Gallring av säkerhetshandlingar

Författning har tagits fram som en del i arbetet med föreskrifter som ska ersätta RA-FS 1991:6 om handlingar som är av tillfällig eller ringa betydelse (RA-KS 2021/23). Den ersättande författningen och denna författning om gallring av handlingar inom informationssäkerhet och säkerhetsskydd har dock inte ”tillfällig eller ringa” som utgångspunkt. Det är i stället områden inom myndigheters arbete med säkerhet som är det som samlar handlingarna - på liknande sätt som i gallringsföreskrifter om räkenskaper, upphandling eller personal- och löneadministration.

Författningen reglerar gallring av handlingar som uppstår i myndigheters arbete med informationssäkerhet och säkerhetsskydd. Handlingarna har utöver detta sitt huvudsakliga sammanhang i standarder, säkerhetsskyddslagstiftningen, föreskrifter och vägledningar från Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen (SÄPO). Förslaget har även tagits fram med befintliga myndighetsspecifika gallringsföreskrifter som underlag.

Innehåll

1. Begrepp och struktur i författningen

1.1 Några begrepp

Informationssäkerhet ska förstås som bevarande av konfidentialitet, riktighet och tillgänglighet hos information. Definitionen används inom SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 (fortsättningsvis ISO 27000-serien) och i MSB föreskrifter. I ISO 27000-serien anges krav och åtgärder inom informationssäkerheten och det kan noteras att dessa rymmer både personalsäkerhet, fysisk- och miljörelaterad säkerhet, kommunikationssäkerhet, driftssäkerhet, styrning av åtkomst och hantering av tillgångar mm. Myndigheter ska hantera sina uppgifter på ett säkert sätt men även förvara dem så att obehöriga inte kan komma åt dem.

Säkerhetsskydd har en annan omfattning än den informationssäkerhet som beskrivs i föregående stycke. Den ”grundläggande informationssäkerheten” kan sägas täcka ett större omfång av hot och risker medan säkerhetsskyddet ska skydda säkerhetskänslig verksamhet och säkerhetsskyddsklassificerade uppgifter mot hot och risker som spioneri, sabotage, terroristbrott och andra brott. Säkerhetsskyddslagen identifierar tre säkerhetsskyddsåtgärder; informationssäkerhet, fysisk säkerhet och personalsäkerhet. I 2 § säkerhetsskyddslagen (2018:585) ges definitionen av begreppet informationssäkerhet, som förebyggande arbete för att hindra att uppgifter röjs, ändras görs otillgängliga eller förstörs och att förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. Säkerhetsskyddslagen definierar även i 3 § fysisk säkerhet och i 4 § personalsäkerhet.

Någon definition av autenticitet finns visserligen inte i författningen, men i kapitel *5.2.2 Egenskaper hos vederhäftig verksamhetsinformation, 5.2.2.1 Autenticitet*, i Dokumentation - Hantering av verksamhetsinformation – Del 1: Grunder och principer (ISO 15489-1:2016, IDT) anges att autentisk verksamhetsinformation är den som kan styrkas:

a) vara vad den utger sig för att vara,

b) ha skapats eller skickats av den aktör som uppges ha skapat eller skickat den, och

c) ha skapats eller skickats vid den tidpunkt som uppges.

I Riksarkivets befintliga föreskrifter används begreppet databärare med betydelsen fysiskt underlag för handlingar. I författningen används dock termen *lagringsmedium* med betydelsen ”fysiskt underlag för handlingar som används för att kunna lagra och läsa uppgifter i till exempel USB-minnen, mobiltelefoner, bärbara datorer, kopiatorer och skrivare”. Termen motsvarar termen lagringsmedium som det används i Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd (Permanent minnesmedium som används för att kunna lagra och läsa uppgifter) och Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd samt även i t.ex. kap 8.3 Hantering av lagringsmedia, SS-EN ISO/IEC 27002:2017.

De huvudsakliga principerna för namnsättning av handlingar och uppgifter i författningen är att de antingen benämns på ett visst sätt i lagar, förordningar eller föreskrifter eller att de beskriver funktionen eller syftet som handlingen har.

1.2 Struktur

Bilagorna är i huvudsak strukturerade efter de övergripande områden som anges i säkerhetsskyddslagstiftningen, men som även återfinns i t.ex. ISO 27000-serien:

- Informationssäkerhet
- Personalsäkerhet
- Fysisk säkerhet

Rubrikerna i bilagorna ska alltså inte ses som processer utan som områden där åtgärder vidtas inom myndighetens arbete med informationssäkerhet eller säkerhetsskydd.

Det finns även en viss koppling till *författningsförslaget* till gallring av verksamhetsstödjande handlingar. Denna författnings struktur föreslås att utgå från standarden SS-EN 15221-4:2011 Del 4: Taxonomi, klassificering och strukturer för Facility Management. Begreppet ’Facility Management’ har inte översatts till svenska och det saknas en direkt språklig motsvarighet. I standarden finns processen Health, Safety, Security and Environment (HSSE) och dess definition kan översättas med: tjänster som skyddar från yttre faror eller interna risker och skyddar tillgångar och hälsa och välbefinnande för människorna och ger en säker och hållbar miljö.

1.3 Författningens avgränsningar

Eftersom grundregeln för allmänna handlingar är bevarande är det endast de handlingar som får gallras som återfinns i författningen. I några fall anges dock i bilagornas anmärkningsfält vad som inte avses med handlingstypen och vad som därmed inte är tillåtet att gallra. Inte heller omfattas handlingar i kärnverksamhet och det som ingår i myndighetens uppdrag eller instruktion. Exempel på kärnverksamhet kan vara SÄPOS hantering av ansökan om registerkontroll.

2. Verksamhet och handlingar samt gallring

Handlingarna som får gallras i föreslagen författning uppkommer när verksamheter skyddar sin information eller sin verksamhet. Det kan både röra sig om vad som skulle kunna kallas grundläggande informationssäkerhet (ibland benämnt verksamhetsskydd) eller om säkerhetsskydd.

Med grundläggande informationssäkerhet avses i denna promemoria de åtgärder som myndigheter vidtar inom sitt arbete med informationssäkerhet men där verksamheten inte är säkerhetskänslig och inte faller inom säkerhetskyddslagstiftningens tillämpningsområde. Utgångspunkten för styrning i den grundläggande informationssäkerheten är då bl.a. förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, ISO 27000-serien och MSB föreskrifter och vägledningar samt Riksarkivets föreskrifter om t.ex. informationssäkerhet, hantering, förvaring och skydd. Handlingar som får gallras inom grundläggande informationssäkerhet finns i bilaga 1 till författningen. Grundläggande informationssäkerhet är dock som term inte vedertaget – utan används endast i denna promemoria.

Avseende säkerhetsskydd är naturligtvis säkerhetsskyddslagstiftningen avgörande. Till den kopplas även Försvarsmaktens och SÄPO:s föreskrifter, handböcker och vägledningar. Dock är det inte uteslutet att ISO 27000-serien används för systematiskt arbete även inom säkerhetsskydd. Handlingar som får gallras inom säkerhetsskydd finns i bilaga 2 till författningen.

Säkerhetsområdet är för stort för en detaljredogörelse, vilket innebär att för att fullt ut kunna ta till sig innehållet i författningen krävs vissa förkunskaper. Nedan följer dock ett urval av beskrivningar av områden inom grundläggande informationssäkerhet och säkerhetsskydd.

2.1 Att hantera handlingar och lagringsmedium säkert

Exempel på handlingar som omfattas är handlingar som uppstår vid hantering av behörigheter, registrering, distribuering, kopiering, kvittering och inventering av handlingar och lagringsmedium. Användaråtkomst och behörighetskontroll avser både handlingar och uppgifter om att styra och begränsa åtkomst till både analoga handlingar samt handlingar och uppgifter i informationssystem.

Handlingar som rör lagringsmedium som innehåller säkerhetsklassificerade uppgifter ska förvaras och hanteras på samma sätt som säkerhetsskyddsklassificerade handlingar och har därför samma gallringsfrister och ingår ibland i samma handlingsslag. Fristerna för gallring av kvitton/kvittenser i bilaga 2 överensstämmer med:

- 3 kap. 15 § FFS 2019:2 där det anges att kvittokopian för en handling som är placerad i säkerhetsskyddsklassen konfidentiell eller hemlig ska bevaras i minst 10 år och att kvittokopian för en handling som är placerad i säkerhetsskyddsklassen kvalificerat hemlig ska bevaras i minst 25 år.

- 3 kap. 17 § PMFS 2019:2 där det anges att verksamhetsutövaren ska bevara kvittensen i minst 10 år och att om handlingen är kvalificerat hemlig ska kvittensen bevaras i minst 25 år.

2.2 IT-säkerhet

Även IT-säkerhet kan innefattas av begreppet informationssäkerhet och rör främst de delar som avser säkerheten i den tekniska hanteringen av information som behandlas i IT-system och administration kring detta. För att uppnå rätt säkerhet i IT-system behövs styrdokument som reglerar utformning och användning av IT-system men även tekniska säkerhetslösningar. Vid utformning av säkerhetsskydd för IT-system är följande åtgärder de vanligaste förekommande:

- Behörighetskontroll.
- Säkerhetsloggning.
- Skydd mot skadlig kod.
- Intrångsdetektering.
- Skydd mot intrång.
- Skydd mot röjande signaler.
- Skydd mot obehörig avlyssning.
- Incidenthantering.
- Säkerhetskopiering.
- Kontinuitetsplanering.
- Hantering av digitala databärare/lagringsmedium.

2.2.1 Uppgifter i loggar

Författningen omfattar de loggar som oftast benämns som säkerhetsloggar. I författningen benämns dessa som *uppgifter i loggar som registrerar händelser som kan påverka säkerheten i eller kring ett informationssystem.* Med detta avses manuell eller automatisk registrering av uppgifter i loggar som syftar till att upptäcka och utreda säkerhetskritiska händelser som skadlig eller otillåten påverkan, obehörig åtkomst och funktionsstörningar i informationssystem. Med funktionsstörningar avses t.ex. uppgifter i loggar som syftar till att övervaka tekniska händelser eller för att söka systemfel. Exempel på registrerade händelser i säkerhetsloggar kan vara:

- Användaraktiviteter.
- Systemadministratörers och systemoperatörers aktiviteter.
- Förändringar i åtkomsträttigheter.
- Tekniska fel och avvikelser samt systemfel med betydelse för säker drift.

Aktiviteter som loggas syftar inte bara till att fälla, utan även till att fria oskyldiga. Loggar skapar spårbarhet och de aktiviteter som loggas kan bland annat bidra till att:

- kartlägga omfattningen av ett angrepp,
- upptäcka händelser som utgör eller kan utgöra hot eller risk,
- avvärja fortsatta hot och risker genom att vidta åtgärder,
- utreda inträffade händelser,

- bedöma skadeverkningar eller,
- kunna peka ut otillbörligt ändrade eller raderade filer så att man kan återskapa dem.

Gallringsfrister för uppgifter i loggar behöver ta hänsyn till att tillräcklig tid har gått för att man ska kunna upptäcka och kartlägga oönskade aktiviteter efter att en händelse inträffat. Det som är avgörande för när uppgifter i säkerhetsloggar kan gallras är behovet av spårbarhet, det vill säga hur länge myndigheten behöver kunna följa upp det som registreras i loggen. Frister för loggar är angivna i bilaga 2 men i bilaga 1 får myndigheten huvudsakligen själv avgöra fristerna.

Gallringsfristerna i bilaga 2 överensstämmer med 4 kap. 34 § PMFS 2019:2 där tidsspannet anges till minst 10 år och att säkerhetsloggar i informationssystem som är avsedda för att behandla uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska bevaras i minst 25 år.

2.3 Säkra kryptografiska funktioner

I bilaga 1 till författningen avses endast de handlingar rörande kryptografiska säkerhetsåtgärder som används i verksamhet som inte är säkerhetskänslig och har koppling till säkerhetsskyddslagstiftningen. Hantering av krypteringsnycklar upptas bland annat i kapitel A.10 Kryptering i ISO 27002.

Inom säkerhetsskydd (bilaga 2 i författningen) inbegrips kryptografiska funktioner i begreppet signalskyddstjänst. I huvudsak syftar signalskyddstjänsten till att förhindra avlyssning eller obehörig påverkan av information i informations- och kommunikationssystem. Med signalskyddstjänst avses kryptografiska funktioner som är avsedda för att skydda säkerhetskänslig verksamhet, 3 kap. 5 § säkerhetsskyddsförordning (2018:658). I 3 b § förordningen (2007:1266) med instruktion för Försvarsmakten anges att Försvarsmakten ska leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information.

I Försvarsmaktens föreskrifter (FFS 2021:1) om signalskyddstjänsten finns föreskrifter om hur signalskyddstjänst ska bedrivas. För ytterligare förståelse av verksamhet och begrepp hänvisas särskilt till Försvarsmaktens *Handbok totalförsvarets signalskyddstjänst, grundläggande regler*. I handbokens bilaga 10 anges de 45 myndigheter och företag som bedriver signalskyddsverksamhet i någon form. För ytterligare begreppsförklaringar eller fördjupning hänvisas till nämnda handbok.

De förkortningar av engelska begrepp som används i FFS 2021:1 används även i författningens bilaga 2. Detta eftersom en översättning skulle försvåra förståelsen och tillämpningen av föreskrifterna.

Inom signalskydd finns författningens enda handlingstyp med tvingande gallring. Anledningen att signalskyddsnycklar *ska* gallras är att 24 § FFS

2021:1 föreskriver att de snarast *ska* förstöras när de har upphört att gälla eller när de inte längre behövs för tjänsten.

I FFS 2021:1 finns flera bestämmelser om minsta förvaringstid. Som exempel kan ges att det av 23 § FFS 2021:1 framgår att dokumentationen avseende förstöring av signalskyddsnycklar som är märkta SG TS ska FFS 2021:1 förvaras i minst 25 år samt att dokumentationen avseende signalskyddsnycklar med en annan signalskyddsgrad ska förvaras i minst 10 år. Av 11 § framgår att inventering av signalskyddsnycklar ska dokumenteras och förvaras i minst 5 år. Gallringsfristerna i författningen korrelerar även med övriga bestämmelserna om minsta förvaringstid i FFS 2021:1.

2.4 Rapportering av incidenter

I ISO 27000-serien definieras informationssäkerhetsincident som en enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet. Incidenthantering definieras som informationssäkerhetprocesser för upptäckande, rapportering, bedömning, agerande, hantering och lärande av informationssäkerhetsincidenter. Det som rapporteras kan vara till exempel mänskliga misstag, överträdelser av fysiska skyddsåtgärder, fel i program eller överträdelse av åtkomstregler.

Handlingarna som avses kan till exempel vara:

- Dokumenterade rapporter och anmälningar om svagheter, avvikelser och incidenter.
- Grundorsaksutredningar med underlag.
- Menbedömningar, skadebedömningar eller konsekvensutredningar och klassificeringar.
- Åtgärdsloggar för incidenter.

Alla statliga myndigheter ska rapportera (till MSB) it-incidenter som inträffar i myndighetens informationssystem eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Det är dock inte alla incidenter som ska rapporteras, utan endast de som *allvarligt* kan påverka säkerheten i den informationshantering som myndigheten ansvarar för. Bestämmelser om detta finns i MSB:s föreskrifter (MSBFS 2020:8) om rapportering av it-incidenter för statliga myndigheter. I författningen framkommer vad som menas med en it-incident och hur rapporteringen ska ske.

Incidenter rörande säkerhetskänslig verksamhet ska rapporteras till SÄPO. Vad som ska anmälas framgår bland annat av 2 kap. 10 § säkerhetsskyddsförordningen (2018:658). Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1, ska anmälan göras också till Försvarsmakten.

Anledningar till obligatorisk it-incidentrapportering kan vara att möjliggöra en förbättrad lägesbild över informationssäkerheten, skapa förutsättningar för att vidta rätt skyddsåtgärder och utveckla förmågan att förebygga, upptäcka och hantera IT-incidenter.

Det kan noteras att alla incidenter inte är av samma karaktär eller har samma betydelse. Vissa incidenter är små och analysen kan göras snabbt och kan skrivas av som att ingen betydande skada skett. Andra incidenter kan ha betydelse för säkerheten på en högre nivå. Dessa incidenter kan leda till sådant som brottsutredningar, utveckling av teknik, processer och rutiner. Gallringsfristerna inom området är eller bör därför vara differentierade och avhängiga incidentens karaktär. Exempel på incidenter med mindre betydelse skulle kunna vara de fall när incidenten

- inte föranleder större ändringar i t.ex. processer, rutiner eller i IT-system,
- inte rapporteras till MSB, eller
- inte är en säkerhetshotande händelse inom säkerhetskänslig verksamhet.

Av remissvaren till föreskriftsförslagen (Dnr RA 22-2018/11457 ersatt med RA-KS 2021/23) framgår att det inte är ovanligt att myndigheter hanterar stora mängder incidenter per vecka och att övervägande delen av dessa är av mindre karaktär.

Mitt förslag är att även dokumenterade rapporter om svagheter får gallras med stöd av gallringsbestämmelserna för incidenter. Med svagheter avses att någon observerat eller misstänker något som kan leda till en incident, men sannolikt ännu inte har gjort det (se till exempel SS-EN ISO/IEC 27002:2017). Även incidenter som *möjligen* inte är säkerhetsrelaterade bör få gallras med stöd av samma handlingsslag. Anledningen till detta är det är troligt att begreppet incident fått en allmän betydelse av att höra till myndighetens arbete med säkerhet. Störningar, avbrott eller andra onormala beteenden i ett informationssystem kan, men behöver inte vara, ett tecken på ett angrepp eller faktiska säkerhetsbrister. Exempel på händelser som kan resultera i denna typ av incidenter kan vara oplanerade avbrott, fel i konfigurationsenhet, fel på en speglad disk o.s.v..

Författningen samlar all incidenthantering i en handlingstyp: Handlingar rörande hantering av incidenter och avvikelser. Handlingstypen omfattar incidenter och avvikelser rörande till exempel information, it och personal och som efter en tid förlorar betydelse för verksamheten. Gallringsmedgivandet avser inte handlingar som:

- Ingår i eller leder till brottsutredningar.
- Leder till att betydande åtgärder eller ändringar vidtas i sådant som till exempel interna regelverk eller informationssystem.
- Redogör för att och hur incidenten påverkat riktighet, äkthet, autenticitet, tillförlitlighet eller integritet i handlingar som ska bevaras.
- Redogör för incidenter som innebär otillåten gallring.

2.5 Personalsäkerhet

Personalsäkerhet består huvudsakligen av åtgärderna bakgrundskontroll/säkerhetsprövning och utbildning.

I författningens bilaga 1 används termen *bakgrundskontroll* vilket även är den term som används i ISO 27000-serien och av MSB. Vad som huvudsakligen anges om personalsäkerhet i dessa sammanhang är att verksamheten före anställning ska säkerställa att anställda och leverantörer förstår sitt ansvar och är lämpliga för de roller de är tilltänkta för.

2.5.1 Säkerhetsprövning och grundutredning

Säkerhetsprövning görs endast av den som genom en anställning eller på något annat sätt ska delta i en säkerhetskänslig verksamhet. Säkerhetsprövning är en sammanfattande benämning på åtgärder som ska visa om en person kan antas vara lojal mot de intressen som skyddas genom säkerhetsskyddslagen. I 3 kap. säkerhetsskyddslagen (2018:585) och i 5 kap. regleras sådant som säkerhetsprövning, placering i säkerhetsklass och registerkontroll. Begreppet personalsäkerhet ska enligt lagens 1 kap 4 §

1. förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig, och

2. säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd

Säkerhetsprövningen förutsätter en grundutredning. Med grundutredning enligt 3 kap. 3 § säkerhetsskyddslagen (2018:585) och 5 kap. 2 § säkerhetsskyddsförordningen (2018:658) avses bland annat säkerhetsintervju, kontroll av betyg, intyg och referenser och även en identitetskontroll. I SÄPO:s vägledning om personalsäkerhet anges att säkerhetsprövningsintervjun ska dokumenteras. Av samma vägledning, samt av 5 kap. 5 § säkerhetsskyddsförordningen (2018:658) framkommer att resultatet av säkerhetsprövningen ska dokumenteras i de fall en person har bedömts vara pålitlig från säkerhetssynpunkt och ett beslut har fattats om anställning eller annat deltagande i verksamheten. Förutom anteckningar från intervjun måste den ansvarige kunna visa vilka sårbarheter som är omhändertagna, värderade och bedömda som godtagbara.

I SÄPO vägledning anges att det är den som beslutar om registerkontroll som ansvarar för att samtycke har hämtats in. Man anger vidare att samtycket ska dokumenteras och sparas eftersom samtycket gäller för nya kontroller och utredningar så länge som deltagandet i den säkerhetskänsliga verksamheten pågår.

Framställan om registerkontroll skickas till SÄPO när en person har genomgått en godkänd grundutredning. Bestämmelser om registerkontroll och särskild personutredning som utförs efter ett beslut om placering i säkerhetsklass finns i 12–22 §§ säkerhetsskyddsförordningen (2018:658). Om det redan efter grundutredningen står klart att den som prövningen gäller inte uppfyller kraven för en godkänd säkerhetsprövning enligt 3 kap. 2 § säkerhetsskyddslagen (2018:585) ska registerkontroll och särskild personutredning inte göras.

Registerkontrollen kan ses som en komplettering till eller som att vara en del av säkerhetsprövningen och fungerar som underlag när myndigheten sedan fattar beslut om anställningar. För framställan om registerkontroll och ansökan om särskild personutredning används standardiserade blanketter. Blanketten skickas in till SÄPO som sedan delger resultatet av registerkontrollen. Om det inte framkommer några uppgifter skickar SÄPO tillbaka en svarslista (återredovisning) till myndigheten. Listan innehåller en redovisning av vilka personer som har kontrollerats och information om att det inte finns några uppgifter att redovisa. Om Registerkontrolldelegationen har beslutat att lämna ut uppgifter om den kontrollerade skickar SÄPO en promemoria med dessa uppgifter till myndigheten. Myndighetens beslut ska då antecknas på promemorian och skickas tillbaka till SÄPO.

Enligt 3 kap. 21 § säkerhetslagen ska de handlingar som överlämnats till myndigheten ska snarast återställas till SÄPO. Bestämmelsen ger det lagstöd som behövs för att statliga och kommunala myndigheter ska kunna avhända sig dessa allmänna handlingar (jfr 12 och 15 §§ arkivlagen (1990:782).

Av remissvaren till författningen (Dnr RA 22-2018/11457) framkommer att myndigheter hanterar blanketten framställan om registerkontroll olika. Vissa bevarar en kopia av framställan av spårbarhetsskäl eller för att samtycken och uppgifter och handlingar i grundutredningar ska bevaras. Vissa menar att det inte finns anledning att spara handlingen efter att återrapporteringen har inkommit medan vissa menar att den inte finns kvar inom myndigheten eftersom den skickas till SÄPO.

För både bakgrundskontroller och grundutredningar vid säkerhetsprövning är bedömningen att handlingar för den som anställts ska bevaras. Ur ett förvaltnings- och rättskipningsperspektiv har uppgifterna ett relativt långt värde (5-25 år), t.ex. vid incidenter när det finns behov av att kunna gå tillbaka till tidigare bakgrundskontroller eller grundutredningar för att kontrollera vad som där har framkommit och för att kunna visa vilka sårbarheter som är omhändertagna, värderade och bedömda som godtagbara. Uppgifterna i grundutredningar kan vara integritetskänsliga och kan därför kräva skyddande åtgärder.

En parallell kan dras till *handlingar rörande utvärdering av sökande* i Riksarkivets föreskrifter och allmänna råd (RA-FS 2019:1) om återlämnande eller gallring av handlingar inom löne- och personaladministrativ verksamhet. Där anges att handlingar som avser den anställde ska undantas från gallring. Med handlingar rörande utvärdering av sökande avses i detta sammanhang till exempel testresultat från urvalstester, anteckningar från intervjuer eller referenstagning och enkätfrågor och svar som använts som urvalsinstrument.

I RA-FS 2019:1 regleras redan idag gallring och undantag från gallring av *grunduppgifter i säkerhetsprövningar* samt *handlingar rörande registerkontroll och särskild personutredning*. För grunduppgifter anges att dessa ska bevaras för den anställde. De båda nämnda handlingstyperna kommer att tas

bort genom en ändring av RA-FS 2019:1. Gallringen regleras i stället genom föreliggande författning.

I anmärkningsfältet för *handlingar i grundutredningar i säkerhetsprövningar för den som inte har anställts eller anlitats* anges att säkerhetsskyddsbeslut inte omfattas. Med säkerhetsskyddsbeslut i personärende avses ett beslut taget av myndigheten när det vid inledande eller uppföljande säkerhetsprövning framkommit information som är av sådan art att en person kan antas ha brister i pålitlighet, lojalitet eller vara sårbar. Information som leder till sådana beslut kan ha sitt ursprung i sådant som säkerhetsprövningsintervjuer, registerkontroller eller säkerhetsrapporter. Beslutet kan bestå i att personen ska kvarstå på sin befattning, omplaceras eller skiljas från den skyddsvärda verksamheten.

Säkerhetsprövningen följs upp med utbildning och förnyade samtal under hela den tid deltagandet i den säkerhetskänsliga verksamheten pågår. För den som har en anställning eller liknande som är placerad i säkerhetsklass 1 eller 2 görs en ny registerkontroll vart femte år eller när det finns särskild anledning.

Av bilagan till säkerhetsskyddsförordningen (2018:658) framkommer att det är 94 myndigheter som beslutar om placering i säkerhetsklass.

2.5.2 Tjänstekort

Tjänstekort regleras genom förordningen (1958:272) om tjänstekort. Här finns bland annat bestämmelser om att tjänstekortet ska gälla högst fem år och att ett tjänstekortsregister ska föras. I 1 § i förordningen framgår att ett tjänstekort är en särskild legitimationshandling som utfärdas för den som tjänstgör vid eller innehar uppdrag för statligt eller kommunalt organ och som regelmässigt behöver styrka sin identitet eller tjänsteställning. I Polismyndighetens föreskrifter och allmänna råd (PMFS 2020:4) om tjänstekort finns kompletterande bestämmelser om tjänstekortets utformning, hanteringen och vad som ska dokumenteras.

Utredningens förslag är att författningen omfattar även gallringsbestämmelser om handlingar rörande tjänstekort även om de inte endast fyller funktionen som säkerhetshöjande åtgärd. Alternativen skulle annars vara en egen författning eller att de ingår i föreskrifter om gallring av handlingar inom personal- och löneadministration. Handlingstyperna kring tjänstekort återfinns endast i bilaga 1 eftersom de inte har en direkt koppling till säkerhetsskydd.

2.5.3 Tystnadsplikt

Avseende tystnadsplikt i det allmännas verksamhet tillämpas bestämmelserna i offentlighets- och sekretesslagen (2009:400). Tystnadsplikt regleras även genom säkerhetsskyddslagens 5 kap. 1-2 §§ där det bland annat anges att den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet inte får obehörigen röja eller utnyttja säkerhetsskyddsklassificerade uppgifter. Av 2 kap. 4 § framgår även att en

verksamhetsutövare ska upplysa den som tillåts ta del av säkerhetsskydds-klassificerade uppgifter om räckvidden och innebörden av den sekretess och tystnadsplikt som följer av offentlighets- och sekretesslagen (2009:400) respektive 5 kap. 2 § säkerhetsskyddslagen (2018:585).

I remissvaren till föreskriftsförslagen (Dnr RA 22-2018/11457 ersatt med RA-KS 2021/23) framkommer att handlingstypen kan bedömas olika av olika myndigheter. Vissa menar att handlingstypen bör bevaras eftersom tystnadsplikten inte är tidsbegränsad medan andra menar att den bör få gallras. Frister som föreslås är bland annat 25 år för kvalificerat hemligt och 10 år för övriga nivåer, men även upp till 40 år. Ytterligare förslag som anges är att gallring borde kunna verkställas kort efter uppdragets slut eftersom sekretessupplysningar eller motsvarande inte fyller något juridiskt syfte, eftersom deltagarna ändå är bundna av lagstadgad tystnadsplikt och att spårbarhet avseende deltagande i säkerhetskänslig verksamhet finns i andra handlingar. Min bedömning är att det inte finns något större forskningsvärde i handlingarna och att myndigheter själva kan bedöma lämplig frist utifrån sin verksamhet.

2.6 Säkerhetsskyddad upphandling

Avseende *säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)* bör noteras att även alla som ska delta i ett uppdrag eller verksamhet och som kan antas få del av hemliga uppgifter av betydelse för rikets säkerhet ska säkerhetsprövas. Om uppdraget är placerat i säkerhetsklass ska även en registerkontroll göras. De som får del av hemliga uppgifter eller deltar i verksamheten ska upplysas om den tystnadsplikt som gäller. Gallring av handlingar inom säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) regleras dock genom *Riksarkivets föreskrifter och allmänna råd (RA-FS 2018:3) om återlämnande eller gallring av handlingar vid upphandling.* Mitt förslag är handlingar som rör säkerhetsskyddad upphandling kan kvarstå i RA-FS 2018:3. Hänvisning görs i författningens 3 kap. 2 §.

2.7 Fysisk säkerhet

I ISO 27000-serien definieras fysisk säkerhet i huvudsak som att förhindra otillåten fysisk åtkomst till, skador på och störningar i tillgången till organisationens information och informationsbehandlingsresurser. I 2 kap. 3 § säkerhetsskyddslagen (2018:585) anges att fysisk säkerhet ska förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs, och förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt.

Myndigheten ska alltså kunna förebygga, upptäcka, försvåra och agera på ett fysiskt angrepp eller obehörigt tillträde. Inom t.ex. Försvarsmakten har begreppet en något vidare betydelse, jämfört med säkerhetsskyddslagstiftningen, genom att myndigheten även ska kunna hindra att stöldbegärlig, svårersättlig eller av annan anledning skyddsvärd materiel förstörs eller kommer obehörig till del. Exempel på åtgärder inom fysisk säkerhet är:

- Områdesskydd.
- Intrångsdetektering och larm.
- Behörighetskontrollsystem och zonindelning.
- Skalskydd.
- Bevakning och vakthållning.
- Fysiska barriärer.

Av PMFS 2019:2 och FFS 2019:2 framkommer bl.a. att myndigheter ska ha en förteckning över kort, koder, nycklar eller liknande som hör till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet. I PMFS anges i 5 kap. 5 § att verksamhetsutövare ska utfärda skriftligt tillstånd för besökare som ska få tillträde till en plats där säkerhetskänslig verksamhet bedrivs. I 5 kap. 3 § FFS 2019:2 föreskrivs att det vid myndigheten för varje besökare ska antecknas namn, personnummer, passnummer eller nummer på annan identitetshandling, den myndighet, organisation eller motsvarande som besökaren företräder och dagen för besöket och att sådana anteckningar ska bevaras i minst 10 år.

2.8 Utbildning

I huvudsak återfinns inte några särskilda gallringsbestämmelser om handlingar rörande säkerhetsutbildningar i denna författning. För utbildningshandlingar kan i stället de kommande föreskrifterna om gallring av verksamhetsstödjande handlingar kunna att tillämpas.

3 Övrigt om frister inom informationssäkerhet och säkerhetsskydd

Gallringsfristerna inom säkerhet utgår huvudsakligen från rättskipningens behov av preskriptionstider för vissa brott. Med preskription menas att rättsliga följder upphör efter en viss tid efter det att brottet eller någon annan händelse har inträffat eller ett beslut har fattats. Fristerna utgår från att det ska finnas en möjlighet att kunna söka och återskapa en händelsekedja där handlingar och uppgifter kan bevisa och styrka vissa uppgifter om användare samtidigt som de även kan ge användaren möjlighet att visa på sin oskuld. I de fall när fristen är verksamhetens behov får myndigheten avgöra fristen själv.

Preskriptionstider anges i 35 kap. 1§ brottsbalken:

Påföljd må ej ådömas, med mindre den misstänkte häktats eller erhållit del av åtal för brottet inom

1. två år, om å brottet ej kan följa svårare straff än fängelse i ett år

2. fem år, om svåraste straffet är högre men icke över fängelse i två år,

3. tio år, om svåraste straffet är högre men icke över fängelse i åtta år,

4. femton år, om svåraste straffet är fängelse på viss tid över åtta år,

5. tjugofem år, om fängelse på livstid kan följa å brottet.

I 35 kap. 2 § finns bestämmelser om att bortfallande av påföljd inte gäller bland annat mord eller dråp, terroristbrott eller försök till vissa brott.

Några exempel på tänkbara brottsliga gärningar och preskriptionstider som kan ligga till grund för bedömningen av gallringsfrister är:

- *Dataintrång,* böter eller fängelse i högst två år; preskriptionstid 5 år. 4 kap § 9 c brottsbalken.

- *Brott mot tystnadsplikt* böter eller fängelse i högst ett år; preskriptionstid 2 år. 20 kap. 3 § brottsbalken.

- *Tjänstefel,* böter eller fängelse i högst två år; preskriptionstid 5 år och *grovt tjänstefel* fängelse, lägst sex månader och högst sex år; preskriptionstid 10 år. 20 kap 1 § brottsbalken.

- *Högförräderi*, fängelse på viss tid, lägst tio och högst arton år, eller på livstid eller, om faran var ringa, till fängelse i lägst fyra och högst tio år; preskriptionstid 25 år. 19 kap 1 § brottsbalken.

- *Spioneri,* fängelse i högst sex år; preskriptionstid 10 år. 19 kap 5 §. *Grovt spioneri*, fängelse på viss tid, lägst fyra och högst arton år, eller på livstid; preskriptionstid 25 år. 19 kap 6 § brottsbalken.

- *Obehörig befattning med hemlig uppgift* böter eller fängelse i högst två år; preskriptionstid 5 år. 19 kap 7 § brottsbalken.

4 Regelverk

Som sannolikt redan har framgått av ovanstående kapitel är det särskilt nedanstående lagar och förordningar som författningen utgår från:

- Säkerhetsskyddslagen (2018:585)
- Säkerhetsskyddsförordningen (2018:658)
- Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap
- Förordningen (1958:272) om tjänstekort

4.1 Närliggande reglering

Säkerhetsskyddslagstiftningen är inte den enda reglering som ger ett skydd för samhällsviktig verksamhet. På området finns även skyddslagstiftning för kärnteknisk verksamhet, luftfart, sjöfart, hamnar, transport av farligt gods och landskapsinformation. Nämnas kan även reglerna i lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet.

Skyddslagen (2010:305) skyddsförordningen (2010:523) ligger nära säkerhetsskyddslagen framförallt genom säkerhetsskyddsåtgärden tillträdesbegränsning. När en byggnad, anläggning eller ett område är klassat som skyddsobjekt innebär det att obehöriga inte har tillträde dit. Det är i vanliga fall länsstyrelsen som fattar beslut om vilka objekt som blir skyddsobjekt. En gemensam nämnare för skyddsobjekt är att de utgör samhällsviktiga

byggnader eller objekt som vanligtvis har ett förhöjt skyddsbehov mot sabotage, terroristbrott, spionerи, röjande av hemliga uppgifter som rör totalförsvaret eller grovt rån. Även vattenområden av särskild betydelse för det militära försvaret kan vara skyddsobjekt.

Flera kapitel i *Offentlighets- och sekretesslagen (2009:400)* berör området, men nämnas kan t.ex. 5 kapitlet om registrering av allmänna handlingar och sekretessmarkering samt det 15 kapitlet där det anges vad som är sekretess till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer.

4.2 Föreskrifter om informationssäkerhet och säkerhetsskydd

4.2.1 Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning att en annan myndighet inte har ansvaret. MSB stödjer och samordnar arbetet med samhällets informationssäkerhet och samverkar med myndigheter, kommuner, landsting, organisationer och företag för att identifiera och analysera sårbarheter, hot och risker som kan anses särskilt farlig för samhället och rapporterar sedan resultatet till regeringen. Myndigheten meddelar föreskrifter om risk- och sårbarhetsanalyser för kommuner, landsting och statliga myndigheter. Exempel är:

- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter
- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter
- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:8) om rapportering av it-incidenter för statliga myndigheter

Enligt föreskrifterna ska myndigheter bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav och SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder eller motsvarande. Metodstöd för systematiskt informationssäkerhetsarbete finns på https://www.informationssakerhet.se/metodstodet/.

4.2.2 Säkerhetspolisen (SÄPO)

SÄPO har ett särskilt ansvar för säkerhetsskyddet, bl.a. genom att myndigheten har det huvudsakliga ansvaret för tillsyn och tillämpningsföreskrifter. Säkerhetspolisen kontrollerar säkerhetsskyddet vid myndigheter som inte hör till Försvarsmaktens tillsyn.

SÄPO får bland annat meddela föreskrifter om säkerhetsskyddsåtgärder, säkerhetsskyddsavtal, förfarandet vid registerkontroll samt meddela ytterligare föreskrifter om verkställigheten i övrigt av säkerhetsskyddslagen (7 kap. 4 § säkerhetsskyddsförordningen (2018:658)).

SÄPO har beslutat föreskrifter om säkerhetsskydd genom PMFS 2019:2. Till författningen finns även flera vägledningar. I författningen finns bestämmelser om bevarandetider. SÄPO har även meddelat föreskrifter om tjänstekort genom Polismyndighetens föreskrifter och allmänna råd (PMFS 2020:4) om tjänstekort.

4.2.3 Försvarsmakten

Försvarsmakten har ett särskilt ansvar för säkerhetsskyddet, bl.a. genom att myndigheten (tillsammans med SÄPO) har det huvudsakliga ansvaret för tillsyn och tillämpningsföreskrifter. Försvarsmakten ska bland annat leda och bedriva militär säkerhetstjänst samt leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner för skyddsvärd information. Försvarsmakten kontrollerar säkerhetsskyddet hos Fortifikationsverket, Försvarshögskolan och de myndigheter som hör till Försvarsdepartementet. Vad Försvarsmakten får föreskriva om framgår av 7 kap. 5 § säkerhetsskyddsförordningen (2018:658).

Försvarsmakten har beslutat föreskrifter om säkerhetsskydd genom FFS 2019:2 och om signalskyddstjänsten genom FFS 2021:1. I båda författningarna finns bestämmelser om bevarandetider. Huvuddelen av Försvarsmaktens uppgifter enligt säkerhetsskyddsförordningen hanteras av den militära underrättelse- och säkerhetstjänsten (MUST).

4.2.4 Riksarkivet

I 6 kap. Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:1) om elektroniska handlingar (upptagningar för automatiserad behandling) finns bestämmelser om informationssäkerhet. I 5 kap. finns dokumentationskrav som bland annat innebär att myndigheter ska dokumentera sina elektroniska handlingar för att handlingarna ska kunna framställas, överföras, hanteras, förvaras och vårdas på ett tillfredsställande sätt under den tid som de ska bevaras. I 5 kap. Föreskrifter om ändring av Riksarkivets föreskrifter (RA–FS 1991:1) och allmänna råd om arkiv hos statliga myndigheter (senast ändrad och omtryckt genom RA-FS 2019:2) finns bestämmelser om hantering, förvaring och skydd.

5 Arkivlagen och Riksarkivets föreskrifter om gallring mm

5.1 Arkivlagen m.m.

Av 3 § första stycket arkivlagen (1990:782) framgår att en myndighets arkiv bildas av de allmänna handlingarna från myndighetens verksamhet och sådana handlingar som avses i 2 kap. 12 § tryckfrihetsförordningen och som myndigheten beslutar ska tas om hand för arkivering. Av 3 § andra stycket framgår att myndigheters arkiv utgör en del av det nationella kulturarvet.

I 3 § tredje stycket arkivlagen anges att myndigheternas arkiv ska bevaras, hållas ordnade och vårdas i syfte att tillgodose

- rätten att ta del av allmänna handlingar,
- behovet av information för rättskipningen och förvaltningen, och
- forskningens behov.

Av 10 § första stycket arkivlagen framgår att allmänna handlingar får gallras. I andra stycket anges att vid gallring måste beaktas att arkiven utgör en del av kulturarvet och att det arkivmaterial som återstår efter gallring ska kunna tillgodose de ändamål som anges i 3 § tredje stycket arkivlagen.

Enligt 12 § arkivförordningen (1991:446) får Riksarkivet meddela föreskrifter om gallring och om föreskrifter saknas får Riksarkivet meddela särskilda beslut om gallring.

Av 14 § arkivförordningen framgår att statliga myndigheter får gallra allmänna handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet om inte särskilda gallringsföreskrifter finns i lag eller förordning.

Dataskyddsförordningen innehåller en bestämmelse om att personuppgifter inte ska bevaras under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. I denna bestämmelse anges vidare att personuppgifter får lagras under längre tid i den mån som personuppgifterna behandlas för till exempel arkivändamål av allmänt intresse.[1] Av artikel 6 punkten 3 framgår att vad som är arkivändamål av allmänt intresse ska fastställas i nationell rätt eller i unionsrätten. Sverige har för myndigheter fastställt vad som utgör arkivändamål av allmänt intresse i arkivlagen.[2]

Av 1 kap. 6 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, framgår att bestämmelser i en annan lag ska tillämpas om de avviker från denna lag. Därmed ska arkivlagens bestämmelser tillämpas före den lagen.

5.2 Riksarkivets generella föreskrifter om gallring

Riksarkivet har beslutat flera generella föreskrifter på andra områden som myndigheten behöver ta i beaktande vid gallring. Bestämmelser om gallring av handlingar inom till exempel löne- och personaladministration finns i annan författning. För områden som gallring efter skanning och till exempel IT-drift och som inte är relaterade till informationssäkerhet eller säkerhetsskydd hänvisas även här till andra av Riksarkivets författningar.

I Riksarkivets föreskrifter och allmänna råd (RA-FS 2018:3) om återlämnande eller gallring av handlingar vid upphandling finns bestämmelser om gallring av handlingar vid säkerhetsskyddad upphandling.

---

[1] Artikel 5.1 e Europaparlamentets och rådets förordning [EU] 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[2] Prop. 2017/18:105 Ny dataskyddslag, s. 110 f.

5.3 Riksarkivets myndighetsspecifika föreskrifter

I arbetet med författningen har även Riksarkivets myndighetsspecifika föreskrifter analyserats. Flera handlingar och dess gallringsfrister i författningen är kompatibla med och är sådana som varit återkommande i flera RA-MS. Nämnas kan bland annat:

- Riksarkivets föreskrifter och allmänna råd (RA-MS 2018:42) om gallring hos Fortifikationsverket, Försvarets materielverk, Försvarsmakten, Totalförsvarets forskningsinstitut och Totalförsvarets rekryteringsmyndighet
- Riksarkivets föreskrifter om gallring (RA-MS 2019:21) hos Livsmedelsverket
- Riksarkivets föreskrifter (2018:4) om gallring hos Länsstyrelserna

5.4 Riksarkivets gallrings- och bevarandepolicy

Enligt Riksarkivets gallrings- och bevarandepolicy, Bevarandet av nutiden, ska myndigheter lägga särskild tyngd på handlingar som uppkommit i myndighetens kärnverksamhet. Administrativa eller tekniska stödverksamheter är av mindre betydelse i detta sammanhang. Notera att arkivhandlingar kan användas som information om dels den verksamhet där handlingarna uppkommit, dels om förhållandena i organisationens omvärld. Båda dessa sätt att använda informationen ska beaktas i lika stor utsträckning vid bedömning av bevarande respektive gallring.

6 Sammanfattande överväganden

Eftersom delar av förslaget till föreskrifter bygger på Riksarkivets tidigare myndighetsspecifika föreskrifter och beslut bedömer jag att bevarande och gallring till stora delar kan ses som redan utredda. Vissa överväganden har dock gjorts, varav några har sitt ursprung i de svar som inkom med anledning av genomförd remiss.

Avseende gallring och gallringsfrister har dessa tagit hänsyn till allmänhetens rätt till insyn samt rättskipningens, förvaltningens och forskningens behov. Fristerna grundas huvudsakligen på preskriptionstider för vissa brott men det kan även sägas finnas en lång praxis kring gallringsfrister i Riksarkivets föreskrifter och beslut.

Vissa ändringar i föreskrifternas bilaga har gjorts i enlighet med de förslag som gavs i myndigheternas svar på remiss. I bilaga 2 har särskild hänsyn tagits till Försvarsmaktens och Säkerhetspolisens föreskrifter på så sätt att där det föreskrivs om att en handling ska finnas inom myndigheten en viss tid har gallringsfristen anpassats till detta. Jag har inte funnit något som motsäger detta i förhållande till bevarandeändamålen i 3 § arkivlagen (1990:782).

Handlingar som ska bevaras finns inte med i författningens bilaga. Dock finns i vissa fall angivet i anmärkningsfältet vad som *inte* avses att få gallras. För myndigheterna är det särskilt värt att notera att det med begreppet

får gallras ges möjlighet till dem att antingen förlänga gallringsfristen eller till och med bevara handlingstypen.

7. Källor och referenser

Utöver Riksarkivets föreskrifter har bland annat följande källor har använts som underlag till PM och förslag till föreskrifter.

Försvarsmakten

- ”Försvarsmaktens författningssamling - FFS”
- ”Försvarsmaktens interna bestämmelser – FIB”
- Handbok för Försvarsmaktens säkerhetstjänst Grunder (H SÄK Grunder), 2013 års utgåva
- Handbok för Försvarsmaktens säkerhetstjänst, Informationssäkerhet (H SÄK Infosäk), 2013 års utgåva
- Handbok för Försvarsmaktens säkerhetstjänst, Fysisk säkerhet (H SÄK Fysisk säkerhet), 2015 års utgåva
- Handbok för Försvarsmaktens säkerhetstjänst Säkerhetsprövning 2017 (H SÄK Säkprövn)
- Handbok Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (Handbok SUA) 2010 års utgåva
- Handbok totalförsvarets signalskyddstjänst, grundläggande regler för signalskyddstjänsten (H TST Grunder), 2007 års utgåva.
- https://www.forsvarsmakten.se/sv/organisation/hogkvarteret/militara-underrattelse-och-sakerhetstjansten/

Säkerhetspolisen

- ”Polismyndighetens författningssamling – PMFS”
- Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd, 2019
- Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys, 2019
- Vägledning i säkerhetsskydd – Informationssäkerhet, 2020
- Vägledning i säkerhetsskydd – Fysisk säkerhet, 2020
- Vägledning i säkerhetsskydd – Personalsäkerhet. 2019
- https://www.sakerhetspolisen.se/sakerhetsskydd.html

Myndigheten för samhällsskydd och beredskap

- ”Myndigheten för samhällsskydd och beredskaps författningssamling – MSBFS”
- Informationssäkerhet i samhället (msb.se)

Övrigt

- ”En ny säkerhetsskyddslag” (SOU 2015:25) och ”Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag” (Prop. 2017/18:89)
- http://www.regeringen.se/rattsdokument/proposition/2018/02/prop.-20171889/
- http://www.sakerhetspolitik.se/sakerhetspolitik/vad-ar-sakerhet/
- https://www.informationssakerhet.se/