FÖRSVARSMAKTEN
HÖGKVARTERET

FÖRSVARETS FÖRFATTNINGSSAMLING

FFS 2015:2
Utkom från
trycket 2015-03-30

Försvarsmaktens föreskrifter om säkerhetsskydd;

beslutade den 13 mars 2015.

Försvarsmakten föreskriver med stöd av 11 § andra stycket och 44 § säkerhetsskyddsförordningen (1996:633) följande.

1 kap. Allmänna bestämmelser

1 § Dessa föreskrifter gäller för Fortifikationsverket, Försvarshögskolan samt Försvarsmakten och övriga myndigheter som hör till Försvarsdepartementet utom Statens haverikommission.

2 § I dessa föreskrifter avses med hemlig uppgift, hemlig handling och säkerhetskänslig verksamhet detsamma som anges i 4 § säkerhetsskyddsförordningen (1996:633).

3 § Vad som föreskrivs om hemlig handling gäller även en handling som är av synnerlig betydelse för rikets säkerhet, kvalificerat hemlig handling, om inte annat särskilt anges.

4 § I dessa föreskrifter delas säkerhetsskyddet in i fyra informationssäkerhetsklasser med följande beteckningar och betydelser.

Informationssäkerhetsklass	Betydelse
HEMLIG/ TOP SECRET	1. Hemliga uppgifter vars röjande kan medföra synnerligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet (kvalificerat hemliga uppgifter). 2. Hemlig handling som har åsatts beteckningen TOP SECRET eller motsvarande av en utländsk myndighet eller en mellanfolklig organisation.
HEMLIG/SECRET	1. Hemliga uppgifter vars röjande kan medföra betydande men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen SECRET eller motsvarande av en utländsk myndighet eller en mellanfolklig organisation.
HEMLIG/ CONFIDENTIAL	1. Hemliga uppgifter vars röjande kan medföra ett inte obetydligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen CONFIDENTIAL eller motsvarande av en utländsk myndighet eller en mellanfolklig organisation.

HEMLIG/ RESTRICTED	1. Hemliga uppgifter vars röjande kan medföra endast ringa men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen RESTRICTED eller motsvarande av en utländsk myndighet eller en mellanfolklig organisation.

5 § Beteckningen HEMLIG/TOP SECRET i 4 § i detta kapitel anger en högre informationssäkerhetsklass än beteckningen HEMLIG/SECRET. Beteckningen HEMLIG/SECRET anger en högre informationssäkerhetsklass än beteckningen HEMLIG/CONFIDENTIAL och beteckningen HEMLIG/CONFIDENTIAL anger en högre informationssäkerhetsklass än beteckningen HEMLIG/RESTRICTED.

6 § I 5 § säkerhetsskyddsförordningen (1996:633) finns föreskrifter om säkerhetsanalys. Varje myndighet ska genomföra och dokumentera en säkerhetsanalys avseende vilka hot, risker och sårbarheter som kan påverka myndighetens säkerhetskänsliga verksamhet. En sådan säkerhetsanalys ska hållas uppdaterad.

En säkerhetsanalys ska utgå från en beskrivning av myndighetens verksamhet och organisation (verksamhetsanalys).

Med säkerhetsanalysen som grund ska en säkerhetsplan upprättas där lämpliga säkerhetsskyddsåtgärder anges.

7 § Materiel som innehåller hemliga uppgifter ska ges ett säkerhetsskydd som motsvarar vad som gäller för hemliga handlingar.

7 a § En publikation som innehåller hemliga uppgifter ska ges ett säkerhetsskydd som motsvarar vad som gäller för allmänna handlingar som är hemliga.

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

9 § För signalskyddstjänsten gäller särskilda bestämmelser i fråga om hantering av kryptonycklar och signalskyddsmateriel samt användning av kryptografiska funktioner.

10 § För särskilda underrättelseuppgifter och -handlingar gäller även Försvarsmaktens föreskrifter om säkerhetsskydd för särskilda underrättelseuppgifter och handlingar.

2 kap. Informationssäkerhet

Sekretessmarkering m.m.

1 § En allmän handling som är hemlig ska på första sidan förses med en särskild anteckning (sekretessmarkering). Bestämmelser om sekretessmarkering finns i 5 kap. 5 § offentlighets- och sekretesslagen (2009:400).

Sekretessmarkeringen på den allmänna handlingen ska ha en rektangulär ram. Ramen ska vara enkel för hemlig handling och dubbel för kvalificerat hemlig handling.

En hemlig handling som inte är allmän ska på första sidan förses med en anteckning om att den är hemlig. Anteckningen får utformas på lämpligt sätt.

2 § En hemlig handling ska placeras i en av de informationssäkerhetsklasser som anges i 1 kap. 4 §. Handlingen ska på första sidan förses med en uppgift om i vilken informationssäkerhetsklass den har placerats.

3 § Om en hemlig handling består av flera sidor ska på varje sida finnas en hänvisning till uppgiften om informationssäkerhetsklass på första sidan.

4 § Om en handling som är försedd med sekretessmarkering inte längre bedöms vara hemlig ska beslut om detta antecknas på handlingen. Anteckningen ska innehålla myndighetens namn, datum för beslutet samt vem som har fattat beslutet. Därefter ska sekretessmarkeringen överkorsas och anteckning om beslutet göras i det register där handlingen är diarieförd.

Om en handling, som har försetts med den sekretessmarkering som gäller för en kvalificerat hemlig handling, inte längre bedöms som kvalificerat hemlig ska samråd ske med den som har upprättat handlingen innan åtgärder vidtas enligt första stycket. Anteckning om samrådet ska göras på handlingen.

Om en handling som är försedd med anteckning som avses i 1 § tredje stycket i detta kapitel inte längre bedöms vara hemlig, ska anteckningen överkorsas. På handlingen ska vidare anges vem som har beslutat överkorsningen.

5 § Om en hemlig handling placeras i en annan informationssäkerhetsklass än vad som anges på handlingen ska detta antecknas på handlingen. Anteckningen ska innehålla den nya informationssäkerhetsklassen, myndighetens namn, datum för beslutet samt vem som har fattat beslutet.

Om en handling inte längre ska vara placerad i en informationssäkerhetsklass ska anteckningen om informationssäkerhetsklass överkorsas.

Behörighet att ta del av hemliga uppgifter

6 § Varje myndighet ska besluta vem som är behörig att ta befattning med hemliga handlingar eller uppgifter som är placerade i någon av informationssäkerhetsklasserna HEMLIG/CONFIDENTIAL, HEMLIG/SECRET respektive HEMLIG/TOP SECRET. Ett sådant beslut ska dokumenteras.

Arbetsrutiner med hemlig handling

7 § Är en allmän handling som är hemlig placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre ska det på sändlistan till handlingen eller

i det register där handlingen är diarieförd anges hur många exemplar av handlingen som har framställts och vilka som är mottagare av respektive exemplar.

8 § Vid framställning av en allmän handling som är hemlig och som är placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre ska på första sidan antecknas handlingens beteckning, exemplarnummer, antal sidor samt bilagor, om sådana följer med. Sidorna ska numreras i följd.

Av bilaga och blad i bok med lösbladssystem ska framgå till vilken handling bilagan respektive bladet hör.

9 § Varje myndighet ska besluta vilka rutiner som ska tillämpas i samband med kopiering av eller utdrag ur en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre. Beslutet ska dokumenteras.

Kopia av eller utdrag ur en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET får göras endast efter medgivande av myndighetens chef eller den han eller hon bestämmer.

10 § Har en kopia av eller ett utdrag ur en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre gjorts, ska uppgift om detta liksom uppgift om till vem kopian eller utdraget har lämnats antecknas i register eller liggare.

Om det inte framgår av ett utdrag ur en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre till vilken handling utdraget hör, ska det på utdraget antecknas från vilken handling utdraget har gjorts.

Kvittering

11 § När en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET tas emot ska mottagandet kvitteras med namnteckning och namnförtydligande. Ett namnförtydligande får vara en kod. Kvittensen ska bevaras hos myndigheten i minst 10 år.

När en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET tas emot ska mottagandet kvitteras med namnteckning och namnförtydligande på ett särskilt kvitto med kopia. När en sådan handling återlämnas ska detta antecknas på kvittokopian, som ska bevaras hos myndigheten i minst 25 år.

Vad som föreskrivs i första och andra styckena gäller dock inte när arkiv-, expeditions-, sambands- eller tryckeripersonal tar emot en sådan hemlig handling för registrering, kopiering, distribution, arkivering eller förstöring, om inte den som lämnar över handlingen begär det.

12 § Varje myndighet ska besluta om rutiner för hur kvittering ska göras om uppgifter i en hemlig handling, som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET, lämnas muntligt eller genom visning. Sådana rutiner ska dokumenteras.

Förvaring

13 § I *bilaga* till dessa föreskrifter anges de krav som gäller för respektive skyddsnivå. Ett förvaringsutrymme för hemliga handlingar ska uppfylla de krav som gäller för skyddsnivå 1, 2, 3 eller 4.

14 § En hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/RESTRICTED ska förvaras inlåst eller i en låst lokal som endast den

som är behörig att ta del av handlingen har tillträde till. Förvaringsutrymmet ska uppfylla de krav som gäller för skyddsnivå 1.

15 § En hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET ska förvaras inlåst i ett förvaringsutrymme som uppfyller de krav som gäller för skyddsnivå 3.

16 § En hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET ska förvaras inlåst i ett förvaringsutrymme som uppfyller de krav som gäller för skyddsnivå 4.

17 § Varje myndighet får fatta beslut som avviker från föreskrifterna i 14-16 §§ i detta kapitel under förutsättning att motsvarande skyddsnivå kan upprätthållas. Ett sådant beslut ska dokumenteras.

18 § Om en myndighet har beslutat att anställda under kortare tid får lämna hemliga handlingar framme i ett låst arbetsrum, ska huvudnycklar och reservnycklar förvaras så att någon obehörig inte kan komma åt dem.

19 § I det register där en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre är diarieförd ska anges vem som förvarar handlingen eller om handlingen har förkommit eller gallrats.

Medförande av hemliga handlingar utanför myndighetens lokaler

20 § Varje myndighet ska besluta i vilken omfattning hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre får medföras från myndighetens lokaler. Ett sådant beslut ska dokumenteras.

Hemliga handlingar som medförs från myndigheten ska hållas under omedelbar uppsikt eller förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av handlingarna inom myndighetens lokaler.

Inventering

21 § Inventering av allmänna handlingar som är hemliga och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET liksom inventering av hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET ska protokollföras.

Förstöring av hemlig handling

22 § Förstöring av hemliga handlingar eller av materiel som innehåller hemliga uppgifter ska ske så att åtkomst och återskapande av uppgifterna omöjliggörs.

Förstöring av hemliga handlingar eller materiel som innehåller hemliga uppgifter och som är placerade i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre ska dokumenteras utom såvitt avser karbonpapper, karbonband och färgband.

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

Åtgärder vid distribution av hemlig handling

24 § Varje myndighet ska besluta om rutiner för hur försändelser med hemliga handlingar, som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre, ska sändas från och tas emot av myndigheten. Sådana rutiner ska dokumenteras. Myndigheten ska se till att erforderliga skyddsåtgärder vidtas under distributionen. En försändelse med hemliga handlingar som

har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre ska sändas med en distributör som har godkänts av myndigheten.

25 § I 11 § första stycket säkerhetsskyddsförordningen (1996:633) finns föreskrifter om försändelser med hemliga handlingar till utlandet.

Hemliga handlingar som sänds utomlands ska förses med anteckning om uppgifternas ursprungsland.

Varje myndighet får i avtal med ett annat land eller en mellanfolklig organisation komma överens om att distribuera hemliga handlingar på annat sätt än vad som föreskrivs i 11 § första stycket säkerhetsskyddsförordningen (1996:633).

3 kap. Tillträdesbegränsning

Tillträde och bevakning

1 § Varje myndighet ska besluta om tillträdesrätt till myndighetens objekt, lokaler och områden. Beslutet ska dokumenteras.

2 § Den myndighet som medger en person tillträde till myndighetens objekt, lokaler eller områden där det bedrivs verksamhet som kräver säkerhetsskydd ska se till att personen genom besökstillstånd eller på annat sätt har fått myndighetens tillstånd till tillträde och att personen har styrkt sin identitet. Vid myndigheten ska för varje besökare antecknas dennes namn, den myndighet, organisation eller motsvarande som besökaren företräder och dagen för besöket. Sådana anteckningar ska bevaras i minst 10 år.

Första stycket ska dock tillämpas med beaktande av allmänhetens rätt att utan att uppge sin identitet ta del av allmänna handlingar.

3 § Bevakning med personal eller med teknisk utrustning eller med båda ska finnas vid alla passerställen till platser där det bedrivs verksamhet som kräver säkerhetsskydd.

Nycklar, kort och koder

4 § Nycklar, kort och koder till utrymmen där hemliga uppgifter finns eller där säkerhetskänslig verksamhet bedrivs ska förvaras så att inte någon obehörig kan komma åt dem.

5 § En kod ska bestämmas och ställas in av den som har tilldelats ett förvaringsutrymme.

6 § En nyckel, ett kort eller en kod får innehas endast av den som har ansvaret för förvaringsutrymmet, om inte myndigheten har beslutat annat. Ett sådant beslut ska dokumenteras.

7 § Det ska finnas en förteckning över samtliga nycklar, kort och koder till förvaringsutrymmen som rymmer hemliga handlingar. Av förteckningen ska framgå till vem och när en nyckel, ett kort eller en kod har lämnats samt var reservnyckel, reservkort eller reservkod förvaras.

8 § Om det finns anledning att anta att en nyckel eller ett kort har förlorats eller kopierats, att en kod har röjts eller att en nyckel, kort eller kod har använts av någon obehörig person, ska förhållandet omedelbart anmälas till myndighetens säkerhetsskyddschef eller till den han eller hon bestämmer.

Skyddsnivåer för vissa utrymmen

9 § I *bilaga* till dessa föreskrifter anges de krav som gäller för respektive skyddsnivå. Utrymmen som innehåller växlar, korskopplingar och servrar samt datorhallar ska uppfylla de krav som gäller för skyddsnivå 2, 3 eller 4.

10 § Om det i sådana utrymmen eller datorhallar som anges i 9 § i detta kapitel behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/RESTRICTED ska utrymmena eller datorhallarna uppfylla de krav som gäller för skyddsnivå 2.

Om det i sådana utrymmen eller datorhallar behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET ska utrymmena eller datorhallarna uppfylla de krav som gäller för skyddsnivå 3.

Om det i sådana utrymmen eller datorhallar behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/TOP SECRET ska utrymmena eller datorhallarna uppfylla de krav som gäller för skyddsnivå 4.

11 § Utrymmen och datorhallar som anges i 9 § i detta kapitel ska vara försedda med system för inpasseringskontroll.

12 § Varje myndighet får fatta beslut som avviker från föreskrifterna i 10 § i detta kapitel under förutsättning att motsvarande skyddsnivå kan upprätthållas. Ett sådant beslut ska dokumenteras.

4 kap. Säkerhetsprövning

1 § Varje myndighet ska analysera vilka anställningar vid myndigheten som ska placeras i säkerhetsklass och vilket annat deltagande i myndighetens verksamhet som kan komma att placeras i säkerhetsklass. Resultatet av analysen ska

dokumenteras. Av dokumentationen ska även framgå vem som ska bli föremål för registerkontroll till skydd mot terrorism.

2 § Varje myndighet ska fortlöpande pröva pålitligheten från säkerhetssynpunkt särskilt i fråga om de personer som har anställning eller deltar i verksamhet som är placerad i säkerhetsklass eller som är registerkontrollerade till skydd mot terrorism. Vid denna prövning ska särskild vikt läggas vid de personliga förhållandena.

5 kap. Utbildning

1 § Vid varje myndighet ska det finnas en plan för utbildning i säkerhetsskydd.

2 § Varje myndighet ska föra en förteckning över de anställda som har genomgått utbildning i säkerhetsskydd.

6 kap. Kontroll

1 § Vid varje myndighet ska det finnas en plan för intern kontrollverksamhet. Myndigheten ska föra protokoll över varje kontroll. Protokollen ska förvaras samlade hos myndigheten.

7 kap. Hantering av hemliga uppgifter i IT-system

Definitioner

1 § I detta kapitel avses med

lagringsmedium: permanent minnesmedium som används för att kunna lagra och läsa uppgifter,

IT-system: system av sammansatt hård- och mjukvara som hanterar information,

säkerhetsfunktion: en eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet ska skyddas,

behörighetskontroll: administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att kontrollera en användares identitet, styra en användares behörighet att använda IT-systemet och dess resurser samt registrera användaren,

säkerhetsloggning: manuell eller automatisk registrering, eller både manuell eller automatisk registrering, av händelser som är av betydelse för säkerheten i eller kring ett IT-system,

röjande signaler: inte önskvärda elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs,

intrångsskydd: administrativa eller tekniska åtgärder, eller både administrativa eller tekniska åtgärder, som vidtas för att skydda IT-system mot obehörig åtkomst från ett elektroniskt kommunikationsnät,

intrångsdetektering: administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att detektera intrång, eller försök till intrång eller förberedelse till intrång,

skadlig kod: otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett IT-system, och

ackreditering: ett sådant godkännande av ett IT-system från säkerhetssynpunkt som avses i 12 § tredje stycket säkerhetsskyddsförordningen (1996:633).

Hantering av hemliga uppgifter och lagringsmedium

2 § En hemlig uppgift i ett IT-system ska ha ett säkerhetsskydd som motsvarar det säkerhetsskydd som gäller för den informationssäkerhetsklass som uppgiften har placerats i.

3 § Ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter ska ha ett säkerhetsskydd som motsvarar det säkerhetsskydd som gäller för den informationssäkerhetsklass som lagringsmediet har placerats i.

4 § Ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter får endast hanteras i ett IT-system som uppfyller de krav som gäller för hantering av uppgifter i den högsta informationssäkerhetsklass som någon av uppgifterna på lagringsmediet kan komma att placeras i eller har placerats i.

5 § Ett lagringsmedium som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/SECRET eller HEMLIG/TOP SECRET får inte återanvändas i ett IT-system som är avsett för behandling av hemliga uppgifter som är placerade i en lägre informationssäkerhetsklass.

6 § Ett lagringsmedium som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/RESTRICTED eller HEMLIG/CONFIDENTIAL får återanvändas i ett IT-system om myndigheten har vidtagit åtgärder för att säkerställa att inga hemliga uppgifter längre kan utläsas ur lagringsmediet. Sådana åtgärder ska dokumenteras.

Utveckling, anskaffning, användning och avveckling

7 § Varje myndighet som överväger att införa eller använda ett IT-system som ska användas av flera personer ska noga analysera vilket säkerhetsskydd systemet kräver och vilka åtgärder som måste vidtas för att säkerhetsskyddet ska få avsedd effekt. En sådan analys ska även göras innan en myndighet upplåter ett IT-system till en annan myndighet, ett annat land eller en mellanfolklig organisation.

Analyser som avses i första stycket ska dokumenteras.

8 § Varje myndighet som beslutar att anskaffa eller förändra ett IT-system ska, för att kunna fastställa erforderligt säkerhetsskydd för systemet, göra en sekretess-

bedömning av såväl de enskilda uppgifterna som den totala informationsmängden som avses hanteras i IT-systemet.

9 § Varje myndighet ska dokumentera det säkerhetsskydd som finns i fråga om ett IT-system, från dess utveckling till dess avveckling. Dokumentationen ska hållas aktuell.

Behörighetskontroll

10 § Varje IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer ska vara försett med en av myndigheten godkänd säkerhetsfunktion för behörighetskontroll. En sådan säkerhetsfunktion ska anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

Säkerhetsloggning

11 § Varje IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer ska vara försett med en av myndigheten godkänd säkerhetsfunktion för säkerhetsloggning. En sådan säkerhetsfunktion ska anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

12 § Varje myndighet ska besluta vilket säkerhetsskydd som är erforderligt vad avser förvaring av säkerhetskopierade säkerhetsloggar.

Röjande signaler och obehörig avlyssning

13 § Varje IT-system som är avsett för behandling av hemliga uppgifter ska vara försett med av myndigheten godkända säkerhetsfunktioner för skydd mot röjande signaler och obehörig avlyssning. Sådana säkerhetsfunktioner ska anpassas till

den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

IT-system som är avsedda för behandling av uppgifter som har placerats i högst informationssäkerhetsklassen HEMLIG/RESTRICTED behöver dock inte förses med en säkerhetsfunktion för skydd mot röjande signaler.

Intrångsskydd och intrångsdetektering

14 § Varje IT-system som är avsett för behandling av hemliga uppgifter ska vara försett med av myndigheten godkända säkerhetsfunktioner som skyddar mot intrång och som möjliggör intrångsdetektering. Sådana säkerhetsfunktioner ska anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

IT-system som är avsedda för behandling av uppgifter som har placerats i högst informationssäkerhetsklassen HEMLIG/RESTRICTED behöver dock inte förses med en säkerhetsfunktion som möjliggör intrångsdetektering.

Skadlig kod

15 § Varje IT-system som är avsett för behandling av hemliga uppgifter ska vara försett med en av myndigheten godkänd säkerhetsfunktion som skyddar mot skadlig kod. En sådan säkerhetsfunktion ska anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

Ackreditering

16 § Varje myndighet ska inför en ackreditering granska säkerheten i och kring ett IT-system och därvid särskilt beakta hur IT-systemet är avsett att samverka med andra IT-system. En sådan säkerhetsgranskning ska dokumenteras.

17 § Beslut om ackreditering ska dokumenteras.

8 kap. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal

1 § Med företag förstås i detta kapitel aktiebolag, handelsbolag, föreningar och andra juridiska personer samt enskilda firmor med vilka en myndighet avser att träffa avtal som avses i 8 § säkerhetsskyddslagen (1996:627), (säkerhetsskyddsavtal).

2 § Varje myndighet ska innan en upphandling påbörjas pröva om uppdraget helt eller delvis ska säkerhetsskyddas.

3 § Innan en myndighet lämnar ut hemliga uppgifter till ett företag ska myndigheten göra en bedömning av vilka personer i företaget som ska placeras i säkerhetsklass. Bedömningen ska omfatta företagets styrelse, ledning och övriga anställda.

4 § Om företaget ska hantera eller förvara hemliga uppgifter i egna lokaler ska myndigheten, om detta inte genom egen eller annan myndighets dokumentation är uppenbart obehövligt, genom ett besök kontrollera att företagets lokaler och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt.

5 § Om företaget ska hantera eller förvara hemliga uppgifter utanför myndighetens lokaler, ska det av säkerhetsskyddsavtalet framgå att företaget ska upprätta en säkerhetsskyddsinstruktion som ska granskas och godkännas av myndigheten.

6 § När företaget har fullgjort ett uppdrag som krävt säkerhetsskydd ska myndigheten säga upp säkerhetsskyddsavtalet. Myndigheten ska säkerställa att vad som har avtalats om tystnadsplikt och sekretess i övrigt ska bestå.

7 § Varje myndighet ska utan dröjsmål underrätta Säkerhetspolisen om säkerhetsskyddsavtal som har träffats och om säkerhetsskyddsavtal som har upphört att gälla.

En sådan underrättelse ska lämnas på en blankett som har fastställts av Säkerhetspolisen.

9 kap. Internationell verksamhet

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

10 kap. Undantag

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

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

Ikraftträdande- och övergångsbestämmelser

1. Denna författning träder i kraft den 1 juni 2015.

2. Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd.

3. Föreskrifterna i 2 kap. 2 och 3 §§ i den nya författningen gäller inte handlingar som har tillkommit före den 1 januari 2004 *(äldre handlingar)*. Föreskrifterna får dock tillämpas i fråga om äldre handlingar.

Vad som föreskrivs i första stycket första meningen gäller dock inte kopior av eller utdrag ur äldre handlingar, om kopiorna eller utdragen har framställts efter den 1 januari 2004.

4. Äldre handlingar ska hanteras enligt följande. Har en handling försetts med en särskild anteckning (hemligstämpel) om att den är

a) KVALIFICERAT HEMLIG, ska den anses vara placerad i informationssäkerhetsklassen HEMLIG/TOP SECRET, eller

b) HEMLIG, ska den anses vara placerad i informationssäkerhetsklassen HEMLIG/SECRET.

5. Har myndigheten före den 1 januari 2004 beslutat

a) vem som är behörig att ta befattning med hemliga respektive kvalificerat hemliga handlingar, ska beslutet anses som ett beslut enligt 2 kap. 6 § i den nya författningen,

b) hur kvittering ska göras i fråga om kvalificerat hemliga uppgifter som har lämnats muntligt eller genom visning, ska beslutet anses som ett beslut enligt 2 kap. 12 § i den nya författningen,

c) i vilken omfattning hemliga respektive kvalificerat hemliga handlingar får medföras från myndighetens lokaler, ska beslutet anses som ett beslut enligt 2 kap. 20 § i den nya författningen,

d) hur försändelser med hemliga respektive kvalificerat hemliga handlingar ska sändas från och tas emot av myndigheten, ska beslutet anses som ett beslut enligt 2 kap. 24 § första stycket i den nya författningen, eller

e) godkänna en distributör av hemliga respektive kvalificerat hemliga handlingar, ska godkännandet anses som ett godkännande enligt 2 kap. 24 § andra stycket i den nya författningen.

6. Har myndigheten fattat ett eller flera beslut som avses i första stycket beträffande hemliga handlingar gäller respektive beslut även handlingar som enligt den nya författningen har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL.

7. Har ett beslut om ackreditering fattats före den 1 januari 2004 gäller inte föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen.

8. Ska ett IT-system, på grund av förändringar som kan påverka säkerheten i det, på nytt ackrediteras enligt vad som följer av 12 § tredje stycket säkerhetsskyddsförordningen (1996:633) ska dock föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen tillämpas.

9. Har ett underlag för ackreditering tagits fram före den 1 januari 2004 gäller inte föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen i fråga om detta underlag.

Sverker Göranson

Carin Bratt

Bilaga

Utrymmens indelning i skyddsnivåer

Skyddsnivå 1	Byggnad eller lokal med certifierad dörr i klass 1 enligt svensk standard SS 81 73 45, dörr i klass 2 eller 3 enligt svensk standard SS–EN 1627 eller standarddörrar i trä eller plåt. Väggar, golv och tak ska bestå av trämaterial, gipsskivor eller korrugerad plåt. Flyttbara förvaringsutrymmen med omslutningsytor av tunn plåt eller träkonstruktion.
Skyddsnivå 2	Byggnad eller lokal med certifierad dörr i lägst klass 2 enligt svensk standard SS 81 73 45, dörr i klass 3 eller 4 enligt svensk standard SS–EN 1627 eller 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 eller en stark träkonstruktion. Fönster enligt svensk standard SS 22 44 25 i lägst klass B 3, fönster i kategori P8B enligt svensk 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 svensk standard SS 81 73 45, dörr i klass 4, 5 eller 6 enligt svensk standard SS–EN 1627, 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 svensk standard SS 22 44 25 i lägst klass B 3, fönster i kategori P8B enligt svensk 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 truppservice-förråd samt flyttbara förvaringsutrymmen såsom värde-skåp enligt svensk standard SS 3150 och med lägre än 100 skyddsvärdespoäng, säkerhetsskåp enligt svensk standard SS 3492, svensk standard SS-EN 1143-1 grade 0-III, kassaskåp enligt svensk standard SS 3493, vapenkista med beteckning 1 B, 2 B, 3 B eller 1 TP, vapenkassun som inte är förankrad på bottenplatta eller motsvarande underlag eller tillträdesskyddad container.
Skyddsnivå 4	Byggnad eller lokal med valvdörr, vapenkassundörr, AD-dörr, VDS-dörr, TD-dörr eller VDB-dörr. Väggar, golv och tak ska bestå av betong med dubbel, förskjuten armering med en tjocklek av minst 180 mm. Armeringen får inte medge genomkrypning. Armeringen ska vara minst 12 mm i diameter och avståndet från centrum till centrum mellan armeringsstålen får vara högst 180 mm. Förskjutning av armering krävs inte vid högst 130 mm avstånd från centrum till centrum mellan armeringsstålen. Väggar, golv, tak och dörrar får bestå av annat material

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

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

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