FÖRSVARSMAKTEN

FÖRSVARETS FÖRFATTNINGSSAMLING

FFS 2019:2

Utkom från trycket
2019-02-27

Försvarsmaktens föreskrifter om säkerhetsskydd;

beslutade den 27 februari 2019.

Försvarsmakten föreskriver med stöd av 3 kap. 6 § första stycket, 3 kap. 8 och 10 §§ och 7 kap. 5 § första stycket 2 och 3 säkerhetsskyddsförordningen (2018:658) följande.

1 kap. Allmänna bestämmelser

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

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

Begrepp	**Betydelse**
Elektronisk handling	Upptagning enligt 2 kap. 3 § tryckfrihetsförordningen som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel (upptagning för automatiserad behandling).
Elektroniskt kommunikationsnät	Ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler,

	via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.
Handling	Detsamma som anges i 2 kap. 3 § tryckfrihetsförordningen.
It-utrymme	Utrymme som innehåller växlar, korskopplingar och servrar samt datorhallar.
Lagringsmedium	Permanent minnesmedium som används för att kunna lagra och läsa uppgifter.
Skadlig kod	Otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett informationssystem.
Säkerhetskänslig verksamhet	Detsamma som anges i 1 kap. 1 § säkerhetsskyddslagen (2018:585).
Säkerhetsskyddsklassificerad handling	Detsamma som anges i 1 kap. 4 § säkerhetsskyddsförordningen (2018:658).
Säkerhetsskyddsklassificerat lagringsmedium	Lagringsmedium som innehåller eller är avsett att innehålla säkerhetsskyddsklassificerade uppgifter, om uppgifterna inte är krypterade med kryptografiska funktioner som har godkänts av Försvarsmakten.
Säkerhetsskyddsklassificerade uppgifter	Detsamma som anges i 1 kap. 2 § säkerhetsskyddslagen (2018:585).

3 § Myndigheten ska ha rutiner för att upptäcka, bedöma och hantera incidenter och avvikelser som rör säkerhetskänslig verksamhet samt sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse. Rutinerna ska dokumenteras.

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

Särskilda underrättelseuppgifter och särskilda underrättelsehandlingar

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

2 kap. Säkerhetsskyddsplanering

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

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

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

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

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

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

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

3 kap. Informationssäkerhet

Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter

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

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

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

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

Materiel och tryckta skrifter

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

Bestämmelser om säkerhetsskyddsklassificerade lagringsmedier finns även i 4 kapitlet.

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

Lån av säkerhetsskyddsklassificerade handlingar

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

Anteckning om säkerhetsskyddsklass

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

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

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

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

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

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

9 § Myndigheten ska ha rutiner för ändring respektive borttagning av märkning av säkerhetsskyddsklass.

Rutinerna ska minst reglera vem som får besluta om ändringen respektive borttagningen samt hur ändringen respektive borttagningen ska genomföras.

Rutinerna ska dokumenteras.

10 § Ändring respektive borttagning av märkning av säkerhetsskyddsklass som gäller för en kvalificerat hemlig handling får ske först efter hörande av den myndighet som har upprättat handlingen.

Vid ärende om utlämning av allmän handling enligt tryckfrihetsförordningen får myndigheten höra den myndighet som har upprättat handlingen.

Åtgärder med säkerhetsskyddsklassificerade handlingar och lagringsmedier

11 § En säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre ska på första sidan märkas med handlingens beteckning, exemplarnummer, antal sidor samt bilagor, om såd-

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

För en säkerhetsskyddsklassificerad elektronisk allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre får märkning enligt första stycket istället göras på lämpligt sätt med hänsyn till de informationssystem som handlingen behandlas. Märkningen behöver inte omfatta exemplarnummer och antal sidor.

12 § En säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre ska på handlingens sändlista märkas med hur många exemplar av handlingen som har framställts och vilka som är mottagare av respektive exemplar. Motsvarande uppgifter ska anges i diariet där handlingen är diarieförd, eller i ett register för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.

Första stycket gäller inte för säkerhetsskyddsklassificerade elektroniska allmänna handlingar.

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

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

14 § Myndigheten ska besluta vilka rutiner som ska tillämpas i samband med kopiering av eller utdrag ur en säkerhetsskyddsklassificerad handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre. Rutinerna ska dokumenteras.

Har en kopia av en säkerhetsskyddsklassficerad allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre gjorts, ska uppgift om detta liksom uppgift om till vem kopian eller utdraget har lämnats antecknas i det register eller liggare där handlingen är diarieförd eller i ett register

för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.

Kvittering av säkerhetsskyddsklassificerade handlingar och lagringsmedier

15 § När en säkerhetsskyddsklassificerad allmän handling eller ett säkerhetsskyddsklassificerat lagringsmedium som är placerat i säkerhetsskyddsklassen konfidentiell eller högre tas emot ska mottagandet kvitteras med underskrift, namnförtydligande och datum. Ett namnförtydligande får vara en kod.

När en säkerhetsskyddsklassificerad allmän handling eller ett säkerhetsskyddsklassificerat lagringsmedium återlämnas ska detta antecknas på kvittokopian. Kvittokopian för en handling som är placerad i säkerhetsskyddsklassen konfidentiell eller hemlig ska bevaras i minst 10 år. Kvittokopian för en handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig ska bevaras i minst 25 år.

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

16 § Vad som föreskrivs i 15 § gäller inte när arkiv-, expeditions-, sambands- eller tryckeripersonal tar emot en sådan säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium för registrering, kopiering, distribution, arkivering eller förstöring, om inte den som lämnar över handlingen begär det. Vad som föreskrivs i 15 § gäller inte heller för personal som arbetar med drift av informationssystem för sådana säkerhetsskyddsklassificerade lagringsmedier som hanteras i driften av informationssystemen.

17 § Myndigheten ska ha rutiner för hur kvittering ska göras om uppgifter i en säkerhetsskyddklassificerad allmän handling som är placerad i säkerhets-

skyddsklassen kvalificerat hemlig, lämnas muntligt eller genom visning. Rutinerna ska dokumenteras.

18 § I det diarium där en säkerhetsskyddsklassificerad allmän handling som är placerad i säkerhetsskyddsklassen konfidentiell eller högre är diarieförd ska anges vem som förvarar handlingen eller om handlingen har förkommit, arkiverats eller gallrats. Uppgifterna får istället för i diariet antecknas i ett register för uppföljning av exemplar av säkerhetsskyddsklassificerade allmänna handlingar.

För säkerhetskyddsklassificerade elektroniska allmänna handlingar får det istället anges i vilket informationssystem handlingen behandlas.

19 § Myndigheten ska föra ett register över myndighetens säkerhetsskyddsklassificerade lagringsmedier. Av registret ska det framgå lagringsmediets identifieringsuppgifter, vem som förvarar det och om mediet har förkommit, arkiverats eller förstörts.

Ett säkerhetsskyddsklassificerat lagringsmedium som används endast en gång för omedelbar överföring av säkerhetskyddsklassificerade uppgifter mellan två informationssystem och som därefter omedelbart förstörs behöver inte föras in i registret.

Medförande av säkerhetsskyddsklassificerade handlingar och lagringsmedier utanför myndighetens lokaler

20 § Myndigheten ska besluta i vilken omfattning säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre får medföras från myndighetens lokaler eller områden. Beslutet ska dokumenteras.

Säkerhetsskyddsklassificerade handlingar och lagringsmedier som medförs från myndigheten ska vara under kontroll eller förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av handlingarna respektive lagringsmedierna inom myndighetens lokaler.

En säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium som har medförts utanför myndighetens lokaler eller områden ska snarast möjligt återföras eller överlämnas till den som ska förvara handlingen eller lagringsmediet.

Inventering av säkerhetsskyddsklassificerade handlingar och lagringsmedier

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

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

Säkerhetskyddsklassificerade elektroniska handlingar behöver inte inventeras.

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

Gallring och förstöring av säkerhetsskyddsklassificerade handlingar och lagringsmedier

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

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

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

Åtgärder vid distribution av säkerhetsskyddsklassificerade handlingar och lagringsmedier

25 § Myndigheten ska ha rutiner för hur säkerhetsskyddsklassificerade handlingar och lagringmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre ska distribueras inom och utom myndigheten. Rutinerna ska dokumenteras. Myndigheten ska se till att nödvändiga skyddsåtgärder vidtas under distributionen.

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

Första och andra styckena gäller inte för säkerhetsskyddsklassificerade elektroniska handlingar.

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

Delgivning och distribution till utländsk myndighet och mellanfolklig organisation

27 § I 3 kap. 7 § säkerhetsskyddsförordningen (2018:658) föreskrivs att om en säkerhetsskyddsklassificerad handling kan antas komma att lämnas över till utländska myndigheter eller leverantörer, ska den förses med en anteckning om ursprungsland om det inte är olämpligt.

Om myndigheten har beslutat att en säkerhetsskyddsklassificerad handling får delges till någon utländsk myndighet eller mellanfolklig organisation får handlingens första sida märkas med en sådan upplysning.

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

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

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

En myndighet får inom ramen för ett samarbete med ett annat land eller en mellanfolklig organisation komma överens om att distribuera säkerhetsskyddsklassificerade handlingar på annat sätt än vad som föreskrivs i 3 kap. 10 § första stycket säkerhetsskyddsförordningen.

4 kap. Informationssäkerhet i och kring informationssystem

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

Hantering av säkerhetsskyddsklassificerade lagringsmedier

2 § Ett säkerhetsskyddsklassificerat lagringsmedium får endast hanteras i ett informationssystem som uppfyller de krav som gäller för hantering av uppgifter i den högsta säkerhetsskyddsklass som någon av uppgifterna på lagringsmediet har placerats i eller kan komma att placeras i.

3 § Ett säkerhetsskyddsklassificerat lagringsmedium som innehåller eller har innehållit säkerhetsskyddsklassificerade uppgifter på nivån hemlig eller kvalificerat hemlig får inte återanvändas i ett informationssystem som är avsett för

behandling av säkerhetsskyddsklassificerade uppgifter som är placerade i en lägre säkerhetsskyddsklass.

4 § Ett säkerhetsskyddsklassificerat lagringsmedium som innehåller säkerhetsskyddsklassificerade uppgifter på nivån begränsat hemlig eller konfidentiell får återanvändas i ett informationssystem om myndigheten har rutiner för att säkerställa att inga säkerhetsskyddsklassificerade uppgifter längre kan utläsas ur lagringsmediet.

Åtgärder inför driftsättning

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

Den särskilda säkerhetsskyddsbedömningen ska utgå från verksamhetens säkerhetsskyddsanalys och omfatta vilka hot och sårbarheter som finns i och kring systemet samt en beskrivning av den säkerhetskänsliga verksamhet som systemet ska stödja.

Myndigheten ska i den särskilda säkerhetsskyddsbedömningen, utöver krav på skydd mot röjande av de säkerhetsskyddsklassificerade uppgifter som kommer att hanteras i informationssystemet, också ta ställning till den säkerhetskänsliga verksamhetens krav på tillgänglighet till informationssystemet, och de uppgifter som behandlas i det, och verksamhetens krav på riktighet för dessa uppgifter.

6 § Myndigheten ska granska och godkänna att skyddsåtgärderna i och kring informationssystemet uppfyller de säkerhetskrav som har identifierats i den särskilda säkerhetsskyddsbedömningen och att åtgärderna som beskrivs i 15–27 §§ har implementerats och ger avsedd förmåga. I granskningen ska systemets säkerhetsförmåga testas. Granskningen och godkännandet ska dokumenteras.

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

7 § Myndigheten ska genom granskning eller på annat sätt förvissa sig så långt möjligt om att hård- och mjukvara som ska användas i informationssystem som har betydelse för säkerhetskänslig verksamhet bedöms vara tillförlitlig ur säkerhetsskyddsynpunkt.

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

Begäran om samråd

9 § En begäran om samråd enligt 3 kap. 2 § säkerhetsskyddsförordningen (2018:658) ska ställas till Försvarsmaktens högkvarter. De uppgifter som Försvarsmakten efterfrågar ska tillhandahållas av den begärande myndigheten.

Drift och förvaltning av informationssystem

10 § En myndighet som avser att använda ett informationssystem i säkerhetskänslig verksamhet ska besluta vilka rutiner, resurser och kompetenser för drift, förvaltning, underhåll, övervakning och hantering av incidenter som är nödvändiga ur säkerhetsskyddssynpunkt under hela systemets livscykel. Beslutet ska dokumenteras.

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

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

Dokumentationen ska beskriva systemets hård- och mjukvara, systemets kommunikation och beroenden, informationsflöden och datautbyten samt de skyddsåtgärder som avser systemet och vad som i övrigt är av betydelse för att kunna upprätthålla säkerheten i och kring systemet.

Övervakning

12 § Myndigheten ska kontinuerligt övervaka de informationssystem som är anslutna till ett elektroniskt kommunikationsnät, och som har betydelse för säkerhetskänslig verksamhet, för att kunna upptäcka, analysera och bedöma förändringar och händelser som kan indikera skadlig eller obehörig påverkan, åtkomst eller nyttjande, eller försök till detta, eller obehörig dataöverföring till eller från systemet.

Åtgärder vid förändringar i och kring informationssystem

13 § De skyddsåtgärder i och kring ett informationssystem som ska användas i säkerhetskänslig verksamhet ska fortlöpande anpassas för att möta förändringar i hot och ny kunskap om sårbarheter. Vid behov ska den särskilda säkerhetsskyddsbedömningen och dokumentationen av informationssystemet uppdateras.

14 § Ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska godkännas ur säkerhetsskyddssynpunkt på nytt om det sker förändringar i eller kring systemet som negativt kan påverka säkerheten i systemet. Ett sådant godkännande ska föregås av uppdatering av den särskilda säkerhetsskyddsbedömningen och granskning enligt 5–6 §§.

Autentisering och behörighetskontroll

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

användares identitet och behörighet innan dessa ges tillgång till systemet, samt styra åtkomst till uppgifter, funktioner och resurser i systemet enbart till de användare som har tilldelats behörighet till dessa.

Vad som gäller för användare i första stycket gäller också för informationssystem och processer i informationssystem som ges tillgång till uppgifter, funktioner och resurser.

16 § Tilldelning av identiteter och behörigheter i informationssystem som ska användas i säkerhetskänslig verksamhet ska vara möjlig att granska för att avgöra vilka användare eller resurser som har tillgång till systemet och vilka behörigheter som de har tilldelats i systemet. Myndigheten ska regelbundet granska behörigheterna för att se till att de är ändamålsenliga och aktuella.

Säkerhetsloggning

17 § För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att registrera händelser i eller kring systemet som är av betydelse för säkerheten i säkerhetsloggar. En analys av säkerhetsloggar ska genomföras regelbundet för informationssystem som är avsedd att användas av flera personer. Analysen ska dokumenteras.

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

Intrångsskydd och intrångsdetektering

19 § För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att detektera och avvärja intrång, försök till intrång eller skadlig inverkan på systemet samt detektera och avvärja obehörig kommunikation med systemet.

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

Skydd mot skadlig kod

21 § För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att försvåra och upptäcka inmatning, försök till inmatning, exekvering eller försök till exekvering av skadlig kod eller annan obehörig kod i systemet.

Bevarande av riktighet

22 § För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att upptäcka och försvåra obehörig förändring (bevarande av riktighet) av informationssystemet och dess säkerhetsskydd.

Säkerhetskopiering

23 § För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att säkerhetskopiera och vid behov återställa mjukvara, konfigurationsdata och andra uppgifter som är av betydelse för verksamheten, informationssystemets funktion eller säkerhetsskyddet, och som inte lätt kan återskapas på annat sätt.

Kontroll av att säkerhetskopior kan återläsas ska genomföras regelbundet.

24 § Säkerhetskopior ska förvaras åtskilt från informationssystemet och skyddas så att de finns tillgängliga när de behövs, att deras riktighet bevaras och att obehörig åtkomst till säkerhetskopiorna försvåras.

Skydd mot röjande signaler och obehörig avlyssning

25 § I 3 kap. 4 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om skyddsåtgärder mot röjande signaler. En myndighet ska besluta om säkerhetskrav för skydd mot röjande signaler (RÖS). Beslutet ska dokumenteras.

26 § I 3 kap. 5 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om när säkerhetsskyddsklassificerade uppgifter ska skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

För informationssystem som har betydelse för säkerhetskänslig verksamhet ska en myndighet vidta skyddsåtgärder som ger förmåga att försvåra att uppgifter kommer obehöriga till del, ändras eller förstörs vid kommunikation mellan informationssystemets delsystem eller vid kommunikation till andra informationssystem.

Säkerhetskonfiguration

27 § Ett informationssystem som ska användas i säkerhetskänslig verksamhet ska konfigureras för att minska sårbarheter genom att ta bort eller stänga av funktioner och tjänster som inte behövs, använda lämpliga och möjliga säkerhetsfunktioner i systemet samt konfigurera systemet utifrån vedertagna rekommendationer.

Undantag från krav på skyddsåtgärder

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

5 kap. Fysisk säkerhet

1 § Myndigheten ska vidta de fysiska säkerhetsskyddsåtgärder som krävs för att skydda säkerhetsklassificerade uppgifter och säkerhetskänslig verksamhet. Detta omfattar även detektering av farliga ämnen, vapen samt avlyssnings- och störutrustning.

Tillträde och bevakning

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

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

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

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

5 § Om ett tekniskt bevakningssystem avser

1. utrymmen där säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklassen konfidentiell eller högre förvaras och behandlas, eller
2. platser där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan vara mer än inte obetydlig för Sveriges säkerhet,

ska säkerhetsskyddet av de centrala delarna i det tekniska bevakningssystemet uppfylla de krav på förvaring som gäller för lägst skyddsnivå 2.

Myndigheten ska utreda vilket säkerhetsskydd som behövs för att säkerställa bevakningssystemets funktionalitet. En sådan utredning ska dokumenteras.

6 § Myndigheten ska besluta vilka skyddsåtgärder som ska vidtas vid larm från områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. Beslutet ska dokumenteras.

Nycklar, kort och koder

7 § Nycklar, kort och koder som var för sig ger tillträde till säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig verksamhet ska vara under kontroll eller förvaras i motsvarande skyddsnivå som de ger tillträde till.

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

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

10 § Det ska finnas en förteckning över samtliga nycklar, kort och koder till områden, byggnader eller utrymmen som

1. innehåller säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell eller högre, eller
2. används för säkerhetskänslig verksamhet om en inträffad skada kan vara mer än inte obetydlig för Sveriges säkerhet.

Av förteckningen ska framgå till vem och när en nyckel, ett kort eller en kod har lämnats samt var reservnyckel och kod eller kort i reserv förvaras.

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

Förvaring

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

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

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

15 § En säkerhetsskyddsklassificerad handling som är placerad i säkerhetsskyddsklassen begränsat hemlig ska vara under kontroll eller förvaras inlåst eller i en låst lokal som endast den som är behörig att ta del av handlingen har tillträde till. Lokalen eller förvaringsutrymmet ska uppfylla de krav som gäller för skyddsnivå 1 vid förvaring i eller utanför en administrativ zon eller en säkerhetszon.

16 § En säkerhetsskyddsklassificerad handling som är placerad i säkerhetsskyddsklassen konfidentiell eller hemlig ska vara under kontroll eller förvaras inlåst i ett förvaringsutrymme som uppfyller de krav som gäller för skyddsnivå 2 i en säkerhetszon eller skyddsnivå 3 i en administrativ zon. Om en sådan handling inte förvaras i någon zon ska handlingen förvaras i ett larmat utrymme i lägst skyddsnivå 3.

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

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

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

Utrymmen för muntlig delgivning

20 § Myndigheten ska besluta vilka utrymmen som är godkända för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass konfidentiell eller högre.

Av beslutet ska det framgå hur det säkerställs att endast behörig personal har tillträde till utrymmet samt vilken utrustning som får medföras eller finnas i utrymmet.

Beslutet ska dokumenteras.

Skydd för it-utrymmen

21 § I bilaga 1 till denna författning anges de krav som gäller för respektive skyddsnivå. It-utrymmen ska uppfylla de krav som gäller för skyddsnivå 2, 3 eller 4.

22 § Om det i it-utrymmen behandlas uppgifter som är placerade i säkerhetsskyddsklassen begränsat hemlig ska it-utrymmena uppfylla de krav som gäller för skyddsnivå 2.

Om det i it-utrymmen behandlas uppgifter som är placerade i säkerhetsskyddsklassen konfidentiell eller hemlig ska it-utrymmena uppfylla de krav som gäller för skyddsnivå 3 samt förses med larm.

Om det i it-utrymmen behandlas uppgifter som är placerade i säkerhetsskyddsklassen kvalificerat hemlig ska it-utrymmena uppfylla de krav som gäller för skyddsnivå 4 samt förses med larm.

23 § It-utrymmen ska förses med ett system för inpassering. Av systemet ska det framgå när och vem som har haft tillträde till utrymmet samt andra händelser som är av betydelse för säkerheten.

24 § Ett it-utrymme där säkerhetskänslig verksamhet bedrivs där en inträffad skada kan vara mer än inte obetydlig för Sveriges säkerhet, ska uppfylla de krav som gäller för skyddsnivå 3 samt förses med larm.

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

6 kap. Säkerhetsprövning

1 § Av 3 kap. 1 § säkerhetsskyddslagen (2018:585) framgår att den som genom en anställning eller på något annat sätt deltar i säkerhetskänslig verksamhet ska säkerhetsprövas. Säkerhetsprövningen ska dokumenteras.

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

Placering i säkerhetsklass

3 § Myndigheten ska analysera vilka anställningar samt annat deltagande i myndighetens säkerhetskänsliga verksamhet som ska placeras i säkerhets-

klass, samt vilket övrigt deltagande i den säkerhetskänsliga verksamheten som endast ska vara föremål för säkerhetsprövning. Myndigheten ska därvid särskilt beakta 3 kap. 10 § säkerhetsskyddslagen (2018:585).

Myndigheten ska vidare utgå från myndighetens säkerhetsskyddsanalys och särskilt beakta förekomsten av internationella åtaganden om säkerhetsskydd. Av analysen ska skälet till placering i säkerhetsklass framgå.

Analysen ska dokumenteras.

4 § Myndigheten ska förteckna vilka anställningar och annat deltagande i den säkerhetskänsliga verksamheten som har placerats i säkerhetsklass, eller som endast ska föregås av registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen (2018:585).

Grundutredning

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

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

Grundutredningen ska dokumenteras.

Uppföljande säkerhetsprövning

6 § Myndigheten ska genomföra uppföljande säkerhetsprövning. Prövningen ska fördjupa personkännedomen och särskild vikt ska vid en bedömning läggas vid personliga förhållanden.

Den uppföljande säkerhetsprövningen ska dokumenteras.

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

Avslutande samtal

8 § Myndigheten ska genomföra ett avslutande samtal när personens deltagande i den säkerhetskänsliga verksamheten upphör. Det avslutande samtalet ska dokumenteras.

Om personen har tagit del av säkerhetsskyddsklassificerade uppgifter ska denne upplysas om räckvidden och innebörden av den sekretess och tystnadsplikt som följer av offentlighets- och sekretesslagen (2009:400) eller 5 kap. 2 § andra stycket säkerhetsskyddslagen (2018:585).

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

7 kap. Utbildning och övning

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

2 § Myndigheten ska regelbundet utbilda och öva myndighetens personal och andra som deltar i den säkerhetskänsliga verksamheten i säkerhetsskydd. Omfattningen och innehållet ska utgå från myndighetens säkerhetsskyddsplan.

Myndigheten ska föra en förteckning över de anställda och andra som har genomgått utbildning i säkerhetsskydd, samt vilken utbildning som genomförts och när. En genomförd övning ska dokumenteras.

8 kap. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal

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

Om upphandlingen rör säkerhetskänslig verksamhet ska myndigheten ta fram en plan för hur säkerhetsskyddet ska regleras i uppdraget. Vid behov ska myndighetens säkerhetsskyddsplanering revideras.

Analysen och planen ska dokumenteras.

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

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

En myndighet som avser att genomföra en upphandling som rör säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet ska säkerställa att säkerhetsskyddet upprätthålls.

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

5 § En begäran om samråd enligt 2 kap. 6 § andra stycket 2 säkerhetsskyddsförordningen (2018:658) ska ställas till Försvarsmaktens högkvarter. Till ett sådant samrådsförfarande ska de uppgifter som Försvarsmakten efterfrågar tillhandahållas.

6 § Innan en myndighet lämnar ut säkerhetsskyddsklassificerade uppgifter till en leverantör eller när leverantören ska delta i säkerhetskänslig verksamhet ska myndigheten göra en analys enligt 6 kap. 3 §. Analysen ska omfatta leverantörens ledning och övriga hos leverantören som avses delta i den säkerhetskänsliga verksamheten.

7 § Myndigheten ska se till att den särskilda säkerhetsskyddsbedömningen som anges i 2 kap. 6 § andra stycket 1 säkerhetsskyddsförordningen (2018:658) och sådana analyser och planer som anges i 1 § hålls uppdaterade till dess att säkerhetsskyddsavtalet upphör att gälla.

8 § Om leverantören utanför myndighetens lokaler ska hantera eller förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller när leverantören utanför myndighetens lokaler ska delta i säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, ska myndigheten om det inte är uppenbart obehövligt vidta följande åtgärder.

1. Kontrollera att lokalerna och övriga förhållanden är lämpliga ur säkerhetsskyddssynpunkt,
2. dokumentera kontrollen, och
3. se till att det av säkerhetsskyddsavtalet framgår att leverantören ska upprätta en säkerhetsskyddsinstruktion som ska granskas och godkännas av myndigheten.

Överlåtelse av säkerhetskänslig verksamhet

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

9 kap. Kontroll och tillsyn av säkerhetsskyddet

1 § Myndigheten ska årligen och vid behov kontrollera att regler för säkerhetsskyddet vid myndigheten följs och att säkerhetsskyddet är anpassat till aktuell säkerhetsskyddsplanering.

Kontrollen ska dokumenteras.

2 § Av 2 kap. 6 § andra stycket säkerhetsskyddslagen (2018:585) framgår att en verksamhetsutövare ska kontrollera att en leverantör följer säkerhetsskyddsavtalet. En sådan kontroll ska genomföras regelbundet. Om säkerhetsskyddsavtalet avser kvalificerat hemliga uppgifter eller säkerhetskänslig verk-

samhet som är av synnerlig betydelse för Sverige säkerhet, ska kontrollen genomföras varje år.

Kontrollen ska dokumenteras.

3 § Myndigheten ska ha en plan för kontroll av den egna verksamhetens säkerhetsskydd. En sådan plan ska i förekommande fall även omfatta sådan kontroll som framgår av 2 kap. 6 § andra stycket säkerhetsskyddslagen (2018:585). Planen ska uppdateras löpande och i planen ska det anges vem som är ansvarig för att kontroll och uppföljning genomförs.

4 § När Försvarsmakten genomför tillsyn enligt 7 kap. 1 § första stycket 1 och andra stycket säkerhetsskyddsförordningen (2018:658) ska Försvarsmakten få tillgång till sådan dokumentation som krävs för att kunna utöva tillsyn över säkerhetsskyddet.

10 kap. Anmälan

1 § I 2 kap. 10 § säkerhetsskyddsförordningen (2018:658) framgår när en myndighet ska anmäla säkerhetshotande händelser och verksamhet till Försvarsmakten.

Vid tveksamhet om en säkerhetshotande verksamhet är allvarlig enligt 2 kap. 10 § första stycket 3 säkerhetsskyddsförordningen ska myndigheten samverka med Försvarsmaktens högkvarter.

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

3 § Av en anmälan ska det framgå typ av händelse, tidpunkt och plats för det inträffade, vilka sårbarheter och brister som har identifierats samt vilken säkerhetskänslig verksamhet som har berörts.

11 kap. Internationell verksamhet

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

12 kap. Undantag

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

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

---

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

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

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

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

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

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

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

8. Krav på larm i 5 kap. 16-17 §§, 22 § andra och tredje styckena samt 5 kap. 24 § i den nya författningen avseende larm ska börja gälla den 1 april 2022.

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

Micael Bydén

Carin Bratt

Bilaga 1

Utrymmens indelning i skyddsnivåer

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

	mm i diameter och avståndet från centrum till centrum mellan armeringsstålen får vara högst 250 mm. Fönster enligt norm SS 22 44 25 i lägst klass B 3, fönster i kategori P8B enligt standard SS–EN 356 eller galler certifierade enligt Sveriges Försäkringsförbunds normer för galler i gallerklass 3. Omslutningsytorna får bestå av annat material med motsvarande motståndskraft. Ammunitionsbox som är fast monterad i truppserviceförråd samt flyttbara förvaringsutrymmen såsom värdeskåp enligt norm SS 3150 och med lägre än 100 skyddsvärdespoäng, säkerhetsskåp enligt norm SSF 3492 (SS 3492), standard SS-EN 1143-1 grade 0-III, kassaskåp 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.

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

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

It-utrymme i skyddsnivå 3 som är larmat med seismiska detektorer (vibrationsdetektorer) och magnetdetektorer eller som är ett volymlarmat utrymme. Om larm har utlösts eller angreppsförsök har konstaterats ska en skyddsåtgärd vidtas så att förlust av information kan försvåras.

Bilaga 2

Utrymmens indelning i zoner

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

En säkerhetszon ska vid passerställen vara försedda med ett tekniskt bevakningssystem (system för inpasse-ring) eller personell bevakning eller annan förmåga som säkerställer att endast behöriga har tillträde.

Myndigheten ska vid passerställen till en säkerhetszon kunna kontrollera personer eller fordon.

Myndigheten ska besluta vilka som är behöriga till en säkerhetszon.