Vägledning i säkerhetsskydd

Introduktion

Säkerhetspolisen

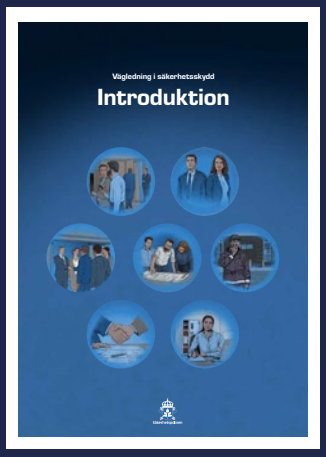
För dig som läser en nedladdad eller utskriven kopia av denna vägledning
Kontrollera att du har den senaste versionen på Säkerhetspolisens webbplats.
Där finns även andra vägledningar inom området säkerhetsskydd.
Version December 2023

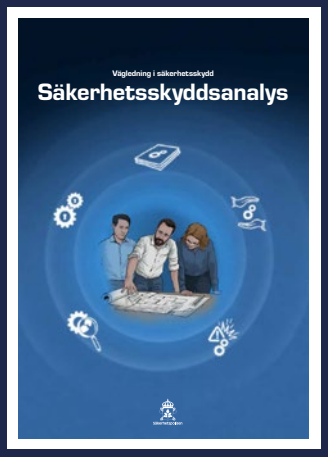
Denna vägledning riktar sig till den som i sitt arbete eller i andra sammanhang kommer i kontakt med säkerhetsskydd.

Vägledningen inleds med översiktliga beskrivningar som följs av fördjupning av centrala begrepp. Läsaren uppmanas att ha läst säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2021:955) och Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd samt kompletterande föreskrifter meddelade av tillsynsmyndigheten om sådana finns. För riksdagen och dess myndigheter finns bestämmelser om säkerhetsskydd i lagen (2019:109) om säkerhetsskydd i riksdagen och dess myndigheter.

Text som skrivs med kursiv stil markerar centrala begrepp. Begreppen utvecklas längre fram i vägledningen och i vissa fall i någon av Säkerhetspolisens andra vägledningar i säkerhetsskydd.

Innehåll





Säkerhetspolisen har tagit fram ett antal vägledningar som kan fungera som ett stöd för verksamhetsutövare i tillämpningen av säkerhetsskyddsregelverket.

1. Introduktion till säkerhetsskydd, 2. Säkerhetsskyddsanalys, 3. Personalsäkerhet, 4. Fysisk säkerhet, 5. Informationssäkerhet, 6. Skyldigheter vid exponering av säkerhetskänslig verksamhet, 7. Besök och utländska delegationer, 8. Avlyssningsskyddade utrymmen

1 Vad är säkerhetsskydd?

I Sverige har vi mycket som är värt att skydda. Vi behöver exempelvis skydda vår yttre säkerhet, demokrati, vårt rättsväsende och dess brottsbekämpande förmåga. Samtidigt är säkerhetshoten komplexa och består bland annat av främmande stater, organisationer och personer som är beredda att använda våld, spionera eller begå andra brott för att orsaka skador på det som är skyddsvärt för Sverige. En antagonist kan orsaka skada för Sveriges säkerhet genom att komma över *säkerhetsskyddsklassificerade uppgifter* eller sabotera och manipulera övrig *säkerhetskänslig verksamhet*.

Säkerhetsskydd är ett system av förebyggande åtgärder för att skydda dessa uppgifter och övrig säkerhetskänslig verksamhet mot antagonistiska handlingar. Säkerhetsskydd innefattar också skydd i andra fall av säkerhetsskyddsklassificerade uppgifter, exempelvis mot att uppgifter röjs som en följd av bristande säkerhetsrutiner.

Säkerhetskänslig verksamhet är sådan verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

Med internationellt åtagande om säkerhetsskydd avses att Sverige förbundit sig att skydda något åt en annan stat eller mellanfolklig organisation, till exempel luftfartsskydd eller uppgifter som utbytts inom militära samarbeten eller samarbeten mot terrorism.

Notera:
Då behoven och förutsättningarna varierar mellan olika verksamhetsutövare finns ingen standardlösning som går att tillämpa på all säkerhetskänslig verksamhet. Detta gör säkerhetsskydd till ett komplext område med många pusselbitar som behöver läggas ihop för att värna Sveriges säkerhet och sådant som Sverige åtagit sig att skydda åt andra stater och mellanfolkliga organisationer.

Grundprincipen inom säkerhetsskydd
Den säkerhetskänsliga verksamheten ska ha samma eller ett likvärdigt skydd oavsett var verksamheten bedrivs eller vem den utförs av. Säkerhetsskyddsavtal är en följd av den principen.

Säkerhetsskydd syftar till att värna Sveriges säkerhet och internationella åtaganden om säkerhetsskydd.

2 Sveriges säkerhet

Uttrycket Sveriges säkerhet saknar definition i lag men förekommer även i annan författning och kan sammanfattas som Sveriges oberoende – i betydelsen självständighet och suveränitet – och bestånd. Detta innefattar okränkta landsgränser, ett bevarande av det svenska självstyret och det demokratiska statsskicket samt samhällets grundläggande funktionalitet.

Såväl myndigheter som enskilda aktörer bedriver samhällsviktig verksamhet som i sin helhet eller delar kan vara av större eller mindre betydelse. Detta brukar illustreras med en pyramid där toppen utgörs av de verksamheterna som är av betydelse för Sveriges säkerhet ur ett nationellt perspektiv. Dessa säkerhetskänsliga verksamheter har ett kvalificerat skyddsbehov och omfattas av säkerhetsskyddslagen.

⊕ *Se figur 1.*

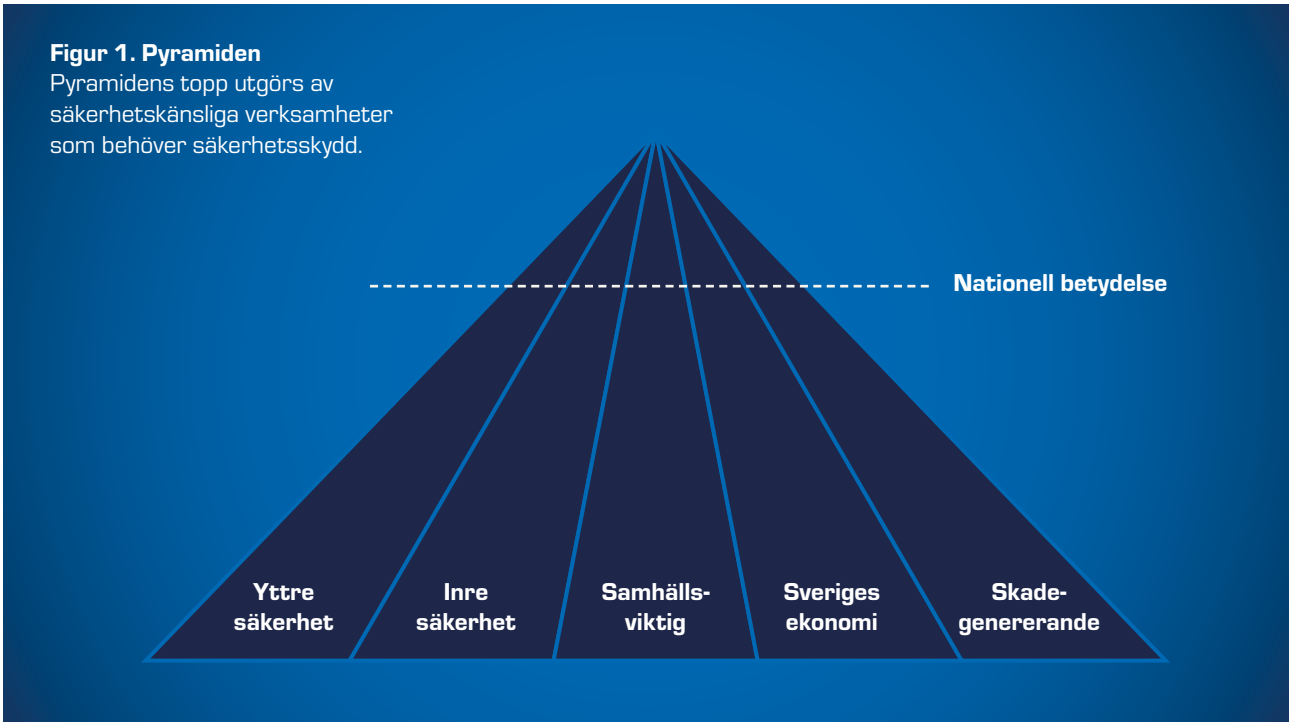
Verksamheter som är nationellt samhällsviktiga ur ett säkerhetsskyddsperspektiv återfinns bland annat inom områdena energiförsörjning, elektroniska kommunikationer, finansiella tjänster och transporter.

⊕ *För närmare beskrivning av samtliga kategorier, se avsnitt 5.1 Kategorisering av säkerhetskänslig verksamhet.*

Notera:
Avgörande för om en samhällsviktig verksamhet kan anses vara av betydelse för Sveriges säkerhet är om en antagonistisk handling mot verksamheten (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra skadekonsekvenser för Sverige säkerhet på nationell nivå. Alla samhällsviktiga verksamheter är således inte säkerhetskänsliga verksamheter.

Vad som är av betydelse för Sveriges säkerhet kan förändras över tid och i takt med att samhället utvecklas. Ett exempel är hur samhällets funktionalitet de senaste åren blivit mer beroende av olika digitaliserade informationssystem och mobiltelefoni. Av denna anledning är det viktigt att verksamhetsutövaren bedriver ett systematiskt säkerhetsskyddsarbete. Detta genom att exempelvis kontinuerligt uppdatera sin säkerhetsskyddsanalys för att identifiera skyddsvärden och nödvändiga säkerhetsskyddsåtgärder samt kontrollera och utvärdera om säkerhetsskyddsåtgärderna ger avsedd effekt.

Figur 1. Pyramiden
Pyramidens topp utgörs av säkerhetskänsliga verksamheter som behöver säkerhetsskydd.



3 Varför behöver säkerhetskänsliga verksamheter ett särskilt skydd?

Säkerhetsskydd behövs för att skydda säkerhetskänsliga verksamheter, främst mot olika typer av antagonistiska handlingar från hotaktörer med varierande *avsikt* och *förmåga*. Det säkerhetspolitiska läget i Sveriges närområde har allvarligt försämrats, vilket har en direkt påverkan på Sverige då de yttre hoten har betydelse för Sveriges säkerhet. Säkerhetshotet från främmande makt är högt, långsiktigt och har även blivit mer komplext. Sverige är ett attraktivt mål när behovet av teknik, information och kunskap hos främmande makt ökar.

Förmågan hos främmande makt kan bestå av såväl stora ekonomiska som personella resurser med tillgång till avancerad teknik och kunskap. Intresset riktas främst mot de myndigheter och enskilda verksamhetsutövare som är av betydelse för Sveriges militära och civila försvar. Sådana verksamheter kan exempelvis finnas inom sektorerna energiförsörjning, elektronisk kommunikation, finansiella tjänster eller i olika typer av internationella samarbeten.

Främmande makt använder olika metoder för underrättelseinhämtning. Några exempel på detta är:

- inhämtning från öppna källor, exempelvis webbplatser, årsredovisningar och rapporter om verksamheters organisation, kris- och krigsberedskap, samt genom att inleda olika typer av samarbeten och delta i upphandlingar
- cyberspionage mot verksamheter i syfte att stjäla uppgifter eller att förbereda sabotage
- signalspaning samt flyg- och satellitspaning
- traditionell personbaserad inhämtning genom rekrytering av uppgiftslämnare och infiltration
- avlyssning av rum och telefoner.

Även sabotage och andra typer av brott såsom till exempel inbrott, förekommer för att testa nivån av säkerhetsskydd och förmågan att hantera störningar samt för att komma över information.

Utöver främmande makt utgör också ideologiskt motiverade grupper och personer ett hot. De kan utföra antagonistiska handlingar riktade mot myndigheter, institutioner och bolag. Avsikten varierar och kan exempelvis vara att, som en del av en ideologisk eller religiös övertygelse, påverka Sveriges inriktning i politiska frågor. Avsikten kan även vara mer specifik såsom att påverka rättssystemet eller myndighetsutövning i enskilda ärenden. Förmågan hos denna typ av hotaktörer varierar och hotet de utgör kan medföra skada för Sveriges säkerhet på både kort och lång sikt. Avgörande för vår motståndskraft är att vi skyddar det mest skyddsvärda.

4 Hur fungerar säkerhetsskydd?

Säkerhetsskydd kan beskrivas som ett system av åtgärder som utifrån vad som identifierats i *säkerhetsskyddsanalysen* tillsammans skyddar den säkerhetskänsliga verksamheten.

Se avsnitt 4.1 Säkerhetskyddsanalys är grunden för säkerhetsskydd och Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys.

Merparten av åtgärderna inom säkerhetsskydd kan sorteras in i någon av de tre säkerhetsskyddsåtgärderna *informationssäkerhet, fysisk säkerhet* och *personalsäkerhet.*

Se avsnitt 7 Säkerhetsskyddsåtgärder och separata vägledningar för varje område för fördjupning.

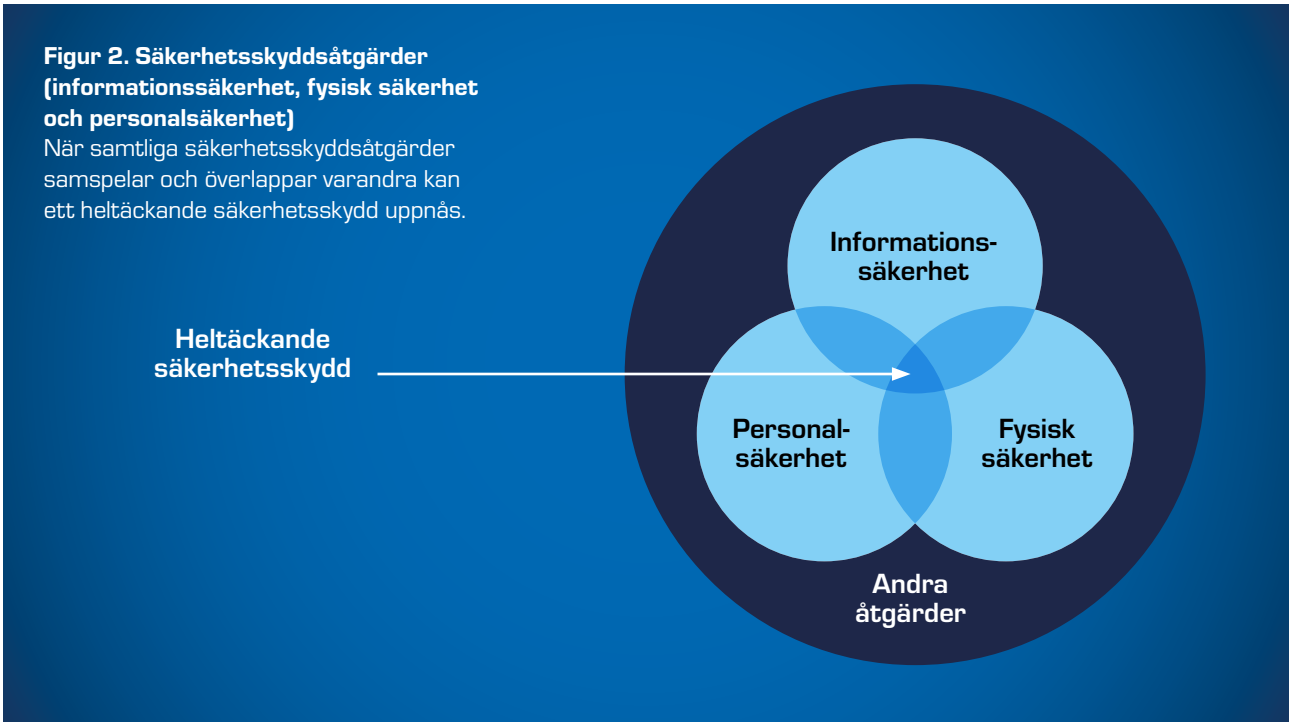
Andra åtgärder är exempelvis hantering av säkerhetshotande händelser och säkerhetsskyddsavtal med aktörer som kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller annan säkerhetskänslig verksamhet.

En grundförutsättning för ett heltäckande säkerhetsskydd är samspelet mellan olika typer av åtgärder som överlappar varandra. Exempelvis räcker det inte att enbart skydda ett informationssystem med informationssäkerhetsåtgärder som hindrar intrång via internet. Det krävs även fysisk säkerhet för att förhindra att obehöriga kommer åt datautrustningen samt personalsäkerhet för att förebygga att personer som inte är pålitliga från säkerhetssynpunkt får arbeta med systemet.

Utöver samspelet måste hela kedjan av åtgärder vara jämnstark och utan svaga länkar. Om exempelvis personal reser med säkerhetsskyddsklassificerade uppgifter mellan verksamhetsutövarens lokaler måste transporten regleras så den inte utgör en *sårbarhet.* I annat fall kan en antagonist utnyttja detta och utföra ett angrepp på en plats där nivån av säkerhetsskydd är lägre än i verksamhetsutövarens lokaler. Säkerhetsskyddsarbetet måste vara en integrerad del i det övriga säkerhetsarbetet och i verksamheten.

Se avsnitt 4.2 Säkerhetsskydd och andra säkerhetsåtgärder.

Figur 2. Säkerhetsskyddsåtgärder (informationssäkerhet, fysisk säkerhet och personalsäkerhet)
När samtliga säkerhetsskyddsåtgärder samspelar och överlappar varandra kan ett heltäckande säkerhetsskydd uppnås.



4.1 Säkerhetskyddsanalys är grunden för säkerhetsskydd

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

§ *2 kap. 1 § säkerhetsskyddsförordningen (2021:955)*

§ *2 kap. 1–11 §§ Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Den som till någon del bedriver säkerhetskänslig verksamhet är skyldig att utreda behovet av säkerhetsskydd. Detta görs genom en säkerhetsskyddsanalys. Säkerhetsskyddsanalysen är grundläggande för ett strukturerat och systematiskt säkerhetsskyddsarbete. Säkerhetsskyddet måste vara heltäckande vilket kan innebära ökade kostnader, minskad effektivitet och ökad administration. Genom att i analysen identifiera skyddsvärden och nödvändiga säkerhetsskyddsåtgärder kan verksamhetsutövaren säkerställa att säkerhetsskyddet läggs på en väl avvägd nivå. Utifrån säkerhetsskyddsanalysen redogörs sedan i en säkerhetsskyddsplan för hur behovet av säkerhetsskyddsåtgärder tas omhand.

För vissa verksamhetsutövare kan det råda osäkerhet om ifall de bedriver säkerhetskänslig verksamhet eller inte. Metoden för säkerhetsskyddsanalys bör då användas i syfte att bedöma om så är fallet. Om verksamhetsutövaren kommer fram till att ingen säkerhetskänslig verksamhet bedrivs bör slutsatserna dokumenteras trots att kravet på att göra en säkerhetsskyddsanalys inte föreligger. Det arbetet behöver genomföras löpande för att upptäcka när verksamheten är att betrakta som säkerhetskänslig, exempelvis kan ett forskningsprojekt förändras snabbt och kräva att analysen omprövas. Den som bedriver säkerhetskänslig verksamhet är skyldig att utan dröjsmål anmäla detta till sin tillsynsmyndighet.

Säkerhetsskyddsanalysen ska ge svar på följande frågor:

1. Vad ska skyddas?
2. Mot vad ska det skyddas?
3. Hur ska det skyddas?

I säkerhetsskyddsanalysen ligger fokus på att identifiera och bedöma *skyddsvärden* utifrån ett konsekvensperspektiv, det vill säga utifrån en bedömning av den skada för Sveriges säkerhet som en antagonistisk handling mot, eller ett röjande av skyddsvärdet kan medföra. Detta skiljer sig från många andra typer av analyser som även tar hänsyn till hur sannolikt det är att en händelse inträffar och får negativa konsekvenser.

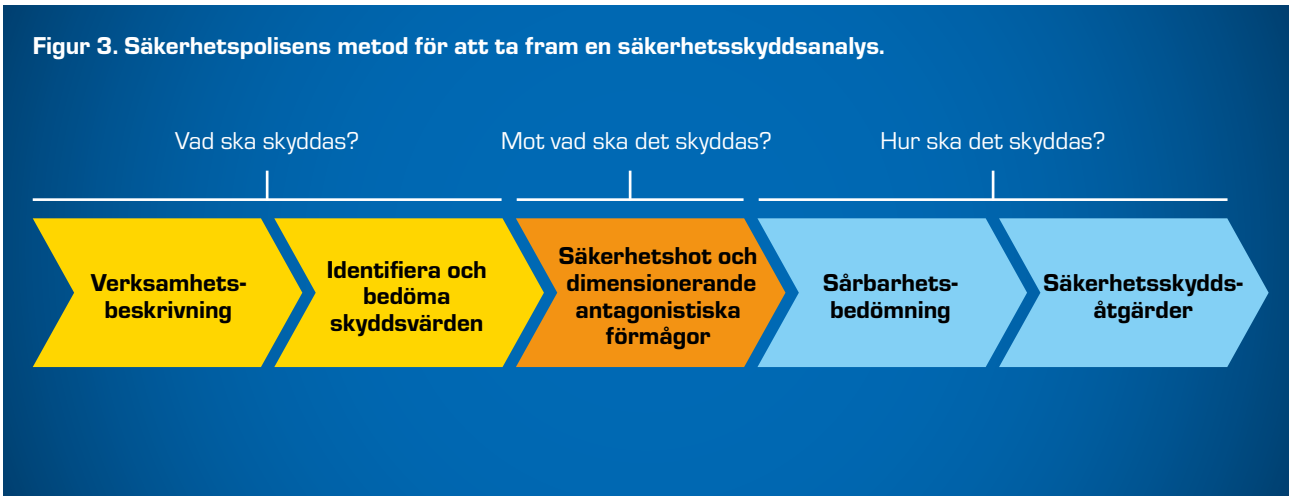
Följande tre typer av skyddsvärden ska identifieras och bedömas i säkerhetsskyddsanalysen:

- säkerhetsskyddsklassificerade uppgifter
- anläggningar, objekt, system, egendom och andra tillgångar
- verksamhet som omfattas av ett för Sverige internationellt åtagande om säkerhetsskydd.

Det är ofta lämpligt att involvera flera kompetenser i säkerhetsskyddsarbetet och i framtagandet av säkerhetsskyddsanalysen. I arbetet med säkerhetsskydd behövs precis som i säkerhetsarbete i stort, en förankring i hela verksamheten, från den strategiska styrningen hos ledningen till enskilda medarbetares handhavande och förståelse i det dagliga arbetet.

+ *Läs mer om säkerhetsskyddsanalys i Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys.*

Figur 3. Säkerhetspolisens metod för att ta fram en säkerhetsskyddsanalys.



4.2 Säkerhetsskydd och andra säkerhetsåtgärder

§ 1 kap. 2 § säkerhetsskyddslagen (2018:585)

Utöver behovet av säkerhetsskydd försöker de flesta verksamheter skydda sig mot olika typer av risker för att inte drabbas av exempelvis produktionsavbrott eller andra störningar i verksamheten. I många fall är verksamhetsskyddet inriktat på olyckor, men det kan i likhet med säkerhetsskydd också ta höjd för antagonistiska handlingar såsom anlagda bränder eller industrispionage. Säkerhetsåtgärder som utgår från verksamhetens egna krav och incitament är valfria, men skyddet av det som faller inom ramen för säkerhetsskydd är obligatoriskt och följer av lag.

Säkerhetsskyddet och andra säkerhetsåtgärder kan i vissa fall vara desamma i syfte att skydda verksamheten. Genom att nyttja befintligt material och analyser kan en verksamhetsutövare korta ner tanke- och handläggningsprocesser. Befintliga analyser kan utgöra en startpunkt och ett inventeringsmaterial inför upprättandet av säkerhetsskyddsanalysen. Det är dock viktigt att klargöra vad som är grunden för respektive analys och åtgärd. I exempelvis en affärsriskanalys kan den bedömda sannolikheten för olika händelser vägas mot eventuella vinster, kostnaden för åtgärder och vilka möjliga förluster organisationen är beredd att acceptera. I en säkerhetsskyddsanalys beaktas inte sannolikheten, utgångspunkten är istället de konsekvenser som måste undvikas. En verksamhetsutövare är skyldig att vidta säkerhetsskyddsåtgärder och säkerställa att nivån av skyddet för den säkerhetskänsliga verksamheten är likvärdigt oavsett var och av vem verksamheten bedrivs.

Säkerhetsskyddets huvudsakliga inriktning att skydda mot antagonistiska handlingar gör att säkerhetsåtgärder som renodlat syftar till att minska konsekvenserna av olyckor i regel inte utgör fullgoda säkerhetsskyddsåtgärder.

4.3 Säkerhetsskyddslagen och annan relevant lagstiftning

Den som bedriver säkerhetskänslig verksamhet behöver ofta förhålla sig till krav även i annan lagstiftning. Detta kan i likhet med behovet av säkerhetsskydd och andra säkerhetsåtgärder innebära såväl utmaningar som möjligheter till synergieffekter.

Se avsnitt 4.2 Säkerhetsskydd och andra säkerhetsåtgärder.

Vissa lagkrav kan uppfyllas med samma eller liknande typer av åtgärder som behövs för säkerhetsskydd, exempelvis skydd mot intrång i informationssystem som hanterar personuppgifter eller skydd mot obehörigt tillträde i hamnar och på kärnkraftverk. Verksamheter som omfattas av såväl säkerhetsskyddslagstiftningen som beredskapsförordningen (2022:524) kan exempelvis nyttja synergier i det cykliska intervall som både risk- och sårbarhetsanalysen och säkerhetsskyddsanalysen har och upprätthålla en aktuell bild över både skyddsvärden, sårbarheter och hot, dock ur olika perspektiv. I andra fall finns motstridiga syften som måste uppfyllas, exempelvis krav på lättframkomliga framkörningsvägar för räddningstjänst ställt mot behovet av hinder som skydd mot angrepp med fordon. Detta kräver särskilt beaktande och noggrann analys så att alla krav kan tillgodoses. I vissa fall finns gränsdragningar och undantag i lag som gör det tydligt om ett krav står över ett annat. Ett sådant exempel är 8 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, som anger att den lagen inte gäller för verksamhet som omfattas av säkerhetsskyddslagen. I många fall behöver en verksamhetsutövare förhålla sig till flera parallella regelverk samtidigt. Så kan till exempel vara fallet vid genomförandet av en säkerhetsskyddad upphandling där både kraven i säkerhetsskyddslagstiftningen och upphandlingslagstiftningen måste uppfyllas. Ett annat exempel är verksamhetsutövare med skyldighet att förebygga och begränsa följderna av allvarliga kemikalieolyckor enligt det så kallade Seveso-direktivet. Dessa verksamhetsutövare har skyldighet att tillhandahålla viss information till allmänheten och samtidigt leva upp till säkerhetsskyddslagens krav på konfidentialitet. Seveso-direktivet är Europaparlamentets och rådets direktiv 2012/18/EU av den 4 juli 2012 om åtgärder för att förebygga och begränsa faran för allvarliga olyckshändelser där farliga ämnen ingår och ändring och senare upphävande av rådets direktiv 96/82/EG.

En annan lag som verksamhetsutövare behöver förhålla sig till är den nyligen tillkomna lagen (2023:560) om utländska direktinvesteringar.


ROSENBAD

5 Säkerhetskänslig verksamhet

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

Säkerhetsskyddslagen gäller för den som till någon del bedriver säkerhetskänslig verksamhet. Med säkerhetskänslig verksamhet avses:

- en verksamhet som är av betydelse för Sveriges säkerhet eller
- en verksamhet som omfattas av ett för Sverige förpliktigande internationellt åtagande om säkerhetsskydd.

Begreppet säkerhetskänslig verksamhet omfattar såväl militär som civil verksamhet. Inom många verksamheter är endast en viss del av verksamheten av betydelse för Sveriges säkerhet.

Verksamhetsutövaren behöver analysera vilka delar som är säkerhetskänsliga så att säkerhetsskyddsåtgärderna inte görs onödigt omfattande men heller inte missar delar som omfattas av säkerhetsskyddslagens krav.

Avgörande för om en verksamhet kan anses röra Sveriges säkerhet bör vara om en antagonistisk handling (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra skadekonsekvenser på nationell nivå. Därtill kan en aktör som till exempel levererar drifttjänster såsom data- och telekommunikation anses bedriva verksamhet som är av betydelse för Sveriges säkerhet. Det kan då vara den samlade betydelsen som aktualiserar behovet av säkerhetsskydd.

Den som hanterar säkerhetsskyddsklassificerade uppgifter bedriver säkerhetskänslig verksamhet eftersom uppgifterna i sig är av betydelse för Sveriges säkerhet. Om säkerhetsskyddsklassificerade uppgifter hanteras hos en aktör till följd av ett förfarande som omfattas av ett säkerhetsskyddsavtal, innebär det dock inte att aktören enbart på den grunden själv bedriver säkerhetskänslig verksamhet.

Internationella åtaganden om säkerhetsskydd

De internationella åtagandena om säkerhetsskydd som Sverige har ingått omfattar i dagsläget framförallt hantering av uppgifter. Sverige har förbundit sig att skydda säkerhetsskyddsklassificerade uppgifter för ett trettiotal andra stater och mellanfolkliga organisationer, bland annat EU och Nato. De flesta av dessa finns publicerade i SÖ-serien på regeringens webbplats. Därutöver har Sverige andra internationella åtaganden gällande exempelvis luftfartsskydd. Verksamheter som omfattas av sådana åtaganden bedriver säkerhetskänslig verksamhet.

5.1 Kategorisering av säkerhetskänslig verksamhet

§ *2 kap. 2 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Säkerhetsskyddsanalysen är ett bra redskap för att identifiera om verksamheten bedriver säkerhetskänslig verksamhet.

+ *Se avsnitt 4.1 Säkerhetskyddsanalys är grunden för säkerhetsskydd.*

Efter det initiala konstaterandet att verksamheten är säkerhetskänslig följer en mer detaljerad analys av på vilket sätt och i vilken utsträckning.

+ *Se Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys. I vägledningen utvecklas centrala begrepp som kort beskrivs nedan och metoden för säkerhetsskyddsanalys beskrivs mer ingående.*

Verksamhetsutövare ska övergripande beskriva sin verksamhet och specificera vilka delar av verksamheten som är av betydelse för Sveriges säkerhet utifrån kategorierna Sveriges yttre säkerhet, Sveriges inre säkerhet, nationellt samhällsviktig verksamhet, verksamhet av betydelse för Sveriges ekonomi och verksamhet som kan generera skada på annan säkerhetskänslig verksamhet. Nedan följer en beskrivning av respektive kategori.

- **Skada för Sveriges yttre säkerhet**
  Sveriges yttre säkerhet kan delas in i förmågan att upprätthålla nationellt försvar (territoriell suveränitet) samt Sveriges integritet, oberoende och handlingsfrihet (politisk självständighet). Utöver Försvarsmakten finns andra verksamheter, till exempel vissa myndigheter och enskilda inom försvarsindustrin, som är viktiga för det militära försvarets förmåga att utföra sitt uppdrag inom ramen för totalförsvaret.
- **Skada för Sveriges inre säkerhet**
  Sveriges inre säkerhet rör förmågan att upprätthålla och säkerställa grundläggande strukturer inklusive det demokratiska statsskicket, rättsväsendet och den brottsbekämpande förmågan på nationell nivå. Detta handlar till stor del om att skydda anläggningar, funktioner och informationssystem som är kritiska för dessa grundläggande strukturer.
- **Skada på nationellt samhällsviktig verksamhet**
  Verksamheter som rör leveranser, tjänster, funktioner och förmågor som är nödvändiga för samhällets funktionalitet på nationell nivå. Dessa verksamheter finns ofta inom, men är inte begränsat till, sektorerna energiförsörjning, elektroniska kommunikationer, transporter och finansiella tjänster.
- **Skada för Sveriges ekonomi**
  Verksamheter som är nödvändiga för den nationella betalningsförmågan och där en ekonomisk skada kan få negativa konsekvenser för Sveriges suveränitet, handlingsfrihet och oberoende.
- **Skadegenererande verksamhet**
  Verksamheter som, om de utsätts för antagonistisk handling, kan generera direkta eller uppenbara indirekta skadekonsekvenser på andra säkerhetskänsliga verksamheter på nationell nivå genom påverkan på liv, hälsa och infrastruktur. Påverkan på liv och hälsa kan uttryckas i att många människor bedöms omkomma eller skadas. Påverkan på infrastruktur avser fysisk förstöring av annan säkerhetskänslig verksamhet.

5.2 Konsekvensnivåer

§ *2 kap. 5 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Skyddsvärden i form av anläggningar, objekt, system, egendom och andra tillgångar som har identifierats vara av betydelse för Sveriges säkerhet ska delas in i konsekvensnivåer enligt nedan beroende på hur allvarlig skada en antagonistisk handling skulle kunna medföra.

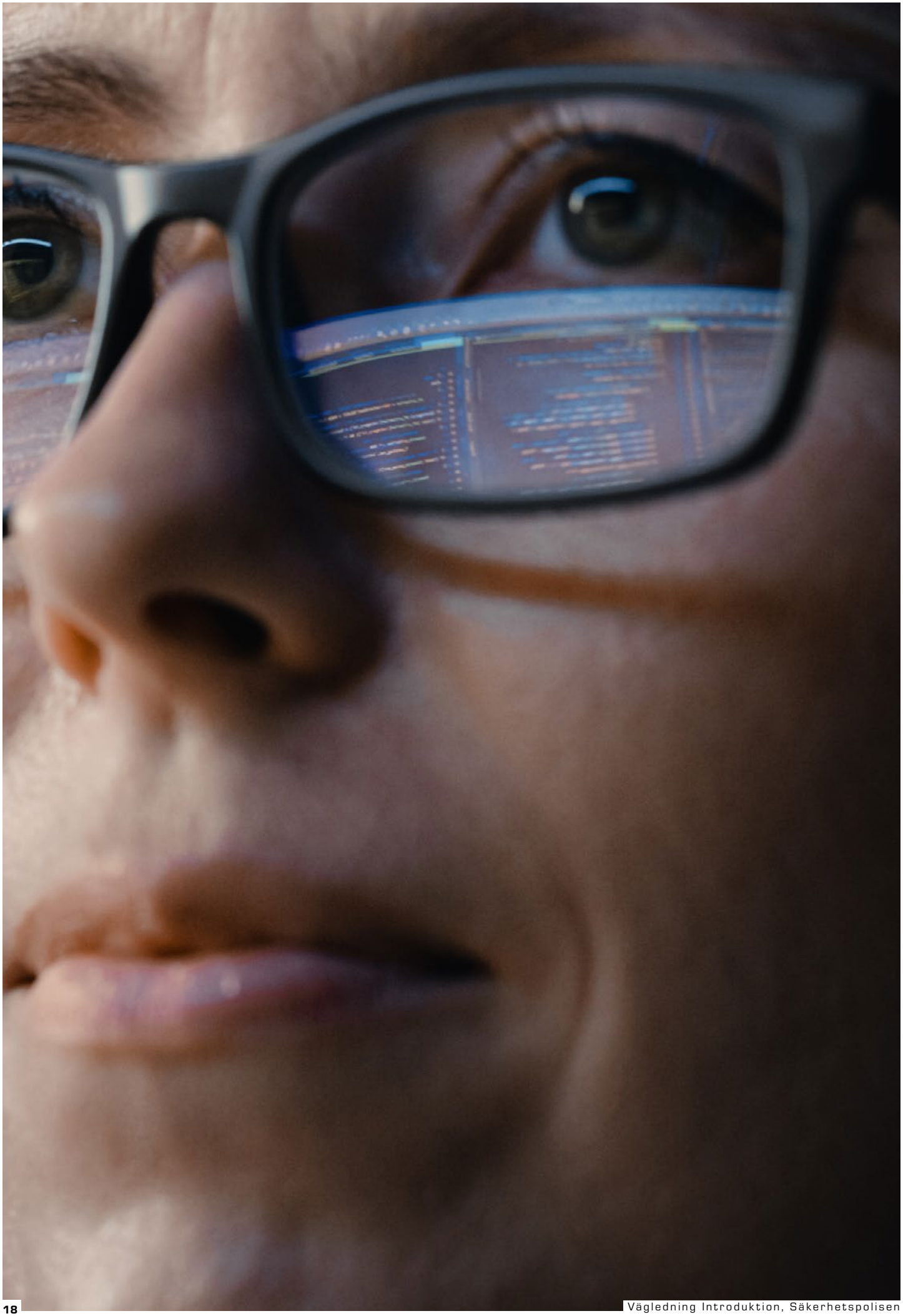
+ *Läs mer om konsekvensnivåerna i Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys.*

Indelningen sker enligt följande konsekvensnivåer:

- **Nivå A:** Synnerligen allvarlig skada för Sveriges säkerhet
- **Nivå B:** Allvarlig skada för Sveriges säkerhet
- **Nivå C:** Inte obetydlig skada för Sveriges säkerhet
- **Nivå D:** Endast ringa skada för Sveriges säkerhet

Konsekvensnivåerna

Nivå A	**Synnerligen allvarlig skada för Sveriges säkerhet**	• Kritiska tjänster, leveranser, funktioner eller förmågor slås ut eller påverkas mycket allvarligt som i sin tur kan medföra att Sverige skulle komma att förlora sin suveränitet, handlingsfrihet eller oberoende, eller • synnerligen allvarlig skada för Sveriges säkerhet till följd av skada på andra säkerhetskänsliga verksamheter, och • mycket svårt att återgå till normalläge.
Nivå B	**Allvarlig skada för Sveriges säkerhet**	• Kritiska tjänster, leveranser, funktioner eller förmågor påverkas allvarligt som i sin tur kan medföra allvarliga begränsningar i Sveriges suveränitet, handlingsfrihet eller oberoende, eller • allvarlig skada för Sveriges säkerhet till följd av skada på andra säkerhetskänsliga verksamheter, och • svårt att återgå till ett normalläge.
Nivå C	**Inte obetydlig skada för Sveriges säkerhet**	• Kritiska tjänster, leveranser, funktioner eller förmågor påverkas påtagligt som i sin tur kan medföra att Sveriges suveränitet, handlingsfrihet eller oberoende skulle komma att påverkas men i begränsad omfattning, eller • inte obetydlig skada för Sveriges säkerhet till följd av skada på andra säkerhetskänsliga verksamheter, och • möjligt att återgå till normalläge inom rimlig tid.
Nivå D	**Endast ringa skada för Sveriges säkerhet**	• Kritiska tjänster, leveranser, funktioner eller förmågor påverkas ringa som i sin tur kan medföra påverkan på Sveriges suveränitet, handlingsfrihet eller oberoende men i i liten omfattning, eller • ringa skada för Sveriges säkerhet till följd av skada på andra säkerhetskänsliga verksamheter, och • möjligt att relativt snabbt återgå till ett normalläge.



6 Skyddsvärda uppgifter och säkerhetsskydds-klassificerade uppgifter

Verksamhetsutövare som bedriver säkerhetskänslig verksamhet har ofta uppgifter som är skyddsvärda ur flera olika perspektiv. Uppgifterna kan ha ett skyddsbehov utifrån andra aspekter än säkerhetsskydd, exempelvis företagshemligheter eller personuppgifter som omfattas av annan lagstiftning och reglering. I detta kapitel beskrivs vilka uppgifter som utgör säkerhetsskyddsklassificerade uppgifter.

Se Vägledning i säkerhetsskydd – Informationssäkerhet.

6.1 Säkerhetsskyddsklassificerade uppgifter

1 kap. 2 § säkerhetsskyddslagen (2018:585)

Inom offentlig verksamhet är säkerhetsskyddsklassificerade uppgifter sådana uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL. Lagen är i regel inte tillämplig hos enskilda verksamhetsutövare, men motsvarande uppgifter behöver ett fullgott skydd även hos dessa.

I definitionen av säkerhetsskyddsklassificerade uppgifter ingår därför även uppgifter som *skulle ha omfattats* av sekretess enligt OSL om den hade varit tillämplig. På så sätt kan säkerhetsskyddsklassificerade uppgifter förekomma även hos enskilda verksamhetsutövare och omfattas därmed av kraven på säkerhetsskydd.

En enskild verksamhetsutövare som bedriver säkerhetskänslig verksamhet men som inte omfattas av OSL behöver alltså göra en bedömning av vilka uppgifter, inom ramen för den säkerhetskänsliga verksamheten, som skulle kunna omfattas av OSL. I förarbetena (Prop. 2017/18:89 s. 52) kallar man detta för en fiktiv sekretessprövning som liknar den som myndigheter gör. Om bedömningen görs att en myndighet hade varit förhindrad att röja motsvarande uppgift är den att anse som säkerhetsskyddsklassificerad (förutsatt att den rör den säkerhetskänsliga verksamheten).

Säkerhetsskyddsklassificerade uppgifter är framförallt sådana uppgifter som är eller skulle ha varit sekretessbelagda enligt

15 kap. 2 § OSL (försvarssekretess).

Även andra sekretessbestämmelser kan vara tillämpliga på uppgifter som rör säkerhetskänslig verksamhet, exempelvis

- *15 kap. 1–1b § (utrikessekretess)*
- *18 kap. 1 § (förundersökningar m.m.)*
- *18 kap. 2 § (sekretess i underrättelseverksamhet)*
- *18 kap. 8 § (säkerhets- eller bevakningsåtgärder)*
- *18 kap. 13 § OSL (risk- och sårbarhetsanalyser m.m.).*

För att uppgifter ska anses vara säkerhetsskyddsklassificerade måste de röra säkerhetskänslig verksamhet *och* omfattas av någon sekretessbestämmelse i OSL, eller skulle ha omfattats av OSL om den hade varit tillämplig. Det är viktigt att komma ihåg att båda kriterierna måste vara uppfyllda. Nedan följer exempel på när så *inte* är fallet:

- **Exempel 1.** Säkerhetspolisen ger varje år ut en lägesbild som publiceras på myndighetens webbplats. Rapporten beskriver Säkerhetspolisens säkerhetskänsliga verksamhet men innehåller inga uppgifter som omfattas av sekretess. Årsboken anses därmed inte innehålla säkerhetskyddsklassificerade uppgifter.

- **Exempel 2.** Ett företag som bedriver säkerhetskänslig verksamhet inom elektronisk kommunikation har även tillverkning av kommunikationsutrustning för vanlig mobiltelefoni. Utrustningen går att köpa på öppna marknaden, så om den till exempel kommer främmande makt tillhanda kan det inte anses orsaka någon skada för Sveriges säkerhet. Om ritningar och uppgifter om tillverkningsprocessen fanns hos en myndighet skulle de dock ha omfattats av sekretess för att skydda företagets ekonomiska intressen. Men, då tillverkningen inte rör den säkerhetskänsliga delen av företagets verksamhet är uppgifterna inte att anse som säkerhetsskyddsklassificerade.

Observera att uppgifter som rör säkerhetskänslig verksamhet utan att vara indelade i säkerhetsskyddsklass ändå kan omfattas av kraven på säkerhetsskydd. Detta gäller ifall uppgifterna behöver vara riktiga (i bemärkelsen oförändrade) och/eller tillgängliga, exempelvis meteorologiska data och kartor som är nödvändiga för nationell flygledning.

Se Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys för fördjupning.

Verksamheten är då beroende av uppgifterna på samma sätt som den är beroende av lokaler, kraftförsörjning etc. och därför ska uppgifterna skyddas mot antagonistiska handlingar.

Indelning av säkerhetsskyddsklassificerade uppgifter

2 kap. 5 § säkerhetsskyddslagen (2018:585)

3 kap. 7 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd

Säkerhetsskyddsklassificerade uppgifter delas in i en av fyra säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet.

- Kvalificerat hemlig (synnerligen allvarlig skada)
- Hemlig (allvarlig skada)
- Konfidentiell (inte obetydlig skada)
- Begränsat hemlig (endast ringa skada).

Bestämmelserna i säkerhetsskyddslagstiftningen utgår inte sällan från vilken säkerhetsskyddsklass de aktuella uppgifterna har. Exempel på sådana bestämmelser är de om logisk och fysisk separation av informationssystem i 4 kap. 15-16 §§ Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd.

Se Vägledning i säkerhetsskydd – Informationssäkerhet.

Skyddet av säkerhetsskyddsklassificerade uppgifter behöver hålla en jämn nivå oavsett i vilken verksamhet de förekommer. Utgångspunkten bör därför vara att den som tar emot en säkerhetsskyddsklassificerad uppgift från en annan verksamhetsutövare godtar den andra verksamhetsutövarens klassificering. Om en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig inte längre ska vara indelad i säkerhetsskyddsklassen kvalificerat hemlig finns särskilda krav i 3 kap. 7 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

Uppgifter som omfattas av internationella åtaganden om säkerhetsskydd

2 kap. 5 § säkerhetsskyddslagen (2018:585)

Säkerhetsskyddsklassificerade uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd ska inte klassificeras på nytt om de redan har tilldelats en säkerhetsskyddsklass av en annan stat eller mellanfolklig organisation.

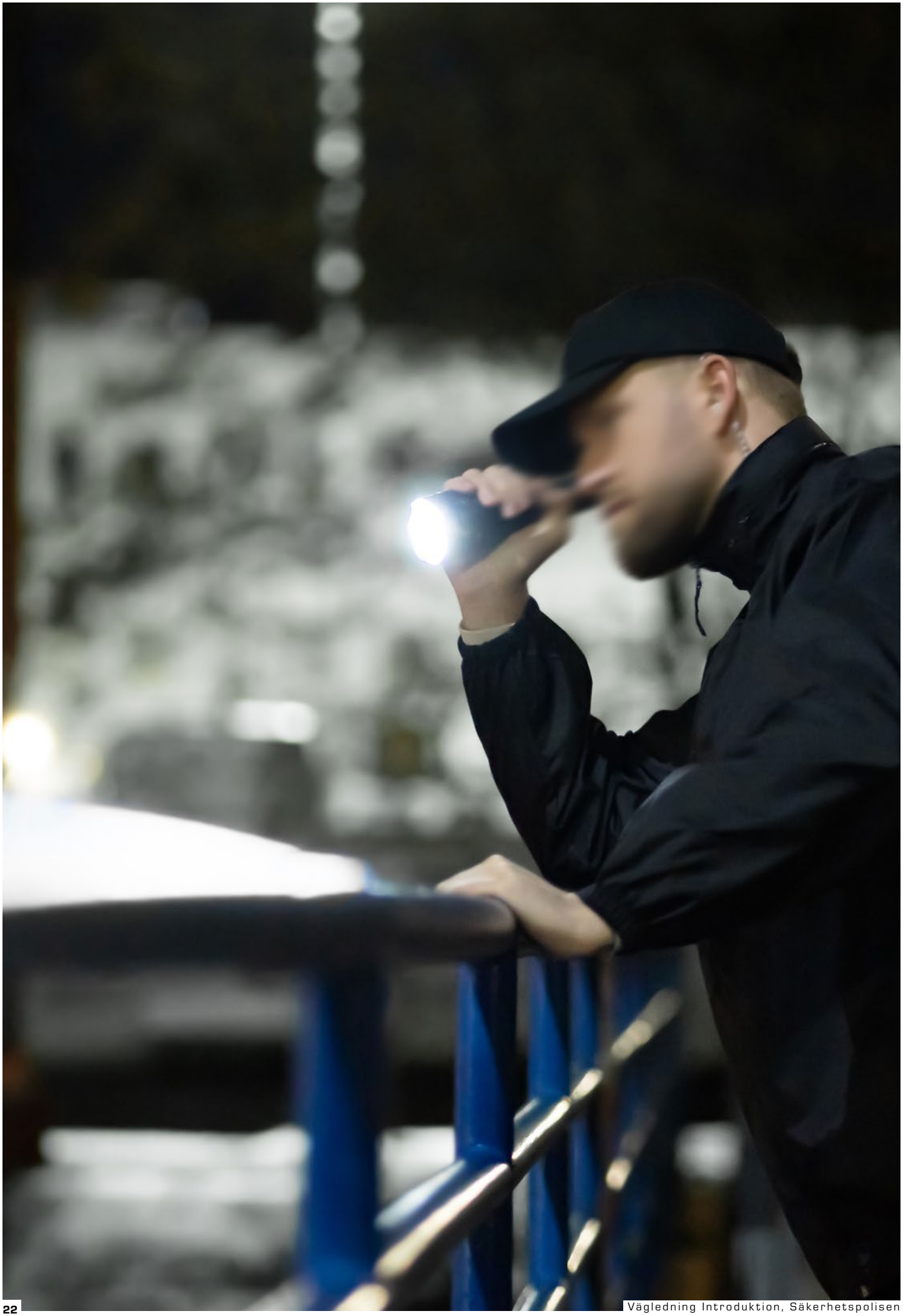
Benämningar avseende exempelvis säkerhetsskyddsklasser varierar mellan olika länder beroende på den nationella lagstiftningen, vilket innebär att det inte finns en enhetlig internationell nomenklatur eller indelning. Varje internationell överenskommelse om säkerhetsskydd innehåller därför bestämmelser där de nationella säkerhetsskyddsklasserna framgår och det är endast dessa benämningar som får användas av avtalsparterna. Sveriges internationella överenskommelser om säkerhetsskydd publiceras normalt på regeringens webbplats under Sveriges internationella överenskommelser (SÖ).

Som exempel kan nämnas EU:s olika säkerhetsskyddsklasser (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 delats in i säkerhetsskyddsklass av den andra parten ska de delas in i säkerhetsskyddsklass utifrån den skada som ett röjande kan medföra för Sveriges förhållande till en annan stat eller mellanfolklig organisation, eller om detta motiverar en högre säkerhetsskyddsklass, den skada ett röjande kan medföra för Sveriges säkerhet.

Uppgifter som rör säkerhetskänslig verksamhet utan att vara indelade i säkerhetsskyddsklass kan ändå omfattas av kraven på säkerhetsskydd. Detta gäller ifall uppgifterna behöver vara riktiga (i bemärkelsen oförändrade) och/eller tillgängliga.



7 Säkerhetsskyddsåtgärder

§ *2 kap. 2-4 §§ säkerhetsskyddslagen (2018:585)*

Merparten av åtgärderna inom säkerhetsskydd utgörs av säkerhetsskyddsåtgärder inom informationssäkerhet, fysisk säkerhet och personalsäkerhet vilka i det här avsnittet förklaras översiktligt. Säkerhetspolisen har även gett ut särskilda vägledningar kring de olika säkerhetsskyddsåtgärderna.

7.1 Informationssäkerhet

§ *2 kap. 2 § säkerhetsskyddslagen (2018:585)*

Alla verksamheter är beroende av att kunna inhämta, lagra, bearbeta och kommunicera information i olika former. Den tekniska utvecklingen har gjort informationssystem till viktiga verktyg i hanteringen. Informationssäkerhet syftar till att skydda information i form av uppgifter och informationssystem. Uppgifterna ska skyddas oavsett hur och var de förekommer.

Informationssäkerhet ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs. Informationssäkerhet ska även förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som rör säkerhetskänslig verksamhet. Informationssäkerhet är inte begränsat till enbart tekniska åtgärder utan inkluderar även bland annat rutiner och utbildning.

Säkerhetsskyddsklassificerade uppgifter kan förekomma i fysisk form som exempelvis utskrivna dokument, fotografier, inspelningar och ritningar. Informationssäkerhetsåtgärder kan i dessa fall exempelvis utgöras av att dokumenten förses med anteckning om aktuell säkerhetsskyddsklass och att förvaring sker på ett betryggande sätt. Säkerhetsskyddsklassificerade uppgifter kan även förekomma muntligt genom samtal och möten. En säkerhetskyddsåtgärd kan då utgöras av att det enbart är tillåtet att ta del av och tala om dessa uppgifter i särskilda skyddade och godkända utrymmen. Behovet av samspel mellan säkerhetsskyddsåtgärder är av stor vikt oavsett i vilken form de säkerhetsskyddsklassificerade uppgifterna förekommer. Personalen som hanterar dokumenten behöver utbildas i säkerhetsskydd och ha kunskap om anteckningens (säkerhetsskyddsklassens) innebörd och förvaringsutrymmena måste dimensioneras i förhållande till den fysiska säkerheten i övrigt. Rutiner för hantering, delning, kopiering och destruktion är andra exempel på åtgärder.

Hantering av säkerhetskyddsklassificerade uppgifter sker idag ofta i olika informationssystem. Ett informationssystem behöver inte innehålla säkerhetsskyddsklassificerade uppgifter för att omfattas av krav på säkerhetsskydd. Det skulle kunna röra sig om fall där det kan uppstå en skada för Sveriges säkerhet om tillgängligheten till och/eller riktighet av uppgifterna som hanteras i systemet påverkas.

7.2 Fysisk säkerhet

§ *2 kap. 3 § säkerhetsskyddslagen (2018:585)*

Fysisk säkerhet ska förebygga obehörigt tillträde till och skadlig inverkan på områden, byggnader och andra anläggningar eller objekt där säkerhetsskyddsklassificerade uppgifter finns eller där säkerhetskänslig verksamhet bedrivs. Skadlig inverkan kan exempelvis vara att med explosiva ämnen eller vapenverkan göra verksamheten otillgänglig. Det omfattar även skydd mot att någon, med eller utan tekniska hjälpmedel, obehörigen får insyn i den säkerhetskänsliga verksamheten.

Utformningen av den fysiska säkerheten har sin grund i säkerhetsskyddsbehovet som identifierats i säkerhetsskyddsanalysens inledande delar. Till detta

kommer de beskrivningar av dimensionerande antagonistiska förmågor som Säkerhetspolisen tillhandahåller.

Den grundläggande principen för fysisk säkerhet består i att genom ett system av personal, rutiner, byggnads- och säkerhetsteknik skapa en förmåga att upptäcka, försvåra och hantera olika typer av antagonistiska handlingar.

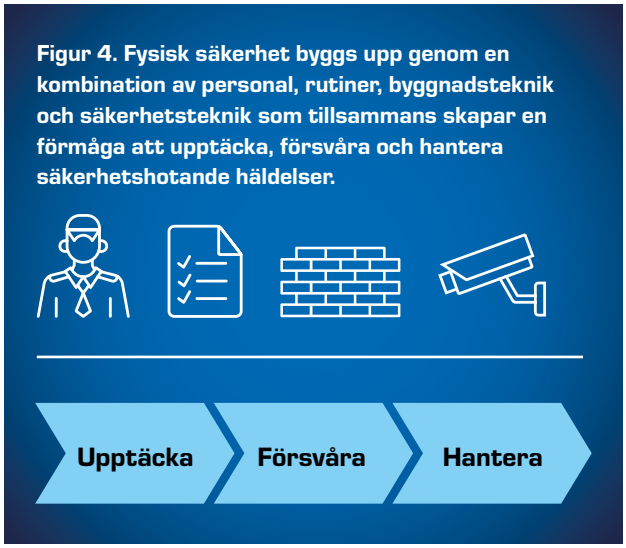
Se figur 4.

Det är viktigt att tidigt upptäcka en antagonist för att övriga delar av den fysiska säkerheten ska vara verkningsfulla. Det är exempelvis ingen större mening med motståndskraftiga dörrar och lås om antagonisten har en hel natt på sig att ta sig igenom det mekaniska skyddet. Upptäckande åtgärder kan exempelvis utgöras av personell bevakning eller teknisk övervakning i form av larmsystem.

De försvårande åtgärderna består av två kategorier. Fördröjande åtgärder som syftar till att uppehålla antagonisten så länge att polis eller annan lämplig resurs hinner ingripa, till exempel dörrar, väggar och andra fysiska barriärer. Skadereducerande åtgärder ska förebygga eller minska skadorna av antagonistiska handlingar som ibland inte går att fördröja eller upptäcka tidigt nog, till exempel beskjutning på avstånd eller fordonsburna sprängladdningar.

För att slutligen kunna stoppa en antagonistisk handling krävs att situationen hanteras. Detta kan exempelvis ske genom att vakter eller polis avbryter den pågående handlingen och om möjligt omhändertar antagonisten. Det är viktigt att de som ska hantera en angripare har rätt utbildning, utrustning och förutsättningar i övrigt för att klara av sitt uppdrag. I det fall angreppet inte har gått att stoppa kan annan hantering krävas i form av konsekvensreducerande åtgärder. Exempel på detta kan vara att stänga ner och utrymma en verksamhet eller flytta skyddsvärda tillgångar vars konfidentiella placering har avslöjats.

Fysisk säkerhet innefattar även bland annat åtgärder för att styra tillträde till platser där säkerhetskänslig verksamhet bedrivs, förvaringsutrymmen för exempelvis säkerhetsskyddsklassificerade handlingar, hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt samt skydd mot obehörig insyn och avlyssning.



Figur 4. Fysisk säkerhet byggs upp genom en kombination av personal, rutiner, byggnadsteknik och säkerhetsteknik som tillsammans skapar en förmåga att upptäcka, försvåra och hantera säkerhetshotande häldelser.

7.3 Personalsäkerhet

§ *2 kap. 4 § och 3 kap. säkerhetsskyddslagen (2018:585)*

Personalsäkerhet består av två delar, säkerhetsprövning och utbildning i säkerhetsskydd. Säkerhetsprövning syftar till att förebygga att personer som inte är pålitliga från säkerhetsynpunkt deltar i säkerhetskänslig verksamhet eller på annat sätt ges tillgång till säkerhetsskyddsklassificerade uppgifter. Utbildning syftar till att säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd för att uppfylla det krav på behörighet och utbildning som deltagandet kräver.

Säkerhetsprövningsprocessen inleds då någon genom en anställning eller på annat sätt ska delta i en säkerhetskänslig verksamhet.

Se figur 5.

Säkerhetsprövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas. Säkerhetsprövningen syftar till att klargöra om en person kan antas vara lojal mot de intressen som ska skyddas i enlighet med säkerhetsskyddslagen och om personen är pålitlig från säkerhetssynpunkt. Vid säkerhetsprövningen ska sådana omständigheter som kan antas innebära sårbarheter i säkerhetshänseende, exempelvis dubbla lojaliteter, behov av att hemlighålla personliga förhållanden och bristande säkerhetsmedvetenhet beaktas.

En säkerhetsprövning består av grundutredning och i de flesta fall registerkontroll samt, i vissa fall särskild personutredning. En grundutredning ska omfatta en säkerhetsprövningsintervju, inhämtning

och bedömning av betyg, intyg, referenser och övriga uppgifter som är av relevans.

Säkerhetspolisen ansvarar för att utföra registerkontroll vid säkerhetsprövning av de personer vars anställning eller deltagande i säkerhetskänslig verksamhet har placerats i säkerhetsklass. Med registerkontroll avses inhämtning av uppgifter ur belastningsregistret, misstankeregistret samt uppgifter som behandlas med stöd av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område och lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.

Beträffande den som placerats i säkerhetsklass 1 och 2 får motsvarande uppgifter inhämtas också beträffande den kontrollerades make, maka eller sambo. Säkerhetspolisen fortsätter kontinuerligt att kontrollera de personer som är föremål för registerkontroll mot aktuella register till dess att verksamhetsutövaren avanmäler en aktiv registerkontroll.Kontrollen upphör alltså först vid avanmälan eller då en sluttid angivits för kontrollen.

En särskild personutredning ska göras vid en registerkontroll som avser den som har placerats i säkerhetsklass 1 och 2 och omfattar bland annat kontroll av ekonomiska förhållanden.

Registerkontroll och särskild personutredning får göras endast om den som säkerhetsprövningen gäller har lämnat sitt samtycke.

Efter den inledande fasen ska säkerhetsprövningen regelbundet fortgå genom uppföljande prövning, i syfte att behålla och fördjupa personkännedomen. På så sätt får verksamhetsutövaren möjlighet att tidigt upptäcka förändringar i attityd och beteende och vidta åtgärder innan det går så långt att en person orsakar skador för den säkerhetskänsliga verksamheten. Områden att utreda i den fortsatta säkerhetsprövningen är bland annat förändringar i livssituation, sociala och ekonomiska förhållanden samt trivsel på arbetsplatsen. Det är viktigt att tidigt uppmärksamma en persons upplevda missnöje med exempelvis arbetssituationen, eftersom det kan leda till en sårbarhet och påverka mottagligheten för yttre påverkan. Även olika former av kontaktförsök eller försök till utpressning kan fångas upp genom en kontinuerlig säkerhetsprövning.

När en anställning eller deltagande i en säkerhetskänslig verksamhet upphör genomförs den sista delen av säkerhetsprövningsprocessen med avslutande samtal och påminnelse om tystnadsplikt samtidigt som registerkontrollen ska avslutas.

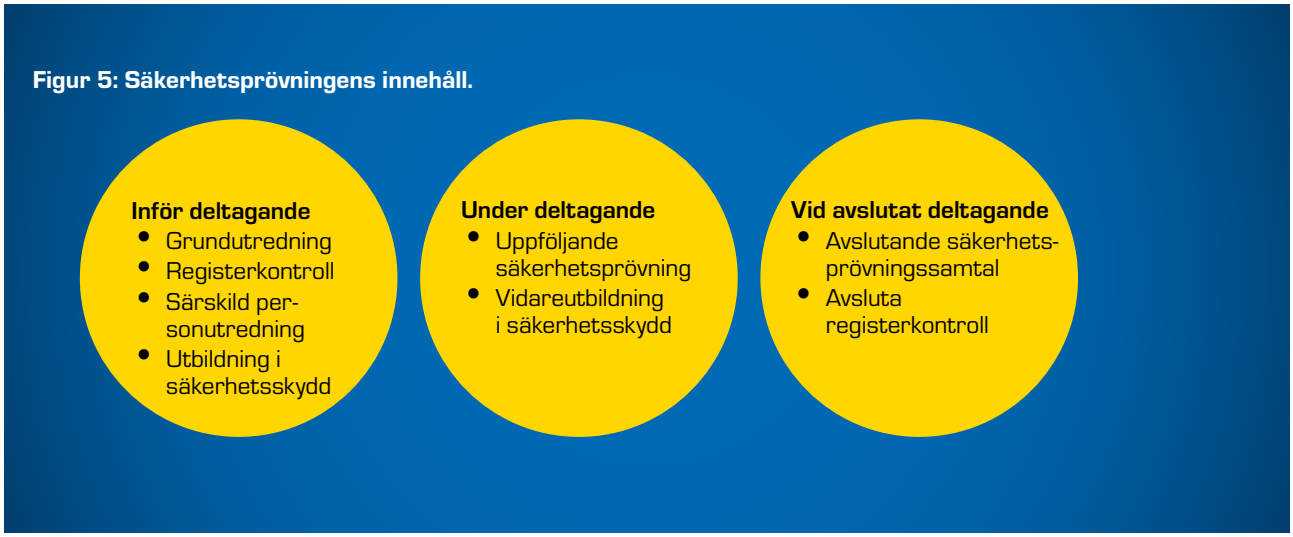
Med utgångspunkt i säkerhetsskyddsanalysen kan beslut fattas om vilka anställningar eller annat deltagande i verksamheten som ska placeras i säkerhetsklass och vilka som endast ska vara föremål för säkerhetsprövning utan att vara placerade i säkerhetsklass. Detta beslut styr omfattningen av säkerhetsprövningen. Behörighet att fatta beslut om placering i säkerhetsklass skiljer sig åt beroende på vilken säkerhetsklass och verksamhetsutövare det rör sig om.

Notera att ett beslut om placering i säkerhetsklass avser en befattning, inte en person, och därmed inte ska förväxlas med ett beslut om anställning. En person kan således vara säkerhetsprövad och registerkontrollerad för flera olika uppdrag inom olika säkerhetskänsliga verksamheter.

En ny säkerhetsprövning ska göras innan varje nytt deltagande i säkerhetskänslig verksamhet. En ny registerkontroll ska göras i de fall befattningen är placerad i säkerhetsklass.

Verksamhetsutövaren ska ha en aktuell förteckning över befattningar med krav på säkerhetsprövning.

Figur 5: Säkerhetsprövningens innehåll.



8 Roller och ansvar

§ *8 kap. säkerhetsskyddsförordningen (2021:955)*

§ *8 kap. 2 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Såväl myndigheter som enskilda verksamhetsutövare kan bedriva säkerhetskänslig verksamhet enligt säkerhetsskyddslagen. En myndighet eller enskild aktör kan också delta i eller ta del av säkerhetskänslig verksamhet utan att själv bedriva den. Säkerhetskänslig verksamhet bedrivs således av många olika aktörer med olika roller och ansvar.

Säkerhetspolisen, Försvarsmakten och ett antal ytterligare myndigheter bedriver tillsyn enligt säkerhetsskyddslagen. Myndigheternas tillsynsområden framgår av säkerhetsskyddsförordningen. Säkerhetspolisen och Försvarsmakten är dessutom samordningsmyndigheter i tillsynsfrågor.

8.1 Verksamhetsutövarens ansvar

§ *2 kap. 1 och 7 §§ och 4 kap. 1–12 §§ säkerhetsskyddslagen (2018:585)*

Den som till någon del bedriver säkerhetskänslig verksamhet har en grundläggande skyldighet att utreda behovet av säkerhetsskydd. Det innefattar bland annat att identifiera förekomst av säkerhetsskyddsklassificerade uppgifter och andra skyddsvärden samt att planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och andra omständigheter. Verksamhetsutövaren ska dessutom kontinuerligt kontrollera och följa upp det egna säkerhetsskyddet.

Om en annan aktör kan få tillgång till den säkerhetskänsliga verksamheten behöver den som bedriver säkerhetskänslig verksamhet även reglera och kontrollera säkerhetsskyddet hos den andra aktören. Ansvaret för den som bedriver säkerhetskänslig verksamhet sträcker sig i så fall således även utanför den egna organisationen.

Notera:
Det finns ingen förteckning, tillståndsprövningsprocess eller liknande som tydligt pekar ut vilka som bedriver säkerhetskänslig verksamhet. Det är istället, i likhet med vad som gäller inom många andra områden, varje verksamhetsutövares ansvar att hålla sig informerad, göra bedömningar och bedriva sin verksamhet enligt säkerhetsskyddslagstiftningen.

Arbetet med säkerhetsskydd behöver inledas med ett aktivt ställningstagande om en verksamhet till någon del är säkerhetskänslig. I praktiken medför detta att verksamhetsutövare, om svaret inte är uppenbart, behöver genomföra det första steget av processen för säkerhetsskyddsanalys.

+ *För närmare beskrivning av de kategorier som kan användas för en initial bedömning, se avsnitt 5.1 Kategorisering av säkerhetskänslig verksamhet.*

Vem är verksamhetsutövare?
För att säkerhetsskyddarbetet ska kunna organiseras och fördelas rätt inom och mellan organisationer är det viktigt att klargöra vem som är verksamhetsutövare. I de flesta fall är detta relativt enkelt, exempelvis i fråga om myndigheter och aktiebolag som bedriver säkerhetskänslig verksamhet och som är definierade med tydliga avgränsningar mot andra organisationer. I andra fall är det kanske inte lika uppenbart, såsom i olika former av myndighetssamarbeten, föreningar och koncerner med helägda dotterbolag.

Det är den juridiska personen som bedriver den säkerhetskänsliga verksamheten som är verksamhetsutövare. Om kommunala bolag eller ett räddningstjänstförbund bedriver säkerhetskänslig verksamhet är det således bolaget eller förbundet som är verksamhetsutövare. Likaså är ideella föreningar som bedriver säkerhetskänslig verksamhet verksamhetsutövare även om verksamheten bedrivs i nära samarbete och med stöd från en myndighet. I fråga om koncerner är respektive bolag i koncernen en verksamhetsutövare.

Varje juridisk person som bedriver säkerhetskänslig verksamhet är alltså en verksamhetsutövare med skyldighet att leva upp till säkerhetsskyddslagens krav.

Säkerhetsskyddslagstiftningen skiljer på offentliga och enskilda verksamhetsutövare. Med enskilda verksamhetsutövare avses alla verksamhetsutövare som inte är en kommun, en region eller en statlig myndighet. Detta medför att exempelvis kommunala bolag och kommunförbund är enskilda verksamhetsutövare på samma sätt som privatägda aktiebolag. Räddningstjänstförbund och andra kommunalförbund är däremot offentliga verksamhetsutövare.

Vem som är behörig att företräda verksamheten kan variera i olika frågor beroende på hur exempelvis en delegationsordning ser ut. En verksamhetsutövare behöver klargöra vem som är behörig företrädare för verksamheten och som får fatta vissa beslut kopplade till säkerhetsskyddslagstiftningen. Det är till exempel enbart verksamhetsutövarens högsta chef eller motsvarande organ som kan fastställa verksamhetens säkerhetsskyddsanalys.

Hos verksamhetsutövaren ska det finnas en säkerhetsskyddschef

Säkerhetsskyddschefen ska leda, samordna och kontrollera att verksamheten bedrivs enligt säkerhetsskyddsbestämmelserna. Säkerhetsskyddschefens ansvar kan inte delegeras och säkerhetsskyddschefen ska vara direkt underställd chefen för verksamhetsutövarens verksamhet. Det innebär att verksamhetens högsta chef har både personalansvar och verksamhetsansvar över säkerhetsskyddschefen. Det stärker kommunikationen mellan säkerhetsskyddsorganisationen och ledningen, samt motverkar att säkerhetsskyddsarbetet bedrivs som en isolerad del av verksamheten. Det är därmed inte tillräckligt att säkerhetsskyddschefen enbart har rapporteringsskyldighet till chefen för verksamhetsutövarens verksamhet. Kravet hindrar dock inte verksamhetsutövare att utforma sitt säkerhetsskyddsarbete på en rad olika sätt och att arbetsuppgifter delegeras, exempelvis till flera enheter i en organisation.

I vissa undantagsfall behöver en verksamhetsutövare inte utse en säkerhetsskyddschef. I dessa verksamheter ska behovet av en utsedd säkerhetsskyddschef vara uppenbart obehövligt. Det kan exempelvis gälla en verksamhet som enbart består av en eller ett fåtal individer och där verksamhetens högsta chef eller ägare tar både verksamhets- och säkerhetsskyddsansvar. I ett sådant fall kan det anses tillräckligt att verksamhetens högsta chef ansvarar för säkerhetsskyddet, utan att utse sig själv till säkerhetsskyddschef. Andra situationer där det är uppenbart obehövligt med en säkerhetsskyddschef kan vara om den säkerhetskänsliga verksamheten är av mycket begränsad omfattning. För bedömningen har det också betydelse vilka säkerhetsskyddsklassificerade uppgifter som finns i verksamheten och hur den säkerhetskänsliga verksamheten är i övrigt.

Leverantörer och andra aktörer

En aktör som inte bedriver säkerhetskänslig verksamhet kan ta del av säkerhetskänslig verksamhet genom att exempelvis vara leverantör till en verksamhetsutövare där säkerhetskänslig verksamhet bedrivs. Aktören ska dock inte anses själv bedriva säkerhetskänslig verksamhet endast på grund av att denne exempelvis utför ett uppdrag inom ramen för ett säkerhetsskyddsavtal.

En aktörs deltagande i en annan verksamhetsutövares säkerhetskänsliga verksamhet utesluter dock inte att aktören själv samtidigt bedriver säkerhetskänslig verksamhet.

Se vidare Vägledning i säkerhetsskydd – Skyldigheter vid exponering av säkerhetskänslig verksamhet.

8.2 Tillsynsmyndigheternas roll

§ *8 kap. 1–12 §§ säkerhetsskyddsförordningen (2021:955)*

Totalt finns det 13 tillsynsmyndigheter. Utöver de två samordningsmyndigheterna Säkerhetspolisen och Försvarsmakten finns det fyra länsstyrelser och ytterligare sju tillsynsmyndigheter som utövar tillsyn över enskilda verksamhetsutövare inom ett avgränsat område. Tillsynsmyndigheterna får även utöva tillsyn hos en aktör som en verksamhetsutövare inom tillsynsmyndighetens tillsynsområde har ingått ett säkerhetsskyddsavtal med.

Notera:
Tillsynsmyndigheterna har utöver tillsyn ett ansvar för vägledning och att vara kontakt för verksamhetsutövare vid frågor om säkerhetsskydd och tillämpning av bestämmelser. Eftersom tillsynsmyndigheterna både har ett vägledning- och tillsynsuppdrag bör tillsynsmyndigheterna i ett enskilt fall inte också vara rådgivande till verksamhetsutövare. En tillsynsmyndighet bör som utgångspunkt vägleda kring exempelvis hur lagstiftningen ska tolkas eller kring en metod för hur någonting ska utföras, men inte kring vad som ska utföras i ett enskilt fall.

Tillsynsmyndigheterna beslutar även i regel om placering i säkerhetsklass för enskilda verksamhetsutövare inom sitt tillsynsområde.

+ *Läs mer om detta i Vägledning i säkerhetsskydd – Personalsäkerhet.*

Tillsynsmyndigheterna (bortsett från Försvarsmakten och Försvarets materielverk) har även rätt att efter samråd med Säkerhetspolisen medge undantag från Säkerhetspolisens föreskrifter om säkerhetsskydd och inom respektive område meddela ytterligare kompletterande föreskrifter.

Föreligger särskilda skäl kan Säkerhetspolisen och Försvarsmakten överta tillsynsansvaret för en verksamhetsutövare som sorterar under en annan tillsynsmyndighets ansvarsområde.

8.3 Vitessanktionerade åtgärdsförelägganden och sanktionsavgifter

§ *6 kap. 6 § och 7 kap. säkerhetsskyddslagen (2018:585)*

En tillsynsmyndighet får besluta att förelägga en verksamhetsutövare att vidta åtgärder för att fullgöra sina skyldigheter enligt säkerhetsskyddslagstiftningen. Ett sådant föreläggande får förenas med vite. Till exempel kan en tillsynsmyndighet förelägga en verksamhet att utarbeta en säkerhetsskyddsanalys eller rutiner som uppfyller författningarnas krav.

Om en verksamhetsutövare åsidosätter vissa centrala skyldigheter i säkerhetsskyddslagstiftningen kan tillsynsmyndigheten besluta att ta ut en sanktionsavgift. Sanktionsavgiften kan uppgå till 50 000 000 kronor som högst för enskilda verksamhetsutövare och 10 000 000 kronor för statliga myndigheter, kommuner och regioner.

9 Ansvarsbestämmelser och tystnadsplikt

§ *8 kap. 1–2 §§ säkerhetsskyddslagen (2018:585)*

§ *2 kap. 3 § säkerhetsskyddsförordningen (2021:955)*

Säkerhetsskyddslagstiftningen innehåller flera krav på åtgärder och aktiviteter som verksamhetsutövare ska vidta i syfte att värna Sveriges säkerhet och internationella åtaganden. Om en verksamhetsutövare åsidosätter sina skyldigheter enligt lagstiftningen får tillsynsmyndigheten besluta om förelägganden och, mot vissa överträdelser, även sanktionsavgifter.

+ *Se avsnitt 8.3 Vitessanktionerade åtgärdsförelägganden och sanktionsavgifter.*

Dessutom kan bristande hantering av säkerhetsskyddsklassificerade uppgifter, även utan uppsåt, i vissa fall leda till straffansvar enligt bestämmelserna i 19 kap. brottsbalken (1962:700), till exempel för vårdslöshet med hemlig uppgift.

Det finns i säkerhetsskyddslagen särskilda bestämmelser om tystnadsplikt hos enskilda verksamhetsutövare. Den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet får inte obehörigen röja eller utnyttja säkerhetsskyddsklassificerade uppgifter. Vidare får den som fått del av uppgifter som förekommer i angelägenhet som avser säkerhetsprövning inte obehörigen röja eller utnyttja dessa uppgifter.

I det allmännas verksamhet tillämpas istället bestämmelserna i offentlighets- och sekretesslagen (2009:400). I praktiken innebär det att tystnadsplikten är lika långtgående oavsett verksamhetsutövare, vilket är i linje med principen att nivån av säkerhetsskyddet ska vara likvärdigt oavsett var, hur och av vem verksamheten bedrivs.

Brott mot tystnadsplikten är straffsanktionerat i 20 kap. 3 § brottsbalken.

+ *Tystnadsplikten och vikten av att utbilda och informera om denna beskrivs mer ingående i Vägledningar i säkerhetsskydd – Personalsäkerhet respektive Skyldigheter vid exponering av säkerhetskänslig verksamhet.*

9.1 Samordningsmyndigheternas roll

§ *8 kap. 2 § säkerhetsskyddsförordningen (2021:955)*

Säkerhetspolisen och Försvarsmakten har ett utökat uppdrag som samordningsmyndigheter i syfte att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn inom säkerhetsskyddsområdet. I uppdraget som samordningsmyndigheter ingår att:

- i samverkan följa upp, utvärdera och utveckla arbetet med tillsyn och samråd
- i samråd ta fram och tillhandahålla metodstöd för tillsyn och samråd
- förmedla relevant hotinformation till tillsynsmyndigheterna
- leda ett samarbetsforum där tillsynsmyndigheterna ingår, i syfte att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

10 Tillhandahållande av dimensionerande antagonistiska förmågor

§ *2 kap. 7 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Beskrivningar av dimensionerande antagonistiska förmågor ger information om de antagonistiska förmågor som vissa säkerhetsskyddsåtgärder ska kunna skydda mot, oavsett om det för tillfället föreligger något identifierat säkerhetshot mot den säkerhetskänsliga verksamheten eller inte. Dessa beskrivningar utgör en central del av säkerhetsskyddsanalysen och behöver följaktligen integreras som en del i analysarbetet.

+ *Läs mer om dimensionerande antagonistiska förmågor i Vägledningar i säkerhetsskydd – Säkerhetsskyddsanalys och Fysisk säkerhet.*

Verksamhetsutövare som bedriver säkerhetskänslig verksamhet ska anmäla det till sin tillsynsmyndighet. Tillsynsmyndigheterna ska uppmärksamma Säkerhetspolisen på vilka av verksamhetsutövarna inom tillsynsmyndigheternas tillsynsområde som har behov av beskrivningar av dimensionerande antagonistiska förmågor.

Säkerhetspolisen begär i sin tur in delar av verksamhetsutövarens säkerhetsskyddsanalys och tillhandahåller, om det inte i ett enskilt fall är olämpligt, beskrivningar av dimensionerande antagonistiska förmågor till verksamhetsutövaren. Utifrån identifierade skyddsvärden, säkerhetshot, beskrivningar av dimensionerande antagonistiska förmågor och sårbarheter ska verksamhetsutövaren sedan dimensionera vissa säkerhetsskyddsåtgärder.

Säkerhets-skyddsavtal

För att kunna säkerställa att säkerhetsskyddet uppfyller författningskraven behöver verksamhetsutövaren ålägga den andra aktören att vidta säkerhetsskyddsåtgärder. Detta görs vanligen genom ett säkerhetsskyddsavtal som ingås mellan parterna.

11 Författaranden med krav på säkerhetsskyddsavtal

§ *4 kap. 1–12 §§ säkerhetsskyddslagen (2018:585)*

§ *6 kap. 1–2 §§, 4-6 §§, 8 § säkerhetsskyddsförordningen (2021:955)*

§ *7 kap. Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Vid vissa förfaranden då en utomstående aktör kan få tillgång till säkerhetskänslig verksamhet behöver verksamhetsutövaren ingå ett säkerhetsskyddsavtal och vidta åtgärder både innan, under och efter förfarandet. Säkerhetsskyddslagen pekar ut fyra situationer: upphandlingar, ingående av avtal, samverkan och samarbeten. I samtliga fall gäller att förfarandet ska kunna orsaka minst en inte obetydlig skada för Sveriges säkerhet, det vill säga att aktören kan få tillgång till:

- säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller
- säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

En verksamhetsutövare som avser att genomföra en upphandling, ingå ett avtal eller inleda en samverkan eller ett samarbete som innebär att den andra aktören kan få tillgång till säkerhetsskyddsklassificerade uppgifter i högst säkerhetsskyddsklassen begränsat hemlig eller annan säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet ska tillse att säkerhetsskyddet regleras på något annat sätt än genom ett säkerhetsskyddsavtal, exempelvis genom en säkerhetsskyddsöverenskommelse.

+ *Läs mer om detta i Vägledning i säkerhetsskydd – Skyldigheter vid exponering av säkerhetskänslig verksamhet.*

Säkerhetsskyddsavtal

Verksamhetsutövaren ska ingå ett *säkerhetsskyddsavtal* med den andra aktören, innan denna får del av den säkerhetskänsliga verksamheten. Genom säkerhetsskyddsavtalet regleras hur den säkerhetskänsliga verksamheten ska skyddas då den andra aktören tar del av den, exempelvis om aktören ska hantera verksamhetsutövarens säkerhetsskyddsklassificerade uppgifter i sina egna lokaler.

Skyldigheten att ingå säkerhetsskyddsavtal gäller även gentemot underleverantörer, exempelvis om aktörer som ska tillhandahålla en tjänst till verksamhetsutövaren i sin tur anlitar en leverantör. Om båda parterna är statliga myndigheter så gäller dock kravet på säkerhetsskyddsavtal endast vid anskaffning av en vara, tjänst eller byggentreprenad.

Genom att ingå ett säkerhetsskyddsavtal förbinder sig den andra aktören att uppfylla de krav på säkerhetsskyddsåtgärder som verksamhetsutövaren bedömer är nödvändiga. Den verksamhetsutövare som exponerar sin säkerhetskänsliga verksamhet har därefter ansvar att kontrollera att motparten uppfyller kraven i avtalet och att kraven vid behov revideras.

Grundprincipen inom säkerhetsskydd
Den säkerhetskänsliga verksamheten ska ha samma eller ett likvärdigt skydd oavsett var verksamheten bedrivs eller vem den utförs av. Säkerhetsskyddsavtal är en följd av den principen.

Särskild säkerhetsskyddsbedömning

För att kunna säkerställa att säkerhetskänslig verksamhet ges det skydd som behövs ska verksamhetsutövaren, inför ett förfarande med krav på säkerhetsskyddsavtal, göra en särskild säkerhetsskyddsbedömning.

Syftet med en särskild säkerhetsskyddsbedömning är att identifiera vilka säkerhetsskyddsklassificerade uppgifter eller annan säkerhetskänslig verksamhet som den andra aktören kan få tillgång till och utreda vilka säkerhetsskyddsåtgärder som behöver vidtas inför det planerade förfarandet. Det gäller såväl sådana åtgärder som ska regleras i säkerhetsskyddsavtalet som vilka åtgärder som verksamhetsutövaren själv kan behöva vidta. Utöver det ska den särskilda säkerhetsskyddsbedömningen även ligga till grund för prövningen om det planerade förfarandet är lämpligt från säkerhetsskyddssynpunkt.

Metoden för att genomföra en särskild säkerhets-

skyddsbedömning kan med fördel baseras på den metod som används vid en säkerhetsskyddsanalys.

Se vidare Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys.

Det framgår också av Säkerhetspolisens föreskrifter vad som ska ingå i den särskilda säkerhetsskyddsbedömningen. Bedömningen ska dokumenteras.

Observera att uttrycket särskild säkerhetsskyddsbedömning även förekommer i 3 kap. 1 § säkerhetsskyddsförordningen men då gällande driftsättning av informationssystem och bedömning av säkerhetskrav i systemet. I dessa fall ska verksamhetsutövaren även samråda med Säkerhetspolisen.

Se Vägledning i säkerhetsskydd – Informationssäkerhet.

Notera:
En verksamhetsutövare som ska exponera sin säkerhetskänsliga verksamhet på ett sådant sätt att den andra aktören också ska tillhandahålla ett informationssystem som ska hantera säkerhetsskyddsklassificerade uppgifter behöver göra två särskilda säkerhetsskyddsbedömningar, en för förfarandet i sig och en gällande driftsättning av informationssystem. Det kan även bli aktuellt med två olika samråd eftersom både samråden och de särskilda säkerhetsskyddsbedömningarna tar olika perspektiv i beaktande och genomförs i olika syften.

Lämplighetsprövning

Inför ett förfarande med krav på säkerhetsskyddsavtal ska verksamhetsutövaren även göra en lämplighetsprövning. Med utgångspunkt i den särskilda säkerhetsskyddsbedömningen och övriga omständigheter ska verksamhetsutövaren bedöma om det planerade förfarandet är lämpligt från säkerhetsskyddssynpunkt. Om lämplighetsprövningen leder till bedömningen att förfarandet inte är lämpligt får förfarandet inte inledas. Om förfarandet ändå inleds har verksamhetsutövarens tillsynsmyndighet möjligheter att ingripa för att förhindra skada för Sveriges säkerhet. Lämplighetsprövningen ska dokumenteras.

Samrådsskyldighet

Om verksamhetsutövaren bedömer att det planerade förfarandet inte är olämpligt krävs i vissa fall samråd med tillsynsmyndigheten *innan* förfarandet med krav på säkerhetsskyddsavtal *inleds*. Så är fallet när förfarandet kan orsaka allvarlig skada för Sveriges säkerhet, det vill säga att aktören kan få tillgång till:

- säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller högre, eller
- säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Under samrådet kan tillsynsmyndigheten förelägga verksamhetsutövaren att vidta åtgärder enligt säkerhetsskyddslagslagen och föreskrifter som har meddelats i anslutning till lagen. Om ett sådant föreläggande inte följs eller om det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas får tillsynsmyndigheten besluta att förfarandet inte får genomföras.

Läs mer om säkerhetsskyddsavtal, särskild säkerhetsskyddsbedömning, lämplighetsprövning och samrådsskyldighet i Vägledning i säkerhetsskydd – Skyldigheter vid exponering av säkerhetskänslig verksamhet.


Skyldigheten att ingå säkerhets-skyddsavtal gäller även gentemot underleverantörer, särskilt vid anskaffning av vara, tjänst eller byggentreprenad.


Inför att säkerhetskänslig verksamhet ska överlåtas behöver åtgärder vidtas för att förhindra att överlåtelsen kan orsaka skada för Sveriges säkerhet.

12 Överlåtelse av säkerhetskänslig verksamhet och viss egendom

§ *4 kap. 13–20 §§ säkerhetsskyddslagen (2018:585)*

§ *6 kap. 3 § säkerhetsskyddsförordningen (2021:955)*

När säkerhetskänslig verksamhet, viss egendom av betydelse för Sveriges säkerhet samt aktier eller andelar i säkerhetskänslig verksamhet ska överlåtas behöver överlåtaren vidta vissa åtgärder.

En överlåtelse är en övergång av äganderätt från en juridisk eller fysisk person till en annan, genom exempelvis försäljning, byte eller gåva. En överlåtelse av säkerhetskänslig verksamhet innebär kortfattat att nya juridiska eller fysiska personer kommer att få tillgång till, eller i olika grad möjlighet att kontrollera, verksamhet av betydelse för Sveriges säkerhet. Det är en situation som är förknippat med risker. En verksamhetsutövare som avser att överlåta säkerhetskänslig verksamhet till någon annan är därför skyldig att vidta vissa åtgärder inför överlåtelsen.

Den som avser att genomföra en överlåtelse av säkerhetskänslig verksamhet eller viss egendom av betydelse för Sveriges säkerhet eller ett förpliktande internationellt åtagande om säkerhetsskydd, ska göra en särskild säkerhetsskyddsbedömning, lämplighetsprövning och samråda med sin tillsynsmyndighet. Kravet på att göra en särskild säkerhetsskyddsbedömning och lämplighetsprövning gäller inte för den som avser att överlåta aktier eller andelar i säkerhetskänslig verksamhet.

Verksamhetsutövaren ska, utifrån den särskilda säkerhetsskyddsbedömningen och övriga relevanta omständigheter, pröva om överlåtelsen är lämplig från säkerhetsskyddssynpunkt. Även lämplighetsprövningen inför en överlåtelse liknar till stora delar den lämplighetsprövning som ska göras inför ett säkerhetsskyddsavtal. Om förfarandet inte är olämpligt ska verksamhetsutövaren samråda med sin tillsynsmyndighet. Tillsynsmyndigheten får besluta om att överlåtelsen inte får genomföras om ett beslut om föreläggande inte följs eller om överlåtelsen är olämplig från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas. En överlåtelse i strid med förbud är ogiltig.

Om ett beslut om föreläggande inte följs eller om överlåtelsen är olämplig från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas, får tillsynsmyndigheten besluta att överlåtelsen inte får genomföras, överlåtelsen är då ogiltig.

+ *Läs mer i Vägledning i säkerhetsskydd – Skyldigheter vid exponering av säkerhetskänslig verksamhet.*

13 Anmälan om säkerhetshotande händelse eller verksamhet

§ *2 kap. 4 § säkerhetsskyddsförordningen (2021:955)*

§ *2 kap. 15-19 §§ Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Säkerhetskänsliga verksamheter ska ha rutiner för hantering av säkerhetshotande händelser som är av betydelse för verksamheten.

En säkerhetshotande händelse ska skyndsamt anmälas till Säkerhetspolisen om:

1. **En säkerhetsskyddsklassificerad uppgift kan ha röjts. Exempel på sådana händelser är:**
   - En deltagare i den säkerhetskänsliga verksamheten har lämnat en säkerhetsskyddsklassificerad uppgift obevakad i ett mötesrum där personer som inte är behöriga att ta del av sådana uppgifter har tillträde.
   - Säkerhetsskyddsklassificerade uppgifter har distribuerats utan att nödvändiga säkerhetsskyddsåtgärder har vidtagits.
2. **En IT-incident har inträffat i ett informationssystem som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet. Exempel på sådana incidenter är:**
   - Verksamhetsutövaren har inte uppdaterat en programvara i informationssystemet vilket inneburit säkerhetsbrister och sårbarheter i informationssystemet under lång tid.
   - Verksamhetsutövaren misstänker att ett intrång har skett i ett informationssystem som innehåller säkerhetsskyddsklassificerade uppgifter.
3. **Verksamhetsutövaren får kännedom eller misstanke om annan för denne allvarlig säkerhetshotande verksamhet. Exempel på sådan verksamhet är:**
   - Det har skett försök av obehöriga att få tillträde till en anläggning där en verksamhetsutövare till någon del bedriver säkerhetskänslig verksamhet.
   - Det har upptäckts försök att sabotera ett skyddsvärde som är av betydelse för nationellt samhällsviktig verksamhet och som i verksamhetsutövarens säkerhetsskyddsanalys har konstaterats kunna medföra allvarlig skada för Sveriges säkerhet om skyddsvärdet görs otillgängligt.

Vid en säkerhetshotande händelse eller verksamhet ska verksamhetsutövaren vidta åtgärder så att skadan på den säkerhetskänsliga verksamheten minimeras och så snart som möjligt återgå till normalläge. Verksamhetsutövaren ska utreda omständigheterna för händelsen eller verksamheten och utvärdera hanteringen av dem. Utifrån värderingen ska det vidtas nödvändiga åtgärder för att minimera skadeeffekten av liknande händelser i framtiden.

Anmälan om samt skadebedömning av en säkerhetshotande händelse eller verksamhet ska göras till Säkerhetspolisen på anvisad blankett, se Säkerhetspolisens webbplats. Vid anmälan ska en skadebedömning av händelsen kopplad till det berörda skyddsvärdet påbörjas skyndsamt. Vidare ska en beskrivning av skadan upprättas kopplad till säkerhetsskyddsklass, konsekvensnivå och perspektiv beroende på vilken typ av skyddsvärde som händelsen berör. Skadebedömningen ska även beskriva den faktiska skada som händelsen kan innebära på den säkerhetskänsliga verksamheten. Vid bedömning av skadan bör verksamhetsutövaren utgå ifrån ett konsekvensperspektiv, det vill säga vilken skada händelsen kan medföra för Sveriges säkerhet. I detta ska således inte hänsyn tas till sannolikheten av att skadan av händelsen har skett.

Om rekvisiten för en anmälan inte är uppfyllda enligt 2 kap. 4 § säkerhetsskyddsförordningen, kan händelsen istället skickas in som tips till Säkerhetspolisen. Vid situationer där det råder osäkerhet om händelsen omfattas av anmälningsplikt uppmanar Säkerhetspolisen att verksamhetsutövare ändå upprättar en anmälan.

Text: Säkerhetspolisen. Form: Intellecta. Tryck: Stibo Complete.

Säkerhetspolisen har tagit fram ett antal vägledningar som kan fungera som ett stöd för verksamhetsutövare i tillämpningen av säkerhetsskyddsregelverket.

1. Introduktion till säkerhetsskydd
2. Säkerhetsskyddsanalys
3. Personalsäkerhet
4. Fysisk säkerhet
5. Informationssäkerhet
6. Skyldigheter vid exponering av säkerhetskänslig verksamhet
7. Besök och utländska delegationer
8. Avlyssningsskyddade utrymmen

Säkerhetspolisen

Box 12312, 102 28 Stockholm
010-568 70 00 | sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se