Vägledning i säkerhetsskydd

Introduktion till säkerhetsskydd

Juni 2019

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

Innehåll

1 Introduktion

Denna vägledning är den första i Säkerhetspolisens serie av vägledningar som riktar sig till den som i sitt arbete eller i andra sammanhang kommer i kontakt med säkerhetsskydd. Syftet med vägledningarna är att förklara krav samt tydliggöra betydelsen av begrepp som förekommer inom säkerhetsskydd och i förlängningen bidra till ett säkrare Sverige.

Regelverket för säkerhetsskydd är omfattande och spänner över flera områden. Säkerhetspolisen har utöver denna introduktion gett ut ett antal detaljerade vägledningar enligt nedan.

- **Säkerhetsskyddsanalys**
  Vägledning och metodstöd för genomförande av säkerhetsskyddsanalys med tillhörande områden såsom identifiering av skyddsvärden, hotbild och dimensionerande hotbeskrivning samt sårbarhetsanalys och säkerhetsskyddsplan.

- **Informationssäkerhet**
  Vägledning kring informationssäkerhet, säkerhetsskyddsklassificerade uppgifter och handlingar samt skyldigheten att i vissa fall samråda med Säkerhetspolisen inför driftsättning och förändring av informationssystem.

- **Fysisk säkerhet**
  Vägledning om hur den fysiska säkerheten ska utformas med upptäckande, försvårande och hanterande skyddsåtgärder samt övergripande principer för en robust och tålig fysisk säkerhet som är i paritet med hotbild och dimensionerande hotbeskrivning.

- **Personalsäkerhet**
  Vägledning kring säkerhetsprövningsprocessen. I vägledningen förtydligas de olika delarna såsom grundutredning, registerkontroll och särskild personutredning samt utbildning.

- **Säkerhetsskyddad upphandling**
  Vägledning kring processen för säkerhetsskyddad upphandling, skyldigheten att i vissa fall samråda med Säkerhetspolisen vid upphandling med säkerhetsskyddsavtal.

1.1 Läsanvisning

Denna vägledning är utformad som en introduktion för att beskriva grundläggande delar och centrala begrepp inom säkerhetsskydd. Vägledningen inleds med översiktliga beskrivningar som följs av fördjupning av begrepp. Vissa förkunskaper behövs för att läsaren fullt ut ska kunna ta till sig innehållet. För den som är helt ny på området kan det krävas flera genomläsningar parallellt med inläsning av relevant lagstiftning.

Text som skrivs med kursiv stil tillsammans med en hänvisning markerar begrepp som är av central karaktär och som utvecklas senare i texten samt i vissa fall i de separata vägledningarna.

I inledningen till vissa avsnitt finns hänvisning till relevanta författningar. Läsaren uppmanas att ha säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2018:658) och Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd tillgängliga som stödmaterial.

2 Vad är säkerhetsskydd?

I Sverige finns mycket som är värt att skydda, till exempel demokrati, rättsväsende, åsiktsfrihet, liv och hälsa samt mänskliga rättigheter. Samtidigt finns många typer av hot i form av främmande stater, organisationer och personer som är beredda att använda våld, spionera eller begå andra brott för att orsaka stora skador på det skyddsvärda och komma över känsliga uppgifter. Säkerhetsskydd är skydd av *säkerhetskänslig verksamhet* mot denna typ av antagonistiska handlingar och skydd även i andra fall av *säkerhetsskyddsklassificerade uppgifter.*

Säkerhetskänslig verksamhet är sådan verksamhet som är av betydelse för *Sveriges säkerhet* eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Uttrycket Sveriges säkerhet tar sikte på sådant som är av grundläggande betydelse för Sverige såsom försvaret, det demokratiska statsskicket, rättsväsendet och samhällsviktig verksamhet som är av betydelse ur ett nationellt perspektiv. 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.

Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av den lagen om den varit tillämplig i den aktuella verksamheten. Genom formuleringen i andra satsen säkerställs att även enskilda verksamhetsutövare (som i regel inte omfattas av offentlighets- och sekretesslagen) ska skydda sådana uppgifter. Detta följer den inom säkerhetsskydd fundamentala principen att skyddet ska vara detsamma oavsett var, hur eller av vem som verksamheten bedrivs.

Säkerhetsskydd kan övergripande beskrivas som ett system av samverkande åtgärder som syftar till att skapa ett heltäckande skydd. Då 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 kan fogas samman på olika sätt för att värna Sveriges säkerhet och det Sverige åtagit sig att skydda åt andra stater och mellanfolkliga organisationer.

Figur 1: Säkerhetsskydd syftar till att värna Sveriges säkerhet och internationella åtaganden

2.1 Säkerhetskydds-analys är grunden för säkerhetsskydd

2 kap. 1 § säkerhetsskyddslagen
2 kap. 1 § säkerhetsskyddsförordningen

Säkerhetsskyddet måste vara heltäckande vilket kan innebära ökade kostnader, minskad effektivitet och ökad administration. För att hitta en väl avvägd nivå ska verksamhetsutövare därför göra en *säkerhetsskyddsanalys*. Utifrån säkerhetsskyddsanalysen implementeras säkerhetsskyddet i form av åtgärder som struktureras i en säkerhetsskyddsplan.

Även om verksamheten är liten kan processen för att genomföra och uppdatera en säkerhetsskyddsanalys vara omfattande.

Säkerhetsskyddsanalysen kan övergripande sammanfattas i tre frågor:

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

Vikten av en väl genomförd och regelbundet uppdaterad säkerhetskyddsanalys kan inte nog betonas. Säkerhetsskyddsanalysen är fundamentet för säkerhetsskyddsarbetet och central för att utforma och över tid upprätthålla säkerhetsskyddsåtgärder. En säkerhetsskyddsanalys utgår från konsekvenserna av en möjlig händelse och arbetet med den skiljer sig därför något från sannolikhetsbaserade analyser. Säkerhetspolisens vägledning *Säkerhetsskyddsanalys* innehåller djupare förklaringar av centrala begrepp och ett metodstöd för att genomföra analysprocessen.

Figur 2: Processen för säkerhetsskyddsanalys är cyklisk och kan sammanfattas med tre korta frågor.

3 Varför behövs säkerhets-skydd?

Säkerhetsskydd behövs för att skydda säkerhetskänsliga verksamheter mot olika typer av antagonistiska handlingar från hotaktörer med varierande *avsikt* och *förmåga.*

Det allvarligaste hotet kommer från främmande makt med avsikt att påverka Sverige som oberoende nation. Förmågan hos främmande makt kan vara mycket hög och kombinerad med ett långsiktigt tidsperspektiv. Förmågan kan bestå i 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 men det kan även riktas mot verksamheter som på andra sätt har betydelse för Sveriges säkerhet. I fredstid bedriver främmande stater och organisationer främst påverkansoperationer och olovlig underrättelseverksamhet genom att inhämta information kopplat till myndigheter och bolags verksamhet, personal, organisering, kris- och krigsberedskap samt fysisk och teknisk infrastruktur.

Inhämtningen av information sker genom öppna källor som webbplatser, årsredovisningar, rapporter och allmänna handlingar samt genom att inleda olika typer av samarbeten och delta i upphandlingar. Inhämtning sker även genom rekrytering av informationslämnare, infiltration, avlyssning av rum och telefoner samt olika former av dataintrång i informationssystem, smarta telefoner och andra elektroniska system. Även sabotage och andra typer av brott såsom inbrott förekommer för att testa nivån av säkerhetsskydd och förmågan att hantera störningar samt för att komma över information.

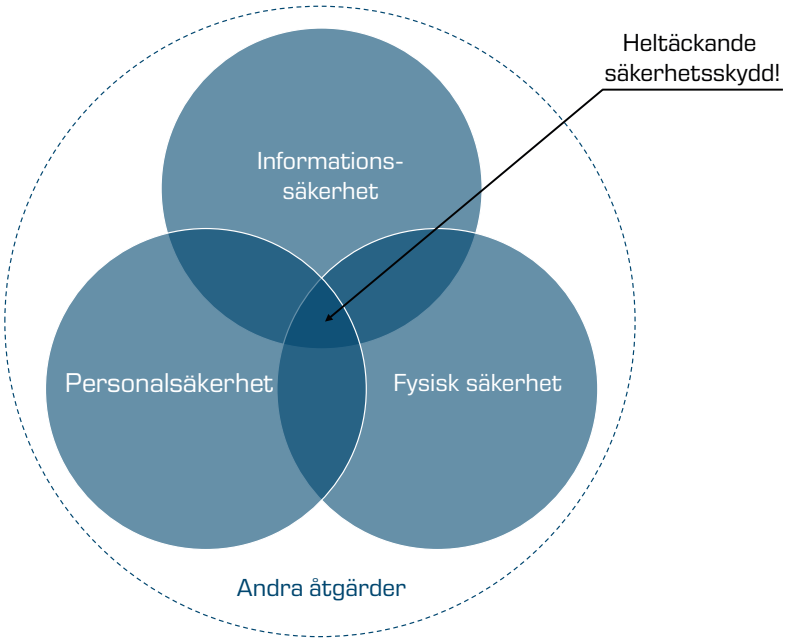
Utöver främmande makt utgör även ideologiskt motiverade grupper och personer ett hot. De kan utföra antagonistiska handlingar riktade mot myndigheter, institutioner, bolag och individer. Avsikten varierar starkt och kan exempelvis vara att som en del av en ideologisk eller religiös agenda påverka Sveriges inriktning i politiska frågor. Avsikten kan även vara mer specifik såsom att påverka rättssystemet, förtroendevalda eller myndighetsutövning i sakfrågor. Förmågan hos denna typ av hotaktörer varierar kraftigt, och hotet de utgör kan medföra skada för Sveriges säkerhet på både kort och längre sikt.

4 Hur fungerar säkerhets-skydd?

Säkerhetsskydd kan som inledningsvis nämnts beskrivas som ett system av åtgärder som utifrån säkerhetsskyddsanalysen tillsammans skyddar den säkerhetskänsliga verksamheten. Merparten av åtgärderna inom säkerhetsskydd kan sorteras in i någon av de tre säkerhetsskyddsåtgärderna *informationssäkerhet*, *fysisk säkerhet* och *personalsäkerhet*, se 11 *Säkerhetsskyddsåtgärder* och separata vägledningar för fördjupning. Andra åtgärder som ingår i systemet av säkerhetsskydd är exempelvis säkerhetsskyddsavtal med leverantörer och anmälan av säkerhetshotande händelser.

En grundförutsättning för ett heltäckande säkerhetsskydd är samspelet mellan olika typer av åtgärder som överlappar varandra, se figur 3. Exempelvis räcker det inte att enbart skydda ett informationssystem med informationssäkerhet 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 ur säkerhetssynpunkt får arbeta med systemet.

Utöver samspelet måste hela kedjan av åtgärder vara jämnstark så att det inte finns några svaga länkar. Om exempelvis personal reser med säkerhetsskyddsklassificerade uppgifter mellan arbetsplatser måste transporten regleras så den inte utgör en sårbarhet. I annat fall kan en angripare utnyttja detta och slå till på en plats där nivån av säkerhetsskydd är lägre än på arbetsplatserna.



Figur 3: Det är bara när samtliga säkerhetsskyddsåtgärder samspelar och överlappar varandra som verksamheten har ett heltäckande skydd.

4.1 Skillnaden mellan säkerhetsskydd och andra säkerhetsåtgärder

1 kap. 2 § säkerhetsskyddslagen

Utöver behovet av säkerhetsskydd försöker de flesta verksamheter skydda sig mot allehanda risker för att inte drabbas av exempelvis produktionsavbrott. I många fall är skyddet inriktat på olyckor, men det kan även i likhet med säkerhetsskydd ta höjd för antagonistiska handlingar såsom anlagda bränder eller industrispionage. Säkerhetsskyddet och andra säkerhetsåtgärder kan mycket väl sammanfalla men det är i så fall viktigt att klargöra vilka perspektiv som är grunden för respektive åtgärd.

Säkerhetsåtgärder som utgår från verksamhetens egna krav och incitament är valfria, medan skyddet av det som faller inom ramen för säkerhetsskydd är tvingande genom lag. Denna skillnad i perspektiv påverkar det grundläggande arbetet med analyser och efterföljande val av åtgärder och hur omfattande dessa behöver vara. I exempelvis en affärsriskanalys kan den bedömda sannolikheten för olika händelser vägas mot kostnaden för åtgärder och vilka möjliga förluster organisationen är beredd att acceptera. I en säkerhetsskyddsanalys beaktas inte sannolikheten, utan utgångspunkten är istället de konsekvenser som måste undvikas. Utrymmet att själv välja vad som är en lagom skyddsnivå är begränsat eftersom principen är att skyddet för en säkerhetskänslig verksamhet ska vara detsamma oavsett vem som är verksamhetsutövare.

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. En vanlig brandskyddsåtgärd är att installera sprinklersystem som automatiskt ska detektera och släcka bränder. Dessa system är dock verkanslösa mot en angripare som först kan stänga av vattentillförseln och därefter anlägga en brand. För att sprinklersystemet ska kunna vara en säkerhetsskyddsåtgärd krävs att det avsiktliga perspektivet beaktas så att systemet även skyddas mot sabotage.

Det finns vissa åtgärder som är förbehållna säkerhetskänslig verksamhet. Merparten av dessa finns inom personalsäkerhetsområdet i form av de registerkontroller som ska utföras innan och under anställning. Det är med stöd av säkerhetsskyddslagen bara tillåtet att göra dessa registerkontroller på personal som kommer att arbeta i säkerhetskänsliga delar av verksamheten. Med detta perspektiv blir det ännu tydligare hur viktigt det är att hålla isär åtgärder som vidtas med avseende på säkerhetsskydd från verksamhetens övriga behov.

5 Roller och ansvar

7 kap. 1-11 §§ säkerhetsskyddsförordningen
9 kap. 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Då säkerhetsskydd omfattar flera typer av verksamheter hos såväl myndigheter som enskilda finns ett stort antal aktörer med olika roller och ansvar.

Säkerhetspolisen och Försvarsmakten är som tillsynsmyndigheter övergripande ansvariga för att bland annat utöva tillsyn och meddela föreskrifter. Försvarsmakten ansvarar för den egna myndigheten, Fortifikationsverket, Försvarshögskolan samt de myndigheter som ligger under Försvarsdepartementets ansvarsområde. Säkerhetspolisen ansvarar för övriga myndigheter samt kommuner och regioner (f.d. landsting).

Utöver Säkerhetspolisen och Försvarsmakten finns ett antal ytterligare tillsynsmyndigheter vilka redogörs för nedan. Tillsynsmyndigheterna får meddela kompletterande föreskrifter inom sitt respektive ansvarsområde. Därutöver har vissa myndigheter rätt att meddela föreskrifter inom speciella områden, exempelvis Försvarsmakten om kryptografiska funktioner och Regeringskansliet samt Försvarets materielverk om utfärdande av säkerhetsintyg för personer respektive leverantörer.

5.1 Säkerhetspolisens roll

Säkerhetspolisen är Sveriges nationella säkerhetstjänst med ansvar för Sveriges inre säkerhet. En av myndighetens uppgifter är enligt 3 § polislagen (1984:387) att fullgöra uppgifter enligt säkerhetsskyddslagen.

Säkerhetspolisen ansvarar för att utföra registerkontroll vid säkerhetsprövning av de personer vars anställning eller deltagande i säkerhetskänslig verksamhet har placerats i säkerhetsklass. Kontrollen innebär slagning mot bland annat belastningsregistret och misstankeregistret. Registerkontroll beskrivs mer utförligt nedan, se 11.3 *Personalsäkerhet* samt Säkerhetspolisens vägledning *Personalsäkerhet*.

Säkerhetspolisen utövar tillsyn av säkerhetsskydd i syfte att kontrollera att verksamhetsutövare följer lag och annan författning. Vidare har Säkerhetspolisen rätt att meddela föreskrifter inom säkerhetsskyddsområdet och ett uppdrag att lämna råd till Regeringskansliet, Justitiekanslern, riksdagen och dess myndigheter.

När Säkerhetspolisen lämnar råd kan detta till exempel bestå av utbildningar, föreläsningar och tester av säkerhetsskyddsåtgärder. Det är viktigt i sammanhanget poängtera att det alltid är verksamhetsutövaren som har ansvaret för sina skyddsvärden och de åtgärder som vidtas för att skydda dessa.

Säkerhetspolisen har även en central roll att verka som samrådsmyndighet, exempelvis i vissa upphandlingssituationer och vid förändring och idrifttagande av informationssystem, se 13 *Samrådsdialoger.* Vidare är det Säkerhetspolisen som tar emot anmälningar vid säkerhetshotande händelser och verksamhet, bland annat it-incidenter eller om säkerhetsskyddsklassificerade uppgifter kan ha röjts.

5.2 Tillsynsmyndigheternas roll

Utöver de två huvudaktörerna Säkerhetspolisen och Försvarsmakten finns ytterligare ett antal tillsynsmyndigheter som utövar tillsyn över enskilda verksamhetsutövare inom en avgränsad sektor eller ett geografiskt område. Följande myndigheter har ansvar för respektive område:

- Affärsverket Svenska kraftnät: elförsörjning
- Post- och Telestyrelsen (PTS): elektronisk kommunikation och posttjänst
- Transportstyrelsen: civil flygtrafiktjänst, militär flygtrafikledningstjänst och verksamhet som i övrigt är av betydelse för luftfartsskydd, hamnskydd och sjöfartsskydd
- Länsstyrelserna: andra enskilda verksamhetsutövare än de som täcks in av ovanstående myndigheters ansvar

Det bör förtydligas att tillsynsmyndigheterna endast har ansvar för tillsyn av enskilda verksamhetsutövare inkluderat statliga, kommunala och regionala bolag. Säkerhetspolisen utövar tillsyn av tillsynsmyndigheterna samt andra myndigheter som tangerar en sektor, till exempel Trafikverket och Energimyndigheten.

Tillsynen får även utövas hos leverantörer som omfattas av ett säkerhetsskyddsavtal och hos enskilda verksamhetsutövare som leverantören i sin tur anlitat inom ramen för avtalet.

I det fall en tillsynsmyndighet vid tillsyn upptäcker allvarliga brister som trots tidigare påpekanden inte rättats till ska myndigheten informera Säkerhetspolisen och Försvarsmakten.

Undantag från informationsplikten finns gällande vissa verksamhetsutövare som är leverantörer. För fördjupning om säkerhetsskyddsavtal och tillsyn av leverantörer, se Säkerhetspolisens vägledning *Säkerhetsskyddad upphandling*.

Säkerhetspolisen och Försvarsmakten kan utöva tillsyn även i de fall en verksamhet sorterar under en tillsynsmyndighets ansvarsområde.

Tillsynsmyndigheterna har utöver tillsyn ett ansvar för rådgivning och är den huvudsakliga kontakten för enskilda verksamhetsutövare vid frågor om säkerhetsskydd och tillämpning av bestämmelser. Det är tillsynsmyndigheterna som beslutar om placering i säkerhetsklass för enskilda verksamhetsutövare, se Säkerhetspolisens vägledning *Personalsäkerhet.* Tillsynsmyndigheterna har även rätt att efter samråd med Säkerhetspolisen medge undantag från Säkerhetspolisens föreskrifter om säkerhetsskydd och inom respektive område meddela ytterligare kompletterande föreskrifter.

5.3 Verksamhetsutövarens ansvar

2 kap. 1 § säkerhetsskyddslagen

Den som bedriver säkerhetskänslig verksamhet har grundläggande skyldigheter att utreda behovet av säkerhetsskydd, planera och vidta säkerhetsskyddsåtgärder samt kontrollera det egna säkerhetsskyddet. Det finns dock 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 lagreglerade

områden, varje verksamhetsutövares egna ansvar att hålla sig informerad, göra bedömningar och bedriva sin verksamhet enligt de författningar som gäller på säkerhetsskyddsområdet.

Arbetet med säkerhetsskydd behöver inledas med ett aktivt ställningstagande om huruvida 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, se 2.1 *Säkerhetsskyddsanalys är grunden för säkerhetsskydd*. I Säkerhetspolisens vägledning *Säkerhetsskyddsanalys* finns ett antal indikatorer att använda som grund för en initial bedömning.

För den som bedriver säkerhetskänslig verksamhet är ansvaret långtgående. Verksamhetsutövaren ska planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter. Om säkerhetskänslig verksamhet utkontrakteras sträcker sig ansvaret även utanför den egna organisationen, i och med behovet av att reglera och kontrollera säkerhetsskyddet hos den anlitade leverantören.

Även om verksamhetsutövarens ansvar är långtgående finns en stor frihet att utforma och bedriva säkerhetsskyddsarbetet på det sätt som passar den egna organisationen. Huvudsaken är att en adekvat nivå av säkerhetsskydd uppnås enligt principen att skyddet bör vara detsamma oavsett var, hur och av vem som verksamheten bedrivs.

6 Ansvarsbestämmelser och tystnadsplikt

5 kap. 1-2 §§ säkerhetsskyddslagen
2 kap. 4 § säkerhetsskyddsförordningen

Inom säkerhetsskyddslagstiftningen finns flera krav på åtgärder och aktiviteter som verksamhetsutövare ska utföra i syfte att värna Sveriges säkerhet och internationella åtaganden. I nuläget saknas dock sanktioner som är direkt kopplade till säkerhetsskyddslagen. Däremot kan bristande hantering av säkerhetsskyddsklassificerade uppgifter, även utan uppsåt, i vissa fall leda till straffansvar enligt bestämmelserna i 19 kap. brottsbalken om brott mot Sveriges säkerhet, 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. Brott mot tystnadsplikten är straffsanktionerat genom 20 kap. 3 § brottsbalken.

För säkerhetskänslig verksamhet som bedrivs i offentlig regi 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 skyddet ska vara detsamma oavsett var, hur och av vem som verksamheten bedrivs. Tystnadsplikten och vikten av att utbilda och informera om denna beskrivs mer ingående i Säkerhetspolisens vägledningar *Personalsäkerhet* respektive *Säkerhetsskyddad upphandling.*

7 Säkerhetsskyddslagen och NIS-direktivet

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, se 4.1 *Skillnaden mellan säkerhetsskydd och andra säkerhetsåtgärder*, innebära såväl utmaningar som möjligheter till synergieffekter. Verksamhetsutövare bör därför på ett eller annat sätt inventera och bedöma vilka lagkrav som ställs på verksamheten för att få en samlad bild och kunna skapa ett effektivt säkerhetsskydd.

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 otillbörligt tillträde i hamnar och på kärnkraftverk. I andra fall finns motstridiga syften som måste uppfyllas, exempelvis krav på lättframkomliga framkörningsvägar för räddningstjänst kontra behovet av hinder som skydd mot attacker med fordon. I vissa fall finns gränsdragningar och undantag inskrivna i lagarna vilket gör det tydligt om ett krav står över ett annat. Ett sådant exempel är de regler som implementerats i svensk rätt till följd av det så kallade NIS-direktivet.

7.1 NIS-direktivet

8 § Lag (2018:1174) om informationssäkerhet i samhällsviktiga och digitala tjänster

NIS-direktivet är den vardagliga benämningen på det inom EU gällande *Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och infrastruktur i hela unionen* som syftar till att förbättra den inre marknadens funktion. I Sverige har NIS-direktivet implementerats genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen gäller för leverantörer inom sju sektorer som tillhandahåller samhällsviktiga tjänster som är centrala för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet samt vissa leverantörer av digitala tjänster. Genom lagen ställs krav på bland annat skydd av informationssystem och incidentrapportering till Myndigheten för samhällsskydd och beredskap (MSB).

Verksamhetsutövare i de sju sektorerna eller verksamhetsutövare som levererar digitala tjänster bedriver i vissa fall även säkerhetskänslig verksamhet vilket skapar en potentiell konfliktsituation med krav från olika lagar. Det finns dock ett undantag i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, som gör att den lagen inte gäller för verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen. Denna gränsdragning kräver särskild uppmärksamhet av verksamhetsutövare som endast till någon del bedriver säkerhetskänslig verksamhet. Vissa delar av verksamheten kan då omfattas av kraven på säkerhetsskydd och andra delar av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Detta är viktigt att beakta vid exempelvis anmälan av säkerhetshotande händelser så att känslig information om en sårbarhet i informationssystem kommuniceras på ett tillräckligt säkert sätt och till rätt myndighet.

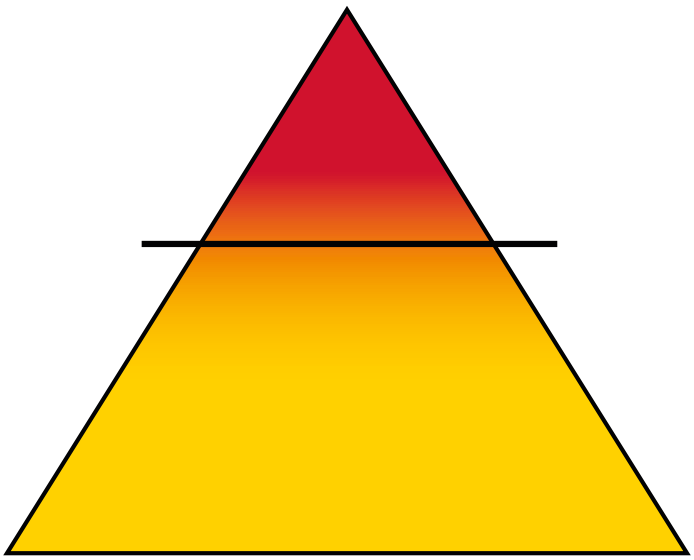
8 Sveriges säkerhet

Säkerhetsskydd har traditionellt uttryckts som olika åtgärder för att skydda totalförsvaret eller *rikets säkerhet* i övrigt. Uttrycket rikets säkerhet är i säkerhetsskyddslagen numera ersatt av *Sveriges säkerhet* men liksom tidigare finns ingen definition i lag. Uttrycket förekommer dock även i annan lagstiftning och kan sammanfattas som Sveriges oberoende – i betydelsen självständighet och suveränitet – och bestånd. Detta innefattar rätt till okränkta landsgränser, ett bevarande av det svenska självstyret och det demokratiska statsskicket samt av nationens grundläggande funktionalitet.

Såväl myndigheter som enskilda driver ett stort antal samhällsviktiga verksamheter som i helhet eller delar kan vara av större eller mindre betydelse. Detta brukar illustreras med en pyramid där den röda toppen utgörs av de verksamheterna som är av betydelse för Sveriges säkerhet ur ett nationellt perspektiv, se figur 4. Dessa verksamheter har ett kvalificerat skyddsbehov och omfattas av säkerhetsskyddslagen.

Uttrycket Sveriges säkerhet tar alltså sikte på sådant som är av grundläggande betydelse för Sverige. I detta ingår bland annat det militära och civila försvaret, den nationella ekonomin, de brottsbekämpande myndigheterna, domstolarna och sådana leveranser av exempelvis livsmedel, elkraft, dricksvatten och drivmedel som är nödvändiga för samhällets funktionalitet på nationell nivå.

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 datasystem och mobiltelefoni. Av denna anledning är det viktigt att verksamhetsutövare med regelbundenhet uppdaterar sin säkerhetsskyddsanalys och bedriver ett fortlöpande säkerhetsskyddsarbete.



Figur 4: Pyramidens topp utgörs av verksamheter, eller delar av verksamheter, som behöver säkerhetsskydd.

9 Säkerhetskänslig verksamhet

1 kap. 1 § säkerhetsskyddslagen

Säkerhetsskyddslagen gäller för den som till någon del bedriver en 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 således såväl militär som civil verksamhet och är oberoende av om verksamheten bedrivs av det offentliga eller av enskilda aktörer. Inom många verksamheter är endast en viss del, tillgång eller funktion av betydelse för Sveriges säkerhet. Verksamhetsutövaren måste då noggrant analysera vilka delar som är säkerhetskänsliga så att säkerhetsskyddsåtgärderna inte görs onödigt omfattande men inte heller missar delar som omfattas av säkerhetsskyddslagens krav.

Utgångspunkten är att verksamheten ska ha direkt betydelse för Sveriges säkerhet men även verksamhetsutövare som till exempel levererar driftstjänster såsom data- och telekommunikation, kan anses bedriva verksamhet som är av betydelse för Sveriges säkerhet. Det kan då vara den samlade betydelsen som indirekt aktualiserar behovet av säkerhetsskydd även om de enskilda uppdragen sedda var och en för sig inte är säkerhetskänsliga.

Den som hanterar säkerhetsskyddsklassificerade uppgifter, se 10 *Skyddsvärda uppgifter*, anses redan på den grunden bedriva säkerhetskänslig verksamhet eftersom uppgifterna i sig är av betydelse för Sveriges säkerhet. Detta oavsett om uppgifterna rör den egna verksamheten eller härrör från någon annan verksamhetsutövare, till exempel vid arkivförvaring av handlingar. Även verksamheter som hanterar allmänt åtkomlig information såsom meteorologiska data och kartor kan vara säkerhetskänsliga. Uppgifterna kan exempelvis behöva vara tillgängliga för nationell flygtrafikledning eller olika former av beredskap för reparationer av nationellt viktig infrastruktur.

De internationella åtagandena om säkerhetsskydd som staten Sverige har åtagit sig omfattar 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. Därutöver har Sverige även andra internationella åtaganden gällande exempelvis luftfartsskydd. Verksamheter som omfattas av sådana åtaganden är att anse som säkerhetskänsliga. Det förekommer att myndigheter vid samarbete med utländska myndigheter självständigt kommer överens om olika typer av skyddsåtgärder. Denna typ av egna överenskommelser gör dock inte att verksamheten omfattas av säkerhetsskyddslagen.

Själva bedömningen av om en verksamhet är säkerhetskänslig eller inte har sin grund i verksamhetens säkerhetsskyddsanalys, se 2.1 *Säkerhetsskyddsanalys 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. För dessa moment har Säkerhetspolisen gett ut en separat vägledning, *Säkerhetsskyddsanalys*, där nedanstående begrepp används och utvecklas.

9.1 Konsekvenskategorier

2 kap. 2 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Verksamhetsutövare ska identifiera anläggningar, objekt, system eller liknande verksamhet som har betydelse för Sveriges säkerhet utifrån vilken typ av skada en antagonistisk handling direkt eller uppenbart indirekt skulle kunna medföra. Identifieringen ska göras enligt följande *konsekvenskategorier*:

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 i form av det demokratiska statsskicket, rättsväsendet och den brottsbekämpande förmågan på nationell nivå. Säkerhetsskyddet för Sveriges inre säkerhet handlar till stor del om att skydda särskilt kritiska anläggningar, funktioner och informationssystem.

Skada på nationellt samhällsviktig verksamhet

Verksamheter som rör leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet på nationell nivå. Dessa verksamheter finns ofta inom, men är inte begränsat till, sektorerna energiförsörjning, livsmedelsförsörjning, elektroniska kommunikationer, vattenförsörjning, 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.

9.2 Konsekvensnivåer

2 kap. 3 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Säkerhetskänslig verksamhet som identifierats tillhöra en konsekvenskategori enligt ovan ska därefter graderas utifrån nedan *konsekvensnivåer* beroende på hur allvarlig skada en antagonistisk handling skulle kunna medföra. Till skillnad från konsekvenskategori kan en verksamhet som helhet bara tillhöra en konsekvensnivå. Om verksamheten återfinns i flera konsekvenskategorier väljs den konsekvensnivå där den potentiella graden av skada för Sveriges säkerhet är som störst.

Indelningen sker enligt följande konsekvensnivåer:

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

Verksamheter som vid ett angrepp endast bedöms kunna medföra skada enligt nivå 1 omfattas inte av kraven på säkerhetsskydd. De verksamheter som bedöms tillhöra konsekvensnivåerna 4 och 5 benämns *särskilt säkerhetskänslig verksamhet* och omfattas av särskilda bestämmelser enligt nedan.

9.3 Särskilt säkerhetskänslig verksamhet

2 kap. 6 och 8 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd

Verksamhet som tillhör de ovannämnda konsekvensnivåerna 4 och 5 benämns som särskilt säkerhetskänsliga verksamheter och omfattas av två särskilda krav:

- rapportering till tillsynsmyndighet
- dimensionering med hjälp av dimensionerande hotbeskrivning (DHB)

Verksamhetsutövare som bedriver särskilt säkerhetskänslig verksamhet ska rapportera till respektive tillsynsmyndighet, se 5 *Roller och ansvar*, att sådan verksamhet bedrivs. Syftet med rapporteringen är att tillsynsmyndigheterna ska kunna ha en samlad bild över vilka verksamhetsutövare som är verksamma inom respektive tillsynsmyndighets ansvarsområde. Detta så att såväl tillsyn och rådgivning ska kunna prioriteras för de verksamheterna som är av störst betydelse för Sveriges säkerhet. De verksamhetsutövare som står direkt under Säkerhetspolisens tillsynsansvar ska rapportera dit, se vidare information på Säkerhetspolisens webbplats.

Säkerhetspolisen tar i samråd med tillsynsmyndigheterna fram dimensionerande hotbeskrivningar (DHB) till de verksamhetsutövare som bedriver särskilt säkerhetskänslig verksamhet. En DHB syftar till att ge en långsiktigt hållbar beskrivning av en antagen angripares förmåga, oberoende av om det för stunden föreligger ett konkret hot mot verksamheten. Verksamhetsutövaren ska använda den tillhandahållna DHB:n för att dimensionera sitt säkerhetsskydd vilket innebär att DHB i praktiken utgör en lägstanivå för vad säkerhetsskyddet ska klara av att skydda mot. Ytterligare beskrivning av DHB finns i Säkerhetspolisens vägledning *Säkerhetsskyddsanalys.*

10 Skyddsvärda uppgifter

Verksamhetsutövare som bedriver säkerhetskänslig verksamhet har uppgifter som är skyddsvärda ur olika perspektiv. I detta kapitel beskrivs bland annat vilka uppgifter som är att anse som *säkerhetsskyddsklassificerade* samt ett förslag på arbetsflöde för bedömning av uppgifter. Ytterligare vägledning finns i Säkerhetspolisens vägledning *Informationssäkerhet*.

10.1 Säkerhetsskyddsklassificerade uppgifter

1 kap. 2 § säkerhetsskyddslagen

Inom offentlig verksamhet är säkerhetsskyddsklassificerade uppgifter sådana uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400). Offentlighets- och sekretesslagen 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 offentlighets- och sekretesslagen om den hade varit tillämplig.

För att bedöma om en uppgift är säkerhetsskyddsklassificerad behöver alltså enskilda verksamhetsutövare i praktiken göra en fiktiv sekretessprövning liknande 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 § i offentlighets och sekretesslagen (försvarssekretess). Men även andra sekretessbestämmelser kan vara tillämpliga på uppgifter som rör säkerhetskänslig verksamhet, exempelvis 15 kap. 1 § (utrikessekretess), 18 kap. 1 § (förundersökningssekretess), 18 kap. 2 § (sekretess i underrättelseverksamhet) och 18 kap. 8 § (säkerhets- och bevakningsåtgärder).

För att uppgifter ska anses vara säkerhetsskyddsklassificerade måste de röra säkerhetskänslig verksamhet och omfattas av någon sekretessbestämmelse i offentlighets- och sekretesslagen. Det är viktigt att komma ihåg att båda två kriterierna måste vara uppfyllda. Nedan följer två exempel på när så inte är fallet:

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

Exempel 2. Ett företag som levererar kommunikationsutrustning till Försvarsmakten har även ett patent på teknologi som används inom vanlig mobiltelefoni. Patentet går att köpa på öppna marknaden så om det röjs kan det inte anses orsaka någon skada på Sveriges säkerhet. Men, om patentet fanns hos en myndighet skulle det omfattats av sekretess för att skydda företagets ekonomiska intressen. Då patentet inte rör den säkerhetskänsliga delen av företagets verksamhet är det inte heller att anse som en säkerhetsskyddsklassificerad uppgift.

Observera att uppgifter som rör säkerhetskänslig verksamhet utan att vara säkerhetsskyddsklassificerade ändå kan omfattas av kraven på säkerhetsskydd. Detta ifall uppgifterna behöver vara riktiga (i bemärkelsen oförändrade) och/eller tillgängliga, exempelvis meteorologiska data och kartor som är nödvändig för nationell flygledning, se Säkerhetspolisens vägledning *Säkerhetsskyddsanalys* för fördjupning. Verksamheten är då beroende av uppgifterna på samma sätt som den är beroende av personal, lokaler, kraftförsörjning etc. och därför ska uppgifterna skyddas mot antagonistiska handlingar.

10.2 Indelning av säkerhetsskyddsklassificerade uppgifter

2 kap. 5 § säkerhetsskyddslagen

Säkerhetsskyddsklassificerade uppgifter ska delas in i en av fyra s*äkerhetsskyddsklasser* utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelning ska ske enligt följande:

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

Bestämmelserna i säkerhetsskyddslagen, säkerhetsskyddsförordningen och Säkerhetspolisens föreskrifter om säkerhetsskydd utgår inte sällan från vilken säkerhetsskyddsklass de aktuella uppgifterna har. Det är därför viktigt med tydliga rutiner för klassificeringen av uppgifter. Exempel på sådana bestämmelser är de om logisk och fysisk separation av informationssystem i 3 kap. 20-21 §§ Säkerhetspolisens föreskrifter (2009:2) om säkerhetsskydd, se Säkerhetspolisens vägledning *Informationssäkerhet*.

Skyddet av säkerhetsskyddsklassificerade uppgifter behöver hålla en jämn nivå oavsett i vilken verksamhet de förekommer. Därför bör den som tar emot en säkerhetsskyddsklassificerad uppgift från en annan verksamhetsutövare som utgångspunkt godta dennes klassificering samt kommunicera om lämpliga skyddsåtgärder. För uppgifter i säkerhetskyddsklass *kvalificerat hemlig* finns särskilda krav, se 13.5 *Samråd vid sänkning av säkerhetsskyddsklass.*

10.3 Uppgifter som omfattas av internationella åtaganden om säkerhetsskydd

2 kap. 5 § säkerhetsskyddslagen

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 varierar mellan olika länder beroende på den nationella lagstiftningen, vilket innebär att det inte finns en enhetlig internationell nomenklatur för de olika säkerhetsskyddsnivåerna. 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 säkerhetsskyddsöverenskommelser publiceras normalt på regeringens webbplats under Sveriges internationella överenskommelser (SÖ).

Som exempel kan nämnas de olika säkerhetsskyddsklasserna inom EU med de svenska motsvarigheterna inom parantes:

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

10.4 Arbetsflöde för bedömning av uppgifter

Vid bedömning och klassificering av uppgifter kan nedanstående arbetsflöde användas, se figur 5. Ordningen på de fem stegen är avsedda att underlätta arbetet genom att i ett tidigt skede sålla bort så många uppgifter som möjligt från vidare bedömning.

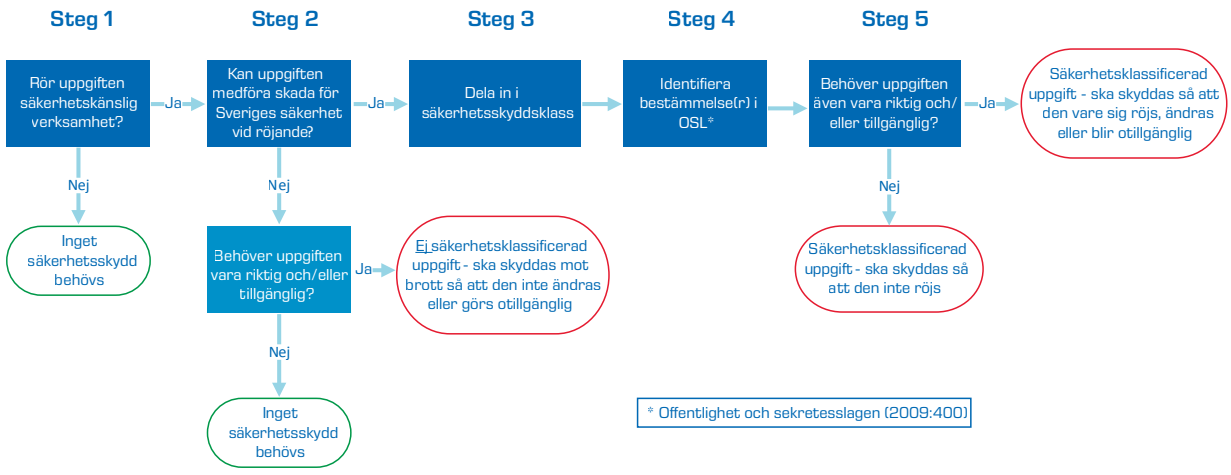
I första steget görs en bedömning av om uppgiften över huvud taget rör säkerhetskänslig verksamhet. För den som endast till någon del bedriver säkerhetskänslig verksamhet innebär detta att många uppgifter kommer falla utanför kraven på säkerhetsskydd.

I det andra steget bedöms om ett röjande av uppgiften kan medföra skada för Sveriges säkerhet. Flertalet uppgifter, såsom tidigare exempel med meteorologiska data, behöver inte skyddas mot att röjas och är därmed inte säkerhetsskyddsklassificerade uppgifter. Uppgifterna kan dock fortfarande behöva vara riktiga (i bemärkelsen oförändrade) och/eller tillgängliga, vilket medför att de ändå omfattas av kraven på säkerhetsskydd.

I det tredje steget delas uppgiften in i en säkerhetsskyddsklass utifrån den skada ett röjande av uppgiften kan medföra för Sveriges säkerhet.

I det fjärde steget identifieras sekretessbestämmelser i offentlighets- och sekretesslagen som är, eller skulle varit, tillämplig på uppgiften. Om ett röjande av uppgiften skulle medföra skada för Sveriges säkerhet så kommer uppgiften i princip alltid att omfattas av en eller flera sekretessbestämmelser.

I det femte och avslutande steget görs bedömningen om uppgiften även behöver vara riktig och/eller tillgänglig eller om den endast behöver skyddas mot att röjas såsom kan vara fallet med exempelvis kopior och arbetsmaterial.



Figur 5: Exempel på arbetsflöde för bedömning av uppgifter

Ordningen i arbetsflödet kan sorteras om för att bättre passa verksamhetsutövarens övriga processer. I de flesta verksamheter finns dock fler uppgifter som omfattas, eller skulle ha omfattats, av sekretess än det finns uppgifter som kan skada Sveriges säkerhet om de röjs. Den föreslagna ordningen med steg två före fyra är då att föredra.

Arbetsflödet kan även utvidgas till att omfatta andra perspektiv, exempelvis interna informationssäkerhetsklasser i en företagskoncern.

Observera att arbetsflödet är avsett för bedömning av enskilda uppgifter och inte för aggregerad eller ackumulerade uppgifter, se Säkerhetspolisens vägledning *Informationssäkerhet* för mer information om bedömning av sådana.

11 Säkerhetsskyddsåtgärder

2 kap. 2-4 §§ säkerhetsskyddslagen

Som inledningsvis nämnts kan säkerhetsskydd övergripande beskrivas som ett system av samverkande åtgärder som syftar till att skapa ett heltäckande skydd.

Merparten av åtgärderna inom säkerhetsskydd kan sorteras in i något av de tre huvudområdena *informationssäkerhet, fysisk säkerhet och personalsäkerhet* vilka här förklaras översiktligt. Säkerhetsskyddslagen benämner dessa tre områden *säkerhetsskyddsåtgärder* och för respektive område har Säkerhetspolisen gett ut specifika vägledningar.

11.1 Informationssäkerhet

2 kap. 2 § säkerhetsskyddslagen

Alla verksamheter är beroende av att kunna inhämta, lagra, bearbeta och kommunicera information i olika former. Den tekniska utvecklingen har på senare år gjort informationssystem till viktiga verktyg i hanteringen, men även pappersdokument används fortfarande. Säkerhetsskyddsåtgärden informationssäkerhet syftar till att skydda information oavsett form och förekomst, elektronisk såväl som fysisk.

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 gäller säkerhetskänslig verksamhet. I likhet med fysisk säkerhet är informationssäkerhet inte begränsat till tekniska åtgärder utan inkluderar även bland annat rutiner och är beroende av en god personalsäkerhet med relevanta utbildningar.

Säkerhetsskyddsklassificerade uppgifter kan förekomma i pappersform som utskrivna dokument, fotografier, ritningar etc. Informationssäkerhet kan då exempelvis innebära att dokumenten förses med anteckning om aktuell säkerhetsskyddsklass och att förvaring sker på ett betryggande sätt i brandskyddade och låsbara skåp. Behovet av samspel mellan säkerhetsskyddsåtgärder blir tydligt i detta exempel. Personalen som hanterar dokumenten behöver utbildas i anteckningens innebörd och förvaringsskåpen måste dimensionerats 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 informationssystem. De flesta verksamhetsutövare använder e-post och digitala meddelandetjänster för kommunikation samt olika former av dataprogram för textbehandling och dokumenthantering. Informationssystemen kan på detta sätt komma att innehålla stora mängder säkerhetsskyddsklassificerade uppgifter vilket gör dem skyddsvärda. Ett informationssystem behöver dock inte innehålla säkerhetsskyddsklassificerade uppgifter för att vara skyddsvärt. Även informationssystem som till exempel samlar in väderdata till flygledning eller styrsystem på kraftverk kan vara viktiga för säkerhetskänslig verksamhet.

I fråga om informationssystem kan informationssäkerhet exempelvis bestå av att systemen ska separeras från andra informationssystem med logiska funktioner såsom ex. brandväggar som hindrar kommunikation

eller genom att ha fysiskt avskilda nätverk som inte kan kommunicera med varandra eller internet. En vanlig åtgärd är att använda kryptografiska funktioner så kallat signalskydd då säkerhetsskyddsklassificerade uppgifter överförs mellan informationssystem. Då informationssäkerhet inte bara handlar om skydd mot att uppgifter röjs behöver informationssystemen också skyddas mot olika former av hot som är inriktande på att störa eller förstöra och sådana som är inriktade mot att obehörigen ändra informationen. Exempel på sådana säkerhetsskyddsåtgärder kan vara säkerhetskopiering, så kallad backup, för att säkerhetsställa tillgänglighet och digitala signaturer som ett sätt att kontrollera så att uppgifter inte obehörigen ändrats.

11.2 Fysisk säkerhet

2 kap. 3 § säkerhetsskyddslagen

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. Fysisk säkerhet är även en viktig förutsättning för att obehöriga inte på annat sätt ska få insyn i verksamheten eller ta del av säkerhetsskyddsklassificerade uppgifter.

Utformningen av den fysiska säkerheten har sin grund i ett genom säkerhetsskyddsanalysen identifierat säkerhetsskyddsbehov, se figur 6. Den grundläggande principen för fysisk säkerhet utgår från att genom ett system av personal, rutiner, byggnads- och säkerhetsteknik skapa en förmåga att *upptäcka, försvåra* och *hantera* olika typer av angrepp.

Figur 6: Förmågor och beståndsdelar i fysisk säkerhet som fyller ett identifierat säkerhetsskyddsbehov

Det är viktigt att tidigt upptäcka en angripare för att resterande skyddsåtgärder ska vara verksamma. Det är exempelvis ingen större mening med starka dörrar och lås om angriparen har en hel natt på sig att ta sig igenom skyddet. Upptäckande åtgärder kan exempelvis vara bevakningspersonal och larmsystem.

De försvårande åtgärderna delas upp i två kategorier: *Fördröjande* åtgärder som syftar till att uppehålla angriparen så länge att polis eller annan lämplig resurs hinner ingripa. Skadereducerande åtgärder ska minska skadorna av ett angrepp eller underrättelseinhämtning som kan genomföras utan förvarning och ibland inte går att fördröja eller upptäcka, till exempel beskjutning från distans eller avlyssning från en intilliggande byggnad.

För att slutligen kunna stoppa en antagonistisk handling krävs att situationen hanteras. Detta kan exempelvis ske genom att vakter eller polis skrämmer angriparen på flykt eller omhändertar denna. Det är viktigt att de som ska hantera en angripare har rätt utbildning och utrustning 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.

11.3 Personalsäkerhet

2 kap. 4 § säkerhetsskyddslagen

Personalsäkerhet består av två delar, säkerhetsprövning och utbildning. Säkerhetsprövning syftar till att förebygga att personer som inte är pålitliga ur 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 kompetens som deltagandet kräver.

Säkerhetsprövningsprocessen, se figur 7, inleds då någon genom en anställning eller på annat sätt ska delta i en säkerhetskänslig verksamhet. Säkerhetsprövningen görs för att klargöra om en person kan antas vara lojal mot de intressen som ska skyddas och i övrigt pålitlig ur säkerhetssynpunkt. Viktiga aspekter att utreda är eventuella dubbla lojaliteter, intressekonflikter, bristande säkerhetsmedvetandet och andra sårbarheter.

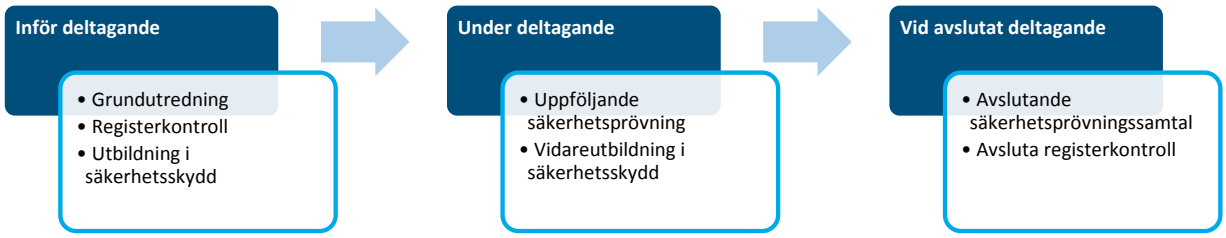
En säkerhetsprövning består av grundutredning och i de flesta fall registerkontroll, samt i vissa fall särskild personutredning. En grundutredning ska omfatta en säkerhetsprövningsintervju, inhämtning och bedömning av betyg, intyg, referenser och övriga uppgifter som är av relevans. Med registerkontroll 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. En särskild personutredning innebär en fördjupad kontroll av exempelvis ekonomiska förhållanden och kontroll av make, maka eller sambo.

Efter den inledande fasen ska säkerhetsprövningsprocessen regelbundet fortgå genom uppföljande säkerhetsprövning, 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 förändringar i livssituation, sociala och ekonomiska förhållanden samt trivsel på arbetsplatsen. Det är viktigt att tidigt uppmärksamma ett upplevt missnöje med arbetssituation och liknande förhållanden som kan tyda på sårbarheter och påverka mottagligheten för yttre påtryckningar. Även olika former av kontaktförsök

eller försök till utpressning kan fångas upp genom en kontinuerlig säkerhetsprövningsprocess. Registerkontroller sker fortlöpande och kan om nya uppgifter tillkommer i register leda till ett så kallat spontanutfall.

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 de fortlöpande registerkontrollerna 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 och inte vara inplacerade i säkerhetsklass. Detta beslut styr i mångt och mycket omfattningen av säkerhetsprövningen. Behörighet att fatta beslut om placering i säkerhetsklass skiljer sig åt beroende på vilken säkerhetsklass 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.



Figur 7: Beståndsdelar i säkerhetsprövningsprocessen

12 Särskild säkerhetsskydds-bedömning

Inom säkerhetsskydd förekommer uttrycket *särskild säkerhetsskyddsbedömning* vid vissa upphandlingar, driftsättning eller ändringar i informationssystem och förändringar i hotbild eller verksamhet. Metoden för att genomföra en särskild säkerhetsskyddsbedömning kan med fördel baseras på den metod som används vid en säkerhetsskyddsanalys, se vidare Säkerhetspolisens vägledning *Säkerhetsskyddsanalys*.

12.1 Statliga myndigheter vid upphandling

2 kap. 6 § säkerhetsskyddsförordningen

Statliga myndigheter ska vid vissa upphandlingar samråda med Säkerhetspolisen, se 13.1 *Samråd för statliga myndigheter vid upphandling* och Säkerhetspolisens vägledning *Säkerhetsskyddad upphandling*. Innan samrådet kan ske ska en särskild säkerhetsskyddsbedömning göras för att identifiera och dokumentera vilka säkerhetsskyddsklassificerade uppgifter eller säkerhetskänsliga informationssystem som leverantören kan få del av och som kräver säkerhetsskydd.

12.2 Inför driftsättning av informationssystem

3 kap. 1 § säkerhetsskyddsförordningen

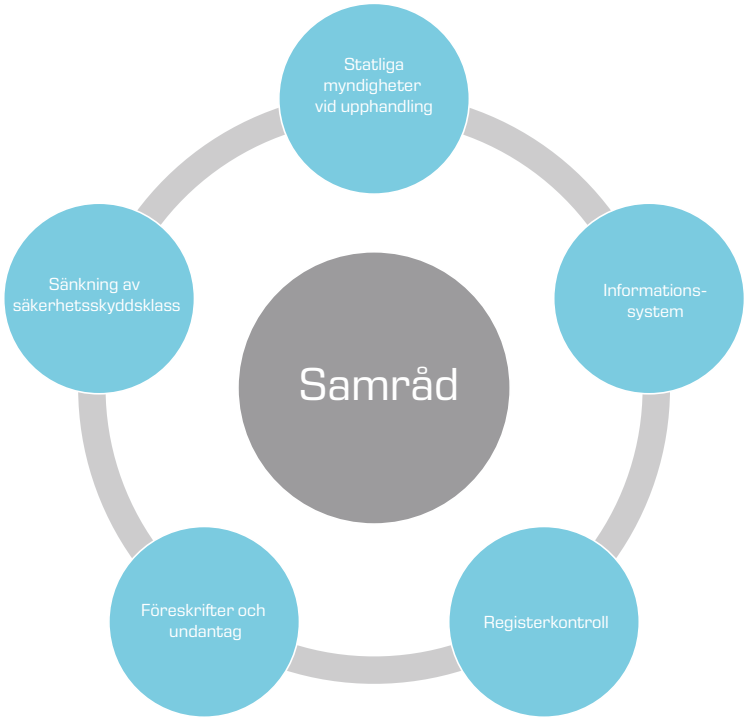
Verksamhetsutövare, oavsett om det är en myndighet eller enskild, ska innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift genomföra och dokumentera en särskild säkerhetsskyddsbedömning. Genom den särskilda säkerhetsskyddsbedömningen ska verksamhetsutövaren ta ställning till vilka säkerhetskrav som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. I vissa fall ska även samråd med Säkerhetspolisen ske, se 13.2 *Samråd gällande informationssystem* och Säkerhetspolisens vägledning *Informationssäkerhet.*

12.3 Vid förändringar av hotbild eller verksamhet

2 kap. 12 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Vid förändringar i hotbilden eller om verksutövaren genomför en förändring som kan antas få betydlig påverkan på verksamheten ska en särskild säkerhetsskyddsbedömning genomföras. En förändring av hotbild kan identifieras av såväl tillsynsmyndigheten som verksamhetsutövaren vid exempelvis säkerhetshotande händelser eller genom omvärldsbevakning. Exempel på förändringarna i verksamheten är upphandlingar, nyetablering, förändringar av säkerhetskänsliga system eller flytt till nya lokaler.

13 Samrådsdialoger



Figur 8: Det finns fem situationer som föranleder samråd

Inom säkerhetsskydd finns fem situationer som medför skyldighet att samråda mellan myndigheter, verksamheter och Säkerhetspolisen, se figur 8. Dessa situationer beskrivs kortfattat nedan tillsamman med hänvisningar till separata fördjupande vägledningar.

13.1 Samråd för statliga myndigheter vid upphandling

2 kap. 6 § säkerhetsskyddsförordningen

Statliga myndigheter som avser genomföra en upphandling som innebär krav på säkerhetsskyddsavtal ska innan förfarandet inleds samråda med Säkerhetspolisen om leverantören kan få:

- tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller högre utanför myndighetens lokaler, eller
- tillgång till säkerhetskänsliga informationssystem utanför myndighetens lokaler och obehörig åtkomst till systemen kan medföra allvarlig skada för Sveriges säkerhet.

Innan samrådet kan ske ska verksamhetsutövaren genomföra en särskild säkerhetsskyddsbedömning, se 12.1 *Statliga myndigheter vid upphandling*, samt ta fram ett utkast på säkerhetsskyddsavtal. Säkerhetspolisen kan inom ramen för samrådet förbjuda myndigheten att genomföra upphandlingen. Mer information om samråd och särskild sä-

kerhetsskyddsbedömning vid upphandling samt säkerhetsskyddsavtal finns i Säkerhetspolisens vägledning *Säkerhetsskyddad upphandling*.

13.2 Samråd gällande informationssystem

3 kap. 2 § säkerhetsskyddsförordningen

Verksamhetsutövare ska i vissa fall skriftligen samråda med Säkerhetspolisen innan ett informationssystem tas i drift eller i väsentliga avseenden förändras. Kravet gäller oavsett om det är en myndighet eller enskild som är verksamhetsutövare.

Samråd ska ske vid driftsättning eller väsentlig förändring av:

- informationssystem som behandlar eller kan komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre
- andra informationssystem om det vid obehörig åtkomst till systemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig

Mer information om samråd gällande informationssystem finns i Säkerhetspolisens vägledning *Informationssäkerhet*

13.3 Samråd och information vid registerkontroll

5 kap. 4 § säkerhetsskyddsförordningen
6 kap. 10 § Säkerhetspolisens föreskrifter om säkerhetsskydd

En tillsynsmyndighet som beslutar om placering i säkerhetsklass eller ansöker om registerkontroll för personal hos en enskild verksamhetsutövare ska vid behov samråda med verksamhetsutövaren i fråga om säkerhetsprövningsåtgärder. Samråd ska ske löpande under hela den tid som deltagandet i den säkerhetskänsliga verksamheten pågår. Det är särskilt viktigt att samråd sker i de fall det vid registerkontroll framkommer uppgifter som kan antas ha betydelse för säkerhetsprövning.

En tillsynsmyndighet kan delegera till en enskild verksamhetsutövare att skicka in ansökningar om registerkontroll direkt till Säkerhetspolisen. Innan delegeringen sker ska tillsynsmyndigheten ge Säkerhetspolisen möjlighet att yttra sig i frågan.

Mer information om samråd vid registerkontroll finns i Säkerhetspolisens vägledning *Personalsäkerhet*.

13.4 Samråd gällande ytterligare föreskrifter och undantag

7 kap. 8 § säkerhetsskyddsförordningen
9 kap. 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd

En tillsynsmyndighet som avser meddela föreskrifter som kompletterar eller ger undantag från bestämmelser i Säkerhetspolisens föreskrifter om säkerhetsskydd ska innan beslut fattas samråda med Säkerhetspolisen. Samrådet är en del i att koordinera kravbilden så att en myndighet inte fattar beslut som leder till en obalans i skyddet för Sveriges säkerhet. Denna obalans kan uppstå om en säkerhetskänslig verksamhet bedrivs i en sektor men påverkar verksamheten i en annan. Så är exempelvis förhållandet i fråga om elförsörjningsverksamhet och elektronisk kommunikation som hanteras av Affärsverket Svenska kraftnät respektive Post- och Telestyrelsen.

13.5 Samråd vid sänkning av säkerhetsskyddsklass

3 kap. 8 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Om det finns skäl att omklassificera en handling med *kvalificerat hemlig* uppgift krävs samråd innan så sker. Samråd ska ske med verksamhetens högsta chef eller motsvarande organ och med den som upprättat handlingen. Anteckning om samrådet ska göras på handlingen. Samråd kan även vara lämpligt i fråga om uppgifter i lägre säkerhetsskyddsklass än kvalificerat hemlig men detta är inget krav. Samråd och hantering av säkerhetsskyddsklassificerade handlingar utvecklas ytterligare i Säkerhetspolisens vägledning *Informationssäkerhet.*

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