsskyddsplanen, jfr. 2 kap. 1 § ovan.

Särskild säkerhetsskyddsbedömning

7 § Av 4 kap. 7 § första stycket och 13 § första stycket säkerhetsskyddslagen (2018:585) samt 3 kap. 1 § säkerhetsskyddsförordningen (2021:955) framgår att en verksamhetsutövare inför vissa förfaranden och driftsättningar av informationssystem ska göra en särskild säkerhetsskyddsbedömning.

Verksamhetsutövaren ska i den särskilda säkerhetsskyddsbedömningen beskriva

1. vilka skyddsvärden som kan komma att påverkas och på vilket sätt,
2. vilka säkerhetshot som finns kopplade till dessa säkerhetsskyddsvärden och den säkerhetskänsliga verksamheten i stort,
3. vilka sårbarheter som finns kopplade till dessa skyddsvärden och den säkerhetskänsliga verksamheten i stort samt hur sårbarheterna påverkas av förfarandet eller driftsättningen av informationssystemet, och
4. vilka säkerhetsskyddsåtgärder som är nödvändiga som en följd av förfarandet eller driftsättningen av informationssystemet.

Av en särskild säkerhetsskyddsbedömning inför driftsättning av ett informationssystem enligt 3 kap. 1 § säkerhetsskyddsförordningen ska även framgå vilka rutiner, resurser och kompetenser för drift, förvaltning, övervakning och hantering av incidenter som är nödvändiga ur säkerhetsskyddssynpunkt under hela systemets livscykel.

Kommentar:

Bestämmelsen är ny; motsvarighet finns i Säkerhetspolisens föreskrifter (2 kap. 13 §). Bestämmelsen beskriver vad som ska ingå i den särskilda säkerhetsskyddsbedömningen. Vid driftsättning av informationssystem ska bedömningen innehålla ytterligare moment, som beskrivs i tredje stycket.

En särskild säkerhetsskyddsbedömning inför driftsättning av ett informationssystem enligt denna paragraf förutsätter att verksamhetsutövaren har analyserat vilken verksamhet informationssystemet ska stödja och hur och vilka uppgifter som ska hanteras i systemet. De analyser och bedömningar som gjorts beskrivs i den särskilda säkerhetsskyddsbedömningen. Se även dokumentationskravet i 1 kap. 5 § i dessa föreskrifter.

Kontroll och uppföljning

8 § Verksamhetsutövaren ska systematiskt

1. utvärdera om säkerhetsskyddsåtgärderna ger avsedd effekt, och
2. identifiera brister och sårbarheter i säkerhetsskyddet.

Kommentar:

Försvarsmaktens tidigare föreskrifter innehöll krav om att regelbundet och vid behov kontrollera säkerhetsskyddet i verksamheten samt om utvärdering av säkerhetsskyddsplaneringen.

Utvärdering och identifiering ska enligt förevarande bestämmelse ske systematiskt, vilket innebär att verksamhetsutövaren aktivt behöver bedöma behovet av att så sker, på vilket sätt och hur ofta. Att utvärdera regelbundet, d.v.s. med fasta intervaller, men utan behovsbedömning, är inte systematiskt. Bestämmelsen motsvaras delvis av 2 kap. 14 § i Säkerhetspolisens föreskrifter, som även innehåller ytterligare krav.

3 kap. Informationssäkerhet

Godkännande av informationssystem

1 § Säkerhetsskyddsklassificerade uppgifter i en viss säkerhetsskyddsklass får endast behandlas i informationssystem eller på lagringsmedium som verksamhetsutövaren godkänt för lägst den säkerhetsskyddsklass som uppgifterna har.

Kommentar:

Bestämmelsen är ny. Motsvarande bestämmelse finns i Säkerhetspolisens föreskrifter (3 kap. 1 §). Ett informationssystem eller lagringsmedium som är avsett för lägre säkerhetsskyddsklass har inte ett tillräckligt säkerhetsskydd för att kunna hantera uppgifter som är placerade i högre säkerhetsskyddsklasser.

Behörighetsförteckning

2 § Verksamhetsutövaren ska dokumentera vilka personer som är behöriga att få del av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre.

Kommentar:

Bestämmelsen finns även i Försvarsmaktens tidigare föreskrifter (3 kap. 1 §).

I 2 kap. 2 § säkerhetsskyddsförordningen anges vilka förutsättningar som ska vara uppfyllda för att en person ska vara behörig att ta del av säkerhetsskyddsklassificerade uppgifter. Om inte något annat följer av bestämmelser i lag, ska personen ha bedömts vara pålitlig från säkerhetssynpunkt, ha tillräckliga kunskaper om säkerhetsskydd, och behöva uppgifterna för att kunna utföra sitt arbete eller på annat sätt medverka i den säkerhetskänsliga verksamheten.

En behörighetsförteckning används så att endast behöriga personer som står med på förteckningen kan komma att ta del av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre. Personer som endast får ta del av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig, ska också uppfylla kravet på behörighet i 2 kap. 2 § säkerhetsförordningen, men behöver inte finnas med i förteckningen.

Behörighetsförteckningen är ett instrument för exempelvis en expedition att säkerställa att den som hämtar upp en handling eller ett lagringsmedium uppfyller villkoren. För att få en tillförlitlig dokumentation bör en behörighetsförteckning innehålla uppgifter så att varje person unikt kan identifieras även vid senare tidpunkter, såsom namn och personnummer.

Rutiner

3 § Verksamhetsutövaren ska ha rutiner för skydd och hantering av säkerhetsskyddsklassificerade uppgifter under hela deras livscykel. Rutinerna ska utformas med beaktande av ett konfidentialitets-, riktighets- och tillgänglighetsperspektiv.

Rutinerna ska minst omfatta vad som gäller för märkning, spårbarhet, upprättande, kopiering, utskrift, utdrag, kvittering, förvaring, distribution, medförande, transport, inventering och förstöring.

Kommentar:

Bestämmelsen är ny; motsvarande finns i Säkerhetspolisens föreskrifter (3 kap. 3 §). Med livscykel avses hantering av säkerhetsskyddsklassificerade uppgifter från upprättande till förstöring.

Rutinerna ska bland annat förebygga att s.k. svartkopior uppstår. Svartkopior är exemplar av säkerhetsskyddsklassificerade handlingar som avses i 5 § och 6 § andra stycket och inte har registrerats i enlighet med 9 §. En förlust av en svart-

kopia kan inte uppmärksammas i en inventering av säkerhetsskyddsklassificerade handlingar då uppgift om kopian (exemplaret) saknas i registret över verksamhetsutövarens säkerhetsskyddsklassificerade handlingar.

4 § Verksamhetsutövarens rutiner för ändring eller borttagning av säkerhetsskyddsklass ska minst reglera vem som får besluta om ändringen eller borttagningen samt hur den ska genomföras.

Kommentar:

Motsvarande bestämmelse finns i Försvarsmaktens tidigare föreskrifter (3 kap. 9 §). Rutiner för vem som får besluta om ändring av säkerhetsklass bidrar till enhetlighet i klassificeringen och till att sådana beslut baseras på sakkunskap om de förhållanden uppgifterna rör, för att kunna avgöra om ändringen är lämplig och får genomföras.

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

Märkning

5 § Allmänna handlingar, och handlingar som skulle betraktas som allmänna handlingar om de hade förvarats hos en myndighet, ska om de innehåller säkerhetsskyddklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre märkas med

1. handlingens beteckning,
2. antal sidor, och
3. antal bilagor om sådana finns.

Fysiska handlingar ska även märkas med exemplarnummer.

Kommentar:

Motsvarande bestämmelse avseende allmänna handlingar hos myndigheter fanns även i Försvarsmaktens tidigare föreskrifter (3 kap. 11 §). Tillägg har gjorts för handlingar hos andra verksamhetsutövare än myndigheter, som tidigare inte omfattades av Försvarsmaktens föreskrifter. Motsvarande bestämmelse finns i 3 kap. 4 och 5 §§ Säkerhetspolisens föreskrifter.

Bestämmelsen gäller endast allmänna handlingar (och motsvarande) med uppgifter i säkerhetsskyddsklassen konfidentiell eller högre. Allmänna krav på att skydda säkerhetsskyddsklassificerade uppgifter innebär dock att alla sådana uppgifter behöver identifieras för att på så sätt kunna styra tillgång och åtkomst. Av 3 kap. 7 § säkerhetsskyddsförordningen framgår att alla säkerhetsskyddsklassificerade handlingar behöver ska förses med anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har.

För att underlätta märkning av säkerhetsskyddsklassificerade handlingar är det lämpligt att stöd för märkningen ingår i dokumentmallar i verksamhetsutövarens informationssystem.

Det som utgör en handling i pappersform kan i ett 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.

En enskild verksamhetsutövare behöver för tillämpning av bestämmelsen bedöma om en handling i säkerhetsskyddsklassen konfidentiell eller högre skulle betraktas som en allmän handling om verksamhetsutövaren hade varit en myndighet. Vad som utgör och inte utgör en allmän handling framgår av 2 kap. tryckfrihetsförordningen (TF). Där anges bl.a. under vilka förutsättningar en handling kan anses vara en minnesanteckning, ett utkast eller ett koncept som inte är allmän handling.

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

Ett säkerhetsskyddsklassificerat lagringsmedium som innehåller uppgifter i säkerhetsskyddsklassen konfidentiell eller högre ska märkas med identifieringsuppgift på höljet.

Om det säkerhetsskyddsklassificerade 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:

Bestämmelsen är en sammanslagning av motsvarande bestämmelser i 3 kap. 8 och 13 §§ i Försvarsmaktens tidigare föreskrifter. Motsvarande bestämmelse finns i 3 kap. 11 § Säkerhetspolisens föreskrifter.

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

Vissa fast monterade lagringsmedier, vanligtvis sådana som är avsedda för drift eller säkerhetskopiering, är inte alltid möjliga att märka. Om ett lagringsmedium inte kan märkas görs märkning istället på det sätt som anges i tredje stycket.

Med lämplig plats menas att märkning behöver vara synlig och i nära anslutning till utrustningen, så att det klart framgår för en person som befinner sig vid utrustningen att den innehåller säkerhetsskyddsklassificerade lagringsmedier. Lämplig plats kan i sådana fall vara placering på en dörr eller lucka till det utrymme där utrustningen är placerad.

Om ett fast monterat lagringsmedium monteras bort måste lagringsmediet märkas.

7 § Av 3 kap. 7 § andra stycket säkerhetsskyddsförordningen (2021:955) framgår att om en säkerhetsskyddsklassificerad handling kan antas komma att lämnas över till en utländsk aktör ska den förses med en anteckning om ursprungsland om det inte är olämpligt.

Detsamma ska gälla för säkerhetsskyddsklassificerade lagringsmedier som kan antas komma att lämnas över till en utländsk aktör.

Kommentar:

Motsvarande bestämmelser fanns i 3 kap. 27 och 28 §§ i Försvarsmaktens tidigare föreskrifter. Bestämmelsen innebär att kravet i 3 kap. 7 § säkerhetsskyddsförordningen om anteckning om ursprungsland även ska tillämpas när lagringsmedier överlämnas till utländsk aktör.

I 3 kap. 9 § säkerhetsskyddsförordningen anges villkoren för att säkerhetsskyddsklassificerade uppgifter kan lämnas till en utländsk aktör eller en mellanfolklig organisation. I 8 kap. 3 § offentlighets- och sekretesslagen (2009:400) (OSL) finns villkor för när uppgifter som omfattas av sekretess får lämnas till en ut-

ländsk aktör 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 att Försvarsmakten, Försvarets materielverk eller Totalförsvarets forskningsinstitut ska kunna lämna ut uppgifter som omfattas av så kallad försvarssekretess enligt 15 kap. 2 § OSL.

8 § Ett beslut att en handling inte längre ska vara indelad i säkerhetsskyddsklassen kvalificerat hemlig får fattas först efter hörande av den verksamhetsutövare som har upprättat handlingen.

Kommentar:

Motsvarande bestämmelse fanns även i Försvarsmaktens tidigare föreskrifter (3 kap. 10 §). Bestämmelsen gäller märkning av säkerhetsskyddsklass på handlingar, inklusive tryckta skrifter och elektroniska handlingar, men beslut kan även påverka märkning av lagringsmedier och utrustning som används för sådana handlingar, se 3 kap. 6 §. Ett motsvarande krav på samråd med den som upprättat handlingen finns i 3 kap. 7 § Säkerhetspolisens föreskrifter.

Register

9 § Verksamhetsutövaren ska föra register över handlingar och lagringsmedier som avses i 5 § och 6 § andra stycket.

Av registret ska handlingens beteckning, säkerhetsskyddsklass, antal exemplar och mottagare av respektive exemplar framgå. För elektroniska handlingar ska i stället framgå beteckning, säkerhetsskyddsklass och vilket informationssystem handlingen behandlas i. För lagringsmedier ska i stället identifieringsuppgifter och säkerhetsskyddsklass framgå.

För varje exemplar som förvaras hos verksamhetsutövaren ska det av registret framgå vem som har kvitterat exemplaret, när det har inventerats och om det har återlämnats, förkommit, arkiverats eller förstörts.

Kommentar:

Motsvarande bestämmelser fanns i 3 kap. 18 och 19 §§ i Försvarsmaktens tidigare föreskrifter. Motsvarande bestämmelse om register över handlingar finns i 3 kap. 10 § Säkerhetspolisens föreskrifter. Jämfört med tidigare föreskrifter används ordet register genomgående för både handlingar och lagringsmedier, mot bakgrund av att föreskrifterna även är tillämpliga på enskilda verksamhetsutövare som, med undantag för offentliga ägda bolag inom vissa sammanhang,

inte är skyldiga att ha ett diarium. Myndigheter som ska ha ett register enligt denna bestämmelse kan låta det utgöra en del av diariet, eller hålla det separerat.

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.

Kvittering

10 § Den som tar emot en handling eller ett lagringsmedium som avses i 5 § eller 6 § andra stycket ska kvittera mottagandet med underskrift, namnförtydligande och datum. Ett namnförtydligande får vara en kod.

Mottagande av en elektronisk handling behöver inte kvitteras om mottagandet sker i ett informationssystem där det i en säkerhetslogg registreras vem som har tagit del av handlingen.

Kommentar:

Motsvarande bestämmelse fanns i 3 kap. 15 § i Försvarsmaktens tidigare föreskrifter. Bestämmelse om kvittering finns i Säkerpolisens föreskrifter.

Kvittering och registrering möjliggör spårbarhet av vilka personer som tagit del av en handling eller ett lagringsmedium och är väsentligt 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.

Både kvittering och återlämnande ska antecknas i registret enligt 3 kap. 9 § i dessa föreskrifter. Kvittensen kan förvaras av verksamhetsutövarens registratur, eller motsvarande funktion, till dess att personen lämnar tillbaka den handling eller det lagringsmedium som kvittot avser. Vid återlämning kan personen får en kopia av kvittensen för att kunna visa att handlingen eller lagringsmediet har återlämnats.

11 § Verksamhetsutövaren ska bevara kvittensen eller säkerhetsloggen i minst tio år. Kvittensen eller säkerhetsloggen för en handling eller ett lagringsmedium i säkerhetsskyddsklassen kvalificerat hemlig ska bevaras i minst 25 år.

För det allmännas verksamhet finns i stället bestämmelser om bevarande och gallring i arkivlagen (1990:782) och föreskrifter som har meddelats med stöd av den lagen.

Kommentar:

Motsvarande bestämmelse fanns i 3 kap. 15 § i Försvarsmaktens tidigare föreskrifter.

Tiden att en verksamhetsutövare ska vara skyldig att bevara kvittenser eller säkerhetsloggar behöver avgränsas. Tiden har satts till 10 respektive 25 år, beroende på säkerhetsskyddsklassen, vilket i de allra flesta fall torde vara en tillräcklig lång tid för att tillmötesgå eventuella behov att konsultera äldre loggar eller kvittenser. Nämnda bevarandetider överensstämmer också med preskriptionstiden för många brott som kan sammankopplas med hantering av säkerhetsskyddsklassificerade handlingar (vissa sådana brott är dock är undantagna från preskription). Samma tider för förvaring finns i 3 kap. 14 § Säkerhetspolisens föreskrifter.

Bestämmelsen avser kvittens eller säkerhetslogg enligt 3 kap. 10 §. Den paragrafen gäller handlingar enligt 3 kap. 5 §, vilket är allmänna handlingar, eller motsvarande hos enskilda verksamhetsutövare, och lagringsmedier enligt 6 § andra stycket.

Med det allmännas verksamhet avses främst verksamhet hos myndigheter men även viss verksamhet i t.ex. offentligt ägda bolag kan omfattas av arkivlagen (1990:782). I dessa fall tillämpas bestämmelser om bevarande och gallring i arkivlagen och de föreskrifter som har meddelats med stöd av den lagen.

12 § Vad som föreskrivs i 10 § 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 eller lagringsmediet begär det.

Kraven gäller inte heller för personal som arbetar med drift av informationssystem för sådana säkerhetsskyddsklassificerade lagringsmedier som hanteras i driften av informationssystemen.

Kommentar:

Motsvarande bestämmelse fanns i 3 kap. 16 § i Försvarsmaktens tidigare föreskrifter och finns i 3 kap. 16 § Säkerhetspolisens föreskrifter.

De angivna personalkategorierna kommer regelbundet i kontakt med eller omhändertar en stor mängd handlingar och lagringsmedier. Syftet med den inledande meningen är att arkiv-, expeditions- och sambandspersonal som regel inte ska behöva kvittera handlingar när de hanterar dem på expedition, för arkivering eller motsvarande.

Vad gäller personal med ansvar för drift av informationssystem kan dessa inte sällan få tillgång till säkerhetsskyddsklassificerade handlingar eller lagringsmedier i utförandet av sina arbetsuppgifter. Deras åtkomst är dock endast av teknisk karaktär och betyder inte att de ska, får eller kommer att ta del av innehållet. Istället betraktas deras hantering som en del av en teknisk åtgärd inom ramen för den säkra förvaringsplats där handlingar eller lagringsmedier befinner sig. Därför bedöms det inte nödvändigt att ha ett kvitteringskrav för sådan hantering.

Muntlig delgivning

13 § När uppgifter i säkerhetsskyddsklassen kvalificerat hemlig lämnas muntligt eller genom visning, ska verksamhetsutövaren dokumentera vilka som har tagit del av uppgifterna.

Verksamhetsutövaren ska bevara dokumentationen i minst 25 år. För det allmännas verksamhet finns i stället bestämmelser om bevarande och gallring i arkivlagen (1990:782) och föreskrifter som har meddelats med stöd av den lagen.

Kommentar:

I 3 kap. 17 § i Försvarsmaktens tidigare föreskrifter fanns bestämmelse om rutiner för kvittering av uppgifter i säkerhetsskyddsklassificerade allmänna handlingar placerade i säkerhetsskyddsklassen kvalificerat hemlig. Ändringar har här gjorts som tydliggör att verksamhetsutövaren ska dokumentera vilka som tagit del av sådana uppgifter. Tillägg har även gjorts med krav på att dokumentationen ska bevaras.

Förvaring

14 § En säkerhetsskyddsklassificerad handling och ett säkerhetsskyddsklassificerat lagringsmedium ska vara under kontroll eller förvaras i ett förvaringsutrymme enligt 5 kap. 12–16 §§.

Kommentar:

Bestämmelsen är ny. Motsvarande bestämmelse finns i Säkerhetspolisens föreskrifter (3 kap. 9 §). Att en verksamhetsutövare ska ha kontroll över eller skydd för säkerhetsskyddsklassade handlingar och lagringsmedier kan anses följa redan av övergripande krav på informationssäkerhet.

Att handlingar och lagringsmedier ska vara under kontroll betyder att ingen obehörig kan komma åt de medförda handlingarna eller lagringsmedierna utan att personen som ansvarar för dem upptäcker det, se även 16 §.

Medförande utanför verksamhetsutövarens lokaler

15 § Säkerhetsskyddsklassificerade handlingar och lagringsmedier i säkerhetsskyddsklassen konfidentiell eller högre får inte medföras från verksamhetsutövarens områden, byggnader och andra lokaler eller objekt utan att sådant medförande har godkänts av verksamhetsutövaren.

Kommentar:

Motsvarande bestämmelse fanns i 3 kap. 20 § i Försvarsmaktens tidigare föreskrifter. Formuleringen har justerats mot bakgrund av att föreskrifterna numera även är tillämpliga på andra än myndigheter.

Med medförande avses här att en person för sitt arbete behöver transportera och förvara handlingar eller lagringsmedier utanför verksamhetsutövarens områden, byggnader och andra lokaler eller objekt.

Utgångspunkten är att handlingar och lagringsmedier förvaras i verksamhetsutövarens lokaler eller de andra platser som nämns i bestämmelsen, där de är under kontroll av verksamhetsutövaren. Verksamheten kan dock vara sådan att anställda ibland har behov av att medföra handlingar och lagringsmedier utanför dessa lokaler. Krav på godkännande innebär att verksamhetsutövaren vid ett sådant beslut enligt denna paragraf kan beakta till vilket ändamål handlingar och lagringsmedier medförs och till vilka platser medförandet sker.

16 § Säkerhetsskyddsklassificerade handlingar och lagringsmedier som medförs från verksamhetsutövaren ska vara under kontroll av den som medför dem eller förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaring av handlingarna respektive lagringsmedierna inom verksamhetsutövarens lokaler eller områden.

Kommentar:

Motsvarande bestämmelse fanns i 3 kap. 20 § i Försvarsmaktens tidigare föreskrifter.

Att handlingar och lagringsmedier ska vara under kontroll betyder att ingen obehörig ska kunna komma åt de medförda handlingarna eller lagringsmedierna utan att personen som medför dem upptäcker det.

Ett exempel på när handlingarna eller lagringsmedierna står under kontroll är om handlingarna eller lagringsmedierna läggs i en väska, portfölj eller liknande som personen alltid bär med sig eller håller under uppsikt under hela medförandet. Ett exempel på motsatsen är när en väska, portfölj eller liknande med handlingar eller lagringsmedier lämnas obevakad av den som medför dem, även om det är en kortare stund, eller om denne lämnar/låser in dem för förvaring hos hotell eller konferensanläggning.

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.

Inventering

17 § Av 3 kap. 8 § första stycket säkerhetsskyddsförordningen (2021:955) framgår att säkerhetsskyddsklassificerade handlingar som innehåller uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska inventeras minst en gång per år. I övrigt gäller att fysiska handlingar och lagringsmedier som avses i 5 § och 6 § andra stycket ska inventeras minst en gång per år.

Av 3 kap. 8 § andra stycket säkerhetsskyddsförordningen framgår att för arkiverade handlingar gäller kravet på inventering enbart för handlingar i säkerhetsskyddsklassificeringen kvalificerat hemlig.

Inventering ska genomföras av en annan person än den som förvarar handlingarna och lagringsmedierna.

Kommentar:

Motsvarande bestämmelser fanns i 3 kap. 21 och 22 §§ i Försvarsmaktens tidigare föreskrifter.

Inventering innebär en regelbunden kontroll av att varje exemplar av en handling är i behåll. 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 handlingar som ska inventeras ska, enligt 3 kap. 9 §, finnas i ett register hos verksamhetsutövaren.

Lagringsmedier som personal har kvitterat vid mottagandet kan 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 eller handling saknas vid en inventering och inte kan återfinnas efter eftersökning, måste händelsen rapporteras enligt 2 kap. 4 § säkerhetsskyddsförordningen.

Distribution

18 § Verksamhetsutövaren ska se till att nödvändiga säkerhetsskyddsåtgärder vidtas vid distribution av säkerhetsskyddsklassificerade uppgifter inom och utom verksamheten.

En försändelse med säkerhetsskyddsklassificerade handlingar eller lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre ska sändas med en distributör som har godkänts av verksamhetsutövaren. Distributören ska kunna verifiera att försändelsen har levererats till mottagaren.

Kommentar:

Motsvarande bestämmelse fanns i 3 kap. 22 § i Försvarsmaktens tidigare föreskrifter.

Observera att det enligt 3 kap. 3 § finns krav på rutiner gällande distribution av handlingar.

Om skyddet för handlingarna och lagringsmedierna blir lägre under distribution utanför verksamheten, jämfört med när de hanteras inom verksamheten, riktas skyddsåtgärderna rimligen mot 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 distributör får vara en utomstående part som tillhandahåller tjänsten att genomföra fysisk distribution av en försändelse till mottagaren. För försändelser med säkerhetsskyddsklassificerade handlingar och lagringsmedier i säkerhetsskyddsklassen begränsat hemlig finns inget krav att distributören ska ha godkänts av verksamhetsutövaren. Det finns dock inte något hinder mot att även för sådana försändelser anlita den distributör som verksamhetsutövaren godkänt för handlingar och lagringsmedier som är placerade i högre säkerhetsskyddsklasser.

Undantag från krav om kurirförbindelser

19 § En verksamhetsutövare får inom ramen för egen verksamhet som bedrivs i utlandet distribuera säkerhetsskyddsklassificerade handlingar på annat sätt än vad som föreskrivs i 3 kap. 10 § första stycket säkerhetsskyddsförordningen (2021:955), om distributionen är under verksamhetsutövarens kontroll och omfattas av säkerhetsskyddsåtgärder för att upptäcka och försvåra obehörig åtkomst till handlingarna.

En verksamhetsutövare får i verksamhet som omfattas av en överenskommelse 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:

Motsvarande bestämmelse fanns i 3 kap. 29 § i Försvarsmaktens tidigare föreskrifter.

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.

Det är inte alltid möjligt att använda Utrikesdepartementets kurirförbindelser. Bestämmelsen ger ett utrymme för distribution på annat sätt inom den egna verk-

samheten i utlandet, under de förutsättningar som anges här. Exempelvis kan i fallet av svensk kontingent i utlandet distributionen underlättas av transport som genomförs av Försvarsmaktens personal i militärt fartyg, luftfartyg eller fordon.

Enligt vissa säkerhetsskyddsavtal mellan länder 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.

Återlämning och förstöring

20 § Verksamhetsutövaren ska se till att säkerhetsskyddsklassificerade handlingar och lagringsmedier återlämnas eller förstörs när de inte längre behövs för arbetet.

Verksamhetsutövaren ska säkerställa att fysiska säkerhetsskyddsklassificerade handlingar och lagringsmedier förstörs på ett sådant sätt att uppgifterna inte går att återskapa.

För säkerhetsskyddsklassificerade allmänna handlingar finns bestämmelser om bevarande och gallring i arkivlagen (1990:782) och föreskrifter som har meddelats med stöd av den lagen.

Kommentar:

Bestämmelsen gäller såväl allmänna handlingar som handlingar som inte är allmänna. Hur förstöringen sker är upp till verksamhetsutövaren att avgöra. I enlighet med 3 kap. 3 § ska verksamhetsutövaren ha rutiner för förstöring av handlingar. Fram till dess att förstöringen är genomförd ska handlingarna och lagringsmedierna förvaras enligt kraven i dessa föreskrifter.

Bestämmelsen gäller alla exemplar av en handling. När en handling eller ett lagringsmedium har förstörts upphör behovet av att upprätthålla kontroll över dessa. Att dokumentera att en handling eller ett lagringsmedium har förstörts är, ur säkerhetsskyddssynpunkt, det sista steget i livscykeln för handlingar och lagringsmedier, se 3 kap. 3 § i dessa föreskrifter.

Av bestämmelsens andra stycke följer att det inte är tillräckligt att förstöring görs så att ett återskapande endast försvåras. Metoder för förstöring måste utgå från de fysiska egenskaperna hos det som ska förstöras, så att ett återskapande av uppgifterna efter förstöring inte är möjligt.

I krig och stridssituationer kan det orsaka skada för Sverige om informationstillgångar faller i orätta händer. 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.

4 kap. Informationssäkerhet i och kring informationssystem

Kommentar:

Såsom framgår av rubrikerna närmast före 1 och 6 §§ gäller bestämmelserna i 4 kap. 1-5 §§ alla informationssystem som har betydelse för säkerhetskänslig verksamhet, medan bestämmelserna från 6 § gäller den snävare kretsen av informationssystem som används i säkerhetskänslig verksamhet.

Informationssystem som har betydelse för säkerhetskänslig verksamhet

Dokumentation

1 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet dokumentera systemens uppbyggnad, logiska samband och inbördes beroenden mellan olika komponenter.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 11 § i Försvarsmaktens tidigare föreskrifter.

För att ett informationssystems säkerhetsskydd ska kunna upprätthållas under systemets livslängd är det nödvändigt att ha dokumentation över systemet och säkerhetsåtgärderna. Dokumentationen måste hållas uppdaterad för att kunna kontrollera att säkerhetsskyddet fortfarande är tillräckligt. Vid förändringar kan det finnas behov av att genomföra nya hot- och sårbarhetsanalyser för systemet.

Dokumentation enligt 1 § behöver i förekommande fall innehålla en beskrivning av systemets hård- och mjukvara, systemets kommunikation och beroende, informationsflöden och datautbyten samt vad som i övrigt är av betydelse för att kunna upprätthålla säkerheten i och kring system.

Granskning vid utveckling och anskaffning

2 § Hård- och mjukvara som ska användas i informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara bedömd som tillförlitlig ur säkerhetssynpunkt före användning.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 7 § i Försvarsmaktens tidigare föreskrifter. Motsvarande bestämmelser finns i 4 kap. 1-2 §§ Säkerhetspolisen föreskrifter.

För att kunna bedöma tillförlitlighet ur säkerhetssynpunkt för hård- eller mjukvaror behöver de sårbarhetsgranskas. Det är inte möjligt att helt förvissa sig om att en hård- eller mjukvara är tillförlitlig. Det är däremot viktigt att göra en helhetsbedömning av om tillförlitligheten är tillräcklig för att hård- och mjukvaran ska kunna användas i ett informationssystem som är av betydelse för säkerhetskänslig verksamhet.

Det behöver även bedömas om det finns säkerhetslösningar som kan minska eller eliminera eventuella sårbarheter. För att kunna ha förtroende för leverantörer och underleverantörer kan leverantörerna samt deras rutiner och åtgärder för säkerhet i utveckling, tillverkning, leverans och kundstöd behöva granskas. Även andra åtgärder kan behövas, såsom skydd under leverans. För hårdvara handlar det främst om fysiskt skydd, för mjukvara kan det också vara logiska skydd, t.ex. med kryptografiska funktioner.

Drift och förvaltning av informationssystem

3 § Verksamhetsutövaren ska planera för fortlöpande drift och förvaltning av de informationssystem som har betydelse för säkerhetskänslig verksamhet så att säkerhetsskyddet i och kring systemen upprätthålls.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 10 § i Försvarsmaktens tidigare föreskrifter.

Att planera för att upprätthålla systemens säkerhetsskydd innebär att verksamhetsutövaren behöver känna till vilka resurser, rutiner och kompetenser som krävs för drift och förvaltning av systemet och säkerställer att säkerhetsskyddet i och kring informationssystemet kan upprätthållas under hela systemets livscykel. Drift och förvaltning behöver planeras tidigt vid framtagning av informationssystemet. Om tillräckliga resurser med rätt kompetens inte finns kan säkerheten i ett informationssystem inte upprätthållas över tid.

Övervakning

4 § Verksamhetsutövaren ska kontinuerligt övervaka de informationssystem som har betydelse för säkerhetskänslig verksamhet.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 12 § i Försvarsmaktens tidigare föreskrifter.

Övervakning av informationssystem sker i syfte att kunna upptäcka, analysera, spåra och bedöma förändringar och händelser som kan indikera skadlig eller obehörig påverkan, åtkomst eller nyttjande av systemet. Övervakningen är en del av säkerhetsskyddsarbetet och sker i enlighet med de rutiner som verksamhetsutövaren har beslutat. Hur den kontinuerliga övervakningen ska genomföras behöver bedömas med beaktande av den säkerhetskänsliga verksamhet som systemet används inom och i vilken säkerhetsskyddsklass de uppgifter som behandlas i systemet är placerade. För system som inte är anslutna till elektroniska kommunikationsnät, behöver verksamhetsutövaren tillse att övervakningen sker på annat sätt.

5 § Verksamhetsutövaren ska förse informationssystem som har betydelse för säkerhetskänslig verksamhet och som kommunicerar med andra informationssystem med funktioner för intrångsdetektering och intrångsskydd.

Kommentar: Motsvarande bestämmelse fanns i 4 kap. 19 § i Försvarsmaktens tidigare föreskrifter.

Intrångsdetektering och intrångsskydd är tekniska åtgärder som vidtas för att detektera och avvärja intrångsförsök, skadlig inverkan på informationssystemet och obehörig kommunikation med systemet.

Informationssystem som används i säkerhetskänslig verksamhet

Godkännande

6 § Verksamhetsutövaren ska inför ett godkännande enligt 3 kap. 3 § säkerhetsskyddsförordningen (2021:955) granska vidtagna säkerhetsskyddsåtgärder.

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

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 6 § i Försvarsmaktens tidigare föreskrifter.

Av 3 kap. 3 § säkerhetsskyddsförordningen framgår att informationssystem som används i säkerhetskänslig verksamhet ska godkännas av verksamhetsutövaren.

Syftet med granskning av skyddsåtgärderna inför godkännande är dels att tillse att dessa uppfyller de krav som ställs, dels att kunna upptäcka och åtgärda eventuella brister innan informationssystemet tas i drift. Skyddsåtgärder innehåller ofta tekniska säkerhetsfunktioner i systemet men kan också vara administrativa eller fysiska, eller en kombination av dessa.

Syftet med att granskningen utförs av andra än dem som utvecklat systemet är att åstadkomma ett oberoende perspektiv på skyddsåtgärderna. Att låta den som tagit fram en skyddsåtgärd också granska den innebär en risk att sårbarheter förbises.

Åtgärder vid förändringar i och kring informationssystem

7 § 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 förändringar ska den särskilda säkerhetsskyddsbedömningen och dokumentationen av informationssystemet uppdateras.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 13 § i Försvarsmaktens tidigare föreskrifter.

Om ny kunskap om hot eller sårbarheter pekar på att säkerhetsskyddet måste anpassas ska säkerhetsskyddsåtgärderna ses över. Detta kan göras både genom egna resurser/aktiviteter och genom att ta del av eller dela kunskap med andra verksamhetsutövare. 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. Mindre förändringar, t.ex. säkerhetsuppdatering av programvara, som kan ske utan att ny funktionalitet tillförs och någon påtaglig risk för att skyddet försämras, kan normalt göras utan att uppdatera den särskilda säkerhetsskyddsbedömningen. Informationssystemets dokumentation ska dock uppdateras så att den är aktuell och korrekt. Här bör också observeras att flera mindre förändringar över tid kan ge en ackumulerad, större effekt.

8 § Ett informationssystem som ska användas i säkerhetskänslig verksamhet ska godkännas på nytt om det sker förändringar i eller kring systemet som kan påverka säkerheten i systemet negativt. Ett sådant godkännande ska föregås av förnyad granskning enligt 6 §.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 14 § i Försvarsmaktens tidigare föreskrifter.

Mindre förändringar, som t.ex. säkerhetsuppdatering av programvara, som kan göras utan att ny funktionalitet tillförs och utan någon påtaglig risk för att skyddet försämras, kan normalt göras utan ny granskning och godkännande. Vid väsentliga förändringar finns alltid en risk att skyddet oavsiktligt nedsätts, varför sådana förändringar omfattas av kravet på granskning enligt denna bestämmelse.

Autentisering och behörighetskontroll

9 § Ett informationssystem som ska användas i säkerhetskänslig verksamhet ska kunna verifiera användares identitet och behörighet. Åtkomst till uppgifter, funktioner och resurser i systemet ska vara behörighetsstyrd.

Vad som gäller för användare gäller också för informationssystem och processer i informationssystem.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 15 § i Försvarsmaktens tidigare föreskrifter.

Verifiering av identitet och behörighet syftar till att rätt användare endast kommer åt det som den kan anses ha behov av. Åtkomsten efter verifieringen kan av samma skäl också tidsbegränsas. Verifiering av identitet och behörighet är inte begränsad till vem som får använda ett informationssystem utan gäller även för funktioner och processer i systemet.

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, för att säkerställa rätt behörighet, utföras med verifiering av användarens identitet och behörigheter.

10 § Utställda identiteter ska vara unika över tid.

Kommentar:

Bestämmelsen är ny.

Med unik identitet avses att en identifierare eller ett användarnamn entydigt ska kunna knytas till en person eller ett system och ett konto eller process för att den eller det utan tvetydighet kan kopplas till handlingar eller resurser i ett senare skede.

Med unik över tid menas att identifierare - såsom användarkonton - ska kunna försäkra ansvar och spårbarhet även i loggar och historik över tidigare åtkomst. En ny användare eller ett nytt konto ska inte ärva resurser, behörigheter eller auktorisering från tidigare motsvarande med samma namn.

11 § Verksamhetsutövaren ska systematiskt granska identiteter och behörigheter för att se till att de fortsatt är ändamålsenliga och aktuella.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 16 § i Försvarsmaktens tidigare föreskrifter.

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 när 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

12 § Verksamhetsutövaren ska säkerställa spårbarhet av händelser som är av betydelse för säkerheten i systemet enligt 3 kap. 4 § säkerhetsskyddsförordningen (2021:955) genom att dessa registreras i säkerhetsloggar och analyseras systematiskt.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 17 § i Försvarsmaktens tidigare föreskrifter.

Säkerhetsloggning är registrering, manuellt, automatiskt 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 system. Det kan t.ex. röra sig om in- och utloggningar, förändringar av behörighetsinställningar och åtkomst, överföring av information, uttag eller utskrifter av känsliga uppgifter. Säkerhetsloggarna skapar spårbarhet som vid en systematisk uppföljning såväl som på förekommen anledning kan användas för analys av både intrång eller annan otillåten påverkan och risken för sådana händelser. Säkerhetsloggar avser alla typer av loggar där händelser som har, eller kan ha betydelse för säkerheten registreras, dvs. även driftloggar och applikationsloggar kan vara aktuella.

13 § Verksamhetsutövaren ska vidta åtgärder för att skydda säkerhetsloggar och säkerhetskopior mot obehörig åtkomst, ändring eller förstöring.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 18 § i Försvarsmaktens tidigare föreskrifter.

Loggar och säkerhetskopior behöver skyddas så att de finns tillgängliga när det behövs, att deras riktighet bevaras och att obehörig åtkomst försvåras. Med skydd avses även fysiska skyddsåtgärder. Att loggar och säkerhetskopior finns tillgängliga när de behövs innebär att loggar behöver kunna läsas över tid utan specifik hård- eller mjukvara samt att säkerhetskopior kan återläsas.

Godkänd separationsmekanism

14 § Verksamhetsutövaren ska se till att informationssystem som ska användas i säkerhetskänslig verksamhet separeras fysiskt eller med anpassad av verksamhetsutövaren godkänd separationsmekanism från övriga informationssystem.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 20 § i Försvarsmaktens tidigare föreskrifter.

Separation mellan informationssystem kan vara fysisk eller logisk. Med fysisk separation menas att systemen använder helt olika fysiska infrastrukturer, dvs. olika datorer, servrar, lagring, nätverkskomponenter och kablar.

Vid fysisk separation är det relativt lätt att verifiera att separationen finns och den ger normalt en hög tilltro för att separationen upprätthålls.

Med logisk separation menas att separation upprätthålls genom tekniska åtgärder i informationssystemen, t.ex. brandväggar, nätverksprodukter, filtreringskomponenter eller dioder, eller genom kryptering med olika nycklar. Vid logisk separation finns det en risk för att sårbarheter i de tekniska funktionerna eller misstag vid konfigurationen leder till att separationen inte upprätthålls. Denna typ av risk kan vara mycket svår att upptäcka vid en granskning.

Skydd mot skadlig kod

15 § Verksamhetsutövaren ska ha förmåga att försvåra och upptäcka inmatning, försök till inmatning, exekvering eller försök till exekvering av skadlig kod eller annan obehörig kod i informationssystem som ska användas i säkerhetskänslig verksamhet.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 21 § i Försvarsmaktens tidigare föreskrifter.

Syftet med skydd mot skadlig kod är att förhindra obehörig påverkan på informationssystemet. Eftersom det inte går att avgöra syftet med en kod som förs in i systemet, måste skyddsåtgärder omfatta all obehörig kod, dvs. all kod som inte beslutats ska användas i systemet. Åtgärderna ska även ta sikte på situationer där koden ändå kommit in i systemet och faktiskt exekveras. Syftet är att få ett försvar på djupet som kan förhindra angrepp när skadlig kod trots åtgärderna ändå har förts 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

16 § Verksamhetsutövaren ska ha förmåga att upptäcka och försvåra obehörig förändring av informationssystem som ska användas i säkerhetskänslig verksamhet.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 22 § i Försvarsmaktens tidigare föreskrifter.

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; vilka skyddsåtgärder som ska vidtas måste framgå av den särskilda säkerhetsskyddsbedömningen och tillhörande systemdokumentation.

Säkerhetskopiering

17 § Ett informationssystem som ska användas i säkerhetskänslig verksamhet ska ha funktionalitet för att kunna säkerhetskopiera och återställa

1. mjukvara,
2. konfigurationsdata, och
3. andra uppgifter som är av betydelse för verksamheten, informationssystemets funktion och säkerhetsförmågor, som inte lätt kan återskapas på annat sätt.

Kontroll att säkerhetskopior kan återläsas ska genomföras regelbundet.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 23 § i Försvarsmaktens tidigare föreskrifter.

Data som inte behöver säkerhetskopieras kan t.ex. vara sådant som kan hämtas från en masterdatakälla i ett annat informationssystem eller sådant som uppdateras kontinuerligt från en extern sensor och där historiken inte behöver sparas. Programvara som lätt kan installeras om från installationsmedia behöver 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, men också gällande regelverk. Observera att även loggar kan behöva säkerhetskopieras, se § 13 i detta kapitel.

18 § 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:

Motsvarande bestämmelse fanns i 4 kap. 24 § i Försvarsmaktens tidigare föreskrifter.

Säkerhetskopior av data från ett informationssystem som används i säkerhetskänslig verksamhet innehåller i de flesta fall säkerhetsskyddsklassificerade uppgifter och därför ska ges ett skydd utifrån detta. Skydd mot utpressningspåverkan bör omhändertas vid designen av säkerhetskopieringslösningen. En bedömning måste även göras om säkerhetskopior ska lagras på annan plats utan anslutning till nätverk.

Skydd mot röjande signaler och obehörig avlyssning

19 § Verksamhetsutövaren ska för ett informationssystem som ska användas för att hantera uppgifter i säkerhetsskyddsklassen konfidentiell eller högre vidta åtgärder för att försvåra obehörig inhämtning av röjande signaler utifrån identifierade säkerhetshot.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 25 § i Försvarsmaktens tidigare föreskrifter.

Röjande signaler (RÖS) beskrivs i begreppslistan i 1 kap. i dessa föreskrifter. Det är icke önskvärda elektromagnetiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs. Verksamhetsutövares skyldighet att beakta förekomst av röjande signaler följer av 3 kap. 4 § säkerhetsskyddsförordningen. Kravet på skyddsåtgärder mot röjande signaler gäller informationssystem som avses behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre.

För att uppnå erforderlig nivå på skyddet mot röjande signaler kan olika åtgärder vidtas, som innebär skydd i informationssystem, i anläggningen där informationssystemet finns, eller en kombination av dessa. Åtgärderna kan avse informationssystemets installation, dess placering i anläggningen, separationsavstånd till annan utrustning, dämpande åtgärder i anläggningen m.m.

Skydd mot röjande, ändring och förstöring

20 § Ett informationssystem som ska användas i säkerhetskänslig verksamhet ska ha funktionalitet som försvårar att uppgifter kommer obehöriga till del, ändras eller förstörs vid kommunikation mellan delsystem inom ett informationssystem, eller vid kommunikation till andra informationssystem.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 26 § i Försvarsmaktens tidigare föreskrifter, med den skillnaden att kravet där beskrevs gälla informationssystem som *har betydelse för* säkerhetskänslig verksamhet. Verksamhetsutövaren kan behöva vidta skyddsåtgärder för att säkerställa att informationssystem har funktioner som i möjligaste mån försvårar de icke önskvärda händelser som anges i bestämmelsen.

Säkerhetskonfiguration

21 § Ett informationssystem som ska användas i säkerhetskänslig verksamhet ska konfigureras så att funktioner och tjänster som behövs tillåts. Lämpliga och möjliga säkerhetsfunktioner i systemet ska användas.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 27 § i Försvarsmaktens tidigare föreskrifter. Liknande krav ställs i Säkerhetspolisens föreskrifter (4 kap. 16 §).

Syftet med kraven 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 eller rekommenderade funktioner kan vara tillverkaren, välrenommerade säkerhetsföretag, svenska eller utländska myndigheter.

Samråd

22 § En begäran om samråd enligt 3 kap. 2 § säkerhetsskyddsförordningen (2021:955) ska göras på av Försvarsmakten anvisat sätt.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 9 § i Försvarsmaktens tidigare bestämmelser.

I 3 kap. 2 § första stycket säkerhetsskyddsförordningen anges att en verksamhetsutövare, innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras, ska samråda med Försvarsmakten.

Av andra stycket i samma bestämmelse framgår att samrådsskyldigheten även gäller i fråga om andra informationssystem än sådana som anges i första stycket, om obehörig åtkomst till systemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig.

Försvarsmakten kan i samråd bl.a. efterfråga den särskilda säkerhetsskyddsbedömningen, granskningsrapporter, m.m.

Undantag från krav på skyddsåtgärder

23 § Om det finns synnerliga skäl får Försvarsmakten besluta om undantag från 3 kap. 4 § första stycket säkerhetsskyddsförordningen (2021:955).

Ansökan om undantag ska göras på av Försvarsmakten anvisat sätt.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 28 § i Försvarsmaktens tidigare föreskrifter. I den nya bestämmelsen anges dock att det krävs synnerliga skäl för ett undantag.

Försvarsmakten kommer att ange hur en ansökan om undantag ska ske. Ansökan kommer att behandlas av Försvarsmakten och av ansökan behöver det minst framgå vilka krav som undantaget rör, vad anledningen är till varför de inte bör eller går att uppfylla samt när verksamhetsutövaren bedömer att kraven kommer att kunna uppfyllas.

Hantering av säkerhetsskyddsklassificerade lagringsmedier

24 § 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 delats in i.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 2 § i Försvarsmaktens tidigare föreskrifter.

Ett informationssystem som är avsett för behandling av uppgifter upp till en viss säkerhetsskyddsklass har inte ett tillräckligt säkerhetsskydd för att kunna hantera ett lagringsmedium för uppgifter i en högre säkerhetsskyddsklass. 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 säkerhetsskyddsklass konfidentiell eller begränsat hemlig.

Ett lagringsmedium är ett permanent minnesmedium. Det finns även tillfälliga databärare, som inte omfattas av denna bestämmelses krav. Andra krav på skydd av säkerhetsskyddsklassificerade uppgifter och rutiner för hantering av sådana uppgifter gäller dock när sådana uppgifter finns på en tillfällig databärare.

25 § Ett säkerhetsskyddsklassificerat lagringsmedium som har innehållit uppgifter i säkerhetsskyddsklassen begränsat hemlig eller konfidentiell får återanvändas i informationssystem med samma eller högre säkerhetsskyddsklass om verksamhetsutövaren har rutiner för att säkerställa att tidigare lagrade säkerhetsskyddsklassificerade uppgifter inte kan utläsas ur lagringsmediet.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 4 § i Försvarsmaktens tidigare föreskrifter.

Säkerhetsskyddsklassificerade lagringsmedier kan återvändas under de förutsättningar som beskrivs i bestämmelsen.

26 § Ett säkerhetsskyddsklassificerat lagringsmedium som innehåller eller har innehållit uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig får inte återanvändas i annat informationssystem än där uppgifterna har hanterats.

Kommentar:

Motsvarande bestämmelse fanns i 4 kap. 3 § i Försvarsmaktens tidigare föreskrifter. Den bestämmelsen var dock begränsad till att reglera att ett lagringsmedium som tidigare använts för uppgifter i nämnda säkerhetsskyddsklasser inte återanvändas i system som inte var avsedda för (minst) denna nivå. Den nya bestämmelsen utökar kravet till att återanvändning inte får ske i något annat informationssystem än det eller de där uppgifterna har hanterats.

Kravet gäller även om de aktuella uppgifterna har tagits bort. Borttagning av data från ett lagringsmedium lämnar ofta spår som gör det möjligt att återskapa uppgifterna.

5 kap. Fysisk säkerhet

Åtgärder för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan

1 § Verksamhetsutövaren ska utifrån identifierade säkerhetshot och behov av säkerhetsskyddsåtgärder

1. använda personell bevakning, teknisk bevakning eller en kombination av dessa för att upptäcka obehörigt tillträde till eller skadlig inverkan på den säkerhetskänsliga verksamheten tidigt så att åtgärder för att försvåra och hantera ger avsedd effekt,

2. vidta försvårande åtgärder som fördröjer obehörigt tillträde till den säkerhetskänsliga verksamheten till dess att hanterande åtgärder hinner vidtas,

3. vidta försvårande åtgärder som reducerar skadlig inverkan på den säkerhetskänsliga verksamheten, och

4. se till att åtgärder kan vidtas för att hantera obehörigt tillträde till eller skadlig inverkan på den säkerhetskänsliga verksamheten.

Om Försvarsmakten har tillhandahållit en beskrivning av dimensionerande antagonistiska förmågor ska verksamhetsutövaren även anpassa åtgärderna utifrån den.

Kommentar:

Bestämmelsen är ny. Motsvarande krav finns i Säkerhetspolisens föreskrifter (5 kap. 1 §).

Såsom anges i paragrafens rubrik ska åtgärderna bidra till att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan. Bestämmelsen är utformad på ett sådant sätt att fokus läggs på det som ska uppnås. Detaljerad reglering av åtgärder undviks och i stället ges verksamhetsutövaren utrymme och ansvar att själv välja åtgärder.

Verksamhetsutövarens behov av åtgärder kan varieras vid normalläge, säkerhetspolitisk kris eller krig. Åtgärder behöver därför utgå från identifierade säkerhetshot och eventuella dimensionerande antagonistiska förmågor.

Styrning av tillträde

2 § Verksamhetsutövaren ska styra tillträdet till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs så att endast behöriga får tillträde. Rutiner ska finnas för tilldelning och förändring av behörigheter. Behöriga ska inte ges större tillträde än nödvändigt.

Kommentar:

Motsvarande bestämmelse fanns i 5 kap. 2 § i Försvarsmaktens tidigare föreskrifter. Jämfört med tidigare bestämmelse har kravet formulerats på ett sätt som sätter fokus på verksamhetsutövarens ansvar att styra tillträde samt att vid behov begränsa eller förändra behörighet.

Bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 2 §).

3 § Verksamhetsutövaren ska utfärda tillstånd för besökare till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Tillstånden för besökare ska föras i en förteckning.

Kommentar:

Motsvarande bestämmelse fanns i 5 kap. 3 § i Försvarsmaktens tidigare föreskrifter. Jämfört med tidigare bestämmelse anges inte längre detaljer om kontroll av identitet och dokumentation av besöket. Detta återfinns nu till viss del i 5 kap. 4 §, se kommentar nedan.

En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 3 §).

4 § Verksamhetsutövaren ska besluta på vilket sätt identitet och behörighet ska kontrolleras för tillträde till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Kommentar:

Bestämmelsen har i viss mån sin motsvarighet i 5 kap. 3 § i Försvarsmaktens tidigare föreskrifter, som dock i mer detalj beskrev hur identitetskontroll vid besök skulle kontrolleras och dokumenteras. I den nya bestämmelsen läggs fokus på verksamhetsutövarens ansvar att ta ställning till frågan om hur kontroll av både

identitet och behörighet ska ske. Inom Försvarsmakten har detta skett genom Försvarsmaktens interna bestämmelser med föreskrifter om godkända identitetshandlingar i Försvarsmakten.

En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 4 §).

5 § En förteckning över tillträde ska bevaras

- i två år om uppgifter, handlingar eller lagringsmedier i säkerhetsskyddsklassen begränsat hemlig hanteras inom området, byggnaden, anläggningen eller objektet,
- i tio år om uppgifter, handlingar eller lagringsmedier i säkerhetsskyddsklassen konfidentiell eller hemlig hanteras inom området, byggnaden, anläggningen eller objektet, och
- i 25 år om uppgifter, handlingar eller lagringsmedier i säkerhetsskyddsklassen kvalificerat hemlig hanteras inom området, byggnaden, anläggningen eller objektet.

För det allmännas verksamhet finns i stället bestämmelser om bevarande och gallring i arkivlagen (1990:782) och föreskrifter som har meddelats med stöd av den lagen.

Kommentar:

Bestämmelsen är ny. Förteckningen över tillträde ska motsvara den nivå på vilken kontroll av tillträde sker. Om kontroll exempelvis inte endast sker vid ett områdes yttre gräns utan även inom området, inför tillträde till en särskild avdelning, bör även detta ingå i förteckningen.

Förutom förteckning över tillträde enligt denna bestämmelse finns även krav på förteckning över tillstånd, se 5 kap. 3 §.

Myndigheter som omfattades av Försvarsmaktens tidigare föreskrifter, samt eventuella offentligt ägda bolag som i sin verksamhet ska följa arkivlagen, ska följa bestämmelserna i den lagen och tillhörande föreskrifter. För andra enskilda verksamhetsutövare gäller det som anges i bestämmelsen.

Koder, kort och nycklar

6 § Kort, nycklar och anteckningar med uppgift om kod ska vara under kontroll eller förvaras i ett förvaringsutrymme med motsvarande skyddsnivå som de ger tillträde till, om de var för sig ger tillträde till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Förvaringsutrymmet ska vara godkänt av verksamhetsutövaren enligt 12 §. Krav på godkännande ställs i 13 §. Skyddsnivåer framgår av bilagan till denna författning.

Kommentar:

Motsvarande bestämmelse fanns i 5 kap. 7 § i Försvarsmaktens tidigare föreskrifter. Bestämmelsens formulering har justerats för att följa lydelsen av sin motsvarighet i 5 kap. 5 § i Säkerhetspolisens föreskrifter, med den skillnaden att det där endast anges att förvaringsutrymmet ska vara godkänt av verksamhetsutövaren.

Begreppet under kontroll innebär t.ex. att det dagliga användandet sker på ett sådant sätt att ingen obehörig kan komma åt dessa. Begreppet kan även innebära att innehavaren alltid bär nyckel och kort med sig och på sig, att anteckning om kod inte förvaras tillsammans med kortet eller att den personliga koden döljs vid användandet.

7 § Verksamhetsutövaren ska ha en förteckning över kort, nycklar och koder som ger tillträde till områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Av förteckningen ska det framgå till vem de har lämnats och när de lämnades samt var reservkod eller reservnyckel förvaras. Det ska vidare framgå om och i så fall när återlämnande skett.

Kommentar:

Motsvarande bestämmelse fanns i 5 kap. 10 § i Försvarsmaktens tidigare föreskrifter. En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 6 §). Bestämmelsens krav syftar till att åstadkomma spårbarhet både av kort, nycklar och koder och av personers tillgång till dessa.

Hantering av föremål som är olämpliga ur säkerhetsskyddssynpunkt

8 § Verksamhetsutövaren ska ha rutiner för att säkerställa att föremål som är olämpliga ur säkerhetsskyddssynpunkt inte förs till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Kommentar:

Bestämmelsen är ny. En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 7 § första stycket). Vad som utgör olämpliga föremål får avgöras i sammanhanget. Exempel kan vara vapen, farliga ämnen eller en kamera. Rutinerna för att säkerställa att föremål inte förs in eller till områden m.m. kan exempelvis vara fysisk kontroll eller information till anställda och besökare.

9 § Elektronisk utrustning som kan möjliggöra obehörig avlyssning av samtal får inte medföras vid samtal som behandlar säkerhetsskyddsklassificerade uppgifter.

Kommentar:

Bestämmelsen är ny. En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 7 § andra stycket).

Bestämmelsen gäller all elektronisk utrustning som kan sända eller registrera det som sägs, vilket bland annat innefattar mobiltelefoner, digitala armbandsur och hörapparater. Kravet innebär att en bedömning måste göras om sådan utrustning behöver lämnas på annan plats innan samtalet börjar. Förbudet gäller även vid samtal som inledningsvis inte bedömdes handla om säkerhetsskyddsklassificerade uppgifter men som utvecklas på ett sådant sätt att sådana uppgifter ändå riskerar att behandlas. Om elektronisk utrustning har medförts kan samtalet behöva avbrytas.

Skydd mot obehörig avlyssning av samtal

10 § Verksamhetsutövaren ska besluta om vilka utrymmen som är godkända för regelbundna samtal som behandlar säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre. Av beslutet ska framgå den högsta säkerhetsskyddsklass för de uppgifter som får samtalas om i utrymmet.

Ett utrymme får godkännas endast om det är försett med eller omges av åtgärder för att försvåra obehörig avlyssning utifrån identifierade säkerhetshot. Om Försvarsmakten har tillhandahållit en beskrivning av dimensionerande antagonistiska förmågor ska den särskilt beaktas av verksamhetsutövaren.

Kommentar:

Motsvarande bestämmelse fanns i 5 kap. 20 § Försvarsmaktens tidigare föreskrifter. Nytt är att verksamhetsutövaren i förekommande fall särskilt ska beakta Försvarsmaktens beskrivning av dimensionerande antagonistiska förmågor. En bestämmelse med liknande lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 8 §).

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.

Skydd mot obehörig insyn

11 § Verksamhetsutövaren ska besluta om vilka utrymmen som är godkända för regelbunden behandling av säkerhetsskyddsklassificerade uppgifter. Av beslutet ska framgå den högsta säkerhetsskyddsklass för de uppgifter som får behandlas i utrymmet.

Ett utrymme får godkännas endast om det är försett med eller omges av åtgärder för att försvåra obehörig insyn utifrån identifierade säkerhetshot. Om Försvarsmakten har tillhandahållit en beskrivning av dimensionerande antagonistiska förmågor ska verksamhetsutövaren även utgå från den.

Kommentar:
Bestämmelsen är ny. En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 9 §).

Förvaringsutrymmen

12 § Verksamhetsutövaren ska besluta om vilka förvaringsutrymmen som är godkända för förvaring av

1. säkerhetsskyddsklassificerade uppgifter,
2. säkerhetsskyddsklassificerade lagringsmedier, och
3. kort, nycklar och anteckningar med uppgift om kod, som var för sig ger tillträde till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Kommentar:

Bestämmelsen är ny. Krav på förvaringsutrymmen fanns även i Försvarsmaktens tidigare föreskrifter men nu anges uttryckligen att verksamhetsutövaren ska godkänna sådana utrymmen för förvaring av det som anges i bestämmelsen. En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (5 kap. 10 § första stycket, med den skillnaden att den endast gäller kategorierna 1 och 3 (uppgifter respektive kort, nycklar och anteckningar).

13 § Ett förvaringsutrymme får godkännas endast om det är försett med eller omges av åtgärder för att upptäcka, försvåra och hantera obehörigt tillträde utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Försvarsmakten har tillhandahållit en sådan.

Om Försvarsmakten inte har tillhandahållit en beskrivning av dimensionerande antagonistiska förmågor får ett förvaringsutrymme godkännas endast om det uppfyller kraven enligt 14–16 §§. I bilagan till denna författning anges vilka krav som gäller för respektive skyddsnivå.

Kommentar:

Bestämmelsen är delvis ny. Motsvarighet till första stycket i bestämmelsen finns i Säkerhetspolisens föreskrifter (5 kap. 10 § andra stycket).

En bilaga där kraven för de olika skyddsnivåerna anges, samt hänvisning till denna bilaga, fanns även i Försvarsmaktens tidigare föreskrifter (5 kap. 12 §). I övrigt är bestämmelsen ny. Med utgångspunkt i 5 kap. 1 § i dessa föreskrifter

anges här att identifierade säkerhetshot, dimensionerande antagonistiska förmågor och de krav som anges i dessa föreskrifter styr verksamhetsutövarens godkännande av förvaringsutrymmen.

Kommentar:

14 § Säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade lagringsmedier i säkerhetsskyddsklassen begränsat hemlig
ska vara under kontroll eller förvaras inlåsta i ett förvaringsutrymme eller i en låst lokal. Endast den som är behörig att ta del av uppgiften eller lagringsmediet ska ha tillträde till lokalen eller förvaringsutrymmet. Lokalen eller förvaringsutrymmet ska uppfylla de krav som gäller för skyddsnivå 1.

Motsvarande bestämmelse fanns i 5 kap. 15 § i Försvarsmaktens tidigare föreskrifter. Observera att kravet på behörighet enligt denna bestämmelse även gäller för tillträde av drift- eller förvaltningspersonal, t.ex. i IT-utrymmen, men att det inte innebär att denna personalkategori därmed är fria att ta del av innehållet i handlingar eller lagringsmedier.

15 § Säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade lagringsmedier i säkerhetsskyddsklassen konfidentiell eller hemlig ska vara under kontroll, eller förvaras inlåsta i ett förvaringsutrymme som uppfyller de krav som gäller för lägst skyddsnivå 3 och som är försett med larm.

Kommentar:

Motsvarande bestämmelse fanns i 5 kap. 16 § i Försvarsmaktens tidigare föreskrifter. Där angavs dock olika skyddsnivåer (2 och 3) beroende på om det rörde sig om en säkerhets- respektive administrativ zon. Möjlighet till att besluta om avsteg från kravet i denna bestämmelse finns, se 5 kap. 17 §.

16 § Säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade lagringsmedier i säkerhetsskyddsklassen kvalificerat hemlig ska vara under kontroll, eller förvaras inlåsta i ett utrymme som uppfyller de krav som gäller för skyddsnivå 4 och som är försett med larm.

Kommentar:

Motsvarande bestämmelse fanns i 5 kap. 17 § i Försvarsmaktens tidigare föreskrifter.

Avsteg från krav på förvaringsutrymmen

17 § Om det finns särskilda skäl får verksamhetsutövaren besluta om förvaringsutrymmen som avviker från kraven i 14–16 §§ förutsatt att motsvarande skydd kan upprätthållas.

Kommentar:

Motsvarande bestämmelse fanns i 5 kap. 18 § i Försvarsmaktens tidigare föreskrifter.

6 kap. Personalsäkerhet

Utbildning

1 § Utbildning i säkerhetsskydd enligt 5 kap. 1 § säkerhetsskyddsförordningen (2021:955) ska genomföras systematiskt.

Kommentar:

Bestämmelserna om utbildning fanns tidigare i ett separat kapitel, Utbildning och övning, men är nu sammanslagna med kapitlet om personalsäkerhet för att tydliggöra att personalsäkerhet omfattar såväl säkerhetsprövning som utbildning i säkerhetsskydd.

Förändringen är även en anpassning till Säkerhetspolisens föreskrifter.

I Försvarsmaktens tidigare föreskrifter användes begreppet ”regelbundet” i 7 kap. 2 § och syftade där på periodicitet. I nuvarande föreskrifter används i stället begreppet ”systematiskt”. Att utbildningen ska genomföras systematiskt menas att den ska genomföras enligt en upprättad utbildningsplan samt vara behovsanpassad utifrån de krav som ställs på den enskilda befattningen.

Att systematiskt utbilda personal, eller andra som deltar i verksamheten, bidrar till att motverka oaktsamhet och bristande kunskap 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 särskilt viktigt i säkerhetskänslig verksamhet.

2 § Verksamhetsutövaren ska se till att innehållet i utbildningen anpassas efter deltagarnas funktioner och ansvar i verksamheten. Innehållet i utbildningen ska framgå av en utbildningsplan.

Deltagande i utbildning ska dokumenteras. Av dokumentationen ska även tidpunkt för utbildningen och dess innehåll framgå.

Kommentar:

I Försvarsmaktens tidigare föreskrifter reglerades i 7 kap. 2 § första stycket att omfattningen och innehållet i utbildningen skulle utgå från myndighetens säkerhetsskyddsplan. Denna bestämmelse är nu ersatt med en bestämmelse som anger att innehållet ska framgå av en utbildningsplan. Syftet med denna förändring är att belysa att det väsentliga är att det finns en plan för systematisk utbildning, och att det är mindre viktigt var planen finns dokumenterad. Det finns dock inga hinder mot att utbildningsplanen utgör en del av säkerhetsskyddsplanen.

Förändringen är även en anpassning till Säkerhetspolisens föreskrifter.

En utbildningsplan utgår från målgruppernas olika utbildnings- och övningsbehov. Det kan vara lämpligt att det framgår vilken utbildning i säkerhetsskydd som olika personalkategorier ska genomgå samt olika utbildningsmål för olika målgrupper, exempelvis grundläggande utbildning i säkerhetsskydd samt en säkerhetsgenomgång för vissa och mer specialiserade utbildningar för andra.

En utbildningsplan kan behöva revideras på grund av exempelvis reviderad säkerhetsskyddsplanering eller ändrade regler och rutiner avseende säkerhetsskydd.

Andra stycket: Genom att förteckna vem som genomgått vilken utbildning i säkerhetsskydd samt när kan verksamhetsutövaren även följa upp en enskilds utbildningsbehov. En förteckning ger även stöd för en långsiktig planering av utbildningsinsatser. Förteckningen kan även användas för att låta den enskilda skriftligen bekräfta att man tagit del av utbildning.

3 § Verksamhetsutövaren ska se till att berörd personal och andra aktörer som deltar i den säkerhetskänsliga verksamheten får kännedom om vilka skyddsvärden som har identifierats vara säkerhetsskyddsklassificerade eller ansetts utgöra säkerhetskänslig verksamhet i övrigt.

Kommentar:

Bestämmelsen är ny; syftet är att mer specifikt ange vad kravet på utbildning av personal i detta kapitel innebär vad gäller kunskap om skyddsvärden i verksamheten.

För att förebygga sådana sårbarheter som den s.k. mänskliga faktorn kan utgöra i en verksamhet är information och utbildning om säkerhetsskydd viktiga delar av säkerhetsskyddet. Sårbarheter vid t.ex. myndigheter kan inte sällan direkt kopplas samman med anställda som av okunskap, obetänksamhet eller bekvämlighet inte följer de krav på säkerhetsskydd som gäller för verksamheten.

Säkerhetsskyddsåtgärder kan uppfattas som krångliga, tidsödande och begränsande. Att, inom ramen för utbildning, tydligt beskriva vad som är skyddsvärt, varför det är skyddsvärt samt hur dessa skyddsvärden ska hanteras ökar sannolikheten att personal och andra aktörer får en bättre förståelse och i förlängningen kan hantera dessa skyddsvärden mer korrekt.

Säkerhetsprövning

Befattningsanalys

4 § Verksamhetsutövaren ska analysera vilka anställningar samt annat deltagande i verksamhetsutövarens säkerhetskänsliga verksamhet som ska

1. placeras i säkerhetsklass,
2. föranleda säkerhetsprövning utan placering i säkerhetsklass, och
3. föregås av registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen (2018:585).

Verksamhetsutövaren ska vid analysen utgå från verksamhetsutövarens säkerhetsskyddsanalys och särskilt beakta förekomsten av internationella åtaganden om säkerhetsskydd.

Kommentar:

Motsvarande bestämmelse fanns i 6 kap. 3 § i Försvarsmaktens tidigare föreskrifter, men har fått en tydligare disposition. Dokumentationskravet som tidigare reglerades i tredje stycket gäller fortsatt genom ny bestämmelse i 1 kap. 5 §.

Genom en befattningsanalys kommer man fram till i vilken omfattning en befattningshavare tar del av säkerhetsskyddsklassificerade uppgifter samt vilken möjlighet den har att orsaka skada för Sveriges säkerhet. Befattningsanalysen ska resultera i en bedömning av vilken säkerhetsklass en befattning ska vara placerad i. Den ska även omfatta befattningar som inte når upp till kraven för placering i säkerhetsklass, det vill säga befattningar som endast får tillgång till säkerhetsskyddsklassificerade uppgifter upp till begränsat hemligt och som till följd av sitt deltagande endast kan orsaka ringa skada för Sveriges säkerhet.

Observera att vid genomförande av befattningsanalysen ska en befattning enligt 3 kap. 10 § säkerhetsskyddslagen endast placeras i säkerhetsklass om behovet av

säkerhetsskydd inte kan tillgodoses på något annat sätt. Ett sådant skydd kan exempelvis vara åtgärder inom fysiskt skydd och informationssäkerhet.

Ett internationellt åtagande om säkerhetsskydd avser överenskommelser om säkerhetsskydd som Sverige har ingått med andra stater och mellanfolkliga organisationer. Dessa överenskommelser innehåller vanligen bestämmelser som innebär att den part som tar emot säkerhetsskyddsklassificerade uppgifter ska placera uppgifterna i den säkerhetsskyddsklass som motsvarar den avsändande partens säkerhetsskyddsklass. Om uppgifter har säkerhetsskyddsklassificerats av en annan stat eller mellanfolklig organisation ska den klassificeringen godtas.

Befattningsanalysen dokumenteras på ett sådant sätt att grunden till placering i säkerhetsklass framkommer. Befattningsanalysen behöver normalt uppdateras om säkerhetsskyddsanalysen förändras eller om nya befattningar tillkommer.

5 § Verksamhetsutövaren ska förteckna vilka anställningar samt annat deltagande i den säkerhetskänsliga verksamheten som har föranlett

1. placering i säkerhetsklass,
2. säkerhetsprövning utan placering i säkerhetsklass, och
3. registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen (2018:585).

Kommentar:

Motsvarande bestämmelse fanns i 6 kap. 4 § i Försvarsmaktens tidigare föreskrifter. En skillnad från tidigare reglering är att det har förtydligats att förteckningen även ska omfatta befattningar som föranlett säkerhetsprövning utan placering i säkerhetsklass. Säkerhetspolisen har motsvarande bestämmelse i sina föreskrifter (6 kap. 3 §).

Förteckningen utgör en sammanställning av de befattningar som verksamhetsutövaren fattat beslut om avseende säkerhetsprövning. För att förteckningen ska vara korrekt behöver den uppdateras löpande för att inkludera anställningar som tillkommit eller nya beslut om placering i säkerhetsklass.

Behörighet

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

Kommentar:

Bestämmelsen är oförändrad; motsvarande bestämmelse fanns i 6 kap. 2 § i Försvarsmaktens tidigare föreskrifter.

Bestämmelsen träffar exempelvis personer som administrerar registerkontroller, genomför samtal och intervjuer, genomför den uppföljande säkerhetsprövningen eller fattar beslut i säkerhetsprövning.

Verksamhetsutövaren bedömer vad som utgör en relevant utbildning utifrån den egna verksamhetens förutsättningar. Personen i fråga ska ha genomgått utbildningen innan den arbetar med eller tar del av uppgifter inom ramen för säkerhetsprövning. Individens kompetens ska sedan upprätthållas vilket kan innebära fortbildning.

Eftersom bestämmelsen innehåller ett krav på att den person som genomför säkerhetsprövning ska vara lämplig, behöver verksamhetsutövaren göra en sådan bedömning. Relevanta faktorer att beakta vid en bedömning av personens lämplighet är exempelvis utbildningsnivå, säkerhetsmedvetenhet, kunskap och förståelse för säkerhetsskydd, regelefterlevnad samt personliga egenskaper i övrigt.

Observera att en person som tidigare har bedömts vara lämplig att genomföra säkerhetsprövningar ändå kan vara olämplig i ett specifikt ärende, exempelvis om det finns en jävsliknande situation gentemot den prövade som gör att opartiskheten kan ifrågasättas, eller om den prövades öppenhet under utredning och samtal kan påverkas av att den som genomför prövningen är (blivande) chef eller nära kollega.

Grundutredning

7 § Grundutredning enligt 5 kap. 2 § säkerhetsskyddsförordningen (2021:955) ska innehålla en säkerhetsprövningsintervju där den prövades lojalitet, pålitlighet och sårbarhet ska bedömas.

Vid grundutredning inför placering i säkerhetsklass 3 och vid övrigt deltagande i säkerhetskänslig verksamhet utan placering i säkerhetsklass, får verksamhetsutövaren inhämta uppgifter från den prövade på annat sätt. Säkerhetsprövningsintervju ska dock genomföras om det behövs för att klarlägga omständigheter av betydelse för säkerhetsprövningen.

Kommentar:

Bestämmelsen motsvarar i viss mån bestämmelsen i 6 kap. 5 § i Försvarsmaktens tidigare föreskrifter. Första stycket är en anpassning till Säkerhetspolisens föreskrifter (jfr. 6 kap. 4 § Säkerhetspolisens föreskrifter). Den justerade lydelsen av bestämmelsen förtydligar att grundutredningens syfte är att kunna bedöma den prövades lojalitet, pålitlighet och sårbarhet i säkerhetshänseende. Dokumentationskravet för grundutredningen gäller fortsatt enligt ny bestämmelse (1 kap. 5 §) och innefattar dokumentation av säkerhetsprövningsintervju.

I syfte att effektivisera säkerhetsprövningsprocessen införs en möjlighet att inhämta uppgifter från den prövade genom t.ex. ett frågeformulär istället för genom en intervju. Av andra styckets sista mening framgår dock att en säkerhetsprövningsintervju ändå ska genomföras om det exempelvis framkommit omständigheter som behöver klarläggas genom ett personligt samtal eller som i övrigt inte lämpar sig för en skriftlig redogörelse.

Genom att ersätta säkerhetsprövningsintervjun med ett skriftligt frågeformulär kan grundutredningen i de flesta fall effektiviseras avsevärt. Ur ett säkerhetsskyddsperspektiv innebär det en ökad risktagning, vilket kan behöva hanteras genom systematisk uppföljning av säkerhetsprövningen och andra säkerhetsskyddsåtgärder. En enklare säkerhetsprövningsprocess i säkerhetsklass 3 frigör dock även personalresurser och möjliggör prioritering av högre säkerhetsklasser, där den potentiella skadan för Sveriges säkerhet är större.

8 § Uppgifter som framkommit vid säkerhetsprövningen och som behövs för att verksamhetsutövaren ska kunna följa upp säkerhetsprövningen under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår ska dokumenteras.

Kommentar:

Bestämmelsen är ny och innebär ett förtydligande av vad dokumentation av säkerhetsprövning ska omfatta.

Säkerhetsprövningen ska följas upp så länge personen deltar i den säkerhetskänsliga verksamheten. Personkännedomen ska fördjupas i syfte att verksamhetsutövaren ska kunna förebygga, tidigt uppmärksamma och åtgärda omständigheter som kan få negativa säkerhetsmässiga konsekvenser för personen eller verksamheten.

Uppföljningen av säkerhetsprövning kan bestå av regelbundna kontakter och uppföljande samtal, men kan även genomföras genom ifyllnad av ett frågeformulär om det bedöms som lämpligt. Uppföljningens omfattning bör anpassas efter typ av deltagande och säkerhetskänslig verksamhet, men ska alltid innefatta en bedömning avseende lojalitet, pålitlighet och sårbarhet.

Uppföljning

9 § Verksamhetsutövaren ska ha rutiner för att förebygga och hantera brister i lojalitet och pålitlighet samt sårbarheter i säkerhetshänseende hos personer som deltar i verksamhetsutövarens säkerhetskänsliga verksamhet.

Kommentar:

Bestämmelsen innebär ett förtydligande av bestämmelsen i 6 kap. 7 § Försvarsmaktens tidigare föreskrifter. Bestämmelsen saknar motsvarighet i Säkerhetspolisens föreskrifter.

Hantering av situationer som uppstått kan behöva ske arbetsrättsligt men även genom åtgärder för att skydda verksamheten från förlust av skyddsvärden. Exempel på en sådan åtgärd är att begränsa en persons tillträde till vissa lokaler eller tillgång till säkerhetsskyddsklassificerade uppgifter. Ett annat exempel är regelbundna uppföljande samtal i syfte att kontrollera och följa en persons utveckling. Det kan även behövas vidtas åtgärder till skydd för individen, t.ex. för att inte öka eller överföra sårbarhet samt skydda den från exponering eller påtryckningar.

Förebyggande åtgärder kan bestå av utbildning och information.

Rutinerna ska dokumenteras enligt bestämmelsen i 1 kap. 5 § i dessa föreskrifter.

10 § Verksamhetsutövaren ska genomföra ett avslutande samtal när personens deltagande i den säkerhetskänsliga verksamheten upphör. Ett sådant samtal behöver inte genomföras om det är uppenbart obehövligt.

Personen ska informeras om författningsreglerad sekretess och tystnadsplikt.

Kommentar:

Bestämmelsen motsvarar bestämmelsen i 6 kap. 8 § i Försvarsmaktens tidigare bestämmelser.

Första stycket: Exempel på när ett avslutande samtal kan vara uppenbart obehövligt är om deltagandet varit kortvarigt eller om annat samtal inom ramen för den uppföljande säkerhetsprövningen nyligen genomförts.

Andra stycket: Den som ska ta del av säkerhetsskyddsklassificerad uppgift har tystnadsplikt enligt 8 kap. 1–2 §§ säkerhetsskyddslagen. I det allmännas verksamhet tillämpas istället bestämmelser i offentlighets- och sekretesslagen (OSL). Tystnadsplikt innebär att den som, på grund av sin anställning eller annat deltagande i säkerhetskänslig verksamhet, tar del av uppgifter som omfattas av sekretess enligt OSL, inte obehörigen får röja eller utnyttja en sådan uppgift.

När en person slutar i verksamheten är det viktigt att personen upplyses om tystnadsplikten och 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 ett sekretessbevis undertecknas.

7 kap. Skyldigheter när en annan aktör kan få tillgång till säkerhetskänslig verksamhet

Samråd

1 § En begäran om samråd inför förfaranden som kräver säkerhetsskyddsavtal enligt 4 kap. 7 och 9 §§ säkerhetsskyddslagen (2018:585) ska göras på av tillsynsmyndigheten anvisat sätt.

Kommentar:

Motsvarande bestämmelse fanns i 8 kap. 5 § i Försvarsmaktens tidigare föreskrifter. Den bestämmelsen avsåg dock endast statliga myndigheters samråd med Försvarsmakten enligt den tidigare säkerhetsskyddsförordningen (2018:658).

Samråd enligt 4 kap. 7 och 9 §§ säkerhetsskyddslagen ska ske med tillsynsmyndigheten. Tillsynsmyndighet för de verksamhetsutövare som omfattas av dessa föreskrifter är Försvarsmakten eller Försvarets materielverk, FMV. Tillsynsmyndigheten ska som mottagare av begäran om samråd kunna meddela anvisningar om hur en sådan ska göras.

Säkerhetsskyddsavtal

2 § Ett säkerhetsskyddsavtal enligt 4 kap. 1 § säkerhetsskyddslagen (2018:585) ska ingås på någon av följande nivåer.

– Nivå 1: Om den andra aktören kommer att få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller få tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet utanför verksamhetsutövarens områden, byggnader och andra anläggningar eller objekt.

– Nivå 2: Om den andra aktören kommer att få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller få tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet inom verksamhetsutövarens områden, byggnader och andra anläggningar eller objekt.

– Nivå 3: Om den andra aktören kan komma att få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller kan komma att få tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet inom verksamhetsutövarens områden, byggnader och andra anläggningar eller objekt.

Kommentar:

Bestämmelsen är ny. En bestämmelse med samma lydelse finns i Säkerhetspolisen föreskrifter (7 kap. 2 §).

Det som skiljer nivå 1 från nivå 2 och 3 är platsen där en annan aktör kan få tillgång till uppgifter eller verksamhet – utanför respektive inom verksamhetsutö-

varens byggnader m.m. Skillnaden mellan nivå 2 och nivå 3 är syftet med att den andra aktören får tillgång till säkerhetsskyddsklassificerade uppgifter eller verksamhet – om det bedöms som en nödvändig del av deras uppdrag alternativt något som inte är nödvändigt men som kan inträffa under uppdragets genomförande.
Observera att de krav som följer av respektive nivå inte alltid kan tillämpas rakt av i samtliga avtalssammanhang; ett exempel är när den andra aktören, med vilken verksamhetsutövaren har ingått ett avtal, anlitar en underleverantör, vars tillgång till säkerhetskänslig verksamhet sker inom den andra aktörens lokaler och styrs av denne.

3 § Vid samverkan eller samarbete mellan aktörer som bedriver säkerhetskänslig verksamhet kan ett säkerhetsskyddsavtal ingås mellan fler än två parter. Avtalet ska då ingås i en nivå som motsvarar den högsta nivå som hade gällt i fall parterna i stället ingått bilaterala avtal.

Kommentar:

Bestämmelsen är ny. En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (7 kap. 3 § första stycket).

Bestämmelsen möjliggör att säkerhetsskyddsavtal upprättas mellan fler än två parter, där respektive parts skyldigheter beskrivs och inom vilka områden, byggnader och andra anläggningar eller objekt en part kommer att få tillgång till en annan parts säkerhetskänsliga verksamhet.

Verksamhetsutövare som har säkerhetskänslig verksamhet vilken kan komma att exponeras ska enligt 6 kap. 5 § säkerhetsskyddsförordningen anmäla det ingångna säkerhetsskyddsavtalet till den som beslutar om planering i säkerhetsklass samt till tillsynsmyndigheten. När säkerhetskänslig verksamhet vid endast en av verksamhetsutövarna kommer att exponeras genom förfarandet, behöver endast den verksamhetsutövaren anmäla det ingångna säkerhetsskyddsavtalet. Vid ömsesidig exponering är det tillräckligt om en gemensam anmälan av säkerhetsskyddsavtalet görs av en av parterna.

Anmälan om säkerhetsskyddsavtal

4 § Anmälan enligt 6 kap. 4 och 5 §§ säkerhetsskyddsförordningen (2021:955) ska göras på av tillsynsmyndigheten anvisat sätt.

Kommentar:

Av 6 kap. 4 och 5 §§ säkerhetsskyddsförordningen följer att verksamhetsutövare ska anmäla till tillsynsmyndigheten att de avser att ingå, respektive har ingått ett säkerhetsskyddsavtal enligt 4 kap. 1 § säkerhetsskyddslagen.

Tillsynsmyndigheten för verksamhetsutövare som omfattas av dessa föreskrifter är Försvarsmakten eller Försvarets materielverk. Tillsynsmyndigheten som är mottagare av anmälningar enligt 6 kap. 4 och 5 §§ ska kunna meddela anvisningar om hur detta ska göras.

Godkännande av lokaler eller utrymmen

5 § En verksamhetsutövare som avser att ingå ett säkerhetsskyddsavtal i nivå 1 ska kontrollera att motpartens säkerhetsskydd beträffande lokaler och utrymmen uppfyller kraven i säkerhetsskyddsavtalet.

En kontroll behöver dock inte genomföras om en sådan tidigare har genomförts eller om det är uppenbart obehövligt.

Kommentar:

Bestämmelsen är ny. Säkerhetspolisens föreskrifter innehåller en motsvarande bestämmelse (7 kap. 4 §).

Kontrollen syftar till att verksamhetsutövaren, innan motparten får tillgång till den säkerhetskänsliga verksamhet, kan försäkra sig om att denne vidtagit de åtgärder som enligt säkerhetsskyddsavtalet krävs för att kraven på säkerhetsskydd ska kunna tillgodoses under förfarandet.

I kontrollen att ”lokaler eller utrymmen” uppfyller kraven ingår de åtgärder som vidtas för att kunna upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan. Detta innefattar bland annat styrning av tillträde, åtgärder vid larm och angreppsförsök, hantering och förvaring av koder, kort och nycklar, skydd mot obehörig insyn och avlyssning, förvaringsutrymmen och i förekommande fall godkännande av utrymmen för regelbundna samtal som ska behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre.

Att en verksamhetsutövare i vissa fall får avstå från en kontroll enligt denna bestämmelse betyder att hänsyn kan tas till om verksamhetsutövaren t.ex. sedan tidigare och utifrån tidigare säkerhetsskyddsavtal med samma motpart har kännedom om motpartens lokaler och utrymmen och därtill kopplade åtgärder.

Säkerhetsprövning

6 § Verksamhetsutövaren ska göra en analys enligt 6 kap. 4 § över motpartens deltagande i säkerhetskänslig verksamhet. Verksamhetsutövaren ska också upprätta en förteckning enligt 6 kap. 5 §.

Analysen och förteckningen ska omfatta motpartens ledning, personal och övriga hos motparten som ska delta i den säkerhetskänsliga verksamheten.

Analysen och förteckningen ska uppdateras när deltagande tillkommer eller väsentligen förändras.

Kommentar:

Motsvarande bestämmelse fanns i 8 kap. 6 § i Försvarsmaktens tidigare föreskrifter. En bestämmelse med jämförbart innehåll finns även i Säkerhetspolisens föreskrifter (7 kap. 5 §).

Med ”ledning” avses motpartens högsta chef (exempelvis verkställande direktör där en sådan finns), styrelse, säkerhetsskyddschef och andra ledningsbefattningar som kommer få eller kan bereda sig tillgång till eller insyn i den säkerhetskänsliga verksamheten i förfarandet.

Motpartens högsta chef är i regel den som ansvarar för att säkerhetsskyddsavtalet efterlevs. Högsta chefen samt dennes säkerhetsskyddschef ska kunna hantera uppgifter som rör brister i säkerhetsskyddet och andra säkerhetshotande händelser som kan uppdagas under ett förfarandes genomförande, exempelvis brister i pålitlighet, lojalitet och sårbarheter i säkerhetshänseende vid den egna personalen.

Med ”personal och övriga hos motparten” avses även de befattningar som inte nödvändigtvis får en aktiv roll i den säkerhetskänsliga verksamheten men som ändå kan få tillgång till den på något sätt, exempelvis personal med uppgifter att utföra bevakning, fastighetspersonal, lokalvårdspersonal, IT-personal osv.

7 § Av 3 kap. 3 § första stycket säkerhetsskyddslagen (2018:585) framgår att säkerhetsprövningen får göras mindre omfattande om det finns särskilda skäl. Vid förfaranden mellan aktörer som bedriver säkerhetskänslig verksamhet behöver grundutredning, registerkontroll och särskild personutredning inte genomföras om personen i fråga redan är föremål för en säkerhetsprövning som omfattar förfarandet mellan aktörerna.

Kommentar:

Bestämmelsen är ny. Genom bestämmelsen ges en möjlighet att avstå från moment i en säkerhetsprövning som skulle utgöra en onödig upprepning av en redan genomförd prövning av samma person. En förutsättning är att den säkerhetskänsliga verksamhet som personen redan deltar i och som utgör grunden för prövning hos den ena aktören motsvarar deltagandet i det aktörsgemensamma förfarandet.

I sammanhanget bör beaktas att även om säkerhetsprövningen redan är genomförd behöver det också finnas en uppföljning under den tid som deltagandet i det gemensamma förfarandet pågår.

Se även 7 kap. 11 § om undantag vid förfaranden mellan aktörer som bedriver säkerhetskänslig verksamhet.

Säkerhetsskyddsinstruktion

8 § Verksamhetsutövaren ska, när ett säkerhetsskyddsavtal har ingåtts i nivå 1, säkerställa att motparten dokumenterar hur denna uppfyller kravet på säkerhetsskydd enligt avtalet i en säkerhetsskyddsinstruktion. Verksamhetsutövaren ska godkänna säkerhetsskyddsinstruktionen.

Kommentar:

Motsvarande bestämmelse fanns i 8 kap. 8 § p. 3 i Försvarsmaktens tidigare föreskrifter. En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (7 kap. 7 §).

Säkerhetsskyddskraven enligt säkerhetsskyddsavtalet omsätts i säkerhetsskyddsinstruktionen till praktiska moment (genomförandebeskrivningar). Säkerhetsskyddsinstruktionen har två huvudsakliga syften:
1. Motpartens ledning, personal och övriga får genom säkerhetsskyddsinstruktionen läsanvisningar för hur verksamheten ska utföras i de olika avseendena för att kraven på säkerhetsskydd enligt säkerhetsskyddsavtalet ska kunna tillgodoses.
2. Verksamhetsutövaren får, genom dennes godkännande av motpartens säkerhetsskyddsinstruktion, ett förtroende till att skyddsvärdena i verksamheten får det säkerhetsskydd som behövs enligt säkerhetsskyddsavtalet.

Kontroll av efterlevnad

9 § Verksamhetsutövaren ska fastställa en plan för den kontroll som ska göras enligt 4 kap. 5 § säkerhetsskyddslagen (2018:585). Om säkerhetsskyddsavtalet avser kvalificerat hemliga uppgifter eller skyddsvärden indelade i konsekvensnivå A, ska en uppföljning genomföras varje år.

Kommentar:

4 kap. 5 § säkerhetsskyddslagen innehåller krav på att verksamhetsutövaren kontrollerar att motparten följer säkerhetsskyddsavtalet. Att en plan för kontroll ska fastställas innebär att denna kontroll sker systematiskt. Bestämmelsens andra mening ställer krav på en viss regelbundenhet vid avtal som omfattar högsta säkerhetsskyddsklass eller konsekvensnivå. Konsekvensnivåerna för skyddsvärden framgår av 2 kap. 3 § i dessa föreskrifter.

När säkerhetsskyddsavtalet upphört

10 § När ett säkerhetsskyddsavtal har upphört ska verksamhetsutövaren upplysa motparten om den tystnadsplikt som gäller för de säkerhetsskyddsklassificerade uppgifterna som motparten har fått tillgång till genom förfarandet.

Motparten ska återlämna eller förstöra alla säkerhetsskyddsklassificerade handlingar och lagringsmedier enligt verksamhetsutövarens anvisningar.

Kommentar:

Bestämmelsen är ny. En bestämmelse med samma lydelse finns i Säkerhetspolisens föreskrifter (7 kap. 9 §).

Regler om tystnadsplikt finns i 8 kap. 1 och 2 §§ säkerhetsskyddslagen, se även 6 kap. 10 § i dessa föreskrifter om information vid avslutande samtal. I samband med att ett säkerhetsskyddsavtal upphör ska upplysning genomföras.

När säkerhetsskyddsavtalet har upphört att gälla är motparten inte längre behörig att hantera eller förvara de säkerhetsskyddsklassificerade handlingarna och lagringsmedierna. Återlämnandet eller förstöringen av säkerhetsskyddsklassificerade handlingar och lagringsmedier bör därför ske innan eller i så nära anslutning som möjligt till att säkerhetsskyddsavtalet upphör att gälla.

Undantag vid förfaranden mellan aktörer som bedriver säkerhetskänslig verksamhet

11 § Vid förfaranden mellan aktörer som bedriver säkerhetskänslig verksamhet ska 7 kap. 5, 6, 8 §§ och 10 § första stycket inte tillämpas.

Kommentar:

Bestämmelsen är ny. Motsvarande undantag görs i Säkerhetspolisens föreskrifter (7 kap. 10 §).

Motparten ansvarar i dessa fall själv för analys enligt 7 kap. 6 § vad gäller dennes egen ledning, personal och övriga. Verksamhetsutövaren behöver dock, innan motpartens deltagande i den säkerhetskänsliga verksamheten inleds, förmedla uppgifter till motparten om vilka skyddsvärden i verksamhetsutövarens verksamhet som kan komma att exponeras för motparten genom förfarandet (de skyddsvärden som identifierats i verksamhetsutövarens särskilda säkerhetsskyddsbedömning). Detta för att såväl verksamhetsutövaren som motparten ska kunna säkerställa att säkerhetsprövningen av motpartens ledning, personal och övriga är rätt dimensionerad, vilket inkluderar att uppgifterna i kontrollorgansexterna (vid registerkontroll) ger en rättvisande bild.

Förfaranden utan krav på säkerhetsskyddsavtal

12 § En verksamhetsutövare som avser att genomföra ett förfarande där en annan aktör kan komma att få tillgång till säkerhetsskyddsklassificerade uppgifter i högst säkerhetsskyddsklassen begränsat hemlig eller till annan säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, ska säkerställa att säkerhetsskyddet uppnås på annat sätt än genom ett säkerhetsskyddsavtal.

Kommentar:

Bestämmelsen är ny. Motsvarande reglering finns i Säkerhetspolisens föreskrifter (7 kap. 11 §).

Av 4 kap. 1 § säkerhetsskyddslagen framgår att krav på att ingå ett säkerhetsskyddsavtal inte föreligger i den situation som bestämmelsen beskriver. Det innebär dock inte att verksamhetsutövaren kan bortse från säkerhetsskyddet under ett visst förfarande. Det måste istället omhändertas på andra sätt i förfarandet med den andra aktören. Krav på säkerhetsskydd för begränsat hemliga uppgifter kan också finnas i det civilrättsliga avtal som ligger till grund för förfarandet, exempelvis ett kontrakt eller ett samverkansavtal.

Genom en säkerhetsskyddsöverenskommelse med aktören kan verksamhetsutövaren reglera personalsäkerhet, informationssäkerhet och fysisk säkerhet i den utsträckning som behövs för begränsat hemliga uppgifter eller motsvarande verksamhet. Bestämmelser i säkerhetsskyddslagen, säkerhetsskyddsförordningen eller dessa föreskrifter där det inte uttryckligen anges att de endast ska tillämpas vid säkerhetsskyddsklass konfidentiell eller högre eller motsvarande konsekvensnivåer gäller normalt. Kraven i en säkerhetsskyddsöverenskommelse kan dock inte göras lika långtgående som vid ett säkerhetsskyddsavtal då det exempelvis inte finns lagstöd att genomföra säkerhetsprövning om säkerhetsskyddet regleras på annat sätt än genom ett säkerhetsskyddsavtal.

Överlåtelse av säkerhetskänslig verksamhet och viss egendom

13 § En begäran om samråd enligt 4 kap. 15 § första stycket säkerhetsskyddslagen (2018:585) ska göras på det sätt tillsynsmyndigheten anvisat.

Kommentar:

Motsvarande bestämmelse fanns i 8 kap. 9 § i Försvarsmaktens tidigare föreskrifter. Den bestämmelsen avsåg dock endast samråd med Försvarsmakten, vilket var i enlighet med regler i den tidigare säkerhetsskyddsförordningen (2018:658).

Samråd enligt 4 kap. 15 § säkerhetsskyddslagen ska ske med tillsynsmyndigheten. Tillsynsmyndighet för de verksamhetsutövare som omfattas av dessa föreskrifter är Försvarsmakten eller Försvarets materielverk, FMV, som därför är mottagare av begäran om samråd. Detaljer i de tidigare föreskrifterna angående anmälan om samråd har utgått och har ersatts av hänvisning till tillsynsmyndighetens anvisningar i frågan. I Säkerhetspolisens föreskrifter finns bestämmelse om samråd i 13 §.

8 kap. Hantering av brister samt säkerhetshotande händelser och verksamhet

1 § Verksamhetsutövaren ska ha rutiner för att upptäcka, bedöma, rapportera, hantera och anmäla

1. händelser som har påverkat, eller misstänks ha påverkat, den säkerhetskänsliga verksamheten eller säkerhetsskyddet på ett negativt sätt,
2. brister i säkerhetsskyddet som är mer än av ringa betydelse, och
3. säkerhetshotande verksamhet.

Kommentar:

Krav på hantering fanns i 1 kap. 3 § och 10 kap. i Försvarsmaktens tidigare föreskrifter. Motsvarande bestämmelse finns i 2 kap. 15 § Säkerhetspolisens föreskrifter. Krav på anmälan av säkerhetshotande händelser eller verksamhet finns i 2 kap. 4 § säkerhetsskyddsförordningen. Observera dock att bestämmelsens krav på rutiner är betydligt bredare än den anmälningsskyldighet som följer av förordningen.

Huruvida en brist i säkerhetsskydd är av mer än ringa betydelse kan inte alltid fastställas direkt vid upptäckten av bristen. Insikt i bristen och dess konsekvenser kan leda till att verksamhetsutövaren vid en senare tidpunkt gör en annan bedömning.

2 § Verksamhetsutövaren ska utreda omständigheterna vid säkerhetshotande händelser eller verksamhet, som är av betydelse för den säkerhetskänsliga verksamheten, och utvärdera hanteringen av dessa. Utifrån utvärderingen ska verksamhetsutövaren vidta nödvändiga åtgärder för att minimera skadeeffekten av liknande händelser, eller verksamheter, i framtiden.

Kommentar:

Bestämmelsen är ny; motsvarighet finns i Säkerhetspolisens föreskrifter (2 kap. 17 §).

Kravet i föregående paragraf att ha rutiner för att bedöma och hantera händelser och verksamhet syftar främst till att åtgärda dessa. Bestämmelsen i denna paragraf ställer krav på verksamhetsutövaren att även titta på omständigheterna kring dessa händelser eller verksamheter och på hur dessa har hanterats. Syftet är att åstadkomma en bredare analys av vad den säkerhetshotande händelsen eller verksamheten kan förmedla till verksamhetsutövaren om potentiell skada vid upprepning och behov av förändringar i sitt säkerhetsskydd. Arbete enligt denna bestämmelse dokumenteras, se 2 kap. 5 §.

3 § En anmälan enligt 2 kap. 4 § säkerhetsskyddsförordningen (2021:955) till Försvarsmakten ska göras på det sätt Försvarsmakten anvisat.

Kommentar:

Skyldighet för samtliga verksamhetsutövare att anmäla säkerhetshotande händelse eller verksamhet till Säkerhetspolisen framgår av 2 kap. 4 § första stycket säkerhetsskyddsförordningen. Enligt 2 kap. 4 § andra stycket ska verksamhetsutövare som tillhör Försvarsmaktens tillsynsområde dessutom göra anmälan till Försvarsmakten. Bestämmelsen är således inte tillämplig på de enskilda verksamhetsutövare som faller inom Försvarets materielverks tillsynsområde.

9 kap. Undantag

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

Kommentar:

Motsvarande bestämmelse fanns i 12 kap. 1 § i Försvarsmaktens tidigare föreskrifter.

Ikraftträdande- och övergångsbestämmelser

1. Denna författning träder i kraft den 1 juli 2026.

Kommentar:

Det datum för ikraftträdande av föreskrifterna som framgår av denna bestämmelse har satts med beaktande av att berörda myndigheter och enskilda verksamhetsutövare ska börja tillämpa föreskrifterna då. Deras anpassning till de nya eller ändrade krav som introduceras genom föreskrifterna bedöms generellt kunna ske utifrån detta datum.

Kommentar:

2. Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.

De nya föreskrifterna (FFS 2025:3) om säkerhetsskydd ersätter Försvarsmaktens tidigare föreskrifter (FFS 2019:2), som därmed upphör att gälla. De bestämmelser i tidigare föreskrifter vars giltighet Försvarsmakten har velat bibehålla har förts in i de nya föreskrifterna.

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 klass 0-III, kassaskåp enligt 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.

Kommentar:

Motsvarande bestämmelse fanns i bilaga 1 till Försvarsmaktens tidigare föreskrifter. Vad gäller skyddsnivå 4 har ett specifikt krav för IT-utrymmen utgått.