Vägledning i säkerhetsskydd

Säkerhetsskyddsanalys

Juni 2019

Produktion: Säkerhetspolisen, juni 2019
Grafisk formgivning: Säkerhetspolisen
Typografi: Eurostile och Swift

Innehåll

1 Introduktion

Denna vägledning riktar sig till verksamhetsutövare (enskilda verksamhetsutövare, statliga myndigheter, regioner och kommuner) som avser att ta fram eller uppdatera en säkerhetsskyddsanalys. Fokus i vägledningen är att ta fram en säkerhetsskyddsanalys, dock kan modellen även användas som stöd för att genomföra en särskild säkerhetsskyddsbedömning.

Vägledningen är utformad för att beskriva såväl modellen som de olika delarna i framtagandet av en säkerhetsskyddsanalys. Modellen är inte tvingande utan andra modeller kan användas för att uppfylla de krav som finns i lag, förordning och föreskrifter.

Vissa förkunskaper kan komma att krävas för att fullt ut kunna ta till sig innehållet i vägledningen. Läsaren rekommenderas att ha tagit del av Säkerhetspolisens föreskrifter om säkerhetsskydd och vägledningen Introduktion till säkerhetsskydd innan denna vägledning läses.

Tips! I vägledningen finns ett antal rutor med tips som är viktiga att komma ihåg vid arbete med säkerhetsskyddsanalysen.

2 Vad är säkerhetsskydds-analys?

1 kap. 1–2 §§ och 2 kap. 1 § säkerhetsskyddslagen (2018:585)
2 kap. 1§ säkerhetsskyddsförordningen (2018:658)

En säkerhetsskyddsanalys är en grundläggande och viktig del i ett strukturerat och systematiskt säkerhetsskyddsarbete och en förutsättning för att kunna vidta effektiva säkerhetsskyddsåtgärder. Säkerhetsskyddsanalysen ska ge svar på:

- Vad ska skyddas?
- Mot vad ska det skyddas?
- Hur ska det skyddas?

Antagonistiska hot som spionerі, sabotage och terroristbrott samt andra brott som kan hota verksamheten och skada Sveriges säkerhet ska beaktas i säkerhetsskyddsanalysen.

I säkerhetsskyddsanalysen identifieras och bedöms skyddsvärden utifrån ett konsekvensperspektiv, det vill säga utifrån hur allvarlig konsekvensen av en eventuell skada blir, istället för att fokusera på sannolikheten för att ett säkerhetshot realiseras.

Tips! För mer information om begrepp och definitioner inom säkerhetsskydd, se vägledningen Introduktion till säkerhetsskydd.

3 Vem ska göra en säkerhetsskyddsanalys?

2 kap. 1 § säkerhetsskyddslagen (2018:585)

Den som bedriver säkerhetskänslig verksamhet är skyldig att utreda behovet av säkerhetsskydd. Detta görs genom en säkerhetsskyddsanalys. Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter. För vissa verksamhetsutövare, särskilt inom den privata sektorn, kan det vara svårt att avgöra om de bedriver säkerhetskänslig verksamhet eller inte. I sådana fall kan säkerhetsskyddsanalysen även användas som ett verktyg för att bedöma om så är fallet.

En leverantör som endast deltar i annans säkerhetskänsliga verksamhet med stöd av ett säkerhetsskyddsavtal bör som utgångspunkt inte anses bedriva säkerhetskänsliga verksamhet och behöver därför inte heller göra en säkerhetsskyddsanalys. Om leverantören däremot deltar i säkerhetskänslig verksamhet hos flera andra verksamhetsutövare kan det samlade uppdraget göra att leverantören får anses bedriva säkerhetskänslig verksamhet. Leverantören är då skyldig att göra en säkerhetsskyddsanalys för att bedöma behovet av ytterligare säkerhetsskydd i den egna verksamheten än vad som följer av avtalen. Se mer i vägledningen Säkerhetsskyddad upphandling.

4 Vägen fram till en säkerhetsskyddsanalys

Figur 1: Säkerhetspolisens modell för att ta fram en säkerhetsskyddsanalys.

Säkerhetspolisens modell för att ta fram en säkerhetsskyddsanalys är indelad i fem delar, se figur 1 ovan. Respektive del kommer att beskrivas mer i detalj i nästa kapitel. Efter varje del finns även en lista med förslag på aktiviteter.

Det praktiska genomförandet av en säkerhetsskyddsanalys är inte alltid så sekventiellt som modellen visar, därför kan vissa delar sammanfalla eller behöva göras flera gånger. I Säkerhetspolisens modell bedöms säkerhetshot före sårbarheter men bedömningarna behöver inte nödvändigtvis genomföras i den ordningen. Det viktiga är att alla delar i modellen genomförs och att arbetet dokumenteras så att det finns spårbarhet.

En generell bedömning av nödvändiga säkerhetsskyddsåtgärder redovisas i säkerhetsskyddsanalysen för att sedan utformas mer detaljerat i en separat säkerhetsskyddsplan.

Olika funktioner eller kompetenser kommer att behöva delta i olika delar av säkerhetsskyddsanalysen. Exempelvis kan en representant från kärnverksamheten behöva delta vid sårbarhetsbedömningen och en representant från säkerhetsorganisationen vid bedömningen av vilka säkerhetsskyddsåtgärder som ska vidtas. En bedömning behöver även göras om de som kommer att delta i arbetet med de olika delarna av säkerhetsskyddsanalysen behöver vara säkerhetsprövade och om de har relevant utbildning i säkerhetsskydd.

En verksamhetsutövare kan vara beroende av en annan verksamhetsutövare för att kunna genomföra sin verksamhet. Samverkan med interna och externa aktörer är därför viktigt för att avgöra om någonting är skyddsvärt och hur det ska skyddas.

Säkerhetsskyddsanalysen kan vara skyddsvärd i sig, delvis eller i sin helhet, och kan komma att innehålla säkerhetsskyddsklassificerade uppgifter. Detta påverkar såväl det praktiska arbetet och hantering av dokumentation samt vilka som kan engageras i arbetet. Exempelvis kan sårbarhetsbedömningen innehålla uppgifter som är indelade i en högre säkerhetsskyddsklass jämfört med de andra delarna av säkerhetsskyddsanalysen, vilket påverkar hur den kan tas fram och av vem.

Säkerhetspolisens modell för att ta fram en säkerhetsskyddsanalys kan även användas

för att ta fram en särskild säkerhetsskyddsbedömning. För närmare beskrivning av om och när en särskild säkerhetsskyddsbedömning ska genomföras se vägledningen Introduktion till säkerhetsskydd.

Tips! Efter varje del i processen finns en lista med förslag på aktiviteter. Listan är inte uttömmande utan även andra aktiviteter kan vara nödvändiga att genomföra.

5 Verksamhetsbeskrivning

Syftet med verksamhetsbeskrivningen är att beskriva och urskilja vad i verksamheten som utgör säkerhetskänslig verksamhet och som därmed ska ges ett säkerhetsskydd. Verksamhetsutövaren bör inleda med att övergripande beskriva hela verksamheten samt dess mål och syfte.

För att identifiera säkerhetskänslig verksamhet är det bra att utgå från den övergripande beskrivningen av verksamheten och verksamhetsutövarens instruktion eller motsvarande styrdokument. Utifrån detta bör verksamhetsutövaren besvara om det till någon del bedrivs verksamhet som:

- hanterar säkerhetsskyddsklassificerade uppgifter,
- omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd, eller
- är av betydelse för Sveriges säkerhet.

De verksamheter som är av betydelse för Sveriges säkerhet ryms alla inom en eller flera av följande kategorier (utvecklas mer i avsnitt *6.3.1 Konsekvenskategorier*):

- Sveriges yttre säkerhet
- Sveriges inre säkerhet
- nationellt samhällsviktig verksamhet
- Sveriges ekonomi
- skadegenererande verksamhet

Om svaret på någon av de ovanstående frågorna är ja bedrivs säkerhetskänslig verksamhet. Om det vid verksamhetsbeskrivningen råder ovisshet om en viss del av verksamheten är säkerhetskänslig eller inte bör den delen av verksamheten inkluderas i den fortsatta säkerhetsskyddsanalysen. Beskriv även varför en verksamhet bedöms utgöra säkerhetskänslig verksamhet.

För den säkerhetskänsliga verksamheten bör det även undersökas om det finns direkta eller uppenbart indirekta beroenden till andra verksamheter, både internt och externt.

I kapitel 6 *Identifiera och bedöma skyddsvärden* görs en mer detaljerad genomgång av den säkerhetskänsliga verksamheten. Där identifieras och bedöms även specifika skyddsvärden.

5.1 Förslag på aktiviteter

- ☐ Beskriv övergripande verksamheten samt dess mål och syfte.
- ☐ Identifiera säkerhetskänslig verksamheten med utgångspunkt i den övergripande beskrivningen av verksamheten, och utifrån verksamhetsutövarens instruktion eller motsvarande styrdokument. Besvara frågorna om det till någon del bedrivs verksamhet som:
  - ○ hanterar säkerhetsskyddsklassificerad uppgift,
  - ○ omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd eller
  - ○ är av betydelse för Sveriges säkerhet.
- ☐ Beskriv varför en verksamhet bedöms som säkerhetskänslig.
- ☐ Identifiera om det hos den säkerhetskänsliga verksamheten finns direkta eller uppenbart indirekta beroenden till andra verksamheter, både internt och externt.

6 Identifiera och bedöma skyddsvärden

2 kap. 1§ Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

En säkerhetskänslig verksamhet innehåller ett eller flera skyddsvärden. Syftet med denna del av säkerhetsskyddsanalysen är att med utgångspunkt i verksamhetsbeskrivningen identifiera och bedöma specifika skyddsvärden samt att bedöma från vilket eller vilka perspektiv den säkerhetskänsliga verksamheten är skyddsvärd.

Följande tre kategorier av skyddsvärden ska identifieras och bedömas (förklaras närmare i kapitel 6.1 – 6.3):

- säkerhetsskyddsklassificerade uppgifter
- verksamheter eller uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd
- säkerhetskänslig verksamhet i övrigt

Uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd utgör säkerhetsskyddsklassificerade uppgifter och ryms därför per definition även inom den första kategorin skyddsvärden. På samma sätt kan ett informationssystem som identifieras inom den sista kategorin skyddsvärden även innehålla säkerhetsskyddsklassificerade uppgifter. Uppdelningen i kategorierna syftar framförallt till att säkerställa att samtliga skyddsvärden omhändertas. Skyddsvärden som ryms inom den sista kategorin ska dock bedömas enligt en särskild modell, se kapitel *6.3 Säkerhetskänslig verksamhet i övrigt.*

Verksamhetsutövaren ska bedöma ur vilket eller vilka perspektiv (konfidentialitet, tillgänglighet och riktighet) den identifierade säkerhetskänsliga verksamheten är skyddsvärd. Bedömningen görs lämpligen i samband med identifieringen av skyddsvärden.

De olika perspektiven beskrivs närmare i kapitel *6.4 Perspektiven konfidentialitet, tillgänglighet och riktighet.*

6.1 Säkerhetsskyddsklassificerade uppgifter

2 kap. 5 § säkerhetsskyddslagen (2018:585)
2 kap. 1 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

Säkerhetsskyddsklassificerade uppgifter som finns i verksamheten ska löpande delas in i någon av de fyra säkerhetsskyddsklasserna:

1. *Kvalificerat hemlig* (synnerligen allvarlig skada)
2. *Hemlig* (allvarlig skada)
3. *Konfidentiell* (en inte obetydlig skada)
4. *Begränsat hemlig* (endast ringa skada)

Indelningen av uppgifter i säkerhetsskyddsklass är alltså inte ett moment i säkerhetsskyddsanalysen. Om det under genomförandet av säkerhetsskyddsanalysen upptäcks säkerhetsskyddsklassificerade uppgifter som inte har delats in i säkerhetsskyddsklass ska det dock självklart göras.

Ett vanligt förekommande fall är att en verksamhet hanterar information som säkerhetsskyddsklassificerats av en annan verksamhetsutövare som bedriver säkerhetskänslig verksamhet. Det kan exempelvis vara en kommun som av Försvarsmakten blir delgiven uppgifter om totalförsvaret. I sådana fall kommer också den organisatoriska delen av kommunen som hanterar den typen av informationen att bedriva säkerhetskänslig verksamhet.

Att identifiera varje enskild uppgift inom ramen för en säkerhetsskyddsanalys kan vara omfattande. Därför kan det i vissa fall finnas ett behov av att göra bedömningen på en mer övergripande nivå, till exempel utifrån huvudtyper eller kluster av informationsmängder.

I det fall flera uppgifter hanteras i ett system ska en bedömning göras om den totala mängden uppgifter som hanteras i systemet medför ett högre skyddsvärde. I den bedömningen är det främst de två aspekterna aggregerade uppgifter och ackumulerade uppgifter som bör beaktas.

För ytterligare stöd med att säkerhetsskyddsklassificera uppgifter och bedöma aggregerade eller ackumulerade uppgifter, se vägledning om Informationssäkerhet.

Tänk på! Om en eller flera säkerhetsskyddsklassificerade uppgifter identifieras anses verksamhetsutövaren bedriva säkerhetskänslig verksamhet och omfattas då av säkerhetsskyddslagen.

6.2 Verksamheter eller uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd

2 kap. 5 § säkerhetsskyddslagen (2018:585)
2 kap. 1 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

De för Sverige förpliktande internationella åtagandena om säkerhetsskydd handlar framförallt om skydd av säkerhetsskyddsklassificerade uppgifter. Sverige har ingått ett antal internationella överenskommelser om säkerhetsskydd, såväl bilaterala som multilaterala, med andra stater och mellanfolkliga organisationer som exempelvis EU och Nato.

Uppgifter som redan klassificerats av en annan stat eller en mellanfolklig organisation ska inte klassificeras på nytt. Varje internationellt åtagande om säkerhetsskydd innehåller bestämmelser där de nationella säkerhetsskyddsklasserna framgår. Enligt åtagandet är det endast dessa benämningar som får användas av avtalsparterna. Dessa benämningar varierar mellan olika länder beroende på den nationella lagstiftningen. Det finns inte en enhetlig internationell nomenklatur för de olika säkerhetsskyddsnivåerna.

Som exempel kan nämnas EU:s olika säkerhetsskyddsnivåer (motsvarande svenska inom parentes):

- TRÈS SECRET UE / EU TOP SECRET (kvalificerat hemlig)
- SECRET UE / EU SECRET (hemlig)
- CONFIDENTIEL UE / EU CONFIDENTIAL (konfidentiell)
- RESTREINT UE / EU RESTRICTED (begränsat hemlig)

Om uppgifterna inte har tilldelats en säkerhetsskyddsklass ska de klassificeras utifrån den skada som ett röjande kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation.

Tänk på! Om en eller flera verksamheter eller uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd har identifieras anses verksamhetsutövaren bedriva säkerhetskänslig verksamhet och omfattas då av säkerhetsskyddslagen.

6.3 Säkerhetskänslig verksamhet i övrigt

2 kap. 13 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

Säkerhetskänslig verksamhet i övrigt är verksamhet som är av betydelse för Sveriges säkerhet av annan anledning än att den innehåller säkerhetsskyddsklassificerade uppgifter eller omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Med verksamhet avses här anläggningar, objekt, system eller liknande verksamhet. Det kan exempelvis röra en anläggning som är av betydelse för Sveriges försvarsförmåga eller ett informationssystem som är av betydelse för Sveriges säkerhet oavsett om det däri hanteras säkerhetsskyddsklassificerade uppgifter eller inte.

Med utgångspunkt i verksamhetsbeskrivningen ska anläggningar, objekt, system eller liknande, identifieras och bedömas. Identifiering och bedömning görs utifrån konsekvenskategorier och konsekvensnivåer.

6.3.1 Konsekvenskategorier

2 kap. 2 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

Identifieringen av säkerhetskänslig verksamhet i övrigt görs utifrån vilken typ av skada för Sveriges säkerhet en antagonistisk handling mot en anläggning, ett objekt, ett system eller liknande skulle medföra. Konsekvenskategorierna är följande:

- skada för Sveriges yttre säkerhet
- skada för Sveriges inre säkerhet
- skada på nationell samhällsviktig verksamhet
- skada för Sveriges ekonomi
- skadegenererande verksamhet

De fem konsekvenskategorierna beskrivs mer i detalj nedan. Respektive del inleds med den kategoribeskrivning som återfinns i bilagan till Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd. Observera att en verksamhet som är säkerhetskänslig i övrigt eller delar av denna kan omfattas av *flera* av dessa kategorier.

Skada för Sveriges yttre säkerhet

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

En viktig beståndsdel är den nationella försvarsförmågan av Sveriges territorium, där Försvarsmakten har huvudansvaret. I den uppgiften ligger att kunna försvara Sverige, upptäcka och avvisa kränkningar av det svenska territoriet samt värna om Sveriges suveräna rättigheter och nationella intressen inom Försvarsmaktens verksamhetsområde. Utöver Försvarsmakten finns andra verksamheter som är viktiga för det militära försvarets förmåga att utföra sitt uppdrag, såsom det civila försvaret inklusive planeringsarbetet och försvarsindustrier.

Sveriges oberoende och handlingsfrihet handlar om att kunna upprätthålla förmågan att förebygga och avvärja brott mot Sveriges säkerhet, en uppgift som Säkerhetspolisen har huvudansvaret för. Försvarsmakten har ett delansvar vad avser att identifiera sådana brottsliga kopplingar mot Sverige i utlandet, samt att identifiera spioneri och olovlig underrättelseverksamhet riktad mot Försvarsmakten och dess skyddsvärden.

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.

Denna kategori avser påverkan på förmågan att upprätthålla och säkerställa Sveriges statsidé avseende funktion, handlingsfrihet och oberoende.

Säkerhetsskyddet för Sveriges inre säkerhet handlar till stor del om att skydda kritiska anläggningar, funktioner och informationssystem som rör Sveriges demokratiska statsskick, rättsväsende eller brottsbekämpande förmåga.

Skada på nationellt samhällsviktig verksamhet

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

Verksamheter som definieras som nationellt samhällsviktiga ur ett säkerhetsskyddsperspektiv återfinns främst inom sektorerna energiförsörjning, elektroniska kommunikationer, finansiella tjänster (centrala betalningssystem), livsmedelsförsörjning, vattenförsörjning och transporter. Avgörande för om sådan verksamhet kan anses ha bäring på Sveriges säkerhet är om en antagonistisk handling (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra direkta eller uppenbara indirekta skadekonsekvenser på nationell nivå.

Exempel på sådana verksamheter kan vara:

- Anläggningar, system och funktioner som genom sitt läge eller sin funktion i stamnätet har en viktig roll för upprätthållandet av det nationella elsystemet. Dessa återfinns till exempel hos elproducenter och eldistributörer.
- Anläggningar, system och funktioner som genom sitt läge eller funktion i infrastrukturen för elektronisk kommunikation har en viktig roll för upprätthållandet av kommunikationen. Dessa återfinns till exempel hos teleoperatörer och internetleverantörer.
- De centrala system som genom sitt läge eller sin funktion i infrastrukturen kopplat till det centrala betalningssystemet har en viktig roll för upprätthållandet av betalningsflödena.

Skada för Sveriges ekonomi

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

Här avses endast konsekvenser av antagonistisk handling som har en direkt eller uppenbar indirekt påverkan på Sveriges betalningsförmåga. Vidare avses förmågan att hantera, administrera, granska, styra och stödja den nationella finansiella stabiliteten.

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.

Exempel på skadegenererande verksamheter kan vara kärntekniska verksamheter, större dammar och kemitekniska industrier.

6.3.2 Konsekvensnivåer

2 kap. 3 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

Säkerhetskänslig verksamhet som identifierats tillhöra en eller flera konsekvenskategorier enligt ovan ska graderas i olika konsekvensnivåer beroende på hur allvarlig skada en antagonistisk handling skulle kunna medföra. Till skillnad från konsekvenskategori kan dock en säkerhetskänslig verksamhet som helhet bara tillhöra en konsekvensnivå. Om verksamheten återfinns i flera konsekvenskategorier väljs den konsekvens-

nivå där en potentiell skada för Sveriges säkerhet är som mest allvarlig. Indelningen sker enligt följande:

- Nivå 5: Synnerlig 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

De fem konsekvensnivåerna beskrivs mer i detalj nedan. Samma beskrivning återfinns i bilagan till Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).

Nivå 5 Synnerlig 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. Verksamheter eller uppgifter bedömda på denna nivå bedriver inte säkerhetskänslig verksamhet.

6.3.3 Matris med konsekvenskategorier och konsekvensnivåer

För att få en bättre överblick över vilka konsekvenskategorier och konsekvensnivåer de olika skyddsvärdena befinner sig i kan de placeras ut i en matris, se nedan. Matrisen, som återfinns i bilagan till Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd, kan även användas som ett stöd vid identifiering och bedömning av skyddsvärden i konsekvenskategorier och konsekvensnivåer.

Tänk på! Om en eller flera anläggningar, objekt, system eller liknande identifierats där en antagonistisk handling skulle medföra skada för Sveriges säkerhet anses verksamhetsutövaren bedriva säkerhetskänslig verksamhet och omfattas då av säkerhetsskyddslagen.

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				

Figur 2: Matris med konsekvenskategorier och konsekvensnivåer.

6.4 Perspektiven konfidentialitet, tillgänglighet och riktighet

2 kap. 4 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

Verksamhetsutövaren ska bedöma från vilket eller vilka perspektiv (konfidentialitet, tillgänglighet och riktighet) den identifierade säkerhetskänsliga verksamheten är skyddsvärd. Bedömningen görs lämpligen i samband med identifieringen av skyddsvärden.

Säkerhetsskyddsklassificerade uppgifter (inklusive sådana uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd) är framförallt skyddsvärda utifrån perspektivet konfidentialitet, men kan även vara skyddsvärda utifrån perspektiven tillgänglighet och riktighet. Säkerhetskänsliga verksamheter i övrigt är däremot framförallt skyddsvärda utifrån perspektiven tillgänglighet och riktighet, men kan även i enstaka fall vara skyddsvärda utifrån konfidentialitet.

För ytterligare stöd i hur man kan bedöma de olika perspektiven när det gäller information, se vägledningen Informationssäkerhet.

6.4.1 Konfidentialitet

Med konfidentialitet menas att uppgifter eller verksamheter är skyddsvärda utifrån att ett röjande kan medföra skada för Sveriges säkerhet.

Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklass utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Detta är en bedömning utifrån uppgifternas konfidentialitet.

Även när det gäller säkerhetsskyddsklassificerade uppgifter som omfattas av ett för Sverige förpliktande internationella åtaganden om säkerhetsskydd avser åtagandet främst skydd utifrån konfidentialitet, det vill säga mot att de röjs till någon obehörig.

Det är främst uppgifter som är skyddsvärda utifrån perspektivet konfientialiet men det kan även i enstaka fall vara verksamheter.

Exempel: En verksamhetsutövare med en roll inom totalförsvaret anordnar övningar i syfte att testa om de uppgifter som verksamheten ålagts går att genomföra i praktiken. Planeringen och rutinerna som övas samt utvärderingarna av resultaten utgör säkerhetsskyddsklassificerade uppgifter och är skyddsvärda ur perspektivet konfidentialitet. Men, genom att observera övningen går det att uttyda motsvarande uppgifter om verksamhetsutövarens resurser, kapacitet, förfaranden och eventuella brister. Verksamhetsutövaren bedömer att även övningarna är skyddsvärda ur perspektivet konfidentialitet och vidtar åtgärder för att förhindra insyn.

6.4.2 Tillgänglighet

Med tillgänglighet menas att uppgifter eller verksamheter är skyddsvärda utifrån att de är tillgängliga när de behövs.

I bedömningen ska det beaktas vilken skada som kan uppstå för Sveriges säkerhet om förväntad tillgänglighet inte uppfylls. Även tidsaspekten behöver beaktas, det vill säga om det är efter en kort eller lång tidsperiod som bristfällig tillgänglighet kan medföra skada för Sveriges säkerhet. För att säkerställa att rätt nivå på tillgänglighet uppnås kan verksamhetsutövaren behöva vidta vissa åtgärder.

Exempel: En säkerhetskänslig verksamhet har en driftcentral som är i drift dygnet runt men ibland stängs ner för systemunderhåll i maximalt en timme. Ett strömavbrott till driftcentralen bedöms kunna vara flera timmar vilket då skulle medföra skada för Sveriges säkerhet. Verksamhetsutövaren

bedömer att med avseende på tidsaspekten behövs ett reservkraftverk men att helt avbrottsfri kraftförsörjning med batterier inte är nödvändigt.

6.4.3 Riktighet

Med riktighet menas att uppgifter eller verksamheter är skyddsvärda utifrån att de inte får ändras av obehöriga.

I bedömningen ska det beaktas vilken skada som kan uppstå för Sveriges säkerhet om förväntad riktighet inte uppfylls. För att säkerställa att riktighet uppnås kan verksamhetsutövaren behöva vidta vissa åtgärder.

Exempel: En verksamhetsutövare med ansvar för ledning av nationella insatser har ett informationssystem som med GPS automatiskt positionerar resurser. Ifall uppgifter om var resurser befinner sig obemärkt manipuleras kommer insatsen att ledas ineffektivt med skada för Sveriges säkerhet som följd. Verksamhetsutövaren väljer att kryptera datakommunikationen så det framgår ifall uppgifterna ändrats och kan om så sker gå över till manuell positionering.

6.5 Särskilt säkerhetskänslig verksamhet

2 kap. 6 och 8 §§ Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

Verksamhet som bedöms tillhöra konsekvensnivå 4 och 5, synnerligen allvarlig skada respektive allvarlig skada för Sveriges säkerhet, benämns som särskilt säkerhetskänslig. Verksamhetsutövaren är då skyldig att:

- rapportera till tillsynsmyndigheten att sådan verksamhet bedrivs, och
- dimensionera säkerhetsskyddsåtgärderna utifrån den dimensionerande hotbeskrivningen (DHB).

Syftet med rapporteringen är att tillsynsmyndigheterna ska kunna ha en samlad bild över vilka verksamhetsutövare som finns inom respektive ansvarsområde så att såväl tillsyn som rådgivning kan prioriteras för de verksamheter som är av störst betydelse för Sveriges säkerhet.

Säkerhetspolisen upprättar efter samråd med tillsynsmyndigheterna en DHB till de verksamhetsutövare som bedriver särskilt säkerhetskänslig verksamhet. För ytterligare beskrivning av DHB se kapitel *7.2 Dimensionerande hotbeskrivning (DHB)*.

6.6 Förslag på aktiviteter

Skyddsvärden – säkerhetsskyddsklassificerade uppgifter

- ☐ Identifiera förekomsten av säkerhetsskyddsklassificerade uppgifter.
- ☐ Om det upptäcks säkerhetsskyddsklassificerade uppgifter som inte har delats in i säkerhetsskyddsklass så ska det ske. Bedöm vilken skada ett röjande kan medföra för Sveriges säkerhet.

Skyddsvärden – verksamheter eller uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd

- ☐ Identifiera uppgifter som klassificerats av en annan stat eller mellanfolklig organisation och som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.
- ☐ Identifiera om det finns uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd men som inte har delats in i säkerhetsskyddsklass. Bedöm vilken skada ett röjande kan medföra för Sveriges förhållande till den andra staten eller mellanfolkliga organisationen.

- ☐ Identifiera om det finns verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd på annan grund än att det behandlas uppgifter i verksamheten.

Skyddsvärden – säkerhetskänslig verksamhet i övrigt

- ☐ Identifiera skyddsvärden i säkerhetskänslig verksamhet i övrigt utifrån konsekvenskategorier (ett skyddsvärde kan tillhöra en eller flera konsekvenskategorier).
- ☐ Bedöm konsekvensnivå för de skyddsvärden som identifierats i den säkerhetskänsliga verksamheten i övrigt (ett skyddsvärde kan endast tillhöra en konsekvensnivå).
- ☐ Utifrån konsekvenskategori och konsekvensnivå, placera ut respektive skyddsvärde som identifierats som övrig säkerhetskänslig verksamhet i den matris som återfinns i kapitel *6.3.3 Matris med konsekvenskategorier och konsekvensnivåer.*

Perspektiv – konfidentialitet, tillgänglighet och riktighet

- ☐ Bedöm utifrån vilket eller vilka perspektiv de säkerhetsskyddsklassificerade uppgifterna är skyddsvärda.
- ☐ Bedöm utifrån vilket eller vilka perspektiv de verksamheter eller uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd är skyddsvärda.
- ☐ Bedöm utifrån vilket eller vilka perspektiv den säkerhetskänsliga verksamheten i övrigt är skyddsvärd.

Särskilt säkerhetskänslig verksamhet i övrigt (gäller endast konsekvensnivå 4 och 5)

- ☐ Rapportera till tillsynsmyndigheten att särskilt säkerhetskänslig verksamhet bedrivs.

7 Säkerhetshot

2 kap. 1 § säkerhetsskyddsförordningen (2018:658)
2 kap. 7–8 §§ Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

En viktig del i säkerhetsskyddsanalysen är att identifiera vad den säkerhetskänsliga verksamheten ska skyddas mot. För att besvara frågan ska verksamhetsutövaren utifrån Säkerhetspolisens hotbild och egna identifierade hot bedöma hur hotet kan påverka den säkerhetskänsliga verksamheten och om det finns behov av att vidta säkerhetsskyddsåtgärder.

För särskilt säkerhetskänslig verksamhet (konsekvensnivå 4 och 5) ska verksamhetsutövaren dimensionera säkerhetsskyddsåtgärderna utifrån en dimensionerande hotbeskrivning (DHB) som tillhandahålls av Säkerhetspolisen. För de verksamheter som graderas inom konsekvensnivå 2 och 3 kommer Säkerhetspolisen inte att upprätta en DHB. Det finns då heller inget krav på att dimensionera säkerhetsskyddsåtgärderna efter en sådan.

7.1 Hotbild

2 kap. 7 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

Säkerhetshot uppstår då en aktör har både avsikt och förmåga att genomföra skadliga handlingar riktade mot den säkerhetskänsliga verksamheten. Eftersom en aktörs avsikt kan förändras snabbt är en hotbild kortsiktig och behöver uppdateras löpande. Ett exempel på en förändring i avsikt skulle kunna vara att verksamhetsutövaren får information om att en statlig aktör som tidigare inte varit intresserad av den säkerhetskänsliga verksamheten nu har börjat visa intresse. Det bör då utredas ifall förändringen medför ett behov av kompensatoriska säkerhetsskyddsåtgärder, det vill säga säkerhetskyddsåtgärder som behöver vidtas utöver ordinarie skydd eller för att täcka upp tillfälliga brister i det ordinarie säkerhetsskyddet.

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

Säkerhetspolisens hotbilder är generella och beskriver på kort till medellång sikt, upp till två år framåt, hotaktörers avsikt och förmåga att fullfölja ett agerande. Med utgångspunkt i hotbilden kan verksamhetsutövaren bedöma vilka hot som är relevanta för verksamheten samt komplettera hotbilden med till exempel egna incidenter, information från öppna källor eller från samverkan med liknande verksamheter.

Tips! Besök Säkerhetspolisens webbplats för mer information om Säkerhetspolisens hotbild.

7.2 Dimensionerande hotbeskrivning (DHB)

2 kap. 8 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

Med DHB avses en beskrivning av en antagen antagonistisk förmåga som säkerhetsskyddsåtgärderna förväntas kunna skydda mot, även om inte det föreligger något identifierat hot mot den säkerhetskänsliga

verksamheten. DHB:n är ett underlag som används för att långsiktigt dimensionera säkerhetsskyddsåtgärder.

Verksamhetsutövaren bör bryta ned de förmågor som beskrivs i DHB:n till konkreta åtgärder, i syfte att verifiera om befintligt säkerhetsskydd skyddar mot dessa förmågor. Ett exempel skulle kunna vara att förmågan att avlyssna ett rum på distans beskrivs i DHB:n, vilket medför att en verksamhets säkerhetsskyddsåtgärder för avlyssning kan behöva förbättras.

7.3 Förslag på aktiviteter

Hotbild

- ☐ Förslag på källor:
  - ○ Säkerhetspolisens hotbild
  - ○ egna incidenter
  - ○ öppna källor (exempelvis öppen information från Försvarsmakten, FRA, MSB, FOI och ämnesspecifika tidskrifter och rapporter).
  - ○ samverkan med andra liknande verksamheter
  - ○ samverkan lokalt (kommun, länsstyrelse, polis och räddningstjänst)
  - ○ information från respektive tillsynsmyndighet
- ☐ Sammanställ materialet till en samlad hotbild för identifierade skyddsvärden.
- ☐ Utifrån den hotbild som Säkerhetspolisen tillhandahåller, identifiera vilka hot som bedöms relevanta för den egna verksamheten.
- ☐ Undersök om någon annan hotaktör, som inte nämns i Säkerhetspolisens hotbild, genomfört antagonistiska handlingar mot verksamheten eller mot annan jämförbar verksamhet.
- ☐ Undersök om det finns information avseende säkerhetshot mot den egna verksamheten som anses vara relevant ur ett säkerhetsskyddsperspektiv.
- ☐ Utifrån Säkerhetspolisens hotbild samt egen inhämtad information, bedöm hur identifierade säkerhetshot kan påverka den säkerhetskänsliga verksamheten.
- ☐ Givet verksamhetens skyddsvärden och beroenden, bedöm om det finns någon överförd hotbild mot verksamheten.

DHB

- ☐ Om verksamheten bedriver särskilt säkerhetskänslig verksamhet i konsekvensnivå 4 eller 5,
  - ○ efterfråga en DHB från tillsynsmyndigheten
  - ○ dimensionera säkerhetsskyddet utifrån DHB:n

8 Sårbarhetsbedömning

2 kap. 9 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

I denna del ska sårbarheter i den säkerhetskänsliga verksamheten identifieras. Verksamhetsutövaren ska bedöma hur sårbarheterna påverka verksamhetens säkerhetsskydd och om det finns behov av att vidta säkerhetsskyddsåtgärder.

I sårbarhetsbedömningen kan det exempelvis ingå praktiska tester av säkerhetsskyddet, analys av inträffade incidenter och erfarenhetsbaserade bedömningar. Dessa praktiska tester samt andra underlag kan sedan sammanställas och bedömas i syfte att föreslå lämpliga säkerhetsskyddsåtgärder.

Vilka personer som ska delta i sårbarhetsbedömningen bör anpassas utifrån vilken typ av säkerhetskänslig verksamhet som har identifierats. Exempelvis kan personer med kompetens inom internrevision delta för att granska processer och rutiner där skyddsvärden finns, medan extern expertis kan behöva anlitas för penetrationstester och andra praktiska tester av säkerhetsskyddsåtgärder.

8.1 Förslag på aktiviteter

- ☐ Bedöm befintligt underlag i syfte att ta fram en bild över kända sårbarheter. Utnyttja till exempel:
  - ○ befintlig säkerhetsskyddsanalys
  - ○ tidigare revisioner
  - ○ befintlig riskanalys
  - ○ befintlig risk- och sårbarhetsanalys
  - ○ incidentrapporter
  - ○ andra sårbarhetsbedömningar/tester
- ☐ Identifiera sårbarheter för den säkerhetskänsliga verksamheten genom att exempelvis granska processer och rutiner för att undersöka om de efterlevs och om det finns brister som kan medföra en sårbarhet.
- ☐ Identifiera om det finns någon förmåga som säkerhetsskyddet inte skyddar mot. (Utgå ifrån hotet och vilka förmågor säkerhetsskyddet ska klara av att skydda mot.)

9 Säkerhetsskyddsåtgärder

2 kap. 2–4 §§ säkerhetsskyddslagen (2018:585)
2 kap. 1 § säkerhetsskyddsförordningen (2018:658)

I denna del ska verksamhetsutövaren övergripande beskriva vilka säkerhetsskyddsåtgärder som behöver vidtas utifrån skyddsvärde i relation till säkerhetshot och sårbarheter. En mer detaljerad beskrivning innehållande exempelvis prioritering, resurssättning och tidssättning görs i säkerhetskyddsplanen, se kapitel 11 *Säkerhetsskyddsplan*.

Som stöd i beskrivningen av säkerhetskyddsåtgärderna kan verksamhetsutövaren utgå från bestämmelserna i 2 kap. 2–4 §§ säkerhetsskyddslagen. Där beskrivs vad säkerhetsskyddsåtgärderna inom de olika huvudområdena *informationssäkerhet, fysisk säkerhet* och *personalsäkerhet* ska förebygga. Säkerhetspolisens vägledningar inom de olika huvudområdena samt vägledningen Introduktion till säkerhetsskydd ger också ett bra stöd.

Tänk på! Ett väl fungerande säkerhetsskydd är ett system av säkerhetsskyddsåtgärder där de olika åtgärderna samverkar med varandra.

9.1 Förslag på aktiviteter

- ☐ Beskriv övergripande vilka säkerhetsskyddsåtgärder som behöver vidtas inom huvudområdena (se Säkerhetspolisens vägledning Introduktion till säkerhetsskydd samt vägledningarna inom respektive huvudområde):
  - ○ informationssäkerhet
  - ○ fysisk säkerhet
  - ○ personalsäkerhet

10 Sammanställning och fastställande

2 kap. 1 § säkerhetsskyddslagen (2018:585)
2 kap. 10 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

När säkerhetsskyddsanalysens samtliga delar är genomförda ska resultatet skriftligen sammanställas och fastställas av verksamhetsutövarens högsta chef eller motsvarande organ. Det kan vara generaldirektör vid en myndighet, verkställande direktör för en enskild verksamhetsutövare eller kommunchef för en kommun. Beslutet får delegeras. Analysen ska uppdateras vid behov, dock minst en gång vartannat år.

Den fastställda analysen ligger till grund för en säkerhetsskyddsplan där konkreta åtgärder identifieras och resurssätts, se kapitel 11 *Säkerhetsskyddsplan.*

Det kan finnas behov av att förmedla hela eller delar av säkerhetsskyddsanalysen till den egna verksamheten men även externt. Exempelvis behöver viss personal veta vad som är skyddsvärt för att kunna hantera skyddsvärdena på ett korrekt sätt. Det kan även vara till fördel att viss personal känner till hotbilden mot verksamheten för att öka förståelsen för vissa säkerhetsskyddsåtgärder. Samtidigt är det viktigt att betänka att säkerhetsskyddsanalysen kan vara skyddsvärd i sig, delvis eller som helhet. Endast personal som är behörig får ta del av säkerhetsskyddsanalysen då en sådan i princip alltid kommer att innehålla säkerhetsskyddsklassificerade uppgifter.

10.1 Förslag på aktiviteter

- ☐ Sammanställ analysens alla delar, säkerställ att spårbarhet finns mellan alla delar i processen.
- ☐ Säkerhetsskyddsklassificera analysen.
- ☐ Fastställ uppdateringsfrekvens, minst vartannat år.
- ☐ Förankra analysen i ledningsgruppen eller motsvarande.
- ☐ Verksamhetsutövarens högsta chef eller motsvarande fastställer säkerhetsskyddsanalysen.

11 Säkerhetsskyddsplan

2 kap. 11 § Säkerhetspolisen föreskrifter (PMFS 2019:2) om säkerhetsskydd

De säkerhetskyddsåtgärder som övergripande beskrivs i säkerhetsskyddsanalysen, beskrivs i detalj och sammanställs i en plan. 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.

För vägledning kring vilka specifika säkerhetsskyddsåtgärder som är lämpliga att vidta inom respektive huvudområde hänvisas till Säkerhetspolisens vägledningar inom de olika huvudområdena.

11.1 Förslag på aktiviteter

- ☐ Beskriv i detalj vilka säkerhetsskyddsåtgärder som behöver vidtas utifrån skyddsvärde i relation till säkerhetshot och sårbarhet inom huvudområdena:
  - ○ informationssäkerhet
  - ○ fysisk säkerhet
  - ○ personalsäkerhet
- ☐ Prioritera säkerhetsskyddsåtgärder baserat på konsekvensen för Sveriges säkerhet.
- ☐ Utse ansvarig funktion eller person för respektive säkerhetsskyddsåtgärd.
- ☐ Redogör för när respektive säkerhetsskyddsåtgärd ska påbörjas och vara genomförd.
- ☐ Redogör för vilka resurser respektive säkerhetsskyddsåtgärd kommer att kräva med avseende på tid och kostnad.
- ☐ Undersök om det finns beroenden som kan påverka om, när och hur en säkerhetsskyddsåtgärd genomförs, till exempel ombyggnation eller flytt av verksamheten.
- ☐ Fastställ hur ofta säkerhetsskyddsplanen ska uppdateras.
- ☐ Säkerhetsskyddschefen eller den han eller hon bestämmer fastställer säkerhetsskyddsplanen.

Säkerhetspolisen

Säkerhetspolisen • Box 12312 • 102 28 Stockholm
Tel: 010-568 70 00 • Fax: 010-568 70 10
E-post: sakerhetspolisen@sakerhetspolisen.se
www. sakerhetspolisen.se