
FFS 2025:3

Utkom från trycket

2025-11-19

Försvarsmaktens föreskrifter om säkerhetsskydd;

beslutade den 14 november 2025.

Försvarsmakten föreskriver följande med stöd av 3 kap. 6, 8 och 10 §§ samt 8 kap. 7 § säkerhetsskyddsförordningen (2021:955).

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.

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

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.

<i>Lagringsmedium</i>	Permanent minnesmedium som används för att kunna lagra och läsa uppgifter.
<i>Röjande signaler</i>	Elektromagnetiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs.
<i>Skadlig kod</i>	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.
<i>Säkerhetsskyddsklassificerat lagringsmedium</i>	Lagringsmedium som innehåller, eller är avsett att innehålla, säkerhetsskyddsklassificerade uppgifter, om uppgifterna inte är krypterade med kryptografiska funktioner som har godkänts av Försvarsmakten.

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.

Krav på dokumentation

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

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.

Särskilda underrättelseuppgifter och särskilda underrättelsehandlingar

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

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.

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.

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.

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).

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.

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.

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.

Kontroll och uppföljning

8 § Verksamhetsutövaren ska systematiskt

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

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.

Behörighetsförteckning

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

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.

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.

Märkning

5 § Allmänna handlingar, och handlingar som skulle betraktas som allmänna handlingar om de hade förvarats hos en myndighet, ska om de innehåller säkerhetsskyddsklassificerade 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.

6 § Ett säkerhetsskyddsklassificerat lagringsmedium ska på höljet förses med en märkning om den högsta säkerhetsskyddsklass som 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.

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.

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.

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.

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.

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.

12 § Vad som föreskrivs i 10 § gäller inte när arkiv-, expeditiions-, sambands- eller tryckeripersonal tar emot en 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.

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.

Förvaring

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

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.

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.

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 säkerhetsskyddsklassen kvalificerat hemlig.

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

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.

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 överenskommele 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.

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.

4 kap. Informationssäkerhet i och kring informationssystem

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.

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.

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.

Övervakning

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

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

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.

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.

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 §.

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.

10 § Utställda identiteter ska vara unika över tid.

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

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.

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

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.

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.

Bevarande av riktighet

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

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.

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.

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.

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.

Säkerhetskfiguration

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

Samråd

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

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.

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.

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.

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 hantearats.

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.

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.

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.

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.

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.

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 §.

Skyddsnivåerna framgår av bilagan till denna författning.

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 även framgå om och i så fall när återlämnande skett.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

6 kap. Personalsäkerhet

Utbildning

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

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.

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.

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.

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).

Behörighet

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

Grundutredning

7 § Grundutredning enligt 5 kap. 2 § säkerhetsskyddsförordningen (2021:955) ska innehålla en säkerhetsprovningsintervju 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 verk-

samhetsutövaren inhämta uppgifter från den prövade på annat sätt. Säkerhetsprövningsintervju ska dock genomföras om det behövs för att klarlägga omständigheter av betydelse för säkerhetsprövningen.

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.

Uppföljning

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

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.

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.

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.

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.

Anmälan om säkerhetsskyddsavtal

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

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 har genomförts tidigare eller om det är uppenbart obehövt.

Säkerhetsprövning

6 § Verksamhetsutövaren ska göra en analys enligt 6 kap. 4 § av 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.

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.

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.

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.

När säkerhetsskyddsavtalet upphört

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

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

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.

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.

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.

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 säkerhets känsliga verksamheten eller säkerhetsskyddet på ett negativt sätt,
2. brister i säkerhetsskyddet som är mer än av ringa betydelse, och
3. säkerhetshotande verksamhet.

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

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

9 kap. Undantag

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

-
1. Denna författning träder i kraft den 1 juli 2026.
 2. Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.

Michael Claesson

Kerstin Bynander

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 be-teckning 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

Bilaga 1

annat material med motsvarande motståndskraft. Byggnad eller lokal får inte ha fönster.

Flyttbara förvaringsutrymmen såsom värdeskåp enligt norm SS 3150 med minst 100 skyddsvärdespoäng, standard SS-EN 1143-1 lägst klass IV, säkerhetsbox med beteckning 301 eller 302 samt vapenkassun som är förankrad på bottenplatta eller motsvarande underlag.

Utrymme i skyddsnivå 3 som är försett med larm med seismiska detektorer (vibrationsdetektor) och magnetdetektorer eller som har placerats i ett utrymme som är försett med volymlarm. Om larm har utlösts eller angreppsförsök har konstaterats ska en särskild avdelad styrka vara på plats, inom sådan tid att ett intrång i utrymmet kan försvåras.