VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Rekommendation om behandling av säkerhetsklassificerade handlingar

Nämnder

Finansministeriets publikationer – 2021:10

Finansministeriets publikationer 2021:10

Rekommendation om behandling av säkerhetsklassificerade handlingar

Informationshanteringsnämden

Finansministeriet Helsingfors 2021

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Finansministeriet

ISBN pdf: 978-952-367-520-9
ISSN pdf: 1797-9714

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2021

Presentationsblad

11.2.2021

Rekommendation om behandling av säkerhetsklassificerade handlingar

Finansministeriets publikationer 2021:10		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämden		
Språk	Svenska	**Sidantal**	71

Referat

Myndigheter vid statliga ämbetsverk och inrättningar, statliga affärsverk, domstolar och nämnder som har inrättats för att behandla besvärsärden ska enligt 18 § i lagen om informationshantering inom den offentliga förvaltningen säkerhetsklassificera handlingar och förse dem med anteckning om säkerhetsklass som visar vilket slag av informationssäkerhetsåtgärder som ska vidtas vid behandlingen av dem. Anteckning om säkerhetsklass ska göras, om en handling eller informationen i den är sekretessbelagd enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i lagen om offentlighet i myndigheternas verksamhet och om obehörigt avslöjande eller obehörig användning av handlingen kan orsaka skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet.

Syftet med rekommendationen är att stödja myndigheter som använder säkerhetsklassificering.

Informationshanteringsnämnden godkände rekommendationen den 11 februari 2020 och denna uppdaterade publikation den 18 december 2020.

Nyckelord informationshanteringslagen, informationshanteringsnämnden, nämnder, informationssäkerhet, offentlig förvaltning, klassificeringar, handlingar, information, rekommendation

ISBN PDF	978-952-367-520-9	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-520-9		

Kuvailulehti

11.2.2021

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

Valtiovarainministeriön julkaisuja 2021:10		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	Ruotsi	**Sivumäärä**	71

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetun lain 18 §:n mukaan valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.

Suosituksen tavoitteena on tukea turvallisuusluokitusta käyttäviä viranomaisia.

Tiedonhallintalautakunta hyväksyi suosituksen 11.2.2020, ja tämän toisen, päivitetyn julkaisun 18.12.2020

Asiasanat	tiedonhallintalaki, tiedonhallintalautakunta, lautakunnat, tietoturva, julkinen hallinto, luokitukset, asiakirjat, tieto, suositus

ISBN PDF	978-952-367-520-9	**ISSN PDF**	1797-9714
Julkaisun osoite	http://urn.fi/URN:ISBN:978-952-367-520-9		

Description sheet

11 February 2021

Recommendation on the handling of classified documents

Publications of the Ministry of Finance 2021:10		**Subject**	Board
Publisher	Ministry of Finance		
Group Author	Information Management Board		
Language	Swedish	**Pages**	71

Abstract

Under section 18 of the Act on Information Management in Public Administration, authorities operating in ministries, government agencies, public bodies and unincorporated state enterprises, along with courts of law and boards established to handle appeals shall security classify documents and mark them with a security classification to indicate the information security measures to be complied with when handling the documents. A security classification marking shall be applied if the document or information contained within it is secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities and the unauthorised disclosure or unauthorised use of the information contained in the document could prejudice national defence, preparedness for exceptional circumstances, international relations, combating of crime, public safety or the functioning of government finances and the national economy, or the safety of Finland in some other comparable manner.

The purpose of the recommendation is to support the work of authorities which use the security classifications.

The Information Management Board approved the recommendation on 11 February 2020, and this second, updated publication on 18 December 2020.

Keywords Information Management Unit, Information Management Act, advisory boards, information management, public administration, responsibilities, definitions

ISBN PDF	978-952-367-520-9	**ISSN PDF**	1797-9714
URN address	http://urn.fi/URN:ISBN:978-952-367-520-9		

Innehåll

1 Inledning

Denna rekommendation från informationshanteringsnämnden bereddes i dess sektion för säkerhetsklassificerade handlingar. Sektionen har tillsatts för perioden 1.4.2020–31.12.2021 med informationsförvaltningsråd Tuija Kuusisto från finansministeriet som ordförande och ledande specialsakkunnig Tuula Seppo från Myndigheten för digitalisering och befolkningsdata som sekreterare. Nämnden har även tillsatt experter från olika informationshanteringsenheter som medlemmar i sektionen, som vid möten, workshoppar och seminarier också hört många utomstående experter. Utkastet till rekommendation var utlagt i den öppna utlåtandetjänsten 23.11-4.12.2020.

Lagen om informationshantering inom den offentliga förvaltningen (906/2019, IHL eller informationshanteringslagen) tillämpas på offentliga informationshanteringsenheter och myndigheter samt privatpersoner, sammanslutningar och offentligrättsliga samfund som inte är myndigheter till den del som de sköter offentliga förvaltningsuppgifter. IHL reglerar deras ansvar för informationssäkerhetsåtgärder och åtgärdernas miniminivå. Enligt 18 § i informationshanteringslagen ska myndigheter vid statliga ämbetsverk, inrättningar och affärsverk samt domstolar och nämnder som har inrättats för att behandla besvärsärenden säkerhetsklassificera vissa handlingar.

Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019, nedan förordningen om säkerhetsklassificering, FSK) reglerar säkerhetsklassificeringen och märkningen av de handlingar som avses i 18 § i informationshanteringslagen samt statliga myndigheters informationssäkerhetsåtgärder för behandlingen av säkerhetsklassificerade handlingar.

Denna rekommendation vägleder informationshanteringsenheterna och myndigheterna med avseende på informationssäkerhetskraven i förordningen om säkerhetsklassificering. Målet är att den ska vara ett stöd för myndigheter som gör säkerhetsklassificeringar. Rekommendationen ger råd om hur man bedömer behovet och graden av säkerhetsklassificering samt riskerna med säkerhetsklassificerad information och hur man beaktar skyddet av informationen i alla skeden av behandlingen och i olika områden under dess hela livscykel. Råden kompletteras av praktiska exempel och tillvägagångsätt. Rekommendationen ger även råd om korrekt behandling till mottagare av säkerhetsklassificerad information. Observera att kraven i förordningen kan uppfyllas på flera sätt och vilka som väljs beror i hög grad på myndighetens riskhantering.

Enligt informationshanteringslagen ska informationssäkerhetsåtgärderna bygga på en riskbedömning. Med avseende på säkerhetsåtgärder för *sekretessbelagd* information rekommenderas att de avvägs utifrån rekommendationerna gällande handlingar i säkerhetsklass IV så att behandlingskraven för sekretessbelagda handlingar blir kompatibla med TL IV-kraven. Då behöver man inte ha parallella informationssystem för samma ändamål, ett för behandling av sekretessbelagda handlingar och ett för handlingar i säkerhetsklass IV, t.ex. flera ärendehanteringssystem avsedda för alla personer på ämbetsverket. Därtill undviks att handlingar i säkerhetsklass IV av misstag behandlas i system som inte uppfyller kraven för den klassen. Informationssäkerhetsåtgärder för sekretessbelagd information kan från fall till fall även avvägas utifrån rekommendationerna gällande handlingar i säkerhetsklass I-III. Om inget något annat särskilt föreskrivs ska myndigheten sekretessbelägga de handlingar som avses i 24 § i offentlighetslagen inklusive deras uppgifter. Säkerhetsklassificering sker ifall handlingen eller dess uppgifter ska sekretessbeläggas enligt 24 § 1 mom. 2, 5 eller 7–11 punkterna i offentlighetslagen. Därtill finns ett skaderekvisit, dvs. att obehörigt avslöjande eller obehörig användning av information som ingår i handlingen kan orsaka skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet.

När förordningen om säkerhetsklassificering tillämpas ska även andra centrala bestämmelser om säkerhetsklassificering och sekretess beaktas. 12 § i Finlands grundlag (731/1999) och lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan offentlighetslagen eller OffL) reglerar bl.a. myndighetshandlingars offentlighet, sekretessgrunder och utlämning av handlingar.

Europaparlamentets och rådets förordning (EU) 2016/679 (EU:s allmänna dataskyddsförordning) och den nationella dataskyddslagen (1050/2018) har bestämmelser om behandling av personuppgifter och om tystnadsplikt. Lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018) har bestämmelser om bl.a. behandling av personuppgifter, förebyggande, avslöjande och utredning av brott, åtalsprövning och skydd mot eller förhindrande av hot mot den allmänna säkerheten. Statliga myndigheter ska utöver denna rekommendation beakta annan särskild reglering av deras verksamhet och behandling av personuppgifter. Dataombudsmannen är en nationell tillsynsmyndighet som övervakar efterlevnaden av dataskyddslagstiftningen (tietosuoja.fi).

Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) reglerar sekretessen för handlingar som har säkerhetsklassificerats enligt internationella förpliktelser och uppfyllelsen av dessa. Nationella säkerhetsmyndigheten (NSA) har gett ut en anvisning om behandling av säkerhetsklassificerad information (utrikesministeriet NSA 2020) (på finska).

Informationshanteringsnämnden gav ut denna rekommendation första gången 2020 och föreliggande version är den andra.

2 Utgångspunkter för säkerhetsklassificering

Med säkerhetsklassificerad handling åsyftas i denna rekommendation handlingar som avses i 18 § 1 mom. i informationshanteringslagen. Klassificeringskravet gäller statliga myndigheter, inrättningar och affärsverk samt domstolar och nämnder som har inrättats för att behandla besvärsärenden.[1]

2.1 Klassificeringsgrunder

En säkerhetsklassificerad handling är alltid sekretessbelagd, men en sekretessbelagd handling är inte alltid säkerhetsklassificerad. Säkerhetsklassificering sker ifall handlingen eller dess uppgifter ska sekretessbeläggas enligt 24 § 1 mom. 2, 5 eller 7–11 punkterna i offentlighetslagen. Därtill finns rekvisitet att obehörigt avslöjande eller obehörig användning av information som ingår i handlingen kan orsaka skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet.[2]

En handling får inte förses med en anteckning om säkerhetsklass i andra fall än sådana som avses i 1 mom., om anteckningen inte behövs för att fullgöra en internationell förpliktelse som gäller informationssäkerhet eller om handlingen annars har samband med internationellt samarbete. Handlingar som avses i lagen om internationella förpliktelser som gäller informationssäkerhet ska förses med anteckning om säkerhetsklass i enlighet med den lagen.

1 se 18 § 1 mom. IHL

2 3 § i förordningen om säkerhetsklassificering beskriver för varje säkerhetsklass vilken skada obehörigt röjande eller obehörig användning av handlingen eller information i den kan orsaka.

2.2 Bedömning av säkerhetsklasser

Bedömningen av en handlings säkerhetsklass grundas på vilken skada ett obehörigt avslöjande av uppgifter i handlingen skulle orsaka. Vid bedömning av skaderekvisitet i säkerhetsklassificeringen ska bl.a. följande beaktas:

- vilket skyddat intresse i lagen orsakas skada
- skadans bedömda omfattning, storlek och varaktighet
- skadans eventuella konsekvenser
- huruvida ackumulering av handlingar utgör en risk (s.k. kumulativ effekt)
- vilka hot kan medföra att en skada eventuellt uppstår.

3 § 1 mom. 1–4 punkterna i förordningen om säkerhetsklassificering beskriver indelningen av handlingar i säkerhetsklasser:

1. handling i säkerhetsklass I, om obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen kan orsaka särskilt stor skada för ett sådant skyddat intresse som avses i 18 § 1 mom. i informationshanteringslagen
2. handling i säkerhetsklass II, om obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen kan orsaka betydande skada för ett sådant skyddat intresse som avses i 18 § 1 mom. i informationshanteringslagen
3. handling i säkerhetsklass III, om obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen kan orsaka skada för ett sådant skyddat intresse som avses i 18 § 1 mom. i informationshanteringslagen
4. handling i säkerhetsklass IV, om obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen kan orsaka lindrig skada för ett sådant skyddat intresse som avses i 18 § 1 mom. i informationshanteringslagen.

Myndigheterna rekommenderas att göra en förhandsbedömning av skaderiskerna så att klassificeringen blir enhetlig. Riskbedömningen ska beakta vilken skada skyddade intressen eventuellt orsakas om information avslöjas eller används på obehörigt sätt. En konkret bedömning av konsekvenserna för hela det skyddade intresset bör eftersträvas.

I enskilda fall är det möjligt att informationen ska sekretessbeläggas enligt 24 §: 1 mom. 2, 5 eller 7–11 punkterna, men att obehörigt avslöjande eller obehörig användning *inte kan* orsaka skada för Finland säkerhet såsom beskrivs i 18 § i informationsförvaltningslagen eller på jämförbart sätt. Då används märkningen **SEKRETESSBELAGD**. Trots att detta är möjligt i enskilda fall kan man i regel anse att skaderekvisitet i 18 § i informationshanteringslagen är uppfyllt då den motsvarande klausulen för sekretess enligt offentlighetslagen (24 § 1 mom. 2, 5 eller 7–11 punkterna) uppfylls.

För att undvika över- och underklassificering ska organisationen vara insatt i den särskilda regleringen av det egna verksamhetsområdet och se till att personalens kunskap om sekretess- och säkerhetsklassningsregleringen stärks. Organisationen ska säkerställa att handlingarna säkerhetsklassificeras på behörigt sätt. En informationshanteringsenhets ledning ska ta hand om ansvarsfördelning, vägledning, utbildning, tillgång till ändamålsenliga verktyg och tillsyn i informationshanteringen (4 § IHL). En rekommendation från Informationsförvaltningsnämnden tar mer specifikt upp genomförandet av ledningens ansvar (finansministeriet 2020:18).

Informationen ska klassificeras av den person som lämnar ett uppdrag i ärendet eller för första gången skapar informationen, eller av den person som beslutar om klassificering av handlingen. Den som gör klassificeringen bedömer eventuell sekretess och sekretessgrund (bestämmelse). Informationen ska säkerhetsklassificeras om den är sekretessbelagd enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i offentlighetslagen och om obehörigt avslöjande eller obehörig användning av informationen kan orsaka skada för försvaret, förberedelser inför undantagsförhållanden, internationella relationer, brottsbekämpningen, den allmänna säkerheten eller stats- och samhällsekonomins funktion eller på något annat jämförbart sätt för Finlands säkerhet. En handling med säkerhetsklassificerad information ska bedömas utifrån graden av potentiell skada och märkas med säkerhetsklass enligt denna grad. Bilaga 1 beskriver bedömningsprocessen för sekretess och säkerhetsklassificering (bilden tar inte hänsyn till lagen om internationella förpliktelser som gäller informationssäkerhet). Tabellen i bilaga 2 ger exempel på bedömning av skaderekvisitet i säkerhetsklassificeringen utifrån ett skyddat intresse.

Klassificeringen ska alltid ske utifrån en riskbedömning av det enskilda fallet. Effekten av att uppgifter sammankopplas och ackumuleras ska beaktas vid riskbedömningen och dimensioneringen av informationssäkerhetsåtgärder eftersom dessa faktorer kan höja risken och kräva säkerhetsåtgärder i informationshanteringen. Då t.ex. två uppgifter i TL IV-klass kopplas ihop kan slutresultatet bli TL IV-I. Hänsyn till ackumuleringen av information behandlas närmare i avsnitt 5.4.

Enligt 5 § i offentlighetslagen anses en handling ha blivit upprättad av en myndighet även när den har upprättats på uppdrag av myndigheten. På dessa tillämpas offentlighetslagens (eller andra) sekretessbestämmelser, och beslut om utlämnande av uppgifter ur dem fattas i regel hos den myndighet som givit uppdraget (14 § i offentlighetslagen). Uppdragsgivaren och -tagaren rekommenderas att avtala om säkerhetsklassificeringen ifall handlingar som ska säkerhetsklassificeras kommer att behandlas. Då t.ex. ett privat företag för en klassificeringsskyldig statlig myndighets räkning exempelvis ska utveckla och tillverka hårdvara eller mjukvara bör parterna i uppdragsavtalet komma överens om hur uppdragstagaren säkerhetsklassificerar handlingarna ifall information och handlingar som ska säkerhetsklassificeras kommer att produceras under uppdraget. Det är bra om parterna i varje fall på övergripande nivå avtalar om klassificeringen överlag samt nivån på säkerhetsklassen för vissa typer av uppgifter. Då kan den klassificeringsskyldiga myndigheten anses ha fattat det ursprungliga beslutet om klassificering av de berörda uppgifterna och sedan instruerat uppdragstagaren att följa det.

2.3 Motsvarighet till internationell säkerhetsklassificering

De handlingar som avses i lagen om internationella förpliktelser som gäller informationssäkerhet är informationsmaterial med särskilt skydd och ska säkerhetsklassificeras på det sätt som anges i denna lag. Med information i lagen åsyftas säkerhetsklassificerad information från andra stater eller internationella organisationer. 4 § i förordningen om säkerhetsklassificering reglerar den finländska säkerhetsklassificeringens motsvarighet vid tillgodoseende av internationella förpliktelser som gäller informationssäkerheten. Bestämmelsen tillämpas om inte något annat följer av internationella förpliktelser som gäller informationssäkerheten. Nationella säkerhetsmyndigheten (NSA) har gett ut en särskild anvisning om behandling av internationell säkerhetsklassificerad information. Tabellen nedan visar nationella och EU-säkerhetsklasser med förkortningar. Klassificeringsreglerna skiljer sig och när handlingar med EU-säkerhetsklasser behandlas ska man följa EU:s säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter. [3]

3 Se EU-rådets säkerhetsbestämmelser (2013/488/EU)

Tabell 1. Säkerhetsklasser med förkortningar och EU-motsvarigheter.

Nationell säkerhetsklass				EU-säkerhetsklass	
Säkerhetsklass I	TL I	YTTERST HEMLIG	(E)	TRÈS SECRET UE/EU TOP SECRET	TS-UE/ EU-TS
Säkerhetsklass II	TL II	HEMLIG	(S)	SECRET UE/EU SECRET	S-UE/ EU-S
Säkerhetsklass III	TL III	KONFIDENTIELL	(L)	CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/ EU-C
Säkerhetsklass IV	TL IV	BEGRÄNSAD TILLGÅNG	(R)	RESTREINT UE/EU RESTRICTED	R-UE/ EU-R

3 Anteckning om säkerhetsklass

3.1 Anteckningssätt

Anteckningen om säkerhetsklass visar hurdana informationssäkerhetsåtgärder man ska iaktta vid behandling av handlingen. En anteckning om säkerhetsklass får inte användas om det inte finns någon grund för säkerhetsklassificering. Sekretessgrunden ska anges vid anteckningen.

3 § 2–5 mom. i förordningen om säkerhetsklassificering reglerar märkningen av säkerhetsklasser. Antalet säkerhetsklasser inklusive märkningar är fyra:

- Handlingar i säkerhetsklass I förses med märkningen ”ERITTÄIN SALAINEN”,
- Handlingar i säkerhetsklass II förses med märkningen ”SALAINEN”,
- Handlingar i säkerhetsklass III förses med märkningen ”LUOTTAMUKSELLINEN” och
- Handlingar i säkerhetsklass IV förses med märkningen ”KÄYTTÖ RAJOITETTU”.

Utöver nämnda märkning kan märkningarna ”TL I”, ”TL II”, ”TL III” och ”TL IV” användas.

Handlingar i säkerhetsklass I-IV förses med klassens stämpel enligt mallen i bild 1 och vid behov även med stämpeln ”sekretessbelagd”. Lagrummet för sekretessgrunden ska anges på handlingen och i metadata. Anteckningar om sekretess grundar sig på offentlighetslagen och tas därmed inte upp i denna rekommendation.

Bild 1. Stämpelmallar för säkerhetsklassmärkning.

Anteckningen om säkerhetsklass görs på svenska i handlingar som har upprättats på svenska eller översatts till svenska. Anteckningen på svenska kan göras även i andra fall, om myndigheten anser det vara behövligt. Märkningen i fråga om säkerhetsklass I är då ”YTTERST HEMLIG”, i fråga om säkerhetsklass II ”HEMLIG”, i fråga om säkerhetsklass III ”KONFIDENTIELL” och i fråga om säkerhetsklass IV ”BEGRÄNSAD TILLGÅNG”.

Handlingens säkerhetsklass ska också framgå av uppgifterna om handlingen i det ärenderegister som avses i 25 § i informationshanteringslagen eller i något annat datalager som en myndighet allmänt använder för informationshantering.[4] Säkerhetsklassen kan anges i en bilaga eller separat handling som fogas till den säkerhetsklassificerade handlingen, om det inte är tekniskt möjligt att ange säkerhetsklassen genom en märkning i handlingen eller ändra en tidigare märkning, eller om de krav på behandlingen som svarar mot säkerhetsklassen behövs endast under en bestämd kortare tid.[5]

Av handlingen ska det klart framgå vilken del som innehåller säkerhetsklassificerade uppgifter. Detta kan t.ex. anges före relevanta paragrafer, kapitel eller bilagor med hjälp av säkerhetsklassernas finska förkortningar (E), (S), (L) eller (R). Om alla avsnitt har samma säkerhetsklass kan dessa sättas inom hakparantes och följande anges i början av handlingen: ”hakasulkeilla merkitty teksti on salassa pidettävää ja turvallisuusluokan X tietoa” (all text inom hakparentes är sekretessbelagd och innehåller uppgifter i säkerhetsklass X).

Uppgifternas säkerhetsklass kan också anges muntligt, till exempel då säkerhetsklassificerad information behandlas på ett möte. Allmän praxis internationellt är att säkerhetsklass, sidnummer och datum tydligt anges på varje sida. I handlingar i säkerhetsklass TL III - TL I som distribueras i flera exemplar anges ofta även kopians nummer på varje sida. Dessa förfaranden rekommenderas även för säkerhetsklassificerade nationella handlingar.

4 se 3 § 4 mom. i förordningen om säkerhetsklassificering

5 se 3 § 5 mom. i förordningen om säkerhetsklassificering

3.2 Slopande eller ändring av en märkning

När det inte längre finns några grunder för säkerhetsklassificeringen av handlingen enligt lag eller när det är nödvändigt att ändra säkerhetsklassen ska en behörig anteckning om slopad eller ändrad anteckning införas i den handling i vilken den ursprungliga anteckningen har införts samt i uppgifter om handlingen som avses i 3 § 4 mom. FSK. Senast när handlingen lämnas ut till utomstående ska märkningens korrekthet kontrolleras (5 § 1 mom. FSK).

Då klassificeringen ändras vidtas följande åtgärder:

- Ifall det är en handling på papper överstryks säkerhetsklassen eller sekretesstämpeln.
- Under stämpeln skriver den behöriga tjänstemannen ”salassapito päättynyt” (sekretessen upphävd), datum och sin namnteckning.
- Uppgift om att handlingen blivit offentlig införs i dokumentregistret.
- I elektroniska handlingar sker märkningen genom att metadata ändras. Handlingar som begärs ut förses med ett följebrev som anger när sekretessen upphävdes.
- Ändringen av metadata sparas i dokumentloggen.

Om en handling har mottagits av en annan myndighet, får en anteckning som gäller säkerhetsklass slopas eller ändras endast med tillstånd av den myndighet som har upprättat handlingen eller den myndighet som ska avgöra ärendet i dess helhet, såvida det inte är klarlagt att det inte längre finns några grunder för användningen av säkerhetsklass (5 § FSK). Behovet av en märkning som gäller säkerhetsklassificering i fråga om arkiverade handlingar eller handlingar som bevaras hos en statsförvaltningsmyndighet ska bedömas när statsförvaltningsmyndigheten tar upp handlingen till ny behandling (16 § FSK).

3.3 Tidigare klassificeringar och märkningar

Äldre handlingar som behandlades 2010–2019, innan den nuvarande förordningen och då Statsrådets förordning om informationssäkerheten inom statsförvaltningen var i kraft, behåller sina ursprungliga märkningar tills handlingen behöver tas upp till ny behandling. Då bedöms sekretessen och säkerhetsklassificeringen från fall till fall i enlighet med de uppdaterade bestämmelserna. Uppgifter med skyddsnivå I-IV kan då sekretessbeläggas och ifall kraven uppfylls också säkerhetsklassificeras. Tabellen nedan ger stöd för omprövningen.

Tabell 2. Sekretessen och säkerhetsklassificeringen ska prövas på nytt för varje handling.

Klassificering 2010 -2019	Klassificering 2020–
YTTERST HEMLIG, skyddsnivå I (SN I)	YTTERST HEMLIG TL I
HEMLIG, skyddsnivå II (SN II)	HEMLIG TL II
KONFIDENTIELL, skyddsnivå III (SN III)	KONFIDENTIELL TL III
BEGRÄNSAD TILLGÅNG, Skyddsnivå IV (SN IV)	BEGRÄNSAD TILLGÅNG TL IV
SEKRETESSBELAGD, Skyddsnivå III (SN III), Skyddsnivå IV (SN IV)	SEKRETESSBELAGD

Observera att då uppgifter efter omprövning har sekretessbelagts men inte säkerhetsklassificerats ska informationssäkerhetsåtgärder avvägas utifrån en riskbedömning i enlighet med informationshanteringslagen. Med avseende på informationshanteringsåtgärder för sekretessbelagd information rekommenderas att de avvägs utifrån rekommendationerna gällande handlingar i säkerhetsklass IV. Informationssäkerhetsåtgärder för sekretessbelagd information kan från fall till fall även avvägas utifrån rekommendationerna gällande handlingar i säkerhetsklass I-III.

4 Krav på behandlingen av handlingar

4.1 Registrering och uppföljning av behandlingen

En informationshanteringsenhet ska över ärenden som behandlas eller har behandlats hos en myndighet upprätthålla ett ärenderegister för information om ärenden, ärendebehandling och handlingar (25 § i informationshanteringslagen). Myndigheten ska utan dröjsmål i ärenderegistret registrera handlingar som har inkommit till myndigheten eller som den upprättat. Ärenderegister förs i syfte att uppfylla offentlighetsprincipen, specificera uppgifter som begärs ut, strukturera handlingar och motsvarande uppgifter, organisera ärendehanteringen, följa upp handläggningstider och styra processer. Utöver vad som föreskrivs i 26 § IHL om obligatoriska uppgifter i ärenderegister ska också handlingens ankomsttidpunkt framgå av registreringen.

14 § i förordningen om säkerhetsklassificering avser åtgärder som ska vidtas för att följa upp behandlingen av handlingar såsom registrering för säkerhetsändamål. Då rätt att behandla handlingar ges ska man beakta kraven avseende behandlingsrättigheter och förteckningen över dem i 8 § i förordningen om säkerhetsklassificering.

Vid registrering ska t.ex. 26 § i informationshanteringslagen beaktas med nedanstående preciseringar.

Behandlingsuppgifter som ska registreras:

- behandlare (person eller organisation, om ej myndigheten) och
- datum.

Mottagningsuppgifter som ska registreras:

- ursprunglig avsändare (organisation eller person),
- mottagare,
- annan behandlare, om handlingen tas emot av någon annan (t.ex. registratorskontoret).
- ankomstdatum,
- registreringsdatum och
- ankomstsätt (analogiskt/elektroniskt).

Avsändningsuppgifter som ska registreras:

- ursprunglig användare,
- annan behandlare, om handlingen skickas av någon annan (t.ex. registratorskontoret),
- mottagare,
- extern mottagare (organisation eller person),
- avsändningsdatum.
- registreringsdatum och
- avsändningsmetod (analog/elektronisk).

I informationshanteringsnämndens sektion för verksamhetsdriven ärendehantering bereds en rekommendation om informationshanteringsenheters ärendehantering samt registrering av handlingar.

4.1.1 Registrering och uppföljning av handlingar TL IV

Handlingar i säkerhetsklass IV (TL IV) ska i första hand upprättas och registreras i ärendehanteringssystemet, om det uppfyller TL IV-kraven. Mottagande organisationer eller personer ska antecknas på handlingen, följebrevet eller i anslutning till handlingen. Handlingar i säkerhetsklass IV förses med stämpeln för säkerhetsklass IV och vid behov även med stämpeln ”sekretessbelagd”. Lagrummet för sekretessgrunden ska anges på handlingen och i metadata. Ärendehanteringssystemet för handlingar i säkerhetsklass IV är oftast samma som används för allmän ärendehantering.

4.1.2 Registrering och uppföljning av handlingar TL III

Handlingar i säkerhetsklass III (TL III) upprättas i ett ärendehanteringssystem som uppfyller TL III -kraven eller något annat system som uppfyller TL III -kraven. Sändning och mottagning av handlingar ska registreras (14 § FSK). Behandlingen av handlingar i säkerhetsklass I–III ska följas upp i en elektronisk logg, i informationssystemet, i ett ärenderegister eller i själva handlingen (14 § FSK).

Om ärenderegistret inte uppfyller TL III-kraven ska handlingen registreras och följas upp manuellt eller via ett annat elektroniskt ärenderegister som har sekretessbelagts och säkerhetsklassificerats. TL III-I ärenderegister är oftast andra register än TL IV-ärenderegister

eller ärendehanteringssystem. Ärendenumren kan dock hanteras i ett och samma ärenderegister för offentliga, sekretessbelagda och säkerhetsklassificerade ärendenummer. Då ska man se till att sekretessbelagda eller säkerhetsklassificerade uppgifter inte införs i metadata för det offentliga ärenderegistret eller ärendehanteringssystemet.

Handlingar i säkerhetsklass III förses med stämpeln för säkerhetsklass III och vid behov även med stämpeln ”sekretessbelagd”. Lagrummet för sekretessgrunden ska anges på handlingen och i metadata.

Mottagande organisationer eller personer ska antecknas på handlingen, följebrevet eller i anslutning till handlingen. En förteckning ska föras över de personer som behandlar handlingar i säkerhetsklass III (14 § 1 mom. 4 punkten FSK). Förteckningen kan t.ex. finnas på ett försättsblad där man anger mottagaren av handlingen och vilka som tagit del av uppgiften. När handlingen är tillbaka på registratorskontoret (registreringsstället) ger försättsbladet uppgift om vilka som tagit del av uppgifterna. Om man har ett system som uppfyller TL III-kraven och möjliggör elektronisk uppföljning kan loggen eller annan systeminformation användas för att följa upp behandlarna.

Registreringsskyldigheten gäller bara uppgifter i form av handlingar. Utväxling av enstaka TL III-uppgifter (t.ex. samtal eller kort meddelande) som senare kan verifieras hos parterna i informationsutbytet behöver inte registreras särskilt. De som t.ex. tagit del av uppgifter på möten kan senare verifieras genom deltagarförteckningen.

TL III-handlingar ska helst behandlas elektroniskt, varvid ärendehanteringssystemet logg oftast räcker. När behandling, sändning och mottagning registreras manuellt ska man i första hand använda ärendehanteringssystemet där ärendet behandlas. Behandlingen kan även registreras på eller i anslutning till en pappershandling men då ska man försöka se till att uppgifterna införs i ett elektroniskt ärenderegister eller ärendehanteringssystemet.

Eftersom sändning och mottagning av handlingar ska registreras per handling får man inte i onödan skriva ut eller kopiera en TL III-handling för utökad distribution om handlingen kan behandlas elektroniskt på det sätt som ärendet kräver.

Den som behandlar TL III-handlingen svarar för att behandlingen registreras. Den som lämnar ut en handling ska manuellt registrera mottagaren då handlingen sänds eller kopieras. Avsändaren eller den angivna mottagaren av handlingen svarar för att sändning (till extern aktör) och mottagning (från en extern aktör) av en TL III-handling registreras.

4.1.3 Registrering och uppföljning av handlingar TL II

Handlingar i säkerhetsklass II (TL II) upprättas i ett ärendehanteringssystem som uppfyller TL II-kraven eller något annat system som uppfyller dessa krav. Sändning och mottagning av handlingar ska registreras (14 §). Behandlingen av handlingar i säkerhetsklass I–II ska följas upp i en elektronisk logg, i informationssystemet, i ett ärenderegister eller i själva handlingen (14 § FSK). Mottagande organisationer eller personer ska antecknas på handlingen, följebrevet eller i anslutning till handlingen.

Handlingar i säkerhetsklass II förses med stämpeln för säkerhetsklass II och vid behov även med stämpeln ”sekretessbelagd”. Lagrummet för sekretessgrunden ska anges på handlingen och i metadata. Registreringen ska visa till vem handlingen delats ut.

Handlingen upprättas i ett ärendehanteringssystem som uppfyller TL II-kraven eller något annat system som uppfyller de kraven. Om ärendehanteringssystemet inte uppfyller TL II-kraven ska handlingen registreras och följas upp manuellt eller via ett annat elektroniskt ärenderegister som har sekretessbelagts och säkerhetsklassificerats.

En förteckning ska föras över de personer som behandlar handlingar i säkerhetsklass II (14 § 1 mom. 4 punkten FSK). Förteckningen kan t.ex. finnas på ett försättsblad där man anger mottagaren av handlingen och vilka som tagit del av uppgiften. När handlingen är tillbaka på registratorskontoret (registreringsstället) ger försättsbladet uppgift om vilka som tagit del av uppgifterna. Om man har ett system som uppfyller TL II-kraven och möjliggör elektronisk uppföljning kan loggen eller annan systeminformation användas för att följa upp behandlarna.

4.1.4 Registrering och uppföljning av handlingar TL I

Handlingar i säkerhetsklass I upprättas manuellt eller på en separat arbetsstation som uppfyller kraven. Sändning och mottagning av handlingar ska registreras (14 § FSK). Behandling av en handling i säkerhetsklass I ska registreras i en elektronisk logg, i informationssystemet, i ett ärenderegister eller i själva handlingen (14 § 1 mom. 1 punkten FSK). Handlingen registreras och följs upp manuellt så att kraven för säkerhetsklass I uppfylls eller via ett elektroniskt ärenderegister som har sekretessbelagts och säkerhetsklassificerats och uppfyller kraven för säkerhetsklass I.

Handlingar i säkerhetsklass I förses med stämpeln för säkerhetsklass I och vid behov även med stämpeln ”sekretessbelagd”. Lagrummet för sekretessgrunden ska anges på handlingen och i metadata.

En förteckning ska föras över de personer som behandlar handlingar i säkerhetsklass I (14 § 1 mom. 4 punkten FSK). Förteckningen kan t.ex. finnas på ett säkerhetsklassificerat försättsblad där man anger mottagaren av handlingen och vilka som tagit del av informationen. När handlingen är tillbaka på registratorskontoret (registreringsstället) ger försättsbladet uppgift om vilka som tagit del av uppgifterna. Om man har ett system som uppfyller TL II-kraven och möjliggör elektronisk uppföljning så att uppgifter i säkerhetsklass I inte ingår i den kan loggen eller annan systeminformation användas för att följa upp personerna.

4.2 Utlämning och mottagning av handlingar

Kraven på behandling av informationsmaterial gäller informationens hela livscykel. Den som behandlar informationen har en särställning när det gäller att uppfylla kraven. Den som personligen behandlar uppgifter svarar i alla delar av informationsarbetet för att detta sker korrekt, enligt arbetsgivarens instruktioner och med verktyg som arbetsgivaren anvisat och godkänt. Myndighetsinformation kännetecknas av att en behörig myndighet eller myndighetsföreträdare ska identifieras eller anges för informationen. Den behöriga myndigheten har det centrala ansvaret för information inom dess behörighetsområde. 26 § 3 mom. i offentlighetslagen reglerar myndigheters skyldighet att se till att uppgifter hemlighålls och skyddas när sekretessbelagda uppgifter lämnas ut för skötseln av uppdrag. Uppgifterna lämnas ut till den som har rätt att ta del av dem. Bestämmelser om sekretess, tystnadsplikt och förbud mot utnyttjande finns i 22 och 23 § i offentlighetslagen.

4.2.1 Utlämning av handlingar

En statsförvaltningsmyndighet ska på förhand säkerställa att en säkerhetsklassificerad handling skyddas på behörigt sätt om myndigheten lämnar ut den till någon annan än en statsförvaltningsmyndighet. Kravet gäller inte utlämnande av information om handlingens innehåll på grundval av en parts rätt att få information. (6 § FSK). Åtminstone följande kan identifieras som situationer då handlingar lämnas ut: allmänna kriterier för utlämning av sekretessbelagda uppgifter, utlämning till en annan myndighet, utlämning till en annan statlig myndighet, utlämning till en uppdragstagare t.ex. företag och övrig utlämning efter begäran om att få ta del av uppgifter.

Myndigheten ska upprätthålla betryggande förfaranden genom vilka endast personer som har rätt att ta del av informationen kan behandla säkerhetsklassificerad information. Myndigheten ska använda tillräckligt starka metoder, t.ex. stark autentisering, för att identifiera personer eller andra aktörer som erbjuds möjlighet att behandla säkerhetsklassificerad information.

Utlämningen av uppgifter ur handlingar som myndigheter innehar bestäms enligt offentlighetslagen. Klassificeringsmärkningen påverkar inte myndigheternas skyldighet att bedöma handlingens offentlighet i varje enskilt fall och för varje handling då någon begär att få ta del av den med stöd av offentlighetslagen. Klassificering enligt lagen om internationella förpliktelser som gäller informationssäkerhet ger inte möjlighet till sekretessprövning till skillnad från offentlighetslagen.

Beslut om att en myndighetshandling lämnas ut ska fattas av den myndighet som innehar handlingen, om inte något annat föreskrivs i lag (14 § i offentlighetslagen). Om någon hos en myndighet begär att få ta del av en handling som har upprättats av någon annan myndighet eller gäller ett ärende som behandlas av en annan myndighet, kan myndigheten överföra begäran till den myndighet som har upprättat handlingen eller som ärendet hör till (15 § 1 mom. OffL). Om någon hos en myndighet begär att få ta del av en handling i vilken enligt informationshanteringslagen en anteckning om säkerhetsklass ska göras och som har upprättats av en annan myndighet, ska myndigheten för avgörande överföra ärendet till den myndighet som har upprättat handlingen. (OffL 15 § 3 mom.).

Då någon begär att få ta del av en handling ska man utreda om det fortfarande finns en grund för sekretess och säkerhetsklassificering. Handlingssekretessen beror på vid vilken tidpunkt saken granskas. Sekretess- eller säkerhetsklassmärkningen återspeglar läget då handlingen upprättades. Konsekvenserna av att information i handlingen avslöjas kan förändras över tid.

Om de i lag angivna grunderna för säkerhetsklassificeringen av en handling upphör att gälla eller säkerhetsklassen behöver ändras, ska en behörig anteckning om slopad eller ändrad i 3 § avsedd märkning införas i den handling i vilken den ursprungliga märkningen har införts samt i de uppgifter om handlingen som avses i 3 § 4 mom. (5 § 1 mom. i förordningen om säkerhetsklassificering). Beslutet om att ändra handlingens säkerhetsklass fattas vanligtvis av den som är föredragande eller avgör ärendet. Senast när handlingen lämnas ut till utomstående ska märkningens korrekthet kontrolleras.

4.2.2 Mottagarnas åtgärder (utanför statsförvaltningen)

Myndigheter vid statliga ämbetsverk, inrättningar och affärsverk samt domstolar och nämnder som har inrättats för att behandla besvärsärenden ska säkerhetsklassificera handlingar (18 § IHL). Sådana krav ställs dock inte på alla mottagare av säkerhetsklassificerade handlingar, t.ex. kommuner, samkommuner, räddningsverk och privata uppdragstagare. I avsnitt 2.2 finns rekommendationer om säkerhetsklassificering och märkning till den som upprättar handlingar på uppdrag av en klassificeringsskyldig myndighet.

Mottagaren ska behandla handlingarna på överenskommet sätt (säkerhetsavtal e.d.) enligt den överlämnande myndighetens instruktioner. Mottagaren ska säkerställa att utomstående inte får del av säkerhetsklassificerade handlingar. En säkerhetsklassificerad handling är alltid sekretessbelagd och omfattas självfallet av offentlighetslagens bestämmelser om sekretess, tystnadsplikt och förbud mot utnyttjande (22 och 23 §) och informationshanteringslagens bestämmelser. Mottagande parter rekommenderas att komplettera sina behandlingsinstruktioner med erhållna instruktioner för behandling av säkerhetsklassificerade handlingar och att anordna utbildning om detta.

Alla informationshanteringsenheter, även den som inte är klassificeringsskyldig, ska i enlighet med 25 § i informationshanteringslagen utan dröjsmål ärenderegistrera en säkerhetsklassificerad handling som kommit in dit eller upprättats där. Mottagaren av handlingen, t.ex. registratorskontoret, kontrollerar vilken tjänsteman som har rätt att behandla den på tjänstens vägnar. När handlingen skickas till tjänstemannen ska transportförfarandena i avsnitt 4.4 beaktas. När mottagaren är någon annan än den informationshanteringsenhet som avses i informationshanteringslagen ska denna aktör kontrollera vilka som har rätt att få ta del av den säkerhetsklassificerade informationen och lämna handlingen endast till dessa.

4.3 Överföring av handlingar via datanätet

Säkerhetsklassificerade handlingar får överföras från en myndighets skyddade säkerhetsområde via informationssystem eller datakommunikationsarrangemang som har en lägre säkerhetsnivå än säkerhetsklassen i fråga endast om handlingarna krypterats med tillräckligt stor tillförlitlighet. Om säkerhetsklassificerade handlingar överförs inom ett säkerhetsområde i andra datanät än det allmänna datanätet och uppgifterna kan skyddas tillräckligt med hjälp av metoder för fysiskt skydd, får okrypterad överföring eller kryptering på lägre säkerhetsnivå användas (12 § FSK). Tillämpning av en okrypterad eller lägre säkerhetsnivå kräver fysisk tillträdeskontroll som förhindrar att obehöriga får åtkomst till informationen. Följande aspekter ska beaktas vid överföring:

1. Då säkerhetsklassificerad information flyttas utanför fysiskt skyddade områden, t.ex. via ett offentligt nät, skyddas materialet eller datatrafiken genom tillräckligt säker kryptering.
    - Till offentliga nät räknas bland annat Internet och teleoperatörernas MPLS-nät.
    - I praktiken kan man för kryptering exempelvis använda VPN-lösningar mellan användarnas terminaler och myndighetens informationssystem, IPSec-kryptering mellan organisationers nätverk samt olika lösningar för e-postkryptering och filkryptering som tillhandahålls slutanvändarna.

2. Vid överföring av säkerhetsklassificerad information mellan fysiskt skyddade områden och inom ett nät med åtminstone motsvarande skyddsnivå är det utifrån riskhanteringsprocessens resultat möjligt att använda överföring med lägre skyddsnivå eller utan kryptering.
3. Processer för hanteringen av krypteringsrutiner och -nycklar har planerats och implementerats. Användarna har fått beskrivningar av, instruktioner om och utbildning i rutinerna och processerna.
4. Endast behöriga användare och processer har tillgång till krypteringsnycklarnas skyddade uppgifter. Processerna ska åtminstone kräva
    - kryptografiskt tillräckligt starka nycklar,
    - säker nyckeldistribution,
    - säker nyckelförvaring,
    - regelbundna nyckelutbyten,
    - utbyte av gamla eller avslöjade nycklar och
    - förhindrande av obehöriga nyckelutbyten.

I valet av skyddslösningar för säkerhetsklassificerad myndighetsinformation rekommenderas främst krypteringslösningar som bedömts och godkänts av Cybersäkerhetscentrets NC-SA-funktion (Traficom 2020). Observera att krypteringslösningarna ska konfigureras samt användas med inställningar som bedömts vara säkra.

4.4 Transport av handlingar

Riskerna vid transporter ska identifieras och bedömas, och utifrån detta planeras och vidtas behövliga säkerhetsåtgärder. Enligt 13 § i förordningen får säkerhetsklassificerade handlingar transporteras från säkerhetsområden om de elektroniska datamedierna skyddas med tillräcklig kryptering. Myndigheten kan välja en adekvat krypteringslösning för säkerhetsklassen. Ifall datamediet skyddas med tillräcklig kryptering kan det t.ex. postas till mottagaren. Transporter av säkerhetsklassificerade handlingar utanför fysiskt skyddade säkerhetsområden ska utföras säkert. Krypteringslösningarnas säkerhet behandlas närmare i avsnitt 7.11.

4.4.1 Transport av okrypterade handlingar i säkerhetsklass IV

Vid transport av handlingar i säkerhetsklass IV måste man beakta att 13 § i förordningen om säkerhetsklassificering ställer krav på tillräcklig kryptering av elektroniska datamedier (t.ex. usb-minne, cd eller dvd). Särskilda krav på transport av dessa eller TL IV-pappersdokument ställs inte, och de kan packas på normalt sätt t.ex. för inlämning till posten. Det får dock inte framgå utvändigt att försändelsen innehåller sekretessbelagd, säkerhetsklassificerad information.

4.4.2 Transport av okrypterade handlingar i säkerhetsklass III–I

Vid transport av handlingar i säkerhetsklass III-I måste man beakta att 13 § i förordningen om säkerhetsklassificering ställer krav på tillräcklig kryptering av elektroniska datamedier (t.ex. usb-minne, cd eller dvd). Okrypterade handlingar (papper eller elektroniska datamedier, t.ex. usb-minne, cd eller dvd) i säkerhetsklass III-I packas på lämpligt sätt och transporteras till mottagaren under kontinuerlig övervakning eller på något annat säkert sätt som godkänts av den statliga myndigheten och genom vilket handlingens konfidentialitet och integritet garanteras på ett tillräckligt sätt för säkerhetsklassen i fråga. Handlingen kan t.ex. skickas med en kurir eller kurirtjänst eller hämtas av mottagaren. Myndigheten ska ha godkänt förfarandet och aktörerna utifrån en riskbedömning av transporter med handlingar i denna säkerhetsklass.

Organisationen kan använda en intern funktion, vanligtvis registratorskontoret, för central inlämning av okrypterade handlingar i säkerhetsklass III-I som ska transporteras. Funktionen ska ha alla förfaranden, instruktioner och verktyg som behövs för säker transport. Endast godkänd personal får ingå i den interna funktionen och behandlingskedjan.

Organisationen ska ha säkerhetskuvert, hemliga kuvert eller säkerhetspåsar för transport av handlingar i säkerhetsklass III-I. Dessa ska alltid inneslutas i ett vanligt kuvert. Observera att det aldrig får framgå utvändigt att försändelsen innehåller säkerhetsklassificerad information. Det yttre kuvertet ska förses med mottagaradress (typiskt myndighetens registratorskontor) och avsändaradress, så att försändelsen kan returneras om mottagaren inte nås. Att försändelsen innehåller säkerhetsklassificerad information framgår först när man öppnar ytterkuvertet. Kuvert eller förpackningar ska vara ogenomskinliga.

Då handlingen går som internpost kan den finnas i en förseglad påse eller lämnas personligen till mottagaren. Avsändarorganisationen ska registrera försändelsedatumet och -mottagaren, och avsändaren ska bevaka försändelsens framkomst. Mottagaren kontrollerar att förseglingen är intakt och meddelar omgående eventuella misstankar om att den brutits. Avsändaren får en mottagningsbekräftelse via en returblankett i försändelsekuvertet eller någon annan uppföljningsmetod.

Försändelser med information i säkerhetsklass III-I delas företrädesvis ut till myndighetens registratorskontor eller någon annan ansvarig för registrering av försändelser och handlingar. På själva handlingen är det rekommendabelt att så noga som möjligt ange mottagarna (person eller befattning) och deras organisationsuppgifter.

4.5 Kopiering av handlingar

Säkerhetsklassificerade handlingar får kopieras både på papper och elektroniskt, om man iakttar kopieringsbegränsningarna, reglerna för hantering av kopior och andra krav på t.ex. informationssystem och datakommunikation vid behandling av säkerhetsklassificerade handlingar. En handling i säkerhetsklass II-I får inte kopieras utan tillstånd av den myndighet som har upprättat handlingen (14 § FSK). Tillståndet ska dokumenteras och uttryckligen nämna kopiering och eventuell utökad distribution av handlingen. Tillståndet ska arkiveras i anslutning till handlingen. Uppgifter om vilka som tagit del av den införs i arkivet. En förteckning över kopior av handlingar i säkerhetsklass II-I och över de som behandlar dessa ska upprättas (14 § FSK). Alla kopior som tas ska numreras och förtecknas.

Handlingar i säkerhetsklass II-I ska kopieras centralt inom organisationen enligt särskilda kopieringsinstruktioner. Myndigheten ska ha godkänt kopieringsutrustningen för den berörda säkerhetsklassen då det tas papperskopior av handlingar.

4.6 Förvaring av uppgifter

4.6.1 Förvaring av uppgifter i säkerhetsklass IV (TL IV)

Datalager som innehåller handlingar i säkerhetsklass IV BEGRÄNSAD TILLGÅNG (TL IV) och de informationssystem som används för behandlingen av dessa handlingar ska placeras inom ett säkerhetsområde och pappershandlingar i säkerhetsklass IV ska förvaras inom ett säkerhetsområde (FSK 10 §). Pappershandlingar i säkerhetsklass TL IV ska förvaras inom ett administrativt eller skyddsområde i låsbara kontorsmöbler som bedöms vara lämpliga. De kan tillfälligt förvaras utanför ett skydds- eller administrativt område om den som innehar handlingarna förbundit sig att följa de ersättande åtgärder som fastställs i myndighetens säkerhetsinstruktioner.

Då information i säkerhetsklass IV behandlas och förvaras i terminaler utanför säkerhetsområden ska uppgifterna vara skyddade med en tillräckligt säker krypteringslösning för den berörda säkerhetsklassen. Framförallt ska terminalens integritet säkerställas för den berörda säkerhetsklassen så att informationens konfidentialitet inte äventyras av en integritetsförlust. Skydd av informationssystem och datakommunikation behandlas närmare i kapitel 7.

4.6.2 Förvaring av uppgifter i säkerhetsklass III, II och I (TL III, TL II, TL I)

Handlingar i säkerhetsklassen YTTERST HEMLIG (TL I) får förvaras eller på annat sätt behandlas endast inom skyddsområden (10 § FSK).

Handlingar i säkerhetsklasserna KONFIDENTIELL (TL III) och HEMLIG (TL II) får behandlas inom och utanför säkerhetsområden, men datalager som innehåller handlingar i dessa säkerhetsklasser och datasystem där handlingarna behandlas ska placeras inom ett skyddsområde och pappershandlingar i säkerhetsklass II och III ska förvaras inom ett skyddsområde (10 § FSK).

Pappershandlingar i säkerhetsklass TL III, TL II och TL I ska förvaras inom ett skyddsområde i en förvaringslösning som bedöms vara lämplig, såsom kassaskåp eller valv.

Handlingar i säkerhetsklass II-III får behandlas inom eller utanför förvaltningsområden via terminaler och datakommunikation som uppfyller kraven. Terminalutrustning som används för behandling av handlingar i säkerhetsklass II ska dock förvaras inom ett skyddsområde. Om elektroniska handlingar i säkerhetsklass III förvaras i terminalutrustning utanför skyddsområden, ska de skyddas med en krypteringslösning som är tillräckligt säker för säkerhetsklassen. Datasäkerheten hos terminalutrustningen ska tryggas. (10 § FSK) Skyddet av informationssystem och datakommunikation behandlas närmare i kapitel 7.

4.7 Förstöring av handlingar

Enligt 15 § i förordningen om säkerhetsklassificering ska en säkerhetsklassificerad handling som inte längre behövs förstöras på ett sådant sätt att det för säkerhetsklassen i fråga tillräckligt tillförlitligt går att förhindra att informationen helt och hållet eller delvis återställs eller sammanställs på nytt. Mottagare av handlingar ska också se till att de förstörs på behörigt sätt. Om handlingen har upprättats av en annan myndighet, ska förstöringen av en handling i säkerhetsklass II–I som inte längre behövs anmälas till den myndighet som upprättat handlingen, om handlingen inte återlämnas till myndigheten (15 § FSK). Myndigheterna som är avsändare och mottagare kan avtala om praktiska förfaranden t.ex. att anmälningar som gäller säkerhetsklass II ska göras halvårsvis. Handlingar i säkerhetsklass I och II får förstöras endast av en person som myndigheten har förordnat för uppgiften. Versioner från de olika skedena i beredningen får förstöras av den person som har upprättat dem.

De tekniska framstegen påverkar även förstöringen av säkerhetsklassificerade uppgifter. Tillgänglig beräkningskapacitet möjliggör t.ex. effektivare återskapande av uppgifter från strimlade pappershandlingar. Det är allt oftare befogat att förstöra elektroniska lagringsmedier (hårddiskar, usb-minnen o.d.) genom t.ex. smältning i stället för att strimla på traditionellt sätt.

Informationen måste skyddas ända till slutet av livscykeln, vilket ska beaktas i synnerhet då tredjepartstjänster används för att förstöra informationen t.ex. genom smältning av hårddiskar. Det vanligaste förfaringssättet är att den organisation som ansvarar för informationen övervakar förstöringsprocessen till slutet av informationslivscykeln.

Här finns skäl att beakta personalens roll. Organisationen ska välja ett entydigt sätt på vilket personalen kan förstöra säkerhetsklassificerade uppgifter. I praktiken innebär det t.ex. ändamålsenliga dokumentförstörare och säkerställande av personalens säkerhetsmedvetenhet.

4.7.1 Strimlingskrav för säkerhetsklass IV (TL IV)

Exempel på strimlingskrav för information i säkerhetsklass IV:

- högst 30 mm2 stora partiklar av pappersmaterial (DIN 66399 / P5 eller DIN 32757 / DIN 4),
- högst 320 mm2 stora partiklar av magnetiska hårddiskar (DIN 66399 / H-5),
- högst 10 mm2 stora partiklar av SSD-hårddiskar och USB-minnen (DIN 66399 / E-5) och
- högst 10 mm2 stora partiklar av optiska medier (DIN 66399 / O-5).

4.7.2 Strimlingskrav för säkerhetsklass III (TL III)

Exempel på strimlingskrav för information i säkerhetsklass III:

- högst 30 mm2 stora partiklar av pappersmaterial (DIN 66399 / P5 eller DIN 32757 / DIN 4),
- högst 10 mm2 stora partiklar av magnetiska hårddiskar (DIN 66399 / H-6),
- högst 10 mm2 stora partiklar av SSD-hårddiskar och USB-minnen (DIN 66399 / E-5) och
- högst 5 mm2 stora partiklar av optiska medier (DIN 66399 / O-6).

4.7.3 Strimlingskrav för säkerhetsklass II (TL II)

Exempel på strimlingskrav för material i säkerhetsklass II:

- högst 10 mm2 stora partiklar av pappersmaterial (DIN 66399 / P6),
- högst 10 mm2 stora partiklar av magnetiska hårddiskar (DIN 66399 / H-6),
- högst 1 mm2 stora partiklar av SSD-hårddiskar och USB-minnen (DIN 66399 / E-6) och
- högst 5 mm2 stora partiklar av optiska medier (DIN 66399 / O-6).

4.7.4 Strimlingskrav för säkerhetsklass I (TL I)

Strimlingskraven för säkerhetsklass II kan användas då information i säkerhetsklass I (TL I) förstörs ifall skyddet kompletteras med myndighetsgodkända förfaranden. Vanliga förfaranden är bl.a. efterbehandling där man bränner eller smälter partiklarna under övervakning.

4.7.5 Kombination av metoder vid förstöring

Andra metoder som ersätter eller kompletterar strimlingsskyddet kan användas om metoden tillförlitligt förhindrar återskapande av uppgifterna (t.ex. smältning av partiklarna från en hårddisk). Kryptering av säkerhetsklassificerad information kan minska riskerna avsevärt i olika skeden av informationens och utrustningens livscykel. Detaljerade beskrivningar av hur elektronisk information förstörs finns i Cybersäkerhetscentrets överskrivningsanvisning (Kommunikationsverket 2016) (på finska).

4.7.6 Förstöring av elektronisk information

Särskilt förfarandena för tillförlitlig förstöring av elektroniskt material bör omfatta all utrustning som någon gång under livscykeln haft sparad säkerhetsklassificerad information. Förfarandena ska avtalas med tjänsteleverantörerna. Man ska också säkerställa att personalen vet hur man följer dem. Särskilt när delar av utrustningen (hårddiskar, minnen, minneskort osv.) tas ur bruk, skickas för underhåll eller går till återanvändning ska säkerhetsklassificerad information förstöras på ett tillförlitligt sätt. Om en tillförlitlig radering (t.ex. överskrivning godkänd av den behöriga myndigheten) inte är möjlig, ska delar som innehåller säkerhetsklassificerad information inte överlämnas till tredje part. När minnet eller motsvarande inte kan raderas på ett tillförlitligt sätt före underhållsarbetet bör man

övervaka det underhåll som utförs av tredje part och försäkra sig om att säkerhetsklassificerad information inte kommer i orätta händer i samband med underhållet.

Det ska finnas ett säkerhetsavtal med underhållsleverantören, som även ska ha namngiven och säkerhetsutredd underhållspersonal innan något underhåll utförs så att man kan försäkra sig om att dess personal och organisation är säker.

5 Utgångspunkter för flernivåskydd av handlingar och databehandling

5.1 Planering av informationshanteringen och säkerheten

Informationshanteringen utgår från behoven i myndighetens verksamhet. Informationshanteringslagen skapar en ram för enhetlig och kvalitativ hantering av myndigheters informationsmaterial. Informationshanteringen planeras med beaktande av olika slags informationsmaterial, behandlingsskeden, administration av deras uppgifter samt förändringar på informationshanteringsenheterna. 5 § i informationshanteringslagen reglerar informationshanteringsmodellen och konsekvensbedömningen av förändringar. När det sker eller planeras väsentliga administrativa förändringar eller tas i bruk informationssystem på informationshanteringsenheterna ska de bedöma vilken betydelse detta har för informationssäkerhetskraven och -åtgärderna. De förändrade kraven ska beaktas i informationshanteringsmodellen. Informationshanteringsnämndens rekommendation för en informationshanteringsmodell (finansministeriet 2020:29) ger vägledning för utarbetande av modellen och rekommendationen om bedömning av förändringar i informationshanteringen (finansministeriet 2020:53) rekommenderar att en konsekvensbedömning görs.

Grundläggande för informationshanteringen är att de centrala arrangemangen och säkerhetsåtgärderna planeras. Planeringen bör utgå från riskhanteringen och kraven på myndighetens verksamhet. Informationssäkerheten bygger på en kombination av olika åtgärder. Flernivåskyddet regleras i förordningen om säkerhetsklassificering (7 § FSK). Genom detta skydd säkerställs att andra säkerhetsåtgärder förebygger, förhindrar och begränsar skador ifall ett skydd fallerar. Dessutom planeras åtgärder för att upptäcka och spåra aktivitet och händelser som äventyrar skyddet. Om säkerheten äventyras ska säkerhetsåtgärderna se till att verksamheten återgår till föregående säkerhetsnivå snarast möjligt.[6]

6 se 7 § i förordningen om säkerhetsklassificering

5.2 Riskbedömning

Skyddet av säkerhetsklassificerade uppgifter bygger på riskhantering. Säkerhetsåtgärderna planeras utifrån en riskbedömning. Olika utvärderingar och revisioner stöder riskhanteringen. Då säkerhetsåtgärder planeras ska man i synnerhet beakta

- myndighetens verksamhet eller verksamhetsområde,
- de säkerhetsklassificerade uppgifternas säkerhetsklass, betydelse och användningsändamål,
- personalsäkerhet, t.ex. risken att tjänstemän utsätts för otillbörlig påverkan,
- mängden och sammanställningen av information,[7]
- sätt på vilka säkerhetsklassificerade uppgifter behandlas,
- miljön där säkerhetsklassificerade uppgifter behandlas och förvaras (byggnadens omgivning, platsen i byggnaden, lokalen eller i en del av den),
- behandlings- och förvaringsmiljön för elektronisk säkerhetsklassificerad information, t.ex. data i molntjänster, som kan finnas i olika stater och på vilka annan lagstiftning därmed är tillämplig,
- hot mot uppgifterna, såsom den risk underrättelsetjänster, brottslig verksamhet och egen personal bedöms utgöra samt
- kostnaderna för informationssäkerhetsåtgärder.

5.3 Hänsyn till ackumuleringen av information

Kumulativ effekt är ett fenomen som handlar om att en stor mängd information kan utgöra en viktigare helhet än de enskilda uppgifterna. Klassificeringen och skyddsbehoven kan då vara annorlunda än för enskilda dataelement. Helheten i ett informationssystem med stor mängd information i en viss säkerhetsklass kan klassificeras högre än de enskilda uppgifterna – exempelvis kan en stor mängd sammankopplad information i säkerhetsklass IV utgöra en informationsresurs i säkerhetsklass III. Mängden är inte den enda faktorn. En anledning till att säkerhetsklassen höjs kan t.ex. vara sammankoppling av två datakällor.

7 se 5.3 Hänsyn till ackumuleringen av information

Man känner inte till något allmängiltigt sätt att beräkna den kumulativa effekten. När den beräknas ska man beakta informationshanteringslagens krav på säkerhetsklassificering. Inte ens en stor mängd sekretessbelagd information utan säkerhetsklassificering medför alltid en kumulativ effekt eller att kriterierna för säkerhetsklassificering uppfylls, utan ofta rör det sig bara om ackumulerad sekretessbelagd information utan säkerhetsklassificering. Likaså medför inte ens stor mängd säkerhetsklassificerad information alltid en kumulativ effekt. När den kumulativa effekten beräknas krävs från fall till fall en utredning av informationsresursens nuvarande och beräknade framtida sakinnehåll och en bedömning av huruvida säkerhetsklassen för den ackumulerade informationen ska höjas.

I vissa fall kan ackumulering till säkerhetsklass IV eller till och med klass III ske även med sekretessbelagda dataelement utan säkerhetsklassificering. Ett exempel är enskilda dataelement om företag som är centrala för Finlands försörjningsberedskap eller underhållet av kritisk infrastruktur, vilka kan tolkas utgöra affärshemligheter och därmed klassificeras som sekretessbelagd information utan säkerhetsklassificering. En viss sammankopplad grupp av dataelement skulle dock kunna skada t.ex. Finlands försvar, försörjningsberedskap eller förberedelser inför undantagsförhållanden, om den kommer i orätta händer. Sakinnehållet i sådan ackumulerad information kanske också behöver skyddas utifrån statens säkerhetsintressen (allmänintresset) och kan uppfylla kriterierna för säkerhetsklassificering.

När säkerhetsklassen för ett informationssystem eller någon annan viktig informationsresurs genom den kumulativa effekten tolkas överstiga de enskilda dataelementens nivå bör de fastställda skyddsmetoderna för informationsresursen uppfylla kraven i den högre säkerhetsklassen. Med fastställda skyddsmetoder avses att dessa bara ger åtkomst till den enskilda eller begränsade del av informationsinnehållet som personen behöver i sin befattning och att försök till obehörig utvidgning av åtkomsten upptäcks.

6 Skydd för behandlingen av handlingar samt informationssystem genom säkerhetsområden

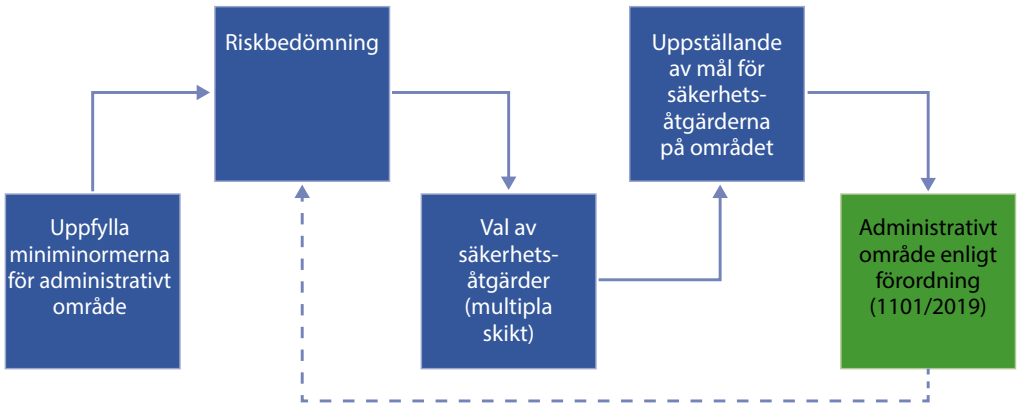
Enligt 9 § i förordningen om säkerhetsklassificering ska informationshanteringsenheten fastställa fysiskt skyddade *säkerhetsområden* för att skydda behandlingen av säkerhetsklassificerade handlingar samt informationssystem. Säkerhetsområdet är ett fysiskt skyddat administrativt område eller ett skyddsområde.

6.1 Skydd i administrativa områden

Med administrativt område avses områden och lokaler avsedda för myndighetens normala arbete såsom kontorsutrymmen eller kontorslokaler inklusive serverrum, datahallar och t.ex. företagslokaler. Den aktör som kontrollerar lokalerna säkerställer att endast personer som har auktoriserats av myndigheten har tillträde dit på egen hand. Några särskilda krav på den områdesavgränsande konstruktionen har inte ställts.

Minimikraven för ett administrativt område i denna rekommendation samt resultatet av myndighetens riskbedömning påverkar valet av fysiska säkerhetsåtgärder. Riskbedömning behandlas i avsnitt 5.2. De enskilda säkerhetsåtgärdernas och hela säkerhetssystemets effektivitet ska bedömas med regelbundna mellanrum. Processen för uppfyllelse av målbilden och regelbunden bedömning åskådliggörs i bilden nedan.

Bild 2. Målbildsprocess och regelbunden bedömning



6.1.1 Mål och metoder för fysiska säkerhetsåtgärder

Målet med fysiska säkerhetsåtgärder är att förhindra obehörig åtkomst till säkerhetsklassificerade uppgifter genom att

a) se till att säkerhetsklassificerade uppgifter behandlas och förvaras på ett lämpligt sätt,

b) möjliggöra kategorisering av personal och åtkomst till säkerhetsklassificerade uppgifter utifrån personernas behov att ta del av informationen och om det behövs utifrån personsäkerhetsutredningar,

c) förhindra, upptäcka och avskräcka från otillåtna handlingar och

d) förhindra eller försena intrång som sker i hemlighet eller genom tvång.

6.1.2 Val av fysiska säkerhetsåtgärder

Myndigheten ska utifrån en riskbedömning och med tillämpning av principen om flernivåskydd fastställa en lämplig och enligt riskbedömningen tillräcklig kombination av säkerhetsåtgärder bestående av administrativa, operativa och fysiska metoder såsom

- strukturella barriärer: fysiskt hinder för att avgränsa området eller utrymmet samt försvåra och försena intrång.
- passerkontroll: kontroller för att begränsa tillträdet till området eller utrymmet. Målet är att upptäcka obehöriga tillträdesförsök och förhindra att

obehöriga får tillträde samt kontrollera vilka som rör sig inom området. Passerkontrollen kan avse ett område, en eller flera byggnader inom ett område eller områden eller rum i en byggnad. Kontrollerna kan ske med mekaniska, elektroniska eller elektromekaniska tekniska system eller andra typer av fysiska metoder. Bevakningspersonal och receptionister kan delta i kontrollerna.

- intrångsdetekteringssystem: ett system för att upptäcka intrång (inbrottslarm) som kan användas till att förbättra den säkerhetsnivå som strukturella barriärer ger. Systemet kan också användas i stället för bevakningspersonal eller för att bistå denna.
- bevakningspersonal: personal som är utbildad, under tillsyn och vid behov säkerhetsutredd på lämpligt sätt kan sättas in bl.a. för att bistå passerkontrollen samt för att upptäcka och förhindra personer med planer på intrång i området eller lokalerna.
- kameraövervakning: övervakningen kan användas till att förebygga incidenter i området eller lokalerna, kontrollera larm och utreda incidenter. Bevakningspersonal kan använda kameraövervakningen för aktiv bildövervakning i realtid eller för passiv analys av bildmaterial i efterhand.
- förfaranden för upprätthållande av säkerheten: fastställande av ansvar och uppgifter, olika processer och handlingsmodeller, såsom behörighetsadministration och nyckelhantering, anvisningar och introduktion till personalen samt service och underhåll av systemen.
- belysning: eventuella inkräktare kan avskräckas med belysning, som ger bevakningspersonalen möjlighet att effektivt övervaka området antingen direkt eller indirekt via ett kameraövervakningssystem.
- andra lämpliga fysiska åtgärder för att avskräcka från eller upptäcka obehörigt tillträde eller förhindra att säkerhetsklassificerade uppgifter går förlorade eller skadas.

6.1.3 Miniminormer för fysiska säkerhetsåtgärder i administrativa områden

Det administrativa område som fastställs av myndigheten ska uppfylla alla miniminormer som anges i tabellen. Myndigheten ska dessutom planera, ansvarsfördela och vidta övriga riskhanteringsåtgärder utifrån riskbedömningen och principen om flernivåskydd samt upprätthålla åtgärderna så att den kvarstående risken med avseende på de säkerhetsklassificerade uppgifterna är acceptabel och målet med säkerhetsåtgärderna kan uppnås.

Tabell 3. Miniminormer för fysiska säkerhetsåtgärder i administrativa områden

Delområde	Miniminormer	Mer information och rekommendationer
Områdets gränser och strukturer (väggar, dörrar, fönster, golv- och takkonstruktioner)	Området ska ha tydligt bestämda synliga gränser. Det ställs inga specifika krav på den områdesavgränsande konstruktionen.	Med tanke på ändamålsenlig passerkontroll ska det vara möjligt att låsa alla öppningar till området som inte används för in- och utpassering. Områdets strukturer ska förstärkas om säkerhetsklassificerade uppgifter förvaras där och inbrottsrisken anses sannolik.
Beviljande av tillträdesrätt (behörigheter)	Endast personer som auktoriserats på behörigt sätt av myndigheten har tillträde till området på egen hand. Myndigheten ska fastställa förfarandena och rollerna i behörighets- och nyckelhanteringen för området.	Tillträdet till området kan begränsas med mekaniska eller elektroniska metoder eller genom personigenkänning. Det ska utses en områdesansvarig som hanterar behörigheterna, passerbrickorna och nycklarna. Myndigheten ska ha fastställt eller godkänt åtminstone följande förfaranden och roller: • förfaranden och roller för behörighets- och nyckelhantering har skapats, dokumenterats och instruerats • det finns en lista över innehavare av behörigheter och nycklar • behörigheterna kontrolleras regelbundet och uppdateras • ansvariga för extrabeställningar och ändringar av nycklar och passerbrickor har utsetts. • nyckelkort, icke utlämnade nycklar och passerbrickor förvaras på lämpligt sätt.

Delområde	Miniminormer	Mer information och rekommendationer
Besökare	Personer som inte har auktoriserats på behörigt sätt av myndigheten (besökare) ska alltid ha en följeslagare.	Myndigheten ska ha antagit riktlinjer som gäller besökare. Myndighetens besöksinstruktioner kan omfatta bl.a. följande: • besökaren identifieras och förses med en besökarbricka • besöket registreras • besökare ska inte släppas in eller lämnas i lokalerna utan tillsyn. Värden ansvarar för utomstående personer under hela besöket. • personalen har fått anvisningar om värdskapet • tillsyn över att besökare inte orättmätigt ser, hör eller på annat sätt får del av säkerhetsklassificerade uppgifter.
Ljudisolering	Områdets ljudisolering ska göra det omöjligt för obehöriga att tydligt uppfatta diskussioner om säkerhetsklassificerade uppgifter. Det ska också finnas ljudisolering inom området ifall man där diskuterar säkerhetsklassificerade uppgifter som alla inte behöver ta del av.	Normen för ljudisolering gäller endast de utrymmen i området där säkerhetsklassificerade uppgifter diskuteras.
Tekniska säkerhetssystem	Myndigheten ska försäkra sig om att säkerhetssystem och utrustning för fysiskt skydd av säkerhetsklassificerade uppgifter (t.ex. lämpliga förvaringslösningar, dokumentförstörare, lås, elektroniska passersystem, kameraövervakningssystem, intrångsdetekterings- och larmsystem) är lämpliga för ändamålet och funktionsdugliga.	Rekommendationen är att utrustningen uppfyller godkända tekniska standarder och miniminormer. Utrustningen hålls i funktionsdugligt skick genom behövliga service- och reparationsåtgärder, funktionstester och uppdaterad dokumentation enligt tillverkarens anvisningar och rekommendationer. Vid hanteringen av systemrättigheter rekommenderas iakttagande av principen om begränsad behörighet (se 7.6).
Intrångs-detekterings-system	Inga normer.	Området eller ingångarna till området kan förses med ett intrångsdetekteringssystem (inbrottslarm) om säkerhetsklassificerade uppgifter förvaras i området och inbrottsrisken anses hög. Övervakning med hjälp av systemet rekommenderas när ingen arbetar i området.

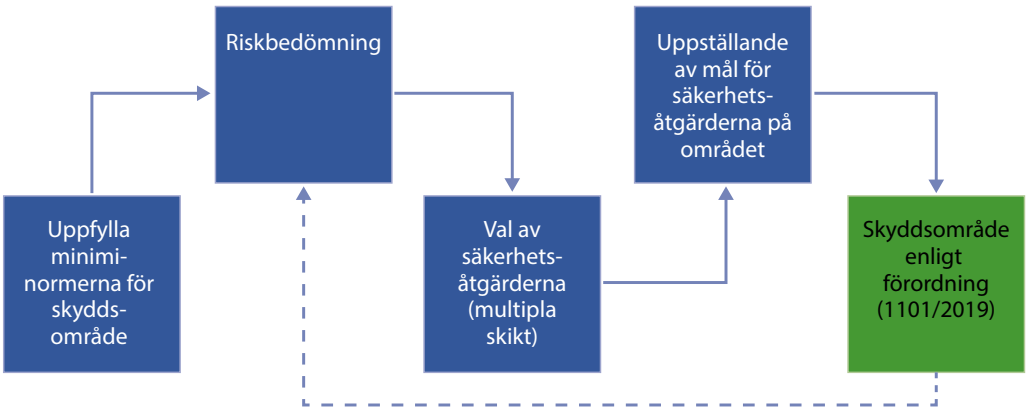
Delområde	Miniminormer	Mer information och rekommendationer
Åtgärder mot tjuvtittande	Om det finns en risk för avsiktligt eller oavsiktligt tjuvtittande på säkerhetsklassificerade uppgifter ska lämpliga åtgärder vidtas för att avvärja risken.	Risken för tjuvtittande kan reduceras bl.a. genom arbetsplatsernas placering och avskärmning samt persienner, gardiner eller skydd för datorskärmar.
Inspektioner av lokaler och utrustning	Myndigheten ska inspektera alla elektroniska apparater innan de används inom ett administrativt område där uppgifter i säkerhetsklass II (HEMLIG) behandlas och ifall hotnivån bedöms som hög även där uppgifter i säkerhetsklass III (KONFIDENTIELL) behandlas. Området ska vid behov inspekteras fysiskt eller tekniskt med regelbundna mellanrum. Området bör också inspekteras efter att någon fått obehörigt tillträde eller vid misstanke om detta.	Om det inte är möjligt att tillförlitligt inspektera berörda elektroniska apparater (t.ex. mobiltelefoner, smartklockor) ska de lämnas utanför lokalerna, t.ex. i en förvaringslösning för detta ändamål.
Förvaring av uppgifter	Information i säkerhetsklass IV (BEGRÄNSAD TILLGÅNG) kan förvaras inom området. Uppgifterna ska förvaras i lämpliga låsbara kontorsmöbler. Om elektroniska handlingar i säkerhetsklass III eller IV förvaras i terminalutrustning utanför skyddsområden, ska de skyddas med en krypteringslösning som är tillräckligt säker för säkerhetsklassen. Datasäkerheten hos terminalutrustningen ska tryggas.	

6.2 Skyddsområden

Med skyddsområde avses områden och lokaler avsedda för myndighetens arbete där säkerhetsklassificerade uppgifter behandlas och förvaras och som har ett bättre skydd än administrativa områden. Exempel på skyddsområden är serverrum, datahallar, arkiv och även företagslokaler som uppfyller skyddsområdeskraven, om man där behandlar eller förvarar säkerhetsklassificerade handlingar såsom avses i 10 § i förordningen om säkerhetsklassificering. Ett skyddsområde kan temporärt inrättas inom administrativt område för att hålla ett säkerhetsklassat möte eller liknande ändamål ifall miniminormerna för skyddsområden är uppfyllda i det berörda utrymmet.

Minimikraven för ett skyddsområde i denna rekommendation samt resultatet av myndighetens riskbedömning påverkar valet av fysiska säkerhetsåtgärder. Riskbedömning behandlas i avsnitt 5.2. De enskilda säkerhetsåtgärdernas och hela säkerhetssystemets effektivitet ska bedömas med regelbundna mellanrum. Processen för uppfyllelse av målbilden och regelbunden bedömning åskådliggörs i bilden nedan.

Bild 3. Målbildsprocess och regelbunden bedömning



6.2.1 Mål och metoder för fysiska säkerhetsåtgärder

Målet med fysiska säkerhetsåtgärder är att förhindra obehörig åtkomst till säkerhetsklassificerade uppgifter genom att

a) se till att säkerhetsklassificerade uppgifter behandlas och förvaras på ett lämpligt sätt,

b) möjliggöra kategorisering av personal och åtkomst till säkerhetsklassificerade uppgifter utifrån personernas behov att ta del av informationen och om det behövs utifrån personsäkerhetsutredningar,

c) förhindra, upptäcka och avskräcka från otillåtna handlingar och

d) förhindra eller försena intrång som sker i hemlighet eller genom tvång.

6.2.2 Val av fysiska säkerhetsåtgärder

Myndigheten ska utifrån en riskbedömning och med tillämpning av principen om flernivåskydd fastställa en lämplig och enligt riskbedömningen tillräcklig kombination av säkerhetsåtgärder bestående av administrativa, operativa och fysiska metoder såsom

- strukturella barriärer: fysiskt hinder för att avgränsa området eller utrymmet samt försvåra och försena intrång.
- passerkontroll: kontrollerna begränsar tillträdet till området eller lokalerna. Målet är att upptäcka obehöriga tillträdesförsök, förhindra att obehöriga får tillträde samt kontrollera vilka som rör sig inom området. Passerkontrollen kan avse ett område, en eller flera byggnader inom ett område eller områden eller rum i en byggnad. Kontrollerna kan utföras genom mekaniska, elektroniska eller elektromekaniska tekniska system, bevakningspersonal eller receptionister eller andra typer av fysiska metoder.
- intrångsdetekteringssystem: ett system för att upptäcka intrång (inbrottslarm) som kan användas till att förbättra den säkerhetsnivå som strukturella barriärer ger. Övervakningen kan också användas i utrymmen, rum och byggnader i stället för bevakningspersonal eller för att bistå denna.
- bevakningspersonal: personal som är utbildad, under tillsyn och vid behov säkerhetsutredd på lämpligt sätt kan användas i säkerhetsövervakningen bl.a. för att bistå passerkontrollen samt för att upptäcka och förhindra personer med planer på intrång i området eller lokalerna (respons).

- kameraövervakning: övervakningen kan användas till att förebygga incidenter i området eller lokalerna, kontrollera larm och utreda incidenter. Bevakningspersonal kan använda kameraövervakningen för aktiv bildövervakning i realtid eller för passiv analys av bildmaterial i efterhand.
- förfaranden för upprätthållande av säkerheten: fastställande av ansvar och uppgifter, olika processer och handlingsmodeller, såsom behörighetsadministration och nyckelhantering, anvisningar och introduktion till personer samt service och underhåll av systemen.
- belysning: eventuella inkräktare kan avskräckas med belysning, som ger bevakningspersonalen möjlighet att effektivt övervaka området antingen direkt eller indirekt via ett kameraövervakningssystem.

- andra lämpliga fysiska åtgärder för att avskräcka från och upptäcka obehörigt tillträde eller förhindra att säkerhetsklassificerade uppgifter går förlorade eller skadas.

6.2.3 Miniminormer för fysiska säkerhetsåtgärder i skyddsområden

Det skyddsområde som fastställs eller godkänns av myndigheten ska uppfylla alla miniminormer som anges i tabellen. Myndigheten ska dessutom planera, delegera och vidta övriga riskhanteringsåtgärder utifrån riskbedömningen och flernivåskyddet samt upprätthålla åtgärderna så att den kvarstående risken med avseende på de säkerhetsklassificerade uppgifterna är acceptabel och målet med säkerhetsåtgärderna kan uppnås.

Tabell 4. Miniminormer för fysiska säkerhetsåtgärder i skyddsområden

Delområde	Miniminormer	Mer information och rekommendationer
Områdets gränser och strukturer (väggar, dörrar, fönster, golv- och takkonstruktioner)	Området ska ha tydligt bestämda synliga gränser. Ifall området saknar en förvaringslösning som anses adekvat för informationen, ska områdets väggar, golv, tak, fönster och dörrar hålla den säkerhetsnivå som krävs för förvaringen.	Med tanke på tillförlitlig passerkontroll ska det vara möjligt att låsa alla öppningar till området som inte används för in- och utpassering. Områdets strukturer ska förstärkas om säkerhetsklassificerade uppgifter förvaras där och inbrottsrisken anses betydande. Om möjligt ska utrymningsvägar från ett administrativt område inte gå genom skyddsområdet. Detta ska beaktas framförallt vid nybyggnation. Utrymningen får inte organiseras så att säkerhetsåtgärderna försvagas.
Passerkontroll	All in- och utpassering vid områdesgränsen ska kontrolleras genom att personerna har passerkort eller identifieras personligen.	Passerkontrollen kan utföras elektroniskt eller bygga på personlig identifiering. Endast behöriga personer har passagerätt till skyddsområdet. Inpasseringar ska kunna verifieras efteråt.

Delområde	Miniminormer	Mer information och rekommendationer
Beviljande av tillträdesrätt (behörighet)	Självständig tillträdesrätt till området kan endast beviljas personer som på behörigt sätt auktoriserats av myndigheten och • vilkas pålitlighet har fastställts • som har ett särskilt tillstånd att få komma in på området. Myndigheten ska fastställa förfarandena och rollerna i behörighets- och nyckelhanteringen för området.	Pålitligheten bör främst fastställas genom förfarandet för personsäkerhetsutredning. Grunden för att få tillträde till området bör vara behovet att ta del av informationen. Från fall till fall kan ett särskilt tillstånd också avse behov av att arbeta i området. Det ska utses en områdesansvarig som hanterar behörigheterna, passerbrickorna och nycklarna. Myndigheten ska ha fastställt eller godkänt åtminstone följande förfaranden och roller: • förfaranden och roller för behörighets- och nyckelhantering har skapats, dokumenterats och instruerats • det finns en lista över innehavare av behörigheter och nycklar • behörigheterna kontrolleras regelbundet och uppdateras • ansvariga för extrabeställningar och ändringar av nycklar och passerbrickor har utsetts. • nyckelkort samt icke utlämnade nycklar och passerbrickor förvaras på lämpligt sätt.

Delområde	Miniminormer	Mer information och rekommendationer
Besökare	Personer som inte har beviljats självständig tillträdesrätt till lokalerna (besökare) ska alltid ha en följeslagare. Om inträde till skyddsområdet i praktiken innebär direkt åtkomst till säkerhetsklassificerade uppgifter som förvaras där gäller dessutom följande krav: den högsta säkerhetsklassen för uppgifter som normalt förvaras i området ska anges tydligt. Ifall tillträde till skyddsområdet innebär direkt åtkomst till säkerhetsklassificerade handlingar som behandlas där eller till uppgifter i dessa ska personer som får tillträde utan följeslagare också ha behov att ta del av dessa uppgifter såsom avses i 8 § 1 mom. Om behov att ta del av uppgifterna saknas ska säkerhetsåtgärder vidtas för att säkerställa att det inte finns någon åtkomst till säkerhetsklassificerade uppgifter.	Myndigheten ska ha antagit riktlinjer som gäller besökare. Myndighetens besöksinstruktioner kan omfatta bl.a. följande: • besökaren identifieras och förses med en besökarbricka, • besöket registreras, • besökare ska inte släppas in eller lämnas i lokalerna utan tillsyn. Värden ansvarar för utomstående personer under hela besöket, • personalen har fått anvisningar om värdskapet; tillsyn över att besökare inte orättmätigt ser eller hör säkerhetsklassificerade uppgifter.
Säkerhets-instruktioner	För varje skyddsområde ska det tas fram säkerhetsförfaranden som bl.a. anger följande: • säkerhetsklassen för de säkerhetsklassificerade uppgifter som får hanteras och förvaras inom området, • vilka övervaknings- och skyddsåtgärder som ska tillämpas, • vilka personer som har tillträde till området utan följeslagare grundat på särskilt tillstånd och fastställd pålitlighet, • vid behov förfaranden för användning av följeslagare eller skydd av säkerhetsklassificerade uppgifter när andra personer beviljas tillträde till området, • andra relevanta åtgärder och förfaranden.	

Delområde	Miniminormer	Mer information och rekommendationer
Ljudiso-lering	Områdets ljudisolering ska göra det omöjligt för obehöriga att tydligt uppfatta diskussioner om säkerhetsklassificerade uppgifter. Det ska också finnas ljudisolering inom området ifall man där diskuterar säkerhetsklassificerade uppgifter som alla inte behöver ta del av.	Normen för ljudisolering gäller endast de utrymmen i området där säkerhetsklassificerade uppgifter diskuteras.
Tekniska säkerhetssystem	Myndigheten ska försäkra sig om att säkerhetssystem och utrustning för fysiskt skydd av säkerhetsklassificerade uppgifter (t.ex. lämpliga förvaringslösningar, dokumentförstörare, lås, elektroniska passersystem, kameraövervakningssystem, intrångsdetekterings- och larmsystem) är lämpliga för ändamålet och funktionsdugliga. Systemen och utrustningen ska inspekteras och underhållas med regelbundna mellanrum.	Rekommendationen är att utrustningen uppfyller godkända tekniska standarder och miniminormer. Utrustningen hålls i funktionsdugligt skick genom behövliga service- och reparationsåtgärder, funktionstester och uppdaterad dokumentation enligt tillverkarens anvisningar och rekommendationer. Vid hanteringen av systemrättigheter rekommenderas iakttagande av principen om begränsad behörighet (se 7.6).
Intrångs-detekterings-system	Områden som inte har tjänstgörande personal dygnet runt ska efter behov inspekteras vid den normala arbetstidens slut och slumpvis utanför arbetstid, utom när området övervakas med intrångsdetekteringssystem (inbrottslarm).	Övervakning med hjälp av systemet rekommenderas när ingen arbetar i området.
Åtgärder mot tjuvtittande	Om det finns en risk för avsiktligt eller oavsiktligt tjuvtittande på säkerhetsklassificerade uppgifter ska lämpliga åtgärder vidtas för att avvärja risken.	Risken för tjuvtittande kan reduceras bl.a. genom avskärmning av arbetsplatser samt persienner, gardiner eller skydd för datorskärmar.
Inspektioner av lokaler och utrustning	I lokaler där uppgifter i säkerhetsklass I eller II behandlas får man endast ta in elektroniska apparater som godkänts av myndigheten. Området ska i så fall inspekteras fysiskt och tekniskt med regelbundna mellanrum. Inspektioner ska också utföras efter att någon fått obehörigt tillträde eller vid misstanke om detta.	Om det inte är möjligt att tillförlitligt inspektera berörda elektroniska apparater (t.ex. mobiltelefoner, smartklockor) ska de lämnas utanför lokalerna, t.ex. i en förvaringslösning för detta ändamål.

Delområde	Miniminormer	Mer information och rekommendationer
Förvaring av uppgifter	I området kan man förvara uppgifter i alla säkerhetsklasser utifrån riskbedömningen och valet av fysiska säkerhetsåtgärder. Uppgifter i säkerhetsklass III (KONFIDENTIELL) eller högre (TL II, TL I) ska förvaras i en förvaringslösning som bedömts vara lämplig. Myndigheten ska fastställa förfaranden för hantering av nycklar och kombinationer till förvaringslösningen. Kombinationerna ska ges till lägsta möjliga antal personer som behöver känna till dem. Dessa personer ska memorera kombinationerna. Kombinationerna till förvaringslösningar som innehåller säkerhetsklassificerade uppgifter ska bytas ut • vid mottagande av ett nytt säkert förvaringsställe • vid varje byte av personal som känner till kombinationen • vid inträffade eller misstänkta fall av röjande • när ett lås har genomgått underhållsarbete eller reparation • minst var tolfte månad. • Förvaring av säkerhetsklassificerade uppgifter i säkerhetsklass I (YTTERST HEMLIG) inom skyddsområdet måste uppfylla något av följande villkor: • tekniskt övervakad förvaringslösning, • förvaringslösning utan teknisk övervakning vars skick kontrolleras regelbundet, • förvaringslösning utan teknisk övervakning som har ett intrångsdetekteringssystem där larmen besvaras av en utbildad responsenhet, • separat utrymme med intrångsdetekteringssystem där larmen besvaras av en utbildad responsenhet.	

7 Minimikrav för skydd av informationssystem och datakommunikation

En informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel (13 § i informationshanteringslagen). Informationshanteringsenheten ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Myndigheten ska på förhand säkerställa att en säkerhetsklassificerad handling skyddas på behörigt sätt när myndigheten lämnar ut en sådan till någon annan än en statsförvaltningsmyndighet (6 § i förordningen om säkerhetsklassificering). Det kan ofta antas att intresset för säkerhetsklassificerade uppgifter kommer från annat håll än intresset för sekretessbelagda uppgifter som inte är säkerhetsklassificerade, t.ex. personuppgifter utan säkerhetsklassificering.

Skyddet av säkerhetsklassificerade uppgifter ska även beakta lagstiftningsrelaterade risker. Med lagstiftningsrelaterade risker avses de möjligheter som finns i olika länders lagstiftning att ålägga tjänsteleverantörer att samarbeta med landets myndigheter och t.ex. ge direkt eller indirekt åtkomst till kundernas sekretessbelagda uppgifter. Lagstiftningsrelaterade risker kan omfatta såväl den fysiska platsen för sekretessbelagd information som utlämning av uppgifter bl.a. via administrativ åtkomst från andra länder. Lagstiftningsbaserad utlämning och rätt att ta del av uppgifter har i många länder inskränkts till att gälla polis- och underrättelsemyndigheterna. Behandlingen av säkerhetsklassificerade uppgifter bör inskränkas till databehandlingsmiljöer och datasystem där myndigheten har kunnat försäkra sig om fullgod informationssäkerhet sett till riskerna.

Relevant för skyddet av data och riskbedömningen är också frågan om uppgifterna berörs av internationella informationssäkerhetsavtal. Om nationella säkerhetsklassificerade uppgifter kan komma att omfattas av en annan myndighets behörighet t.ex. på grund av teknisk underrättelseverksamhet ska man se till att denna eventualitet har behandlats ändamålsenligt i riskbedömningen och att den kvarstående risken är godtagbar. Detaljer i säkerhetsklassificerade internationella projekt behandlas närmare i nationella säkerhetsmyndighetens (NSA) handbok för företag (utrikesministeriet NSA 2015) och anvisningen om behandling av internationellt säkerhetsklassificerat informationsmaterial (utrikesministeriet NSA 2020) (på finska).

7.1 Skydd av uppgifter i och utanför verksamhetslokaler

Då uppgifter i säkerhetsklass IV eller III behandlas och förvaras i klassenlig terminalutrustning utanför säkerhetsområden eller uppgifter i säkerhetsklass III behandlas och förvaras i terminalutrustning inom administrativt område ska uppgifterna skyddas med en krypteringslösning som är tillräckligt säker för säkerhetsklassen och man ska särskilt försäkra sig om terminalutrustningens tillräckliga integritet för säkerhetsklassen så att uppgifternas konfidentialitet inte äventyras vid en förlust av integriteten.

Det vanligaste sättet att försäkra sig om informationssystemens integritet är att skydda dessa med fysisk tillträdeskontroll i säkerhetsområdena, däribland alla fysiska servrar, nätverksenheter, terminaler och kablar som hör till systemet. I skyddet av ett SK IV-informationssystems integritet mot allmänna risker för säkerhetsklassificerade uppgifter kan det t.ex. räcka med att systemets informationsresurser placeras inom ett administrativt eller skyddsområde, och för terminaler med tillräcklig kryptering kan även begränsad förvaring i något annat låsbart utrymme t.ex. hemma hos tjänstemannen vara tillräckligt.

Alla informationssystem för säkerhetsklass III bör placeras inom skyddsområden och **fasta nätverk för t.ex. säkerhetsklass III eller II kan inte byggas ut till ett administrativt område**. Ifall en terminal som används för behandling av uppgifter i säkerhetsklass III behöver förvaras inom ett administrativt område eller till och med utanför säkerhetsområdena kan man försöka kompensera avsaknaden av den fysiska tillträdeskontrollens integritetsskydd t.ex. genom att placera terminalen i ett förvar eller en förpackning som avslöjar obehörig åtkomst. Det finns exempelvis s.k. säkerhetsväskor för detektering av obehöriga åtkomstförsök så att den behöriga användaren av terminalutrustningen eller dennes organisation får ett meddelande vid obehörig åtkomst eller att åtkomstförsöket lämnar spår på förvaret eller förpackningen.

I princip ska man undvika att ta med säkerhetsklassificerad information på utlandsresor och i stället t.ex. använda en resepraxis som innebär att bara nödvändiga uppgifter och apparater tas med på resan. Särskild uppmärksamhet ska fästas vid att apparater med säkerhetsklassificerade uppgifter inte lämnas utan tillsyn under resan, t.ex. i hotellrummets värdeskåp, och att man bara i nödvändiga fall förlitar sig på andra metoder för skydd av integritet och konfidentialitet.

Myndighetens riskbedömning ska dock beakta att verksamhet utanför säkerhetsområdena inbegriper sådana risker för säkerhetsklassificerade uppgifter och den terminalutrustning med vilken uppgifterna behandlas, särskilt från och med säkerhetsklass III, att det i flera fall kan vara ytterst svårt eller rentav omöjligt att reducera dessa tillräckligt. Vid behandlingen ska man även skydda sig mot tjuvtittande och tjuvlyssnade samt riskbaserat t.ex. mot risker med diffus strålning.

7.1.1 Behandlingsverktyg för säkerhetsklass IV (TL IV)

Information i säkerhetsklass IV kan behandlas elektroniskt (även via fjärranslutning) med verktyg och system som arbetsgivaren anvisat, godkänt och instruerat för ändamålet. Handlingar får skrivas ut på en delad nätverksansluten multifunktionsenhet under förutsättning att nätverket och enheten uppfyller kraven för säkerhetsklass IV. Information kan behandlas utanför tjänstestället ifall insyn eller annan åtkomst till den blockeras för utomstående.

7.1.2 Behandlingsverktyg för säkerhetsklass III (TL III)

Information i säkerhetsklass III kan behandlas elektroniskt (även via fjärranslutning) med vissa verktyg och system som arbetsgivaren anvisat, godkänt och instruerat för arbetet. Tjänstemännen får inte ta kopior på erhållna handlingar i säkerhetsklass III så att distributionen utökas eftersom varje utlämning och mottagning av en handling ska registreras.

7.1.3 Behandlingsverktyg för säkerhetsklass II (TL II)

Information i säkerhetsklass II kan behandlas elektroniskt inklusive skrivas ut med vissa verktyg och system som arbetsgivaren anvisat, godkänt och instruerat för arbetet. Ifall information behandlas muntligt ska behandlingen ske i särskilt angivna lokaler (inom ett skyddsområde). En tjänsteman får inte kopiera erhållna handlingar i säkerhetsklass II.

7.1.4 Behandlingsverktyg för säkerhetsklass I (TL I)

Material i säkerhetsklass I behandlas huvudsakligen som material i klass II men enligt dessa strängare krav: uppgifter i säkerhetsklass I får endast behandlas inom skyddsområden, handlingarna ska upprättas på en arbetsstation som uppfyller kraven och får bara skrivas ut och kopieras på en skrivare som uppfyller kraven för säkerhetsklassen och har godkänts av myndigheten. Jämför informationssystem för olika säkerhetsklasser i avsnitt 7.2.

7.2 Avskiljning av informationssystem

Enligt 11 § 1 mom. 1 punkten i förordningen om säkerhetsklassificering ska informationssystem och datakommunikationsarrangemang som används för behandling av säkerhetsklassificerade handlingar genomföras så att de med beaktande av säkerhetsklassen för de handlingar som behandlas i dem avskiljs på ett tillräckligt tillförlitligt sätt från informationssystem eller datakommunikationsarrangemang på lägre säkerhetsnivå. Avskiljning av informationssystem hör till de effektivaste metoderna för att skydda sekretessbelagda

uppgifter. Syftet med avskiljning är att avgränsa miljön där sekretessbelagda uppgifter behandlas till en hanterbar helhet och i synnerhet att begränsa behandlingen till endast tillräckligt säkra miljöer.

Avskiljning av informationssystem och datakommunikationsarrangemang i säkerhetsklass IV från miljöer för andra säkerhetsklasser kan ske med brandväggar och styrning av trafiken i säkerhetskritiska tjänster med lägre säkerhetsklass (webbsidor, e-post o.d.) via proxyservrar som filtrerar innehållet. Informationssystem och datakommunikationsarrangemang i säkerhetsklass IV kan anslutas till internet och andra icke betrodda nätverk under förutsättning att riskerna med anslutningen går att reducera tillräckligt genom andra skydd så att nivån för säkerhetsklass IV uppnås. Då krävs framförallt att man sköter programuppdateringarna, tillämpar principen om begränsad behörighet (se avsnitt 7.6), minimerar systemets sårbarhetsyta och har förmåga att upptäcka incidenter och vidta korrigerande åtgärder.

En vanlig behandlingsmiljö för säkerhetsklass IV är organisationens kontorsdatamiljö där t.ex. arbetsstationer och ärendehanteringssystem avskiljs i nätverket genom olika skydd (t.ex. brandväggar och behörighetsadministration). Motsvarande avskiljning kan också tillämpas för att skydda sekretessbelagda uppgifter utan säkerhetsklassificering liksom för att skydda integriteten och användbarheten av offentliga uppgifter.

Från och med säkerhetsklass III kan avskiljningen i miljöer med olika säkerhetsklasser ske genom tillräckligt säkra gatewaylösningar. Dessa har som allmän planeringsprincip Bell-LaPadula-modellens ”No Read Up”- och ”No Write Down”-regler. Gatewaylösningarna ska med andra ord på ett tillförlitligt sätt hindra att uppgifter i en högre säkerhetsklass förmedlas till en miljö med lägre säkerhetsklass. Ett exempel på sådana är datadioder som bara möjliggör enkelriktad kommunikation. Avskiljning av informationssystem och datakommunikationsarrangemang i säkerhetsklass II kan i princip bara ske via datadiodlösningar med hög tillförlitlighet. Då informationssystem och datakommunikationsarrangemang i säkerhetsklass I avskiljs ska man även beakta att detta i princip ska ske genom fullständig fysisk isolering och bara i undantagsfall via datadiodlösningar. Planeringsprinciperna beskrivs mer detaljerat i Cybersäkerhetscentrets anvisning om gatewaylösningar (Kommunikationsverket 2018) (på finska).

Om internationellt klassificerad information behandlas i datasystemen ska man vid anslutning av informationssystem och datakommunikation också ta hänsyn till internationella förpliktelser gällande informationssäkerhet, som helt kan förbjuda anslutning. Enligt lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011) kan statliga myndigheter begära att Transport- och kommunikationsverket bedömer systemens eller arrangemangens överensstämmelse med kraven. Begäran rekommenderas framförallt innan informationssystem och

datakommunikationsarrangemang i säkerhetsklass I och II ansluts till system och arrangemang med lägre säkerhetsklass, så att den myndighet som ansvarar för säkerheten i dessa ska kunna fatta rishanteringsbesluten med stöd av Cybersäkerhetscentrets expertbedömning av eventuella kvarstående risker vid en anslutning. Se Traficoms (2019) anvisning om processer för bedömning och godkännande av informationssystem (på finska).

7.3 Hantering av sårbarheter i program

Grundläggande för säkerheten i informationssystem är tillförlitligheten hos program som används i systemet (t.ex. operativsystem och applikationer). Det har visat sig vara en utmaning att göra felfria program. I praktiskt taget alla program kan man hitta programmeringsfel, m.a.o. sårbarheter. Dessa kan utnyttjas för att kringgå skyddet av data som behandlas i informationssystemet. Ansvarsfulla leverantörer åtgärdar sårbarheter som upptäcks i deras program. Programriskerna kan reduceras avsevärt genom att man testar programvaran och installerar säkerhetsuppdateringar.

Allra viktigast är

- att ha en fungerande, regelbunden process för installation av säkerhetsuppdateringar och
- att säkerställa att processen fungerar i praktiken.

Viktigt i processen är att uppdateringarna sker tillräckligt snabbt och omfattande. Processen ska omfatta alla program som är relevanta för säkerheten, typiskt operativsystem i servrar och terminaler, systemprogramvara, tredjepartsapplikationer och programvara i nätverksenheter. Att uppdateringsprocesserna fungerar kan t.ex. säkerställas genom regelbundna konfigurationskontroller och tekniska sårbarhetsskanningar.

7.4 Förändringshantering som beaktar säkerheten

Ifall förändringar i informationssystem sker okontrollerat urholkas säkerheten även om systemet planerats för att vara mycket säkert. Trovärdigt upprätthållande av säkerheten kräver förfaranden där säkerhetskonsekvenserna av systemförändringar bedöms och om möjligt testas, och att behövliga extra skydd finns på plats innan ändringarna börjar gälla. Förändringshanteringen möjliggör effektivare systemadministration och stöder andra administrativa processer.

7.5 Säkerhetskopiering

Säkerhetskopiering är ett viktigt skydd som framförallt säkerställer informationens tillgänglighet. Därtill ska förfarandet ofta beakta andra dataskyddsbehov (integritet, konfidentialitet) via liknande förfaranden som för originaldata. Backup- och återställningsprocesserna ska planeras, implementeras, testas och beskrivas i en beredskapsplan så att man kan tillgodose operativa behov som gäller organisationen och informationssystemet samt andra krav. Beakta framförallt

- att backupfrekvensen är tillräcklig för hur kritisk informationen bedöms vara. Kräver utredning av mängden data som kan förloras (recovery point objective, RPO).
- att återställningsprocessen är tillräckligt snabb för verksamhetens krav. Kräver utredning av hur lång tid en återställning kan ta (recovery time objective, RTO).
- att backup- och återställningsprocessens korrekthet testas regelbundet.
- att den fysiska platsen för säkerhetskopiorna är tillräckligt avskild från systemet (ej samma ras- eller brandutrymme, avstånd från systemutrymmet).
- att säkerhetskopiorna skyddas under livscykeln med metoder på minst samma nivå som originaldata. En stor mängd information kan kräva striktare skydd (kumulativ effekt).
- att bara godkända personer eller roller har åtkomst till säkerhetskopiorna enligt principen om begränsad behörighet (se avsnitt 7.6).
- att backup- och återställningsprocesser kan spåras (loggar) och övervakas så att otillåtna handlingar upptäcks.
- då säkerhetskopior förvaras på en annan fysisk plats ska även den ha en fysisk och logisk tillträdeskontroll på minst samma nivå.
- då säkerhetskopior med sekretessbelagd information överförs via nätet utanför ett fysiskt skyddat område (t.ex. mellan datahallar) ska data eller kommunikation krypteras på adekvat sätt.
- då säkerhetskopior med sekretessbelagd information flyttas utanför ett fysiskt skyddat område på lagringsmedier (t.ex. band eller skivor) iakttas anvisningarna i avsnitt 4.4. Kryptering av lagringsmediet eller dess innehåll rekommenderas.
- backupmedier förstörs tillförlitligt.

7.6 Principen om begränsad behörighet

Enligt 11 §1 mom. 3 punkten i förordningen om säkerhetsklassificering ska informationssystem och datakommunikationsarrangemang som används för behandling av säkerhetsklassificerade handlingar genomföras så att användarna endast får sådana uppgifter, rättigheter eller befogenheter som är nödvändiga för att de ska kunna utföra sina uppgifter.

För att säkerställa åtkomsträttigheternas aktualitet krävs oftast regelbunden genomgång av alla anställdas, leverantörers och externa användares åtkomst- och användarrättigheter, t.ex. var sjätte månad. Det måste också finnas ett tydligt och fungerande förfaringssätt för att ändra eller dra in rättigheter då personens arbetsuppgifter förändras, t.ex. vid befordringar, arbetsrotation och framförallt då anställningen upphör. Ett tillvägagångssätt är att närmaste chef ger en ansvarig person förhandsbesked om förändringar så att alla rättigheter kan hållas uppdaterade. Vidare kan det innebära att användar- och åtkomsträttigheter dras in eller ändras i ett centralt administrativt system eller i enskilda system.

Användarrättigheter ska administreras enligt principen om begränsad behörighet:

1) ansvarig(a) för administration av användarrättigheter har utsetts
2) en process för att skapa, godkänna och administrera användarkonton har fastställts
3) användarna av databehandlingsmiljön får endast sådana uppgifter, rättigheter eller befogenheter som är nödvändiga för att de ska kunna utföra sina uppgifter
4) åtskillnadsprincipen ska tillämpas vid administration av användarrättigheter så att beställaren, godkännaren och utföraren är olika personer
5) det ska föras en förteckning över systemets användare det ska finnas kvar en anteckning om varje beviljad användarrättighet (papper eller elektronisk)
6) i samband med beviljandet ska man kontrollera att den som tilldelas användarrättigheten hör till personalen eller annars ska ha sådan rätt
7) behandlingen och beviljandet av användarrättigheter ska instrueras
8) onödiga användarkonton och rättigheter ska tas bort (t.ex. då användaren lämnar organisationen eller om användarkontot har varit oanvänt under en förutbestämd tid.)

9) det ska finnas ett tydligt och fungerande förfaringssätt för att ge berörda parter besked om personalförändringar och ett fungerande förfaringssätt för att göra behövliga ändringar

10) användar- och åtkomsträttigheterna ska ses över regelbundet, minst årligen Översynen ska även beröra personer som har åtkomst till systemets loggar, databas eller servrar.

7.7 Identifiering av användare och utrustning

7.7.1 Inom fysiskt skyddat administrativt område eller skyddsområde

Enligt 11 § 1 mom. 5 punkten i förordningen om säkerhetsklassificering ska informationssystem och datakommunikationsarrangemang som används för behandling av säkerhetsklassificerade handlingar genomföras så att de personer som använder dem samt utrustningen och informationssystemen identifieras tillräckligt tillförlitligt.

Identifieringen av användare och utrustning för säkerhetsklass IV ska uppfylla samtliga krav nedan:

1) alla har individuella personliga användaridentiteter

2) alla användare identifieras och autentiseras

3) identifiering och autentisering sker med känd teknik som anses säker och förenlig med moderna säkerhetskrav eller på annat tillförlitligt sätt

4) låsning av användaridentiteten efter för många misslyckade identifieringsförsök i rad

5) individuella program- och systemadministratörsidentiteter. Ifall detta inte är tekniskt möjligt i alla system eller program krävs avtalade och dokumenterade administrativa lösenordsrutiner som möjliggör identifiering av användaren då en delad identitet används.

6) autentiseringen sker enligt godkända lösenordsrutiner med minst ett lösenord. Lösenordsrutinerna bör ses över t.ex. årligen och inkludera rutiner för systemidentiteter.

7) stark, alltid minst tvåfaktorsautentisering av användare vid kommunikation utanför fysiskt skyddade områden och med tillräckligt stark kryptering av anslutningen.

Identifieringen för säkerhetsklass III-II ska uppfylla kraven i punkterna **1-5** samt följande krav:

1) stark, minst tvåfaktorsautentisering av användare

2) terminaler autentiseras tekniskt (via identifiering av enheten, 802.1X e.d.) innan de får åtkomst till nätverket eller tjänsten, om uppkopplingen inte har begränsats med fysiska säkerhetsmetoder (t.ex. en server i ett låst datorskåp inom ett tekniskt säkrat skyddsområde som myndigheten godkänt för den berörda skyddsnivån.)

3) tillräckligt stark kryptering av anslutningen vid kommunikation utanför fysiskt skyddade områden.

Lagen om stark autentisering och betrodda elektroniska tjänster (2016/533) reglerar i 8 a § vilka autentiseringsfaktorer som ska användas i identifieringsmetoden. Minst två av följande autentiseringsfaktorer ska användas. Dessa är

1) en kunskapsbaserad autentiseringsfaktor som personen måste kunna visa att den har kunskap om,

2) en innehavsbaserad autentiseringsfaktor som personen måste kunna visa att den innehar

3) en egenskapsbaserad autentiseringsfaktor som utgår från en kroppslig egenskap hos en fysisk person.

Vid tvåfaktorsautentisering räcker det inte med två eller tre lösenord eftersom dessa bara utgör en faktor (något man vet). Autentisering med t.ex. bankkoder bygger på minst två faktorer: något man vet (användaridentitet och eventuellt lösenord) och något man har (kodtabell, kodkalkylator eller mobil apparat).

7.7.2 Ersättande förfaranden

Stark autentisering av användare och autentisering av terminaler för säkerhetsklass III och II kan i vissa fall ske genom att personen har beviljats individuell tillträdesrätt till ett noga avgränsat, fysiskt skyddat område (oftast tekniskt säkrat skyddsområde, låst datorskåp e.d.) som ger åtkomst till informationssystemet och där minst tvåfaktorsautentisering används i tillträdeskontrollen. Då kan användaren identifieras med ett användar-ID–lösenordspar i själva informationssystemet.

7.7.3 Mer information

I en tillförlitligt organiserad identifiering och autentisering ingår åtminstone

1) att autentiseringsmetoden är skyddad mot man-i-mitten-attacker (man-in-the-middle),
2) att ingen onödig information avslöjas vid inloggningen innan autentisering sker
3) att identifieringsuppgifterna (authentication credentials) alltid krypteras om de skickas över nätet,
4) att autentiseringsmetoden skyddas mot omsändningsattacker och
5) att autentiseringsmetoden är skyddad mot brute force-attacker.

7.8 Nödvändiga funktioner

Enligt 11 § 1 mom. 6 punkten i förordningen om säkerhetsklassificering ska informationssystem och datakommunikationsarrangemang som används för behandling av säkerhetsklassificerade handlingar genomföras så att endast de med tanke på användningskraven nödvändiga funktionerna tas i bruk.

Att skapa säker programkod är en utmaning. Mycket programkod i miljön innebär också fler möjligheter till programfel, m.a.o. sårbarheter. Ju fler tjänster som erbjuds, desto större blir sannolikheten för sårbarheter eftersom tjänsterna är beroende av programkodens säkerhet. Dessa risker kan reduceras genom mindre sårbarhetsyta, dvs. att bara nödvändiga tjänster exponeras för attacker.

Systemen översvämmas vanligtvis av funktioner, som oftast är på som standard och lätta att aktivera, ofta med onödigt osäkra inställningar. Om onödiga funktioner inte tas bort är de också tillgängliga för illvilliga aktörer. Ofta har systemen t.ex. förinställda administrativa lösenord, onödiga användarkonton eller färdiginstallerade, onödiga program.

Minimering innebär att systeminställningarna överlag ändras så att man kan minska systemets sårbarhetsyta. För att reducera riskerna ska man överlag endast ta i bruk de funktioner, apparater och tjänster som är väsentliga med tanke på systemanvändningskraven, och synligheten av t.ex. tjänsterna ska vara den minsta möjliga. Likaså ska automatiska processer bara få data, rättigheter eller behörigheter som är nödvändiga för deras utförande. På så sätt kan man begränsa skadorna vid eventuella olyckor, fel eller obehörig

användning av systemresurser. Eventuella osäkra inställningar och onödiga användarkonton som är förvalda i systemet ska ändras eller tas bort. Mer information om minimering av sårbarhetsytan finns i senaste Katakri.

7.9 Spårbarhet

Enligt 17 § i informationshanteringslagen ska en myndighet ombesörja att logginformation insamlas om användning av dess informationssystem och om utlämnande av information från dem, om användningen förutsätter identifiering eller annan registrering. Ändamålet med loggdata är att kunna följa upp användning och utlämning av information samt utreda tekniska fel i informationssystemet.

Med spårbarhet avses loggning av systemhändelser så att man vid incidenter kan klarlägga vilka åtgärder som utförts i systemmiljön, av vem och vad följderna har blivit. Viktiga loggar är inloggningsdata samt loggdata från de viktigaste nätverksenheterna och servrarna. Mycket ofta ingår även loggdata från t.ex. arbetsstationer o.d.

Omfattningskravet kan oftast uppfyllas genom säkerställande av att loggningen är aktiverad åtminstone i arbetsstationer, servrar, nätverksenheter o.d. (särskilt brandväggar, även arbetsstationernas mjukvarubrandväggar). I nätverksenheternas loggar bör man efteråt även kunna ta reda på vilka åtgärder som berört enheten, när de utförts och av vem. Händelseloggar bör omfatta systemaktivitet, användaraktivitet, säkerhetsrelaterade händelser och incidenter.

Ett rekommendabelt sätt att säkra loggarna är att viktiga loggdata skickas till en central och starkt skyddad loggserver, varifrån dessa dagligen säkerhetskopieras till en miljö med minst samma säkerhetsklass. Insamlingen och lagringen av loggdata ska helst implementeras så att man kan upptäcka radering eller ändring av data även då nätanslutningen mellan loggkällan och logginsamlaren inte är tillgänglig. Likaså krävs en regelbunden process för logginsamling från varaktigt näturkopplade arbetsstationer samt för säkerhetskopiering av insamlade loggdata. Som stöd för administratörernas rättssäkerhet och utredning av eventuella dataintrång rekommenderas att administrationen av loggdata särskiljs från annan loggning som berör administratörerna. Spårbarheten ska implementeras så att man även beaktar situationer där en inloggad användare kan utföra funktioner från ett annat konto (user impersonation). Ansvariga ska följa upp loggnings- och övervakningsprogrammens funktionalitet och kunna upptäcka eventuella störningar med kort fördröjning, t.ex. inom ett dygn efter att loggkällan slutat leverera loggar.

Lagringstiderna för loggdata ska väljas så att behoven i de olika logganvändningsfallen beaktas. I vissa databehandlings- och utlämningsloggar kan det vara befogat att ha andra lagringstider än för loggdata som samlas in med tanke på utredning av incidenter. I t.ex. myndighetsverksamhet kan straffrättsliga preskriptionstider leda till minst femåriga lagringstidsbehov. En allmän praxis är att loggdata från de sex senaste månaderna är tillgängliga i realtid och att äldre loggdata vid behov kan fås inom några arbetsdagar. Olika logganvändningsfall behandlas närmare i informationshanteringsnämndens rekommendationssamling om tillämpning av vissa bestämmelser om informationssäkerhet (finansministeriet 2020:21, kapitel 7).

Implementeringen kräver ofta att loggarnas lagringsutrymme och -tid utökas tillräckligt. Det är rekommendabelt att reservera tillräckligt loggutrymme i miljön utifrån beräkningarna. När lagringstiden bestäms kan man t.ex. utifrån en månads samlade loggar beräkna hur mycket utrymme som behövs för den erforderliga lagringsperioden. Observera att man bör ha en rejäl buffert i lagringsutrymmet eftersom incidenter och vissa typer av attacker ökar mängden loggdata betydligt.

Exempel på implementering:

Kravet för en behandlingsmiljö i säkerhetsklass IV kan uppfyllas genom att alla nedanstående åtgärder vidtas:

1) skriftlig policy eller anvisning för logginsamling, utlämning, larm och uppföljning har tagits fram utifrån verksamhetens krav och förankrats,

2) loggarna är tillräckligt omfattande för att i efterhand kunna konstatera dataintrång eller försök till sådana,

3) viktiga loggar sparas i minst sex månader, såvida det inte krävs längre tid enligt lagstiftning eller avtal. Behandlingsloggar och loggar som t.ex. omfattas av straffrättsliga preskriptionstider i myndighetsverksamhet, sparas i minst fem år,

4) loggdata och loggregistreringstjänster skyddas mot obehörig åtkomst (behörighetsadministration, logisk åtkomstkontroll).

Kravet för behandlingsmiljöer i säkerhetsklass III-II kan uppfyllas genom att man utöver punkterna 1–4 vidtar följande åtgärder:

1) viktiga loggar sparas i minst fem år, såvida det inte krävs längre tid enligt lagstiftning eller avtal. Loggar av ringa betydelse t.ex. för utredning av incidenter eller myndighetsverksamhet i straffrättsligt hänseende kan sparas kortare tid, t.ex. 2-5 år.
2) loggdata säkerhetskopieras regelbundet,
3) klockorna i relevanta datasystem inom samma säkerhetsområde synkroniseras med en avtalad tidkälla,
4) det finns metoder för att säkerställa loggarnas integritet (riktighet) och
5) användning och behandling av loggdata registreras.

7.10 Detektering

Teknisk kapacitet att upptäcka incidenter bygger oftast på tre källor:

1) synliga händelser i nätdatatrafiken,
2) insamlade loggar och
3) synliga händelser hos värdar (hosts).

En adekvat teknisk detektionskapacitet kan oftast skapas genom kombination av ovannämnda källor. Ju noggrannare man känner till databehandlingsmiljön och hur den fungerar normalt, desto bättre är förmågan att upptäckta avvikande händelser. Detta underlättar också upptäckt av attacker där indikationer saknas (Io, Indicator of Compromise). Man bör känna till databehandlingsmiljöns normala funktion under hela livscykeln, från första stund tills den tas ur drift. Förändringshanteringen bidrar till upptäckt av incidenter bl.a. genom regelbunden kontroll av ändringar i hård- och mjukvarukonfigurationer.

Det finns flera möjliga implementeringar för övervakning samt begränsning av konsekvenserna då en attack upptäcks, från kontroll av viktiga noder till sensorer i arbetsstationer eller servrar samt kombinationer av dessa. Oavsett vilka nätverksenheter och leverantörer som används kräver den praktiska implementeringen av detektionsförmågan kännedom om normalläget i nätdatatrafiken. I behandlingsmiljöer för säkerhetsklass IV bör detektionskapaciteten i nätdatatrafiken framförallt täcka nätverkets eller objektets yttre gräns och från och med säkerhetsklass III gatewaylösningens yttre gräns samt kommunikationen inom nätverket eller objektet.

I de flesta miljöer förutsätter upptäckten av attacker eller missbruk i praktiken automatiserade detektions- och larmverktyg. I vissa situationer är det möjligt och rentav nödvändigt att behandla loggdata manuellt t.ex. då en incident inte har upptäckts automatiskt och den kräver noggrannare utredning. Kom ihåg att bara uppgifter som är nödvändiga för informationssäkerhetsåtgärderna får samlas i loggarna, och åtgärderna får inte begränsa yttrandefriheten eller bryta skyddet av förtroliga meddelanden eller den personliga integriteten. Observera att detektionskapacitet överlag förutsätter kännedom om särdragen i varje databehandlingsmiljö, att bl.a. kritiska objekt och övervakade händelser specificeras och att kapaciteten skräddarsys för den aktuella miljön och upprätthålls kontinuerligt.

För att kunna återställa databehandlingsmiljön till ett skyddat tillstånd inom rimlig tid krävs oftast planerade, beskrivna, utlärda och övade processer samt tekniska metoder. Hela personalens roll ska beaktas i utvecklingen och upprätthållandet av detektionskapaciteten. Observationer från bl.a. slutanvändare kan ge värdefull kunskap för detektionen av attacker eller attackförsök.

Exempel på implementering:

Kravet för behandlingsmiljöer i säkerhetsklass IV-II kan uppfyllas genom att alla nedanstående åtgärder vidtas:

1) kännedom om normalläget i nätdatatrafiken (trafikmängd, protokoll och anslutningar). Det finns ett förfarande för att upptäcka händelser som avviker från normalläget (t.ex. avvikande anslutningar eller anslutningsförsök),

2) det finns ett förfarande för att upptäcka avvikelser i insamlade loggar och statusinformation (t.ex. förändringar i loggmängden); framförallt ska försök till obehörig användning av informationssystemet kunna upptäckas,

3) det finns ett förfarande för att upptäcka avvikelser hos objekt i databehandlingsmiljön (hosts, t.ex. arbetsstationer och servrar),

4) det finns ett förfarande för återhämtning från upptäckta avvikelser.

7.11 Krypteringslösningar

Enligt 11 § 1 mom. 7 punkten i förordningen om säkerhetsklassificering ska de krypteringslösningar som används vara tillräckligt säkra med beaktande av säkerhetsklassen för de handlingar som behandlats i informationssystemen eller datakommunikationsarrangemangen.

Bestämmelser om överföring av sekretessbelagd information i det allmänna datanätet finns i 14 § i informationshanteringslagen. Enligt 12 § i förordningen om säkerhetsklassificering får säkerhetsklassificerade handlingar överföras från en myndighets skyddade säkerhetsområde i andra datanät än det allmänna datanätet eller överföras via informationssystem eller datakommunikationsarrangemang som har en lägre säkerhetsnivå än säkerhetsklassen i fråga **endast om handlingarna krypterats**. Dessutom ska överföringen ordnas så att mottagaren verifieras eller identifieras på ett tillräckligt informationssäkert sätt innan mottagaren kommer åt att behandla den överförda sekretessbelagda informationen. Om säkerhetsklassificerade handlingar överförs inom ett säkerhetsområde i andra datanät än det allmänna datanätet och uppgifterna kan skyddas tillräckligt genom metoder för fysiskt skydd, får okrypterad överföring eller kryptering på lägre säkerhetsnivå användas.

Speciellt vid kommunikation över offentliga nät eller nät med lägre säkerhetsklass är krypteringslösningar ofta det enda skyddet för sekretessbelagda uppgifters konfidentialitet och vanligtvis även för deras integritet. Eftersom det ofta är ytterst svårt att kompensera eventuella brister i krypteringslösningarna med andra skydd rekommenderas att valet av krypteringslösning och säker användning av den ägnas särskild uppmärksamhet.

Då sekretessbelagda uppgifter flyttas utanför fysiskt skyddade områden, eller i ett offentligt nät, ska materialet eller datatrafiken skyddas genom tillräckligt säker kryptering. Till offentliga nät räknas bland annat internet och teleoperatörernas MPLS-nät. Praktiska exempel på implementerad kryptering är VPN-lösningar mellan användarnas terminaler och myndighetens informationssystem, kryptering mellan organisationers nätverk (LAN-2-LAN) samt fil- och e-postkrypteringslösningar för slutanvändare. Vid överföring av sekretessbelagda uppgifter mellan fysiskt skyddade områden och inom ett nät med åtminstone motsvarande skyddsnivå kan man utifrån resultaten av riskhanteringsprocessen använda en lägre krypteringsnivå eller okrypterad överföring.

Myndigheten ska använda krypteringslösningar som tillförlitligt visats ha tillräcklig säkerhet. Flera olika faktorer ska beaktas vid bedömning av krypteringslösningar. Man ska försäkra sig om att krypteringen är tillräckligt stark och att produkten fungerar enligt specifikationen samt beakta hotnivån i miljöerna där den används. Hotnivån är t.ex. högre i datatrafik över internet jämfört med kryptering av kommunikation inom ett kontrollerat, fysiskt skyddat område (t.ex. datatrafik mellan två skyddsområden via ett administrativt område). Andra faktorer som ska beaktas vid bedömning av produkterna är t.ex. vilka krav användningstillfällena ställer på uppgifternas sekretesstid och integritet. Mer information finns i Cybersäkerhetscentrets anvisning om kryptografiska krav (Kommunikationsverket 2018) (på finska).

Olika informationsmaterial har olika risker. Exempelvis inser man oftast att myndigheternas säkerhetsklassificerade ska skyddas utifrån statens säkerhetsintressen (allmänintresset). Det kan ofta antas att intresset för säkerhetsklassificerade uppgifter kommer från annat håll än t.ex. intresset för personuppgifter utan säkerhetsklassificering. Skillnaderna mellan riskerna ska beaktas vid valet av krypteringslösning.

I valet av krypteringslösningar rekommenderas att man främst förlitar sig på lösningar som bedömts och godkänts av Cybersäkerhetscentrets NCSA-funktion (Traficom 2020) (på finska). En fastställd användarpolicy är väsentlig i processen för godkännande av krypteringslösningar. I användarpolicyn ingår sådana användningstillfällen och inställningar med vilka lösningen har bedömts ge ett fullgott skydd för uppgifter i den berörda säkerhetsklassen.

Krypteringens skyddseffekt kan gå delvis eller helt förlorad i situationer där svagheter i nyckelförvaltningen kan utnyttjas av obehöriga. Därför ska det finnas planerade, implementerade och beskrivna eller instruerade processer för administration av krypteringsnycklarna. Endast behöriga användare och processer får ha tillgång till de privata (hemliga) nycklarna. Processerna ska åtminstone kräva

a) kryptografiskt starka nycklar,

b) säker nyckeldistribution,

c) säker nyckelförvaring,

d) regelbundna nyckelutbyten,

e) utbyte av gamla eller avslöjade nycklar och

f) förhindrande av obehöriga nyckelutbyten.

Vid riskbedömningen ska myndigheten också ta hänsyn till säkerheten i leveranskedjorna särskilt i fråga om krypteringslösningar. Även om krypteringslösningen är tillräckligt säker då tillverkaren levererar den, kan bristande skydd i leveranskedjan möjliggöra manipulering av krypteringslösningen så att myndigheten implementerar en otrygg lösning i sitt informationssystem eller datakommunikationsarrangemang.

Att mottagaren kan autentiseras tillräckligt säkert beror i hög grad på den krypteringslösning som används. Cybersäkerhetscentret vid Transport- och kommunikationsverket (2020) har i bl.a. användarpolicyerna för krypteringslösningar som centret godkänt för skydd av säkerhetsklassificerade uppgifter (på finska) ofta tagit ställning till identifiering av användare då krypteringslösningen t.ex. används för kommunikation med en person från en annan organisation. I många krypteringslösningar bygger identifieringen av motparter å sin sida på nyckelförvaltningens tillförlitlighet (t.ex. symmetrisk kryptering mellan

organisationens verksamhetsställen eller kryptering mellan två organisationers nätverk (LAN-2-LAN), eller filkryptering med delad nyckel).

Framförallt vid överföring av sekretessbelagda uppgifter utan säkerhetsklassificering ska man beakta vad lagen om tillhandahållande av digitala tjänster (306/2019) säger om identifiering av användare i digitala tjänster som tillhandahålls allmänheten.

7.12 Behandling i molntjänster

Handlingar i säkerhetsklass IV kan behandlas och förvaras i molntjänster som inte bedöms vara exponerade för de lagstiftningsrelaterade risker som beskrivits i kapitel 7 under förutsättning att myndigheten har beaktat alla övriga skyddsbehov och -krav som gäller behandling av säkerhetsklassificerad information. Förvaring av handlingar i säkerhetsklass IV i andra molntjänster kan endast ske när informationen har krypterats så tillförlitligt att den inte kan dekrypteras i tjänsten under sin livscykel. Därmed kan en del av behandlingsmiljön för myndigheters säkerhetsklassificerade information implementeras genom utnyttjande av molnteknik. Finansministeriet har tagit fram riktlinjer och anvisningar om molntjänster (finansministeriet 2018:35, 2020:66, 2020:73) (på finska). Transport- och kommunikationsverkets Cybersäkerhetscenter (2020:13) har gett ut kriterier för bedömning av molntjänsters säkerhet (PiTuKri) (på finska).

14 § i informationshanteringslagen och 11 § 7 punkten och 12 § möjliggör överföring av säkerhetsklassificerad information via ett publikt eller annat icke betrott nät då informationen krypterats med tillräckligt stor tillförlitlighet. Observera framförallt att dekryptering inte ska kunna ske i icke betrodda nät, vilket omfattar såväl krypteringsprogrammet eller -utrustningen som att nyckelhanteringen ska läggas utanför det icke betrodda nätet. Samma princip kan tillämpas då säkerhetsklassificerad information behöver flyttas eller förvaras i icke betrodda databehandlingsmiljöer, t.ex. multinationella molntjänster.

Vid tillämpning av principen ska man dock alltid beakta att molntjänstleverantörerna i princip alltid har åtkomst till behandlade data i tjänsten ifall informationen under sin livscykel finns där i klartextformat (t.ex. bilder som visas för kunden). Vanliga lösningar baserade på t.ex. egna nycklar (BYOK, Bring Your Own Keys) eller fysiska hårdvarumoduler i molntjänstleverantörens datahall (HSM, Hardware Security Module) begränsar men förhindrar vanligtvis inte leverantörens åtkomstmöjlighet till data som behandlas i tjänsten. Kryptering kan dock användas som ett kompletterande skydd i t.ex. särskiljandet av kunddata, destruktionsprocessen för skyddade objekt eller särskiljandet av arbetsuppgifter.

8 Författningar

Rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2013/488/EU)

Europaparlamentets och rådets förordning (EU) 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) (679/2016)

Lagen om tillhandahållande av digitala tjänster (306/2019)

Lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018)

Lagen om informationshantering inom den offentliga förvaltningen (906/2019)

Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004)

Lagen om stark autentisering och betrodda elektroniska tjänster (533/2016)

Lagen om offentlighet i myndigheternas verksamhet (621/1999)

Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019)

Lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011)

Finlands grundlag (731/1999)

Dataskyddslagen (1050/2018)

9 Anvisningar och annat material

Dataskyddsombudsmannens byrå. https://tietosuoja.fi/etusivu

Traficom Transport- och kommunikationsverket 2017. Transport- och kommunikationsverket Traficoms bedömning och godkännande av krypteringsprodukter. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-salaus-tuotearvioinnit-ja-hyvaksynnat.pdf (på finska)

Traficom Transport- och kommunikationsverket Cybersäkerhetscentret 2019. Transport- och kommunikationsverket Traficoms bedömnings- och godkännandeprocesser för informationssystem. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf (på finska)

Traficom Transport- och kommunikationsverket 2020. Krypteringslösningar godkända av NCSA-funktionen. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf (på finska)

Kommunikationsverket Cybersäkerhetscentret 2018. Anvisning om planeringsprinciper och lösningsmodeller för gatewaylösningar. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Yhdyskaytavaratkaisuohje.pdf (på finska)

Traficom Transport- och kommunikationsverkets Cybersäkerhetscenter 2020:13. Kriterier för bedömning av molntjänsters säkerhet (PiTuKri). https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri

Utrikesministeriet 2015. Verktyg för myndigheters informationssäkerhetsauditering 2015 (Katakri) https://um.fi/katakri-verktyg-for-informationssakerhetsauditering-for-myndigheter (på finska)

Utrikesministeriet Nationella säkerhetsmyndigheten (NSA) 2015. Säkerhetsmyndigheternas handbok för företag. https://um.fi/nationella-sakerhetsmyndigheternas-handbok-for-foretag

Utrikesministeriet Nationella säkerhetsmyndigheten (NSA) 2020. Anvisning om behandling av internationellt säkerhetsklassificerat informationsmaterial. https://um.fi/turvallisuusluokitellun-tiedon-kasittelyohje (på finska)

Finansministeriet 2018:35. Molntjänstriktlinjer för den offentliga förvaltningen. https://julkaisut.valtioneuvosto.fi/handle/10024/161294 (på finska)

Finansministeriet 2020:73. Tillämpningsanvisning om molntjänster - Tillämpningsanvisningar för organisationer inom offentlig förvaltning om utnyttjandet av molntjänster. https://julkaisut.valtioneuvosto.fi/handle/10024/162453 (på finska)

Finansministeriet 2020:18. Rekommendation om genomförandet av ledningens ansvar. http://urn.fi/URN:ISBN:978-952-367-320-5

Finansministeriet 2020:29. Rekommendation för en informationshanteringsmodell. https://julkaisut.valtioneuvosto.fi/handle/10024/162176

Finansministeriet 2020:53. Rekommendation om bedömning av förändringar i informationshanteringen. https://julkaisut.valtioneuvosto.fi/handle/10024/162330

Finansministeriet 2020:61. Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet. http://urn.fi/URN:ISBN:978-952-367-295-6

Finansministeriet 2020:66. Produktivitet genom molntjänster: Anvisningar om användning av molntjänster inom den offentliga förvaltningen. https://julkaisut.valtioneuvosto.fi/handle/10024/162451 (på finska)

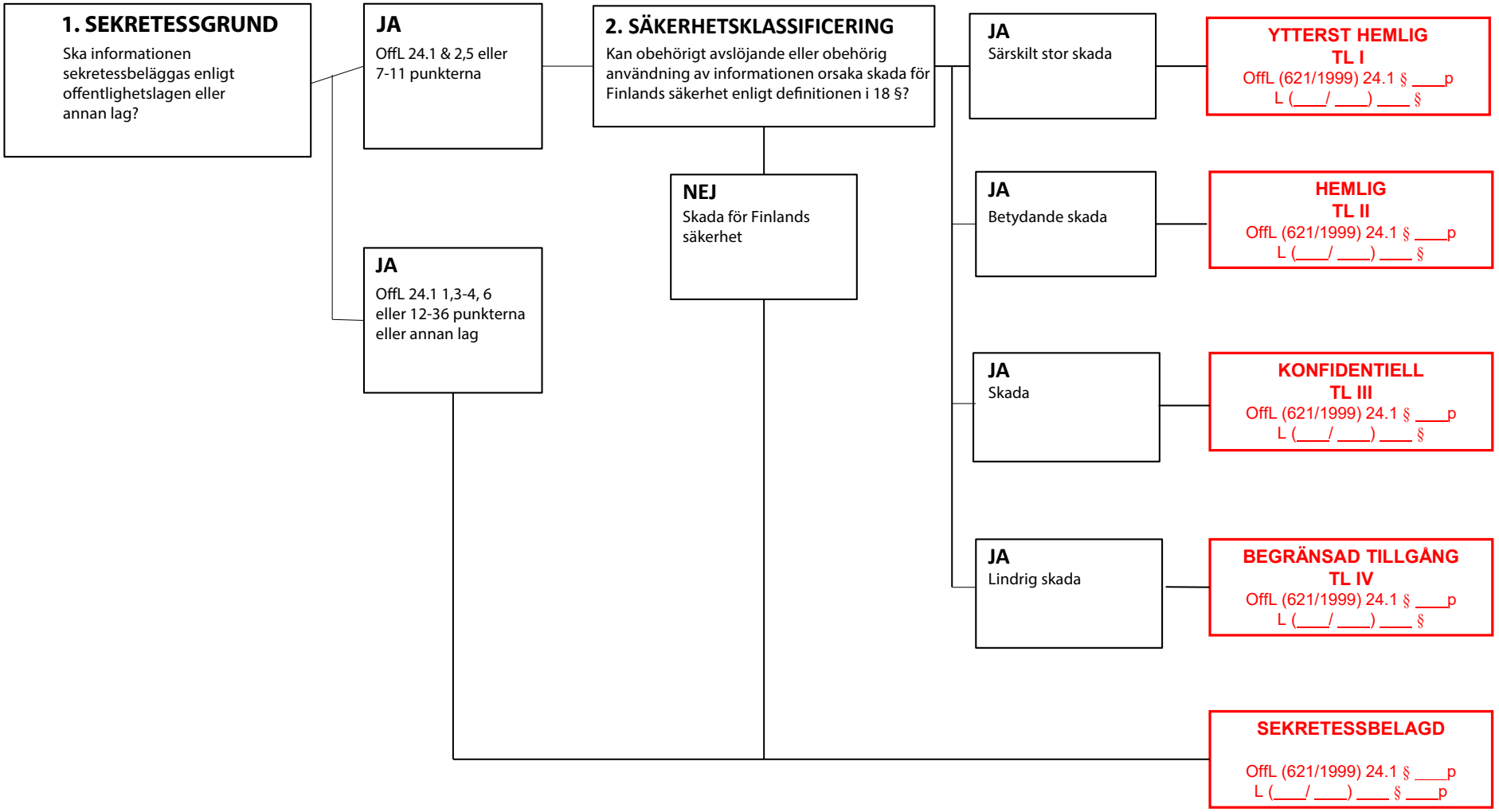
Kommunikationsverket Cybersäkerhetscentret 2016. Hantering av hårddiskars livscykel. Överskrivning och återanvändning. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-ylikirjoitus.pdf (på finska)

Kommunikationsverket Cybersäkerhetscentret. 2018. Kryptografiska krav för konfidentialitet - nationella skyddsnivåer https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf (på finska)

Kommunikationsverket Cybersäkerhetscentret 2018. Anvisning om planeringsprinciper och lösningsmodeller för gatewaylösningar. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Yhdyskaytavaratkaisuohje.pdf (på finska)

Bilaga 1. Bedömningsprocess för sekretess och säkerhetsklassificering.

Observera att bilden inte tar hänsyn till lagen om internationella förpliktelser som gäller informationssäkerhet.



Bilaga 2. Skadebedömningstabell.

Tabellen ger **exempel** på bedömning av skaderekvisitet i säkerhetsklassificeringen utifrån ett skyddat intresse. Klassificeringen ska alltid ske utifrån en riskbedömning av det enskilda fallet. Informationshanteringsenheter rekommenderas upprätta en sektorsspecifik klassificeringsanvisning t.ex. enligt tabellen nedan.

	TL IV	TL III	TL II	TL I
Beskrivning	Obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen **kan orsaka lindrig skada** för det skyddade intresset.	Obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen **kan orsaka skada** för det skyddade intresset.	Obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen **kan orsaka betydande skada** för det skyddade intresset.	Obehörigt röjande eller obehörig användning av sekretessbelagda uppgifter i handlingen **kan orsaka särskilt stor skada** för det skyddade intresset.
Detaljbeskrivning	• Röjande av informationen kan orsaka en konsekvens eller händelse som inte innebär att verksamheten behöver avbrytas, men operativa planer måste kanske ändras	• Röjande av informationen kan orsaka en konsekvens eller händelse som innebär att verksamheten måste avbrytas.	• Röjande av informationen kan orsaka en konsekvens eller händelse som innebär att verksamheten måste avbrytas och att den förhindras en längre tid.	• Avbrott, varaktigt hinder för verksamheten. • Skadan är omfattande och gäller t.ex. samhällsviktiga objekt/funktioner såsom kritisk infrastruktur eller vital verksamhet.
Skyddat intresse: Exempelvis förberedelser inför undantagsförhållanden	• Äventyrar eventuellt myndighetens verksamhet. T.ex. dokument om väsentliga informationssystem såsom säkerhetsarrangemang, sårbarheter, revisionsrapporter, beredskaps- och återhämtningsplaner.	• Äventyrar sannolikt myndighetens verksamhet. T.ex. säkerhetsarrangemang, beredskaps- och återhämtningsplaner för vitala funktioner.	• Förhindrar eventuellt myndighetens verksamhet. Säkerheten för en stor grupp människor kan inte garanteras. T.ex. viktiga dokument om säkerhetsarrangemang, sårbarheter och revisioner i vitala funktioner och datasystem som stöder dessa.	• Förhindrar sannolikt myndighetens verksamhet och uppfyllelsen av • säkerhetsarrangemangens syfte.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

FINANSMINISTERIET
Snellmansgatan 1 A
PB 28, 00023 STATSRÅDET
Telefon 0295 160 01
finansministeriet.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-520-9 (pdf)

Februari 2021