Polismyndighetens författningssamling

ISSN 2002-0139
Utgivare: Martin Valfridsson

Säkerhetspolisens föreskrifter om säkerhetsskydd;

PMFS 2019:2

Utkom från trycket
den 27 februari 2019

beslutade den 11 februari 2019.

Säkerhetspolisen föreskriver följande med stöd av 3 kap. 8 och 10 §§ samt 7 kap. 4 § första stycket säkerhetskyddsförordningen (2018:658).

1 kap. Allmänna bestämmelser

1 § Dessa föreskrifter innehåller kompletterande bestämmelser till säkerhetsskyddslagen (2018:585) och säkerhetskyddsförordningen (2018:658). För de myndigheter som anges i 7 kap. 1 § första stycket 1 säkerhetsskyddsförordningen gäller endast bestämmelserna om registerkontroll i 6 kap. 7–16 §§ i dessa föreskrifter.

2 § Ord och uttryck i föreskrifterna har samma innebörd som i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2018:658).

3 § I föreskrifterna avses med *handling* detsamma som anges i 2 kap. 3 § tryckfrihetsförordningen. Med *fysisk handling* avses en framställning i skrift eller bild och med *elektronisk handling* avses en upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel (upptagning för automatiserad behandling). När begreppet handling används i dessa föreskrifter avses, om inget annat anges, både fysiska och elektroniska handlingar.

4 § I föreskrifterna avses med *tillsynsmyndighet* de myndigheter som anges i 7 kap. 1 § första stycket 3–6 säkerhetsskyddsförordningen (2018:658).

5 § Beslut, granskningar, bedömningar, planer, rutiner och liknande enligt föreskrifterna ska dokumenteras.

2 kap. Grundläggande bestämmelser om säkerhetsskydd

Säkerhetsskyddsanalys

Identifiera och bedöma säkerhetskänslig verksamhet

1 § Av 2 kap. 1 § säkerhetsskyddslagen (2018:585) och 2 kap. 1 § säkerhetsskyddsförordningen (2018:658) följer att den som bedriver säkerhetskänslig verksamhet (*verksamhetsutövaren*) ska göra en säkerhetsskyddsanalys.

En säkerhetsskyddsanalys ska identifiera vilka *skyddsvärden* som finns i verksamheten, det vill säga

1. vilka säkerhetsskyddsklassificerade uppgifter och den totala mängden sådana uppgifter som finns i verksamheten,
2. vilka för Sverige förpliktande internationella åtaganden om säkerhetsskydd som finns i verksamheten, och
3. vilken säkerhetskänslig verksamhet i övrigt som finns i verksamheten.

2 § Identifiering av sådana anläggningar, objekt, system och liknande verksamhet som avses i 1 § andra stycket 3 ska utgå från vilken *typ av skada* för Sveriges säkerhet en antagonistisk handling mot en viss verksamhet skulle kunna medföra. Identifieringen ska göras utifrån följande *konsekvenskategorier*.

- Skada för Sveriges yttre säkerhet
- Skada för Sveriges inre säkerhet
- Skada på nationellt samhällsviktig verksamhet
- Skada för Sveriges ekonomi

Även anläggningar och objekt som vid en antagonistiskt handling kan generera skadekonsekvenser på nationell nivå på andra verksamheter i de ovanstående kategorierna ska identifieras (*skadegenererande verksamhet*).

3 § Den typ av skada som har identifierats enligt 2 § ska graderas utifrån följande *konsekvensnivåer*.

- Nivå 5: Synnerligen allvarlig skada för Sveriges säkerhet
- Nivå 4: Allvarlig skada för Sveriges säkerhet
- Nivå 3: Inte obetydlig skada för Sveriges säkerhet
- Nivå 2: Ringa skada för Sveriges säkerhet
- Nivå 1: Inte mätbar eller inte relevant konsekvens med bäring på Sveriges säkerhet

Om graden av skada bedöms som nivå 1 omfattas verksamheten inte av krav på säkerhetsskydd.

4 § Verksamhetsutövaren ska bedöma från vilket eller vilka perspektiv (konfidentialitet, tillgänglighet eller riktighet) den identifierade säkerhetskänsliga verksamheten är skyddsvärd.

5 § I bilaga till dessa föreskrifter finns en beskrivning av konsekvenskategorierna och konsekvensnivåerna som anges i 2 och 3 §§.

Särskilt säkerhetskänslig verksamhet

6 § Med *särskilt säkerhetskänslig verksamhet* avses i dessa föreskrifter säkerhetskänslig verksamhet där en antagonistisk handling mot verksamheten kan medföra synnerligen allvarlig eller allvarlig skada för Sveriges säkerhet (nivå 5 och 4). Verksamhetsutövaren ska rapportera till tillsynsmyndigheten att sådan verksamhet bedrivs. Verksamheter som står direkt under Säkerhetspolisens tillsyn ska istället rapportera till den myndigheten.

7 § Säkerhetspolisen tillhandahåller hotbilder till verksamhetsutövarna via tillsynsmyndigheterna och till verksamheter som står direkt under Säkerhetspolisens tillsyn.

Verksamhetsutövaren ska utifrån hotbilden och egna identifierade hot bedöma hur hoten kan påverka den säkerhetskänsliga verksamheten och om det finns behov av att vidta säkerhetsskyddsåtgärder.

8 § Säkerhetspolisen upprättar efter samråd med tillsynsmyndigheterna *dimensionerande hotbeskrivningar (DHB*) till de verksamhetsutövare som bedriver särskilt säkerhetskänslig verksamhet. Med DHB avses en beskrivning av en antagen antagonistisk förmåga som säkerhetsskyddsåtgärderna förväntas kunna skydda mot, även om det inte föreligger något identifierat hot mot den säkerhetskänsliga verksamheten.

Verksamhetsutövaren ska för särskilt säkerhetskänslig verksamhet dimensionera säkerhetsskyddsåtgärderna utifrån den dimensionerande hotbeskrivningen.

Bedöma sårbarheter

9 § Verksamhetsutövaren ska göra sårbarhetsbedömningar beträffande den säkerhetskänsliga verksamheten. I säkerhetsskyddsanalysen ska det anges vilka övergripande sårbarheter som har identifierats. Verksamhetsutövaren ska därefter bedöma hur sårbarheterna påverkar verksamhetens säkerhetsskydd och om det finns behov av att vidta säkerhetsskyddsåtgärder.

Beslut att fastställa säkerhetsskyddsanalysen

10 § Verksamhetsutövarens högsta chef eller motsvarande organ, eller den som sådan chef eller sådant organ bestämmer, ska fastställa säkerhetsskyddsanalysen. Den ska uppdateras vid behov, dock minst en gång vartannat år.

Upprättande av säkerhetsskyddsplan

11 § Efter att säkerhetsskyddsanalysen är fastställd ska verksamhetsutövaren upprätta en säkerhetsskyddsplan. Planen ska tydliggöra vilka säkerhetsskyddsåtgärder som behöver vidtas utifrån skyddsvärde i relation till säkerhetshot och sårbarheter (*skyddsdimensionering*). Det ska vidare framgå när åtgärderna ska vidtas och vem som ansvarar för dem.

Säkerhetsskyddsplanen ska fastställas av säkerhetsskyddschefen eller den han eller hon bestämmer.

Särskild säkerhetsskyddsbedömning

12 § Vid förändringar av hotbilden eller om verksamhetsutövaren genomför en förändring som kan antas betydligt påverka den säkerhetskänsliga verksamheten ska en *särskild säkerhetsskyddsbedömning* göras, även i andra fall än som följer av 2 kap. 6 § och 3 kap. 1 § säkerhetsskyddsförordningen

(2018:658). En sådan bedömning kan behöva göras vid t.ex. upphandlingar, nyetableringar av verksamhet och förändringar av säkerhetskänsliga system.

Genom den särskilda säkerhetsskyddsbedömningen ska verksamhetsutövaren klargöra bl.a. om

- förändringen kan antas påverka skyddsvärdena,
- förändringen är lämplig utifrån den påverkan den har på Sveriges säkerhet,
- förändringen medför ett behov av att vidta säkerhetsskyddsåtgärder, eller om
- säkerhetsskyddsanalysen behöver uppdateras.

Den särskilda säkerhetsskyddsbedömningen ska fastställas av säkerhetsskyddschefen eller den han eller hon bestämmer.

Styrning av säkerhetsskyddsarbetet

Funktioner och ansvar

13 § Verksamhetsutövaren ska inrätta de funktioner för säkerhetsskyddsarbetet som behövs för att säkerställa att arbetet kan bedrivas på ett fullgott sätt, systematiskt och kontinuerligt samt att det kan kontrolleras och följas upp.

14 § Verksamhetsutövaren ska se till att ansvaret för säkerhetsskyddsarbetet är tydligt definierat och kommunicerat till berörda funktioner.

Verksamhetsutövaren ska se till att funktioner som kan representera motstående intressen i säkerhetsskyddsfrågor är separerade från varandra.

Regelverk

15 § Verksamhetsutövaren ska ha ett dokumenterat regelverk för att upprätthålla verksamhetens säkerhetsskydd. Verksamhetsutövaren ska genom regelverket

- klargöra ledningens och övriga funktioners ansvar för verksamhetens säkerhetsskydd,
- säkerställa att de funktioner som ska arbeta med verksamhetens säkerhetsskydd har nödvändiga befogenheter, och
- se till att säkerhetsskyddsarbetet bedrivs samordnat samt att det utvecklas löpande och utvärderas regelbundet.

Skyldighet att säkerställa resurser och kompetenser

16 § Verksamhetsutövaren ska säkerställa att det finns resurser och kompetenser tillgängliga i den utsträckning som krävs för att upprätthålla säkerhetsskyddet.

17 § Verksamhetsutövaren ska ha rutiner för tilldelning och förändring av behörigheter, fysiska eller elektroniska nycklar eller annat som ger åtkomst till säkerhetskänslig verksamhet.

Verksamhetsutövaren ska kunna följa upp vilken åtkomst den som deltar i säkerhetskänslig verksamhet har till verksamheten, och regelbundet, minst en gång per år, ompröva sådana åtkomster.

Utbildning

18 § Verksamhetsutövaren ska ge den som deltar i säkerhetskänslig verksamhet relevant utbildning i säkerhetsskydd innan personen får åtkomst till verksamheten. Sådan utbildning ska därefter ges regelbundet i den omfattning som behövs.

Verksamhetsutövaren ska utifrån säkerhetsskyddsanalysen se till att innehållet i de utbildningar som genomförs anpassas efter deltagarnas funktioner och ansvar i verksamheten. Utbildningarna ska framgå av en utbildningsplan.

Kontinuitet i säkerhetskänslig verksamhet

19 § Verksamhetsutövaren ska ha rutiner och funktioner för att upprätthålla kontinuitet i säkerhetskänslig verksamhet om en funktionsstörning kan medföra mer än ringa skada för Sveriges säkerhet. Rutinerna ska utformas och tillämpas på sådant sätt att säkerhetsskyddet så långt det är möjligt bibehålls på motsvarande nivå som under normala förhållanden.

Verksamhetsutövaren ska regelbundet utbilda i, utvärdera och vid behov uppdatera sådana rutiner som avses i första stycket.

Hantering av säkerhetshotande händelser och verksamhet

Rutiner, skademinimering och utvärdering

20 § Verksamhetsutövaren ska ha rutiner för hantering av säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd.

21 § Verksamhetsutövaren ska vid säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd vidta åtgärder så att skadlig inverkan på den säkerhetskänsliga verksamheten minimeras och så att den säkerhetskänsliga verksamheten så snart som möjligt kan återgå till normalläge.

22 § Verksamhetsutövaren ska utvärdera inträffade säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd. Utifrån utvärderingen ska verksamhetsutövaren införa de förbättringar som krävs för att minimera skadeeffekten av liknande händelser i framtiden.

23 § Av 2 kap. 10 § första stycket säkerhetsskyddsförordningen (2018:658) framgår när en anmälan till Säkerhetspolisen om säkerhetshotande händelser och verksamhet ska göras.

24 § Om en säkerhetshotande händelse har inneburit en förlust av säkerhetsskyddsklassificerade uppgifter eller att uppgifterna kan ha röjts, ska verksamhetsutövaren snarast, dock senast i samband med att en anmälan om detta görs till Säkerhetspolisen, påbörja arbetet med en skadebedömning.

25 § Verksamhetsutövaren ska snarast, dock senast i samband med att en anmälan om en säkerhetshotande händelse görs till Säkerhetspolisen, överväga behovet av att informera andra verksamhetsutövare som från säkerhetsskyddssynpunkt kan vara berörda av händelsen.

Förbättringar, kontroll och uppföljning

26 § Verksamhetsutövaren ska regelbundet

- utvärdera om säkerhetsskyddsåtgärderna ger avsedd effekt,
- identifiera brister och sårbarheter i säkerhetsskyddet och genomföra förbättringar,
- kontrollera och följa upp det säkerhetsskyddsarbete som bedrivs på uppdrag av verksamhetsutövaren hos externa aktörer, och
- i övrigt kontrollera och följa upp att verksamheten följer regelverket för säkerhetsskydd.

Verksamhetsutövaren ska dokumentera åtgärderna i en plan som ska uppdateras löpande. I planen ska det anges vilken funktion som är ansvarig för åtgärderna.

3 kap. Behandling av säkerhetsskyddsklassificerade uppgifter och handlingar, m.m.

Grundläggande bestämmelser

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

2 § Innan verksamhetsutövaren överför säkerhetsskyddsklassificerade uppgifter till annan, ska mottagaren uppmärksammas på säkerhetsskyddsklassificeringen.

Rutiner

3 § Verksamhetsutövaren ska ha rutiner för behandling av säkerhetsskyddsklassificerade uppgifter och handlingar. Rutinerna ska reglera vad som gäller för spårbarhet, upprättande, kopiering, utskrift, utdrag, kvittering, förvaring,

distribution, medförande, inventering och destruktion samt vad som behövs i övrigt för att upprätthålla ett fullgott säkerhetsskydd.

Verksamhetsutövaren ska ha rutiner för behandling av uppgifter som behöver skyddas från ett tillgänglighets- eller riktighetsperspektiv.

Anteckningar

4 § I 3 kap. 7 § säkerhetsskyddsförordningen (2018:658) finns bestämmelser om att en säkerhetsskyddsklassificerad handling ska förses med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har.

5 § En säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen konfidentiell eller högre ska förses med en anteckning om handlingens beteckning samt i förekommande fall antal sidor och uppgift om bilagor.

6 § En säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig ska förses med en anteckning om handlingens exemplarnummer.

7 § Om det beslutas att en säkerhetsskyddsklassificerad handling inte längre ska vara indelad i säkerhetsskyddsklass eller ska delas in i annan säkerhetsskyddsklass än vad som anges på handlingen, ska detta antecknas på handlingen. Åtgärden ska för allmänna handlingar antecknas i det register där handlingen är diarieförd.

8 § Om en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig inte längre bedöms vara kvalificerat hemlig, ska samråd ske med den som upprättat handlingen och verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer, innan åtgärder enligt 7 § vidtas. Anteckning om samrådet ska göras på handlingen.

Kopia och utdrag

9 § Kopia av eller utdrag ur en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig får göras endast efter medgivande av verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

Förvaring

10 § En säkerhetsskyddsklassificerad handling ska förvaras i ett förvaringsutrymme med säkerhet som motsvarar den skyddsnivå som skyddsdimensioneringen kräver.

11 § En säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig ska förvaras av verksamhetsutövarens högsta chef eller motsvarande organ i enlighet med kraven i 10 §. Verksamhetsutövarens

högsta chef eller motsvarande organ får dock besluta om andra förvaringsplatser för sådan handling.

12 § I ett register där en säkerhetsskyddsklassificerad fysisk allmän handling är diarieförd ska det framgå var handlingen förvaras eller om den gallrats eller kommit bort.

Märkning av lagringsmedium

13 § Lagringsmedium för säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre ska märkas med säkerhetsskyddsklass och identifieringsuppgift. Om lagringsmediet är fast monterat i annan utrustning ska i stället utrustningen märkas.

Distribution

14 § Verksamhetsutövaren ska ha rutiner för hur en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen konfidentiell eller högre ska distribueras inom och utom verksamheten. Verksamhetsutövaren ska se till att nödvändiga säkerhetsskyddsåtgärder vidtas under distribution.

En försändelse med en säkerhetsskyddsklassificerad fysisk handling eller elektronisk handling på ett lagringsmedium i säkerhetsskyddsklassen konfidentiell eller högre ska sändas med en distributör som har godkänts av verksamhetsutövaren. En sådan distributör ska kunna verifiera att försändelsen har levererats till mottagaren.

15 § I 3 kap. 7 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om att säkerhetsskyddsklassificerade handlingar som kan antas komma att lämnas över till utländska myndigheter eller leverantörer ska förses med en anteckning om ursprungsland, om det inte är olämpligt.

16 § Tillsynsmyndigheterna får medge undantag från bestämmelserna i 3 kap. 10 § första stycket säkerhetsskyddsförordningen (2018:658) om försändelser med säkerhetsskyddsklassificerade handlingar till utlandet.

Kvittering

17 § Den som tar emot en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen hemlig ska kvittera mottagandet med namnteckning och namnförtydligande i register, liggare eller på särskilt kvitto.

Den som tar emot en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen kvalificerat hemlig ska kvittera mottagandet med namnteckning och namnförtydligande på särskilt kvitto i två exemplar.

Om en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen hemlig eller högre återlämnas, ska detta antecknas på kvittensen.

Verksamhetsutövaren ska bevara kvittensen i minst 10 år. Om handlingen är kvalificerat hemlig ska kvittensen bevaras i minst 25 år.

Hos myndigheter och annan verksamhet som offentlighets- och sekretesslagen (2009:400) är tillämplig på gäller kraven i första till fjärde styckena endast för allmänna handlingar.

18 § Verksamhetsutövaren ska anteckna vem som är mottagare av en säkerhetsskyddsklassificerad elektronisk handling i säkerhetsskyddsklassen kvalificerat hemlig i handlingen eller i ett register över kvalificerat hemliga handlingar.

19 § Vad som anges i 17 och 18 §§ gäller inte när arkiv-, expeditions-, sambands- eller tryckeripersonal tar emot en säkerhetsskyddsklassificerad handling för registrering, kopiering, distribution, arkivering eller förstöring, om inte den som lämnar över handlingen begär det. Bestämmelserna gäller inte heller för personal som arbetar med drift av informationssystem när personalen hanterar lagringsmedium som har tilldelats eller ska tilldelas andra personer.

20 § Om uppgifter i en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig lämnas muntligen eller genom visning, ska anteckning om detta göras i handlingen eller i ett register över kvalificerat hemliga handlingar.

Medförande utanför verksamhetsutövarens lokaler

21 § Om en säkerhetsskyddsklassificerad handling medförs till eller från verksamhetsutövarens lokaler ska den hållas under omedelbar uppsikt eller förvaras på ett sätt som så långt som möjligt motsvarar det säkerhetsskydd som gäller för förvaringen av handlingen inom verksamhetens lokaler.

Kraven i första stycket gäller inte om handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

22 § Säkerhetsskyddschefen får i särskilda fall besluta att personal, som är behörig enligt 2 kap. 3 § säkerhetsskyddsförordningen (2018:658), får ta med en försändelse med en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen hemlig eller lägre till utlandet.

23 § En säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig får inte medföras från verksamhetsutövarens lokaler utan tillstånd av verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

Inventering

24 § Av 3 kap. 8 § säkerhetsskyddsförordningen (2018:658) följer att säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska inventeras minst en gång per år.

Säkerhetsskyddsklassificerade fysiska handlingar i säkerhetsskyddsklassen hemlig ska inventeras minst en gång per år.

Lagringsmedier som innehåller uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig ska inventeras minst en gång per år.

Förstöring

25 § Förstöring av säkerhetsskyddsklassificerade uppgifter ska ske så att åtkomst och återskapande av uppgifterna omöjliggörs.

26 § Förstöring av en säkerhetsskyddsklassificerad allmän handling i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig ska dokumenteras.

Avveckling eller återanvändning av lagringsmedium

27 § Verksamhetsutövaren ska ha rutiner för avveckling eller återanvändning av lagringsmedium som används i säkerhetskänslig verksamhet. Rutinerna ska säkerställa att information på lagringsmediet inte kan återskapas.

4 kap. Informationssäkerhet i informationssystem

Definitioner

1 § I detta kapitel avses med

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

intrångsskydd: administrativa eller tekniska åtgärder som vidtas för att skydda informationssystem mot obehörig åtkomst,

skadlig kod: oönskad programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett informationssystem,

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

Säkerhetsskyddsåtgärder

Kontinuerlig anpassning

2 § Verksamhetsutövaren ska kontinuerligt anpassa säkerhetsskyddsåtgärder i informationssystem för att möta förändringar av hot och sårbarheter. Verksamhetsutövaren ska även fastställa hur detta ska genomföras och vem som ansvarar för att identifiera förändringarna.

Kompetens

3 § Verksamhetsutövaren ska se till att den som deltar i utveckling, framtagning av arkitektur, testning och drift av informationssystem som har betydelse för säkerhetskänslig verksamhet har tillräcklig kompetens avseende informationssäkerhet och sårbarheter i aktuellt informationssystem.

4 § Verksamhetsutövaren ska se till att egenutvecklad programvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter.

5 § Verksamhetsutövaren ska se till att tredjepartsprogramvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att programvaran på annat sätt bedöms vara tillförlitlig från säkerhetsskyddssynpunkt.

Åtgärder inför driftsättning eller förändring

6 § Verksamhetsutövaren ska vid en särskild säkerhetsskyddsbedömning enligt 3 kap. 1 § säkerhetsskyddsförordningen (2018:658), beakta såväl de enskilda säkerhetsskyddsklassificerade uppgifterna som den totala mängden sådana uppgifter som kan komma att behandlas i informationssystemet.

7 § Verksamhetsutövaren ska, innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, genomföra tester av säkerhetsskyddsåtgärderna. Resultatet ska dokumenteras och jämföras med de säkerhetskrav som gäller för informationssystemet. Den särskilda säkerhetsskyddsbedömningen ska uppdateras med eventuella avvikelser och de kompensatoriska åtgärder som måste vidtas.

8 § Verksamhetsutövaren ska innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, dokumentera vilka resurser och kompetenser som krävs för att bibehålla fastställt säkerhetsskydd under informationssystemets förväntade livstid.

9 § Verksamhetsutövaren ska, innan samråd enligt 3 kap. 2 § säkerhetsskyddsförordningen (2018:658) sker med Säkerhetspolisen, kontrollera och dokumentera att de säkerhetskrav som identifierats i den särskilda säkerhetsskyddsbedömningen har implementerats och att säkerhetsskyddsåtgärderna ger avsedd effekt.

Rutiner för hantering av informationssystem

10 § Verksamhetsutövaren ska fastställa rutiner för hanteringen av informationssystem som har betydelse för säkerhetskänslig verksamhet under systemets förväntade livstid.

Granskning av säkerheten

11 § Verksamhetsutövaren ska årligen granska säkerheten i informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig eller i informationssystem där en incident kan medföra allvarlig eller synnerligen allvarlig skada för Sveriges säkerhet.

Unika identiteter och spårbarhet

12 § Alla utställda identiteter i ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara unika över tid. Åtkomsten ska vara spårbar till individ, system eller resurs.

Behörighetsstyrning

13 § Verksamhetsutövaren ska tilldela sådana behörigheter som ger systemadministrativ åtkomst eller annan särskild tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet restriktivt. Behörigheterna ska vara tidsbegränsade och följas upp särskilt.

Tilldelning av behörigheter enligt första stycket som inte direkt kan kopplas till någon fysisk individ ska ske särskilt restriktivt och beslutas av säkerhetsskyddschefen eller den han eller hon bestämmer.

Autentisering

14 § Verksamhetsutövaren ska se till att autentisering vid åtkomst till informationssystem som har betydelse för säkerhetskänslig verksamhet baseras på flera faktorer (*flerfaktorsautentisering*).

15 § Verksamhetsutövaren ska fastställa tekniska eller administrativa regler för utformning, byte och hantering av lösenord, om sådana används för att ge tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet. Reglerna ska bl.a. innehålla bestämmelser om återanvändning av lösenord samt lösenordens längd och komplexitet.

16 § Verksamhetsutövaren ska ge kod eller lösenord som ger tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet ett säkerhetsskydd som motsvarar det säkerhetsskydd som informationssystemet ska ha enligt skyddsdimensioneringen.

17 § Vid användning av central funktion för identifiering eller behörighetskontroll, ska verksamhetsutövaren se till att denna funktion ges ett säkerhetsskydd som motsvarar det högsta säkerhetsskydd som de anslutna informationssystemen ska ha enligt skyddsdimensioneringen.

Skydd mot röjande signaler

18 § I 3 kap. 4 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om skyddsåtgärder mot röjande signaler. Verksamhetsutövaren ska besluta om sådana åtgärder.

Kommunikationssäkerhet

19 § Verksamhetsutövaren ska se till att informationssystem som har betydelse för säkerhetskänslig verksamhet

- kommunicerar på ett kontrollerat sätt med komponenter eller delsystem inom samma informationssystem, och
- kommunicerar på ett kontrollerat sätt med informationssystem eller nätverk som inte omfattas av krav på säkerhetsskydd.

20 § Verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller konfidentiell, logiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

21 § Verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig, fysiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

Informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig, ska tillåta endast envägskommunikation vid import respektive export av data.

Kryptering

22 § Verksamhetsutövaren ska analysera behovet av användning av kryptografiska funktioner till skydd för säkerhetsskyddsklassificerade uppgifter och uppgifter som behöver skyddas från ett riktighetsperspektiv.

I 3 kap. 5 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om användning av kryptografiska funktioner som har godkänts av Försvarsmakten.

Konfiguration, uppdatering och dokumentering

23 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet tillämpa konfiguration som använder lämpliga säkerhetsfunktioner, stänger av funktioner som inte används och även i övrigt reducerar sårbarheter.

24 § Verksamhetsutövaren ska se till att programvara i informationssystem som har betydelse för säkerhetskänslig verksamhet hålls uppdaterad så att säkerhetsbrister och sårbarheter motverkas.

Om det finns särskilda skäl får verksamhetsutövaren besluta om undantag från kravet i första stycket.

25 § Verksamhetsutövaren ska ha dokumentation som visar logiska samband och inbördes beroenden mellan komponenter som används i informationssystem som har betydelse för säkerhetskänslig verksamhet.

26 § Verksamhetsutövaren ska för informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen

kvalificerat hemlig, dokumentera vilken hård- och mjukvara som används i informationssystemet och deras inbördes beroenden.

Kraven i första stycket gäller även informationssystem där en incident kan medföra synnerligen allvarlig skada för Sveriges säkerhet.

Skydd mot skadlig kod

27 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet analysera behovet av och i förekommande fall besluta att använda de funktioner för skydd mot skadlig kod som är nödvändiga från säkerhetsskyddssynpunkt.

Riktighet

28 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet vidta säkerhetsskyddsåtgärder som ger förmåga att försvåra och upptäcka obehörig förändring av informationssystemet och dess säkerhetsskydd.

Intrångsdetektering och intrångsskydd

29 § Verksamhetsutövaren ska förse ett informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre och som kommunicerar med andra informationssystem, med funktioner för intrångsdetektering och intrångsskydd.

30 § Verksamhetsutövaren ska förse ett informationssystem där en incident kan medföra mer än ringa skada för Sveriges säkerhet och som kommunicerar med andra informationssystem, med funktioner för intrångsdetektering och intrångsskydd.

Säkerhetsloggning

31 § Verksamhetsutövaren ska logga händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet (*säkerhetsloggning*).

32 § Verksamhetsutövaren ska ha rutiner för loggning av händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet. Rutinerna ska omfatta hur verksamhetsutövaren ska kunna upptäcka skadlig eller obehörig åtkomst eller påverkan samt funktionsstörningar. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser.

33 § För informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter ska rutinerna omfatta loggning av användning och ändring av behörigheter med systemadministrativ åtkomst och av roller med särskild behörighet i informationssystemet.

34 § Verksamhetsutövaren ska bevara säkerhetsloggar i minst 10 år. För informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska säkerhetsloggar bevaras i minst 25 år.

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

Säkerhetsövervakning

36 § Verksamhetsutövaren ska använda funktion för säkerhetsövervakning av informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig.

Kraven i första stycket gäller även informationssystem där en incident kan medföra allvarlig eller synnerligen allvarlig skada för Sveriges säkerhet.

37 § Verksamhetsutövaren ska ha rutiner för säkerhetsövervakning enligt 36 §. Rutinerna ska omfatta vad som ska övervakas och vem som ansvarar för övervakningen. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser.

Kontroll av säkerhetskopior

38 § När säkerhetskopiering av säkerhetsskyddsklassificerade uppgifter eller uppgifter i övrigt som har betydelse för säkerhetskänslig verksamhet genomförs, ska verksamhetsutövaren regelbundet, minst en gång per år, kontrollera att uppgifterna på säkerhetskopiorna går att återskapa.

5 kap. Fysisk säkerhet

Åtgärder för att upptäcka, försvåra och hantera

1 § Av 4 kap. 1 § säkerhetsskyddsförordningen (2018:658) följer att verksamhetsutövaren ska vidta säkerhetsskyddsåtgärder för att upptäcka, försvåra och hantera obehörigt tillträde eller skadlig inverkan.

2 § Verksamhetsutövaren ska, i den omfattning som skyddsdimensioneringen kräver, använda personell bevakning eller teknisk övervakning för att tidigt upptäcka obehörigt tillträde eller skadlig inverkan.

3 § Verksamhetsutövaren ska, i den omfattning som skyddsdimensioneringen kräver, vidta försvårande åtgärder i syfte att fördröja obehörigt tillträde eller reducera skadlig inverkan. Försvårande åtgärder kan vara t.ex. tillträdesbegränsande åtgärder, fysiska barriärer, skyddsavstånd och byggnadstekniska förstärkningar.

4 § Verksamhetsutövaren ska, i den omfattning som skyddsdimensioneringen kräver, se till att hanterande åtgärder kan vidtas i syfte att avbryta

obehörigt tillträde eller skadlig inverkan. Hanterande åtgärder kan vara t.ex. insatser av väktare, skyddsvakter eller polis.

5 § Verksamhetsutövaren ska kontrollera att alla personer som ska få tillträde till en plats där säkerhetskänslig verksamhet bedrivs, har behörighet till det.

Verksamhetsutövaren ska utfärda skriftligt tillstånd för besökare som ska få tillträde till en plats där säkerhetskänslig verksamhet bedrivs.

Kort, koder och nycklar

6 § Verksamhetsutövaren ska ha ett passersystem för identifiering eller behörighetskontroll för åtkomst till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet. Systemet ska omges av säkerhetsskyddsåtgärder som motsvarar vald skyddsdimensionering.

7 § Verksamhetsutövaren ska ställa krav på att kort, koder, nycklar eller liknande som ger åtkomst till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet, förvaras så att någon obehörig inte kan få tillgång till dem. Om det befaras att kort, kod, nycklar eller motsvarande har stulits, förlorats eller kopierats ska detta omedelbart hanteras som en säkerhetshotande händelse enligt 2 kap. 21 § i dessa föreskrifter.

8 § Verksamhetsutövaren ska ha en förteckning över kort, koder, nycklar eller liknande som hör till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet. Av förteckningen ska det framgå till vem och när kort, kod, nyckel eller liknande har lämnats och var reservkod eller reservnyckel förvaras. Det ska vidare framgå när återlämnande skett.

6 kap. Personalsäkerhet

Säkerhetsprövning

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

2 § Verksamhetsutövaren ska med utgångspunkt i säkerhetsskyddsanalysen föra förteckning över vilka anställningar eller annat deltagande i den säkerhetskänsliga verksamheten som placerats i säkerhetsklass eller som ska föregås av registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen (2018:585).

3 § Verksamhetsutövaren ska besluta vilka anställningar eller annat deltagande i den säkerhetskänsliga verksamheten som ska föranleda säkerhetsprövning utan inplacering i säkerhetsklass.

4 § Grundutredning enligt 5 kap. 2 § säkerhetsskyddsförordningen (2018:658) ska innehålla ett personligt samtal där lojalitet, pålitlighet och sårbarhet hos den som prövas bedöms.

Verksamhetsutövaren ska inom ramen för säkerhetsprövningen fortlöpande under anställningen eller deltagandet göra dessa bedömningar.

5 § Bestämmelser om utbildning finns i 5 kap. 1 § säkerhetsskyddsförordningen (2018:658) och i 2 kap. 18 § i dessa föreskrifter.

Avslutande säkerhetssamtal

6 § Verksamhetsutövaren ska genomföra avslutande säkerhetssamtal när personens deltagande i den säkerhetskänsliga verksamheten upphör, om det inte är uppenbart obehövligt.

Registerkontroll och särskild personutredning

Framställan

7 § Verksamhetsutövaren ska göra framställan om registerkontroll och särskild personutredning på av Säkerhetspolisen anvisad blankett. Om anställningen eller deltagandet är tidsbegränsat ska tiden anges.

8 § Vid framställan om registerkontroll i säkerhetsklass 1 eller vid framställan efter beslut av regeringen enligt 5 kap. 13 § andra stycket första meningen säkerhetsskyddsförordningen (2018:658) ska regeringsbeslutet ligga till grund för framställan och finnas tillgängligt hos verksamhetsutövaren.

9 § Framställan om registerkontroll av personal hos en leverantör som verksamhetsutövaren har ingått säkerhetsskyddsavtal med, får göras först när avtalet har anmälts till Säkerhetspolisen.

En framställan om registerkontroll får innehålla hänvisning till endast ett säkerhetsskyddsavtal.

10 § En tillsynsmyndighet får besluta enligt 5 kap. 16 § säkerhetsskyddsförordningen (2018:658) att en enskild verksamhetsutövare får ansöka om registerkontroll först efter att ha gett Säkerhetspolisen tillfälle att yttra sig.

Samtycke

11 § Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska dokumentera att samtycke till registerkontroll och särskild personutredning har lämnats av den som säkerhetsprövningen gäller.

Kontrollorsak

12 § Av framställan om registerkontroll ska kontrollorsaken framgå tydligt, t.ex. vilken typ av säkerhetskänslig verksamhet personen avses delta i samt vilka arbetsuppgifter han eller hon avses få.

Underrättelse till Säkerhetspolisen

13 § Om en uppgift har lämnats ut för säkerhetsprövning enligt 3 kap. 19 § säkerhetsskyddslagen (2018:585) ska den som beslutar om registerkontroll underrätta Säkerhetspolisen om den kontrollerade har godkänts vid säkerhetsprövningen eller inte.

Förnyad kontroll

14 § Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska se till att en förnyad registerkontroll görs när någon som innehar en säkerhetsklassad befattning får en annan befattning som inte omfattas av tidigare kontrollorsak eller den befintliga befattningen blir inplacerad i en annan säkerhetsklass. Detsamma gäller, såvitt avser registerkontrollerade personer i säkerhetsklass 1 eller 2, om den kontrollerade ingått äktenskap eller inlett ett samboförhållande efter den senaste registerkontrollen.

Avanmälan eller ändring av den kontrollerades förhållanden

15 § Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska skriftligen underrätta Säkerhetspolisen om den kontrollerade inte längre har en befattning som är inplacerad i säkerhetsklass. Detsamma gäller, såvitt avser registerkontrollerade personer i säkerhetsklass 1 eller 2, om den kontrollerades äktenskap har upplösts eller om samboförhållandet har upphört. Underrättelsen ska ske på av Säkerhetspolisen anvisad blankett.

Kontaktpersoner

16 § Den verksamhetsutövare som beslutar eller ansöker om registerkontroll ska ha en kontaktperson som svarar för hanteringen av registerkontroller.

Kontaktpersonerna ska redovisas till Säkerhetspolisen på av myndigheten anvisad blankett. Uppgifterna ska hållas uppdaterade gentemot Säkerhetspolisen.

7 kap. Säkerhetsskyddsavtal m.m.

Allmänt

1 § Bestämmelser om säkerhetsskyddad upphandling och samråd vid sådana upphandlingar finns i 2 kap. 6 § säkerhetsskyddslagen (2018:585) och 2 kap. 6 § säkerhetsskyddsförordningen (2018:658). Bestämmelser om särskild säkerhetsskyddsbedömning finns i 2 kap. 12 § i dessa föreskrifter.

En verksamhetsutövare som avser att genomföra en upphandling eller motsvarande som rör säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, ska säkerställa att säkerhetsskyddet regleras på något annat sätt än genom ett säkerhetsskyddsavtal.

2 § Verksamhetsutövaren ska innan ett förfarande enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585) påbörjas, analysera om uppdraget rör säkerhetskänslig verksamhet. Om förfarandet rör sådan verksamhet ska verksamhetsutövaren ta fram en plan för hur säkerhetsskyddet ska regleras i uppdraget.

Nivåer m.m.

3 § Ett säkerhetsskyddsavtal ska ingås på någon av följande nivåer:

- Nivå 1: Leverantören kommer att utanför verksamhetsutövarens lokaler eller utrymmen:
  - få tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller
  - få tillgång till säkerhetskänslig verksamhet där åtkomst till verksamheten kan medföra en inte obetydlig skada för Sveriges säkerhet.
- Nivå 2: Leverantören kommer att i verksamhetsutövarens egna lokaler eller utrymmen:
  - få tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller
  - få tillgång till säkerhetskänslig verksamhet där åtkomst kan medföra en inte obetydlig skada för Sveriges säkerhet.
- Nivå 3: Leverantören kan komma att i verksamhetsutövarens egna lokaler eller utrymmen:
  - få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiellt eller högre, eller
  - få tillgång till säkerhetskänslig verksamhet där åtkomst kan medföra en inte obetydlig skada för Sveriges säkerhet.

4 § Anmälan enligt 2 kap. 7 § säkerhetsskyddsförordningen (2018:658) ska göras på blankett anvisad av Säkerhetspolisen. Verksamhetsutövaren ska bifoga ett aktuellt registreringsbevis eller liknande handling till anmälan.

Bedömning av leverantörens lämplighet samt kontroll

5 § En verksamhetsutövare som avser att ingå ett säkerhetsskyddsavtal i nivå 1 ska på plats kontrollera leverantörens säkerhetsskydd beträffande aktuella lokaler eller utrymmen. Kontroller ska utföras regelbundet under tiden leverantören utför arbete som omfattas av säkerhetsskyddsavtal.

6 § Verksamhetsutövaren ska kontrollera att leverantörens ledning eller berörda delar av ledningen samt övriga hos leverantören som avses delta i den säkerhetskänsliga verksamheten genomgår säkerhetsprövning med registerkontroll.

7 § Verksamhetsutövaren ska kontrollera leverantörens säkerhetsskydd enligt säkerhetsskyddsavtalet för att säkerställa att detta är fullgott. Verksam-

hetsutövaren ska också löpande bedöma om säkerhetsskyddsavtalet behöver revideras.

8 § Verksamhetsutövaren ska säkerställa att personal hos en leverantör som verksamhetsutövaren ingått säkerhetsskyddsavtal med har relevant kunskap inom säkerhetsskydd för arbetet de ska utföra.

Säkerhetsskyddsinstruktion

9 § När ett säkerhetsskyddsavtal har ingåtts i nivå 1 ska leverantören dokumentera i en säkerhetsskyddsinstruktion hur denne uppfyller kravet på säkerhetsskydd enligt avtalet. Verksamhetsutövaren ska godkänna säkerhetsskyddsinstruktionen.

10 § Verksamhetsutövaren ska till Säkerhetspolisen lämna de uppgifter angående säkerhetsskyddsavtal som Säkerhetspolisen begär.

När säkerhetsskyddsavtalet upphört

11 § När ett säkerhetsskyddsavtal har upphört ska verksamhetsutövaren upplysa leverantören om den tystnadsplikt som följer av 5 kap. 2 § första stycket säkerhetsskyddslagen (2018:585). Leverantören ska återlämna eller förstöra alla säkerhetsskyddsklassificerade handlingar enligt verksamhetsutövarens anvisningar.

12 § När ett säkerhetsskyddsavtal har upphört ska verksamhetsutövaren skyndsamt avanmäla säkerhetsskyddsavtalet och de registerkontroller som hör till avtalet. Avanmälan ska ske till Säkerhetspolisen på anvisad blankett.

Blankett vid samråd och överlåtelse

13 § Vid samråd eller överlåtelse enligt 2 kap. 6 § respektive 9 § säkerhetsskyddsförordningen (2018:658) ska blankett anvisad av Säkerhetspolisen användas.

8 kap. Tillsyn

1 § Tillsynsmyndigheterna ska årligen fastställa en tillsynsplan som ska ligga till grund för tillsynsverksamheten. Planen ska uppdateras vid behov och på begäran lämnas till Säkerhetspolisen.

2 § Tillsynsmyndigheterna ska genomföra tillsynen löpande och systematiskt samt skriftligen informera Säkerhetspolisen om det utförda arbetet.

3 § Tillsynsmyndigheterna ska rapportera till Säkerhetspolisen vilka särskilt säkerhetskänsliga verksamheter som finns inom respektive tillsynsområde.

9 kap. Undantag

1 § Säkerhetspolisen och tillsynsmyndigheterna får medge undantag från bestämmelserna i dessa föreskrifter.

Innan en tillsynsmyndighet fattar beslut om undantag ska myndigheten samråda med Säkerhetspolisen.

---

1. Dessa föreskrifter träder i kraft den 1 april 2019.
2. Genom föreskrifterna upphävs Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2015:3.

På Säkerhetspolisens vägnar

KLAS FRIBERG

Sofie Klahr
(Rättsenheten)

Identifiering och gradering av säkerhetskänslig verksamhet i övrigt i form av anläggningar, objekt, system och liknande

Anläggningar, objekt, system och liknande verksamhet ska identifieras och graderas utifrån vilken typ och grad av skada som direkt eller uppenbart indirekt kan uppstå för Sveriges yttre säkerhet, för Sveriges inre säkerhet, på nationellt samhällsviktig verksamhet och för Sveriges ekonomi. Detsamma gäller för anläggningar och objekt där det bedrivs verksamhet som vid en antagonistisk handling kan generera skadekonsekvenser på nationell nivå på andra säkerhetskänsliga verksamheter (s.k. skadegenererande verksamhet). Identifieringen ska göras utifrån följande konsekvenskategorier.

Konsekvenskategorier

Skada för Sveriges yttre säkerhet

Skada för Sveriges förmåga att upprätthålla nationellt försvar (territoriell suveränitet) samt Sveriges integritet, oberoende och handlingsfrihet (politisk självständighet).

Skada för Sveriges inre säkerhet

Skada för Sveriges förmåga att upprätthålla och säkerställa grundläggande strukturer i form av det demokratiska statsskicket, rättsväsendet och den brottsbekämpande förmågan på nationell nivå.

Skada på nationellt samhällsviktig verksamhet

Skada genom påverkan på leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet på nationell nivå.

Skada för Sveriges ekonomi

Skada på den nationella betalningsförmågan, där skadan kan få negativa konsekvenser för Sveriges suveränitet, handlingsfrihet och oberoende.

Skadegenererande verksamhet

En verksamhet som, om den utsätts för en antagonistisk handling, kan generera skadekonsekvenser på andra säkerhetskänsliga verksamheter. Sådana anläggningar eller objekt är ofta redan identifierade och klassificerade utifrån annan lagstiftning t.ex. s.k. *farlig verksamhet* enligt 2 kap. 4 § lagen (2003:778) om skydd mot olyckor men med den skillnaden att här avses bara anläggningar som direkt eller uppenbart indirekt kan generera skadekonsekvenser på nationell nivå.

Typen av skada som har identifierats avseende anläggningar, objekt, system och liknande verksamhet ska sedan graderas utifrån den skada som kan uppstå för Sveriges säkerhet. Graderingen ska göras utifrån följande konsekvensnivåer (1–5).

Nivå 5 Synnerligen allvarlig skada för Sveriges säkerhet

Synnerligen allvarlig skada på system- eller sektorsnivå. Kritiska tjänster, leveranser, funktioner eller förmågor är utslagna eller mycket allvarligt påverkade. Sverige skulle komma att förlora sin suveränitet, handlingsfrihet eller oberoende. Synnerligen allvarlig påverkan på andra säkerhetskänsliga verksamheter. Långsiktiga konsekvenser och mycket svårt att återgå till ett normalläge.

Nivå 4 Allvarlig skada för Sveriges säkerhet

Allvarlig skada på system- eller sektorsnivå. Kritiska tjänster, leveranser, funktioner eller förmågor skulle allvarligt komma att påverkas. Allvarliga begränsningar i Sveriges suveränitet, handlingsfrihet eller oberoende. Allvarlig påverkan på andra säkerhetskänsliga verksamheter. Svårt att återgå till ett normalläge.

Nivå 3 Inte obetydlig skada för Sveriges säkerhet

Påtaglig påverkan på kritiska tjänster, leveranser, funktioner eller förmågor men i begränsad omfattning. Sveriges suveränitet, handlingsfrihet eller oberoende skulle komma att påverkas men i begränsad omfattning. Inte obetydlig skada på andra säkerhetskänsliga verksamheter. Möjligt att återgå till ett normalläge inom en rimlig tid.

Nivå 2 Ringa skada för Sveriges säkerhet

Möjlig påverkan på vissa tjänster, leveranser, funktioner eller förmågor i liten omfattning och med ringa skada. Möjlig påverkan på Sveriges suveränitet, handlingsfrihet eller oberoende men i liten omfattning och med ringa skada. Ringa skada på andra säkerhetskänsliga verksamheter. Möjligt att relativt snabbt återgå till ett normalläge.

Nivå 1 Inte mätbar eller inte relevant konsekvens med bäring på Sveriges säkerhet

Nationella konsekvenser kan inte påvisas, konkretiseras eller mätas.

Konsekvens på Nivå	**Sveriges yttre säkerhet**	**Sveriges inre säkerhet**	**Nationellt samhällsviktig verksamhet**	**Sveriges ekonomi**	**Skadegenererande verksamhet**
5	Synnerligen allvarlig skada på Sveriges försvarsförmåga eller politiska självständighet.	Synnerligen allvarlig skada på det demokratiska statsskicket, rättsväsendet eller den brottsbekämpande förmågan på nationell nivå.	Synnerligen allvarlig skada på nationellt samhällsviktig verksamhet i form av avbrott eller påverkan på leveranser, tjänster och funktioner.	Synnerligen allvarlig skada på Sveriges betalningsförmåga i form av påverkan på förmågan att hantera, administrera, granska, styra och stödja nationell finansiell stabilitet.	Synnerligen allvarlig skada på annan säkerhetskänslig verksamhet genom påverkan på liv, hälsa och infrastruktur från skadegenererande verksamhet.
4	Allvarlig skada på Sveriges försvarsförmåga eller politiska självständighet.	Allvarlig skada på det demokratiska statsskicket, rättsväsendet eller den brottsbekämpande förmågan på nationell nivå.	Allvarlig skada på nationellt samhällsviktig verksamhet i form av avbrott eller påverkan på leveranser, tjänster och funktioner.	Allvarlig skada på Sveriges betalningsförmåga i form av påverkan på förmågan att hantera, administrera, granska, styra och stödja nationell finansiell stabilitet.	Allvarlig skada på annan säkerhetskänslig verksamhet genom påverkan på liv, hälsa och infrastruktur från skadegenererande verksamhet.
3	Inte obetydlig skada på Sveriges försvarsförmåga eller politiska självständighet.	Inte obetydlig skada på det demokratiska statsskicket, rättsväsendet eller den brottsbekämpande förmågan på nationell nivå.	Inte obetydlig skada på nationellt samhällsviktig verksamhet i form av avbrott eller påverkan på leveranser, tjänster och funktioner.	Inte obetydlig skada på Sveriges betalningsförmåga i form av påverkan på förmågan att hantera, administrera, granska, styra och stödja nationell finansiell stabilitet.	Inte obetydlig skada på annan säkerhetskänslig verksamhet genom påverkan på liv, hälsa och infrastruktur från skadegenererande verksamhet.
2	Ringa skada på Sveriges försvarsförmåga eller politiska självständighet.	Ringa skada på det demokratiska statsskicket, rättsväsendet eller den brottsbekämpande förmågan på nationell nivå.	Ringa skada på nationellt samhällsviktig verksamhet i form av avbrott eller påverkan på leveranser, tjänster och funktioner.	Ringa skada på Sveriges betalningsförmåga i form av påverkan på förmågan att hantera, administrera, granska, styra och stödja nationell finansiell stabilitet.	Ringa skada på annan säkerhetskänslig verksamhet genom påverkan på liv, hälsa och infrastruktur från skadegenererande verksamhet.
1	Inte mätbart eller inte av relevans				

Elanders Sverige AB, 2019