VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Rekommendation om behandling av säkerhetsklassificerade handlingar

Nämder

Finansministeriets publikationer – 2020:34

Finansministeriets publikationer 2020:34

Rekommendation om behandling av säkerhetsklassificerade handlingar

Finansministeriet, Helsingfors 2020

Finansministeriet

ISBN PDF: 978-952-367-293-2

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2020

Presentationsblad

Utgivare	Finansministeriet		19.3.2020
Författare	Informationshanteringsnämden		
Publikationens titel	Rekommendation om behandling av säkerhetsklassificerade handlingar		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2020:34		
Diarie-/ projektnummer	-	**Tema**	Nämnder
ISBN PDF	978-952-367-293-2	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-293-2		
Sidantal	36	**Språk**	Svenska
Nyckelord	informationshanteringslagen, informationshanteringsnämnden, nämnder, datasäkerhet, offentlig förvaltning, klassificeringar, handlingar		

Referat

Enligt 18 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019) ska myndigheter vid statliga ämbetsverk och inrättningar, domstolar och nämnder som har inrättats för att behandla besvärsärenden 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 (621/1999) 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.

Anteckningen om säkerhetsklass berättar för mottagaren hur informationen ska behandlas. I informationssystem kan anteckningen göras till exempel i metadata. I en handling kan anteckningen också göras i bilagan till handlingen.

Informationshanteringsnämnden godkände rekommendationen den 11 februari 2020.

Förläggare	Finansministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: vnjulkaisumyynti.fi

Kuvailulehti

Julkaisija	Valtiovarainministeriö		19.3.2020
Tekijät	Tiedonhallintalautakunta		
Julkaisun nimi	Rekommendation om behandling av säkerhetsklassificerade handlingar (Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä)		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:34		
Diaari/hankenumero	-	**Teema**	Lautakunnat
ISBN PDF	978-952-367-293-2	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-293-2		
Sivumäärä	36	**Kieli**	Ruotsi
Asiasanat	tiedonhallintalaki, tiedonhallintalautakunta, lautakunnat, tietoturva, julkinen hallinto, luokitukset, asiakirjat, tiedonhallintalautakunta		

Tiivistelmä

Tiedonhallintalain 18§:n mukaan valtion virastoissa ja laitoksissa 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 (621/1999) 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.

Turvallisuusluokitusmerkinnällä kerrotaan tiedon vastaanottajille, miten tietoja tulee käsitellä. Tietojärjestelmissä merkintä voidaan tehdä esimerkiksi metatietoihin. Asiakirjoissa merkintä voidaan tehdä myös asiakirjan liitteeseen.

Tiedonhallintalautakunta hyväksyi suosituksen 11.2.2020.

Kustantaja	Valtiovarainministeriö
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: vnjulkaisumyynti.fi

Description sheet

Published by	Ministry of Finance		19 Month 2020
Authors	Information Management Board		
Title of publication	Rekommendation om behandling av säkerhetsklassificerade handlingar (Recommendations on the implementation of management responsibilities in information management)		
Series and publication number	Publications of the Ministry of Finance 2020:34		
Register number	-	**Subject**	Board
ISBN PDF	978-952-367-293-2	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-293-2		
Pages	36	**Language**	Swedish
Keywords	Information Management Unit, Information Management Act, advisory boards, information management, public administration, responsibilities, definitions		

Abstract

The purpose of this recommendation is to guide the management of the Information Management Unit in organising information management as required by the Information Management Act and other legislation. In particular, the recommendation puts into concrete terms the requirements laid down in the Information Management Act, the implementation of which must be ensured by the management.

The recommendation is not binding; it describes how the management of the Information Management Unit can implement the requirements laid down in the Act. The recommendation does not comment on the internal organisation of information management units, which may be due to special legislation.

The recommendation was approved by the Information Management Board on 11 February 2020.

Publisher	Ministry of Finance
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: vnjulkaisumyynti.fi

Innehåll

1 Inledning

Informationshanteringsnämnden har lämnat denna rekommendation som handledning för uppfyllande av kraven enligt statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019, nedan SäKlF).

2 Märkning av säkerhetsklass (SäKIF 3.2–3.5 §)

Säkerhetsklasserna anges på finska på följande sätt: handlingar i säkerhetsklass I förses med märkningen ”ERITTÄIN SALAINEN”, i säkerhetsklass II med ”SALAINEN”, i säkerhetsklass III med ”LUOTTAMUKSELLINEN” och i säkerhetsklass IV med ”KÄYTTÖ RAJOITETTU”. Utöver nämnda märkning kan märkningarna ”TL I”, ”TL II”, ”TL III” och ”TL IV” användas.

I handlingar som har upprättats på svenska eller översatts till svenska ska säkerhetsklasserna med avvikelse från vad som föreskrivs i 2 mom. anges på svenska. Märkningen 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.

Säkerhetsklassen kan anges in i en 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.

Enligt 18 § i informationshanteringslagen ska myndigheter vid statliga ämbetsverk och inrättningar, domstolar och nämnder som har inrättats för att behandla besvärsärenden 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 (621/1999) 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.

Anteckningen om säkerhetsklass anger för mottagaren hur uppgifterna ska hanteras. I datasystem kan anteckningen fogas till exempel i metadata. Det är också möjligt att foga anteckningen till bilagan till en handling. I vissa fall är det befogat att framhäva vilken del av en handling som innehåller säkerhetsklassificerade uppgifter. De relevanta avsnitten kan märkas per paragraf eller kapitel med den finska bokstavsförkortningen för säkerhetsklassen, dvs. (E), (S), (L) eller (R).

Uppgifternas säkerhetsklass kan också anges muntligt, till exempel då säkerhetsklassificerad information behandlas på ett möte.

Enligt EU-rådets säkerhetsföreskrifter ska varje sida i en säkerhetsskyddsklassificerad EU-handling tydligt märkas med säkerhetsskyddsklassificeringsnivån och varje sida ska numreras och dateras. Handlingar på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET eller högre ska dessutom ha ett exemplarnummer på varje sida, om de sänds ut i flera exemplar. Motsvarande praxis kan med fördel tillämpas i säkerhetsklassificerade nationella handlingar.

Stämpelmallarna för säkerhetsklassmärkning presenteras nedan.

BEGRÄNSAD TILLGÅNG
TL IV
OffL (621/1999) 24.1 § ____p
L (____/ ____) ____ §

KONFIDENTIELL
TL III
OffL (621/1999) 24.1 § ____p
L (____/ ____) ____ §

HEMLIG
TL II
OffL (621/1999) 24.1 § ____p
L (____/ ____) ____ §

YTTERST HEMLIG
TL I
OffL (621/1999) 24.1 § ____p
L (____/ ____) ____ §

Säkerhetsklasserna, deras förkortningar och EU-motsvarigheter framgår av tabellen nedan.

Nationell säkerhetsklass				EU-säkerhetsskyddsklassificeringsnivå	
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

Tabell 1. Säkerhetsklasserna, deras förkortningar och EU-motsvarigheter.

I Tabell 1 presenteras de nationella säkerhetsklasserna sida vid sida med de motsvarande EU-säkerhetsskyddsklassificeringsnivåerna. Det finns skillnader i reglerna för behandlingen av uppgifter i de olika klasserna och **behandling av EU-säkerhetsskyddsklassificeringsnivåerna ska följa säkerhetsbestämmelserna för skydd av säkerhetsskyddsklassificerade EU-uppgifter**.

2.1 Bestämmelser och tilläggsinformation

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

Nationella säkerhetsmyndighetens anvisning om hantering av internationellt säkerhetsklassificerat informationsmaterial

3 Administrativa områden (SäKIF 9.2 § punkt 1)

Informationshanteringsenheten ska fastställa följande fysiskt skyddade säkerhetsområden för att skydda behandlingen av säkerhetsklassificerade handlingar samt informationssystem på det sätt som avses i 10 §:

1) administrativa områden som har tydligt bestämda synliga gränser och till vilka endast personer som har auktoriserats av en statsförvaltningsmyndighet har tillträde utan följeslagare.

3.1 Administrativt område

Med administrativt område avses i praktiken områden och lokaler avsedda för myndighetens normala verksamhet, som kontor eller flera kontorslokaler sammantaget. Sådana kan till exempel vara serverrum, datahallar eller företags utrymmen. Den aktör som kontrollerar lokalerna ska säkerställa att endast personer med myndighetens på förhand givna auktorisering får tillträde till lokalerna på egen hand. Det föreskrivs inga särskilda krav på utformningen av administrativa områdens gränser.

Utöver de i denna rekommendation angivna miniminormerna för administrativt område (3.5) inverkar resultatet av myndighetens riskbedömning (avsnitt 3.3) på vilka fysiska säkerhetsåtgärder (avsnitt 3.4) som ska väljas för att de uppställda målen (avsnitt 3.2) ska nås. De enskilda säkerhetsåtgärdernas och det övergripande säkerhetssystemets ändamålsenlighet på området ska regelbundet bedömas på nytt.

Processen för att uppnå målläget och de regelbundna bedömningarna åskådliggörs i figuren nedan.

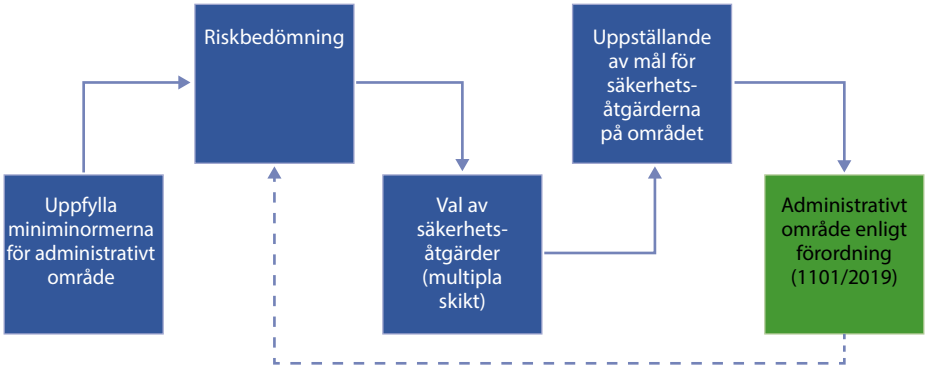

Bild 1. Målbildsprocess och regelbundna bedömningar.

3.2 Mål och metoder för fysiska säkerhetsåtgärder

Syftet med fysiska säkerhetsåtgärder är att förhindra obehörig tillgång till säkerhetsklassificerade uppgifter genom att

- se till att säkerhetsklassificerade uppgifter hanteras och lagras på ett lämpligt sätt
- möjliggöra olika behandling av personalen med avseende på tillgången till säkerhetsklassificerade uppgifter enligt behovsenlig behörighet och, där så är lämpligt, efter säkerhetsprövning
- avskräcka, hindra och avslöja otillåtna handlingar
- förhindra och försena obehörigt intrång.

3.3 Riskbedömning

Valet av fysiska säkerhetsåtgärder ska basera sig på myndighetens riskbedömning. Riskbedömningen ska omfatta alla relevanta faktorer och i synnerhet

- de säkerhetsklassificerade uppgifternas säkerhetsklass
- hanteringsmetod och de säkerhetsklassificerade uppgifternas volym, med beaktande av att stora uppgiftsmängder eller en sammanställning av uppgifter kan göra det nödvändigt att tillämpa striktare riskhanteringsåtgärder

- omgivningarna för den plats där säkerhetsklassificerade uppgifter hanteras och förvaras (byggnadens omgivning samt placering i byggnaden, lokalen eller i en del av den)
- det bedömda hotet för uppgifterna från underrättelsetjänster, brottslig verksamhet och den egna personalen.

3.4 Val av säkerhetsåtgärder

Myndigheten ska utifrån riskbedömning och med tillämpning av principen om multibarriärer fastställa en lämplig och enligt riskbedömningen tillräcklig kombination av säkerhetsåtgärder bestående av administrativa, operativa och fysiska komponenter, inklusive

- strukturella barriärer: ett fysiskt hinder för att avgränsa området eller utrymmet samt försvåra och försena obehörigt intrång.
- behörighetskontroll: kontrollen blockerar tillgången till området eller utrymmet. Syftet är att upptäcka försök av intrång, blockera obehöriga och övervaka dem som rör sig på området. Behörighetskontrollerna kan avse en plats, en byggnad eller byggnader på en plats eller områden eller rum i en byggnad. Kontrollen kan ske med mekaniska, elektroniska eller elektromekaniska system eller andra fysiska metoder. Väktare eller receptionist kan också delta i kontrollerna.
- intrångsdetekteringssystem: ett system för att upptäcka intrång (inbrottslarmsystem) kan användas för att höja den säkerhetsnivå som ges av den strukturella barriären. Systemet kan också användas i stället för bevakningspersonal eller för att bistå denna.
- bevakningspersonal: utbildad, övervakad och när så krävs på lämpligt sätt säkerhetsprövad bevakningspersonal kan sättas in bland annat för att bistå behörighetskontrollen samt för att upptäcka och förhindra personer som planerar intrång på området eller i lokalen.
- övervakningskameror: kameror kan användas för att förhindra incidenter på området eller i utrymmet, kontrollera larm och utreda incidenter. Bevakningspersonalen kan använda övervakningskameror för aktiv bildövervakning i realtid eller för passiv analys av bildmaterial i efterskott.
- förfaranden för upprätthållande av säkerheten: fastställande av ansvar och uppgifter, olika processer och handlingsmodeller, inklusive behörighetshantering och nyckelförvaltning, anvisningar och utbildning av personalen samt service och underhåll av systemen.

- belysning: belysning kan användas i avskräckande syfte mot eventuella inkräktare och för att ge den belysning som är nödvändig för ändamålsenlig övervakning antingen direkt med hjälp av säkerhetspersonalen eller indirekt med övervakningskameror.
- andra lämpliga fysiska åtgärder för att avskräcka och upptäcka obehörigt tillträde eller för att förhindra att säkerhetsklassificerade uppgifter skadas eller går förlorade.

3.5 Miniminormer för de fysiska säkerhetsåtgärderna på administrativa områden

Ett administrativt område som fastställs av myndigheten ska uppfylla de miniminormer som anges i tabellen nedan. Myndigheten ska dessutom planera, delegera och verkställa de övriga riskhanteringsåtgärderna med hänsyn till riskbedömning (avsnitt 3.3) och principen om multibarriärer (avsnitt 3.4) samt upprätthålla åtgärderna så att den kvarstående risken med avseende på de säkerhetsklassificerade uppgifterna är acceptabel och målet med säkerhetsåtgärderna kan uppnås (avsnitt 3.2).

Delområde för säkerhet	Miniminorm	Information och rekommendationer
Områdets gränser och strukturer (väggar, dörrar, fönster, golv- och takkonstruktioner)	Området ska ha tydligt bestämda synliga gränser. Det finns inga specifika normer för utformningen av gränserna.	Med tanke på ändamålsenlig behörighetskontroll ska det vara möjligt att låsa alla andra än de öppningar som används för att röra sig på området. Strukturerna på området ska stärkas om säkerhetsklassificerade uppgifter bevaras på området och risken för intrång är överhängande.
Beviljande av tillgång	Endast personer med myndighetens auktorisering har tillträde till området på egen hand. Myndigheten ska fastställa processerna och rollerna för behörighetshanteringen och nyckelförvaltningen för området.	Tillträdet till området kan kontrolleras med mekaniska eller elektroniska metoder eller med hjälp av personigenkänning. Det ska utses en områdesansvarig som hanterar behörigheterna, passerbrickorna och nycklarna. Myndigheten ska ha fastställt eller godkänt åtminstone följande processer och roller: - Processerna och rollerna för behörighetshantering och nyckelhantering har skapats, dokumenterats och instruerats. - Det finns en lista över dem som givits behörigheter och nycklar. - Behörigheterna kontrolleras regelbundet och uppdateras. - Namngivna personer sköter extrabeställningar och ändringar av nycklar och passerbrickor. - Nyckelkort, ej utgivna nycklar och passerbrickor förvaras på lämpligt sätt.
Besökare	Andra än personer som myndigheten har auktoriserat (dvs. besökare) ska alltid ha en följeslagare.	Myndigheten ska ha antagit riktlinjer för besökare. Myndighetens riktlinjer för besökare kan omfatta bland annat följande: - Identifiera besökaren och ge ut en besökarbricka. - Registrera besöket. - Besökare får inte gå in i eller vistas i utrymmen utan följeslagare. Värden ansvarar för utomstående personer under hela besöket. - Personalen har fått anvisningar för hur de ska bemöta och ta hand om besökare. - Besökare får inte obehörigt se, höra eller på annat sätt ta del av säkerhetsklassificerade uppgifter.
Ljudisolering	Ljudisoleringen på området ska göra det omöjligt för obehöriga att tydligt uppfatta diskussioner om säkerhetsklassificerade uppgifter. Det ska också finnas ljudisolering inom området om där diskuteras sådana säkerhetsklassificerade uppgifter som inte alla behöver ta del av.	Normen för ljudisolering gäller endast de rum på området där säkerhetsklassificerade uppgifter diskuteras.

Delområde för säkerhet	Miniminorm	Information och rekommendationer
Tekniska säkerhetssystem	Vid anskaffning av utrustning för det fysiska skyddet av säkerhetsklassificerade uppgifter på området (t.ex. förmodligen lämplig förvarslösning, dokumentförstörare, lås, elektroniska passerkontrollsystem, övervakningskamerasystem, intrångsdetekteringssystem och larmsystem) ska myndigheten försäkra sig om att utrustningen är funktionsduglig och lämplig.	Utrustningen bör vara förenlig med godkända tekniska standarder och miniminormer. Utrustningen ska hållas i funktionsdugligt skick genom att se till nödvändig service och reparationer, funktionstest och uppdaterad dokumentation enligt tillverkarens anvisningar och rekommendationer. Vid behörighetsförvaltningen bör principen om lägsta behörighet gälla.
Intrångsdetekteringssystem	Inga normer.	Området eller ingångsvägarna till området kan utrustas med ett intrångsdetekteringssystem (inbrottslarmsystem) om säkerhetsklassificerade uppgifter förvaras på området och risken för intrång anses vara överhängande.
Förhindra smygtittande	Om det föreligger en risk för att säkerhetsklassificerade uppgifter kan ses av obehöriga, även oavsiktligt, ska lämpliga åtgärder vidtas för att avvärja risken.	Risken för smygtittande kan reduceras bland annat genom lämplig placering av arbetsplatserna, med hjälp av insynsskydd samt persienner, gardiner eller sekretessfilter för datorn.
Inspektioner av lokaler och utrustning (endast TL II)	Myndigheten ska inspektera alla elektroniska enheter innan de används på ett administrativt område där det hanteras uppgifter av säkerhetsklass HEMLIG, om hotnivån mot uppgifterna anses vara hög. Området ska vid behov inspekteras regelbundet med fysiska eller tekniska metoder. Området bör också inspekteras efter eventuellt obehörigt intrång eller misstanke om intrång.	
Förvaring av uppgifter	På området får förvaras uppgifter av säkerhetsklass BEGRÄNSAD TILLGÅNG. Uppgifterna ska förvaras i lämpliga låsbara kontorsmöbler.	

Tabell 2. Miniminormer för de fysiska säkerhetsåtgärderna på administrativa områden

4 Skyddsområden (SäkIF 9.2 § punkt 2)

Informationshanteringsenheten ska fastställa följande fysiskt skyddade säkerhetsområden för att skydda behandlingen av säkerhetsklassificerade handlingar samt informationssystem på det sätt som avses i 10 §:

2) skyddsområden som har tydligt bestämda och skyddade gränser till vilka allas inträde och utträde övervakas genom identifiering med passerkort eller personligen och till vilka endast personer vilkas pålitlighet har fastställts har tillträde utan följeslagare och som har ett särskilt tillstånd att få komma in på området.

4.1 Skyddsområde

Med skyddsområde avses områden och utrymmen för myndighetens verksamhet där säkerhetsklassificerade uppgifter hanteras och förvaras och som har en högre skyddsnivå än administrativa områden. Skyddsområden är bland annat serverrum, datahallar, arkiv eller exempelvis utrymmen som uppfyller kriterierna för företags skyddsområden. Det är möjligt att upprätta ett tillfälligt skyddsområde på ett administrativt område till exempel för ett möte eller motsvarande ändamål.

Utöver de i denna rekommendation angivna miniminormerna för skyddsområdet (4.5) inverkar resultatet av myndighetens riskbedömning (avsnitt 4.3) på vilka fysiska säkerhetsåtgärder (avsnitt 4.4) som ska väljas för att de uppställda målen (avsnitt 4.2) ska nås. De enskilda säkerhetsåtgärdernas och det övergripande säkerhetssystemets ändamålsenlighet på området ska regelbundet bedömas på nytt.

Processen för att uppnå målläget och de regelbundna bedömningarna åskådliggörs i figuren nedan.

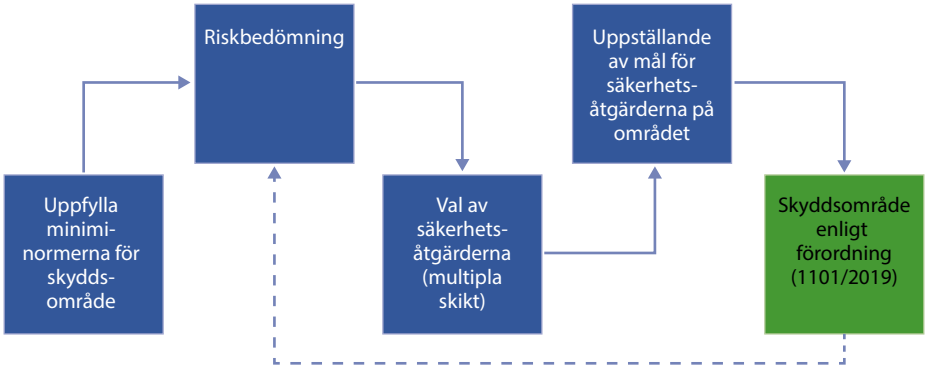

Bild 2. Målbildsprocess och regelbundna bedömningar.

4.2 Mål och metoder för fysiska säkerhetsåtgärder

Syftet med fysiska säkerhetsåtgärder är att förhindra obehörig tillgång till säkerhetsklassificerade uppgifter genom att

- se till att säkerhetsklassificerade uppgifter hanteras och lagras på ett lämpligt sätt
- möjliggöra olika behandling av personalen med avseende på tillgången till säkerhetsklassificerade uppgifter enligt behovsenlig behörighet och, där så är lämpligt, efter säkerhetsprövning
- avskräcka, hindra och avslöja otillåtna handlingar
- förhindra och försena obehörigt intrång.

4.3 Riskbedömning

Valet av fysiska säkerhetsåtgärder ska basera sig på myndighetens riskbedömning. Riskbedömningen ska omfatta alla relevanta faktorer och i synnerhet

- de säkerhetsklassificerade uppgifternas säkerhetsklass
- hanteringsmetod och de säkerhetsklassificerade uppgifternas volym, med beaktande av att stora uppgiftsmängder eller en sammanställning av uppgifter kan göra det nödvändigt att tillämpa striktare riskhanteringsåtgärder

- omgivningarna för den plats där säkerhetsklassificerade uppgifter hanteras och förvaras (byggnadens omgivning samt placering i byggnaden, lokalen eller i en del av den)
- det bedömda hotet för uppgifterna från underrättelsetjänster, brottslig verksamhet och den egna personalen.

4.3 Val av säkerhetsåtgärder

Myndigheten ska utifrån riskbedömning och med tillämpning av principen om multibarriärer (se kommentaren vid figuren) fastställa en lämplig och enligt riskbedömningen tillräcklig kombination av säkerhetsåtgärder bestående av administrativa, operativa och fysiska komponenter, inklusive

- strukturella barriärer: ett fysiskt hinder för att avgränsa området eller utrymmet samt försvåra och försena obehörigt intrång.
- behörighetskontroll: kontrollen blockerar tillgången till området eller utrymmet. Syftet är att upptäcka försök av intrång, blockera obehöriga och övervaka dem som rör sig på området. Behörighetskontrollerna kan avse en plats, en byggnad eller byggnader på en plats eller områden eller rum i en byggnad. Kontrollen kan ske med mekaniska, elektroniska eller elektromekaniska system eller andra fysiska metoder. Väktare eller receptionist kan också delta i kontrollerna.
- intrångsdetekteringssystem: ett system för att upptäcka intrång (inbrottslarmsystem) kan användas för att höja den säkerhetsnivå som ges av den strukturella barriären. Systemet kan också användas i stället för bevakningspersonal eller för att bistå denna.
- bevakningspersonal: utbildad, övervakad och när så krävs på lämpligt sätt säkerhetsprövad bevakningspersonal kan sättas in bland annat för att bistå behörighetskontrollen samt för att upptäcka och förhindra personer som planerar intrång på området eller i lokalen.
- övervakningskameror: kameror kan användas för att förhindra incidenter på området eller i utrymmet, kontrollera larm och utreda incidenter. Bevakningspersonalen kan använda övervakningskameror för aktiv bildövervakning i realtid eller för passiv analys av bildmaterial i efterskott.
- förfaranden för upprätthållande av säkerheten: fastställande av ansvar och uppgifter, olika processer och handlingsmodeller, inklusive behörighetshantering och nyckelförvaltning, anvisningar och utbildning av personalen samt service och underhåll av systemen.

- belysning: belysning kan användas i avskräckande syfte mot eventuella inkräktare och för att ge den belysning som är nödvändig för ändamålsenlig övervakning antingen direkt med hjälp av säkerhetspersonalen eller indirekt med övervakningskameror.
- andra lämpliga fysiska åtgärder för att avskräcka och upptäcka obehörigt tillträde eller för att förhindra att säkerhetsklassificerade uppgifter skadas eller går förlorade.

4.5 Miniminormer för de fysiska säkerhetsåtgärderna på skyddsområden

Ett skyddsområde som fastställs eller godkänns av myndigheten ska uppfylla de miniminormer som anges i tabellen nedan. Myndigheten ska dessutom planera, delegera och verkställa de övriga riskhanteringsåtgärderna med hänsyn till riskbedömning (avsnitt 4.3) och principen om flernivåförsvar (avsnitt 4.4) samt upprätthålla åtgärderna så att den kvarstående risken med avseende på de säkerhetsklassificerade uppgifterna är acceptabel och målet med säkerhetsåtgärderna kan uppnås (avsnitt 4.2).

Delområde för säkerhet	Miniminorm	Information och rekommendationer
Områdets gränser och strukturer (väggar, dörrar, fönster, golv- och takkonstruktioner)	Området ska ha tydligt bestämda synliga gränser. Om området saknar en förvaringslösning som anses vara adekvat, ska områdets väggar, golv, tak, fönster och dörrar säkerställa en säkerhetsnivå som krävs för förvaring av uppgifterna.	Med tanke på tillförlitlig behörighetskontroll ska det vara möjligt att låsa alla andra än de öppningar som används för att röra sig på området. Strukturerna på området ska stärkas om säkerhetsklassificerade uppgifter bevaras på området med en avsevärd risk för intrång. Om möjligt ska utrymningsvägar från ett administrativt område inte gå igenom skyddsområdet. Detta ska beaktas i synnerhet i nybyggen. Arrangemang för utrymning av lokalerna får inte påverka säkerhetsåtgärderna.
Behörighetskontroll	Allas inträde och utträde övervakas vid områdets gräns genom identifiering med passerkort eller personligen.	Behörighetskontrollen kan ske med elektroniska metoder eller med hjälp av personigenkänning.
Beviljande av tillgång	Tillträde utan följeslagare till området kan ges endast till personer som myndigheten har auktoriserat och - vilkas pålitlighet har fastställts - som har ett särskilt tillstånd att komma in på området. Myndigheten ska fastställa processerna och rollerna för behörighetshanteringen och nyckelförvaltningen för området.	Pålitligheten bör säkerställas primärt genom personalsäkerhetsgodkännande. Tillgång till området bör ges utifrån behovsenlig behörighet. Särskilt tillstånd kan i enskilda fall också ges för arbete på området. Det ska utses en områdesansvarig som hanterar behörigheterna, passerbrickorna och nycklarna. Myndigheten ska ha fastställt eller godkänt åtminstone följande processer och roller: Processerna och rollerna för behörighetshantering och nyckelhantering har skapats, dokumenterats och instruerats. - Det finns en lista över dem som givits behörigheter och nycklar. - Behörigheterna kontrolleras regelbundet och uppdateras. - Namngivna personer sköter extrabeställningar och ändringar av nycklar och passerbrickor. - Nyckelkort samt ej utgivna nycklar och passerbrickor förvaras på lämpligt sätt.

Delområde för säkerhet	Miniminorm	Information och rekommendationer
Besökare	Andra än personer som beviljats tillgång till lokalen på egen hand (besökare) ska alltid ha en följeslagare. Om inträde till skyddsområdet innebär i praktiken direkt tillgång till de säkerhetsklassificerade uppgifter som förvaras där gäller dessutom följande krav: - Den högsta säkerhetsklassen för de uppgifter som normalt förvaras på området ska anges tydligt. - Alla besökare ska ha ett särskilt tillstånd för att få komma in på området, de ska alltid ha en följeslagare och deras pålitlighet har fastställts på lämpligt sätt, utom i det fall att besökarna säkert inte kommer åt de säkerhetsklassificerade uppgifterna.	Myndigheten ska ha antagit riktlinjer för besökare. Myndighetens riktlinjer för besökare kan omfatta bland annat följande: - Identifiera besökaren och ge ut en besökarbricka. - Registrera besöket. - Besökare får inte gå in i eller vistas i utrymmen utan följeslagare. Värden ansvarar för utomstående personer under hela besöket. - Personalen har fått anvisningar för hur de ska bemöta och ta hand om besökare. - Besökare får inte obehörigt se eller höra säkerhetsklassificerade uppgifter.
Säkerhetsinstruktioner	För varje skyddsområde ska upprättas säkerhetsförfaranden inklusive anvisningar om följande: - säkerhetsklassen för de säkerhetsklassificerade uppgifter som får hanteras och förvaras på området. - den övervakning och de skyddsåtgärder som ska upprätthållas. - personer som får ges obeledsagat tillträde till området med stöd av särskilt tillstånd och kontrollerad pålitlighet. - vid behov förfaranden för ledsagare eller för skydd av säkerhetsklassificerade uppgifter när andra personer beviljas tillträde till området. - andra relevanta åtgärder och förfaranden.	
Ljudisolering	Ljudisoleringen på området ska göra det omöjligt för obehöriga att tydligt uppfatta diskussioner om säkerhetsklassificerade uppgifter. Det ska också finnas ljudisolering inom området om där diskuteras sådana säkerhetsklassificerade uppgifter som inte alla behöver ta del av.	Normen för ljudisolering gäller endast de rum på området där säkerhetsklassificerade uppgifter diskuteras.

Delområde för säkerhet	Miniminorm	Information och rekommendationer
Tekniska säkerhetssystem	Vid anskaffning av utrustning för det fysiska skyddet av säkerhetsklassificerade uppgifter på området (t.ex. förmodligen lämplig förvarslösning, dokumentförstörare, lås, elektroniska passerkontrollsystem, övervakningskamerasystem, intrångsdetekteringssystem och larmsystem) ska myndigheten försäkra sig om att utrustningen är lämplig för ändamålet. Utrustningen ska inspekteras och underhållas regelbundet.	Utrustningen bör vara förenlig med godkända tekniska standarder och miniminormer. Utrustningen ska hållas i funktionsdugligt skick genom att se till nödvändig service och reparationer, uppdaterad dokumentation och funktionstest enligt tillverkarens anvisningar och rekommendationer. Vid behörighetsförvaltningen bör principen om lägsta behörighet gälla.
Intrångsdetekteringssystem	Områden där tjänstgörande personal inte vistas dygnet runt ska, när så är lämpligt, inspekteras efter den normala arbetstidens slut och med slumpvis valda mellanrum utanför normal arbetstid, utom när intrångsdetekteringssystem har installerats (inbrottslarmsystem).	
Förhindra smygtittande	Om det föreligger en risk för att säkerhetsklassificerade uppgifter kan ses av obehöriga, även oavsiktligt, ska lämpliga åtgärder vidtas för att avvärja risken.	Risken för smygtittande kan reduceras bland annat med hjälp av insynsskydd på arbetsplatserna samt persienner, gardiner eller sekretessfilter för datorn.
Inspektioner av lokaler och utrustning	I utrymmen där det hanteras uppgifter av säkerhetsklass I eller II är det tillåtet att ta in endast sådana elektroniska enheter som godkänts av myndigheten. Området ska i så fall inspekteras regelbundet med fysiska eller tekniska metoder. Området ska också inspekteras efter eventuellt obehörigt intrång eller misstanke om intrång.	Om det inte är möjligt att inspektera ovan nämnda elektroniska enheter eller kontrollera att de har godkänts (mobiltelefoner, smartklockor osv.) ska de lämnas utanför utrymmet, till exempel på en särskild förvaringsplats.

Delområde för säkerhet	Miniminorm	Information och rekommendationer
Förvaring av uppgifter	På området får förvaras uppgifter i alla säkerhetsklasser utifrån riskbedömningen och valet av fysiska säkerhetsåtgärder. Uppgifter av säkerhetsklass KONFIDENTIELL eller högre ska förvaras i en förvaringslösning som bedöms vara lämplig. Myndigheten ska fastställa förfarandena för hantering av nycklarna till och kombinationerna för förvaringslösningen. Kombinationerna ska ges till lägsta möjliga antal personer som behöver känna till dem. Dessa personer ska memorera kombinationerna. Kombinationerna för förvaringslösningar innehållande säkerhetsklassificerade uppgifter ska ändras - vid mottagande av ett nytt säkerhetsskåp - vid varje byte av personal som känner till kombinationen - vid röjande eller vid misstanke om detta när ett lås har genomgått underhållsarbete eller reparation - minst var tolfte månad. Säkerhetsklassificerade uppgifter av säkerhetsklass YTTERST HEMLIG ska förvaras på skyddsområdet under något av följande förhållanden: - tekniskt övervakad förvaringslösning. förvaringslösning utan teknisk övervakning, vars skick kontrolleras regelbundet - förvaringslösning utan teknisk övervakning, som utrustats med intrångsdetekteringssystem och larmen besvaras av en utbildad responsenhet - separat utrymme med intrångsdetekteringssystem och larmen besvaras av en utbildad responsenhet.	

Tabell 3: Miniminormer för de fysiska säkerhetsåtgärderna på skyddsområden

5 Skydd av behandlingen av handlingar och av informationssystemen med hjälp av säkerhetsområden (SäKlF 10 §)

Säkerhetsklassificerade handlingar ska inom och utanför säkerhetsområdena behandlas så att åtkomsten till säkerhetsklassificerade uppgifter skyddas från utomstående.

Handlingar i säkerhetsklass I får förvaras eller på annat sätt behandlas endast inom skyddsområden.

Handlingar i säkerhetsklass II–IV får behandlas inom och utanför säkerhetsområdena, dock så att

1) datalager som innehåller handlingar i säkerhetsklass II eller III och de informationssystem som används för behandlingen av dessa handlingar ska placeras inom ett skyddsområde,

2) pappershandlingar i säkerhetsklass II och III ska förvaras inom ett skyddsområde,

3) datalager som innehåller handlingar i säkerhetsklass IV och de informationssystem som används för behandlingen av dessa handlingar ska placeras inom ett säkerhetsområde,

4) pappershandlingar i säkerhetsklass IV ska förvaras inom ett säkerhetsområde.

Trots vad som i 3 mom. 1 och 3 punkten föreskrivs om placering av informationssystem inom säkerhetsområden, får handlingar i säkerhetsklass II–IV också behandlas inom i 9 § 1 punkten avsedda administrativa områden och utanför dem med hjälp av terminalutrustning och datakommunikationsarrangemang som uppfyller kraven enligt 11 och 12 §. Terminalutrustning som används för behandling av handlingar i säkerhetsklass II ska dock förvaras inom ett skyddsområde. 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.

5.1 Grundläggande principer för hantering och förvaring av uppgifter

	BEHANDLING		FÖRVARIING	
SÄKERHETSKLASS	Administrativt område	Skyddsområde	Administrativt område	Skyddsområde
TL I YTTERST HEMLIG	Nej.	Ja, om åtkomsten till uppgifterna skyddas från utomstående.	Nej.	I en förvaringslösning som bedöms vara lämplig.
TL II HEMLIG	Ja, om åtkomsten till uppgifterna skyddas från utomstående.	Ja, om åtkomsten till uppgifterna skyddas från utomstående.	Nej.	I en förvaringslösning som bedöms vara lämplig.
TL III KONFIDENTIELL	Ja, om åtkomsten till uppgifterna skyddas från utomstående.	Ja, om åtkomsten till uppgifterna skyddas från utomstående.	Nej.	I en förvaringslösning som bedöms vara lämplig.
TL IV BEGRÄNSAD TILLGÅNG	Ja, om åtkomsten till uppgifterna skyddas från utomstående.	Ja, om åtkomsten till uppgifterna skyddas från utomstående.	I låsbara kontorsmöbler som bedöms vara lämpliga.	I låsbara kontorsmöbler som bedöms vara lämpliga.

Tabell 4: Grundläggande principer för hantering och förvaring av uppgifter

Elektronisk behandling eller förvaring utanför säkerhetsområden behandlas i avsnitt 5.6.

5.2 Riskbedömning

De valda fysiska säkerhetsåtgärderna för skydd av behandlingen och förvaringen av uppgifterna ska utgå från myndighetens riskbedömning. Riskbedömningen ska omfatta alla relevanta faktorer och i synnerhet

- de säkerhetsklassificerade uppgifternas säkerhetsklass.
- hanteringsmetod och de säkerhetsklassificerade uppgifternas volym. Det ska noteras att stora uppgiftsmängder eller en sammanställning av uppgifter kan göra det nödvändigt att tillämpa striktare riskhanteringsåtgärder.
- omgivningarna för den plats där säkerhetsklassificerade uppgifter hanteras och förvaras; byggnadens omgivning, placering i byggnaden, lokalen eller i en del av den.
- det bedömda hotet för uppgifterna från underrättelsetjänster, brottslig verksamhet och den egna personalen.

5.3 Förvaring av uppgifter

Uppgifter i säkerhetsklass BEGRÄNSAD TILLGÅNG ska förvaras på administrativt område eller skyddsområde i låsbara kontorsmöbler som bedöms vara lämpliga. De kan tillfälligt förvaras utanför skyddsområde eller administrativt område om uppgiftsinnehavaren har förbundit sig att följa de ersättande åtgärder som fastställs i myndighetens säkerhetsinstruktioner.

Uppgifter i säkerhetsklass KONFIDENTIELL, HEMLIG eller YTTERST HEMLIG ska förvaras på skyddsområde i en förvaringslösning som bedöms vara lämplig, exempelvis kassaskåp eller valv. Elektronisk behandling eller förvaring utanför säkerhetsområden behandlas i avsnitt 5.6.

5.4 Miniminormer för behandling av uppgifter

Uppgifter i säkerhetsklass BEGRÄNSAD TILLGÅNG, KONFIDENTIELL eller HEMLIG ska behandlas inom administrativt område eller skyddsområde.

Uppgifter i säkerhetsklass YTTERST HEMLIG ska behandlas inom skyddsområde.

Handlingar (TL IV–TL II) får behandlas utanför säkerhetsområden förutsatt att det har vidtagits ersättande åtgärder som hänför sig till riskbedömningen för att säkerställa att utomstående inte har åtkomst till säkerhetsklassificerade uppgifter.

Behandlingen av uppgifter ska uppfylla de miniminormer som framgår av Tabell 4. Miniminormerna ska uppfyllas oavsett inom vilket säkerhetsområde uppgifterna behandlas. Utöver miniminormerna ska myndigheten planera och verkställa de övriga riskhanteringsåtgärderna (se avsnitt 5.2) så att den kvarstående risken med avseende på de säkerhetsklassificerade uppgifterna är acceptabel.

5.5 Elektronisk behandling inom administrativt område

Det informationssystem eller datakommunikationsarrangemang som används för behandling av uppgifterna ska vara skyddat enligt ifrågavarande säkerhetsklass. Exempelvis kan terminalutrustning som skyddats enligt säkerhetsklass III placeras inom eller utanför ett administrativt område där terminalen upprättar för behandlingen en enligt säkerhetsklass III krypterad förbindelse till ett enligt säkerhetsklass III skyddat datalager inom

skyddsområdet. Terminalutrustningen får inte lämnas oövervakad på det administrativa området, utan efter behandlingen av uppgifterna ska den återlämnas till förvar inom skyddsområdet, såvida det inte är möjligt att på annat sätt försäkra utrustningens konfidentialitet, integritet och användbarhet (jfr avsnitt 5.6). Det är inte möjligt att har utvidga ett fast informationsnät av säkerhetsklass III eller II till administrativt område.

5.6 Behandling och förvaring av uppgifter av säkerhetsklasser IV eller III i terminalutrustning

I situationer där uppgifter i säkerhetsklass III eller IV behandlas och förvaras i terminalutrustning enligt nämnda säkerhetsklass utanför skyddsområden, eller uppgifter i säkerhetsklass III i administrativt område, ska uppgifterna skyddas med en krypteringslösning som är tillräckligt säker för säkerhetsklassen och i synnerhet ska terminalutrustningens integritet i nämnda säkerhetsklass säkerställas för att uppgifternas konfidentialitet inte ska äventyras vid förlust av terminalutrustningens integritet.

Det vanligaste sättet att trygga integriteten är att skydda terminalutrustningen med fysisk behörighetskontroll av säkerhetsområdena, inklusive bland annat informationssystemets fysiska servrar, nätutrustning, terminalutrustning och kablar. För att skydda till exempel integriteten i ett informationssystem i säkerhetsklass IV mot allmänna risker för säkerhetsklassificerade uppgifter kan det räcka med att datalagren i systemet placeras i administrativt område eller skyddsområde, och terminalutrustning som skyddas med tillräcklig kryptering kan också begränsat förvaras i ett annat låsbart utrymme, exempelvis hemma hos en tjänsteman.

Informationssystem i säkerhetsklass III bör i sin helhet placeras inom skyddsområde. Om terminalutrustning som används för behandling av uppgifter i säkerhetsklass III behöver förvaras inom administrativt område eller till och med utanför säkerhetsområden bör bristerna i integritetsskyddet genom den fysiska behörighetskontrollen kompenseras med hänsyn till riskerna, till exempel genom att placera terminalen i ett skal eller en förpackning som avslöjar obehörigt intrång. Det finns bland annat så kallade säkerhetsväskor som kan detektera försök till obehörig åtkomst till innehållet i portföljen och antingen skickar meddelande till terminalutrustningens behöriga användare eller användarens organisation om intrångsförsök eller det att försöket lämnar spår på skalet eller förpackningen.

Myndigheten ska vid riskbedömningen beakta att verksamhet utanför säkerhetsområden innebär sådana risker för både säkerhetsklassificerade uppgifter och den terminalutrustning med vilken uppgifterna behandlas, speciellt i säkerhetsklass III eller högre, som det kan vara ytterst svårt eller omöjligt att reducera i praktiken. Vid behandling av uppgifterna

behövs dessutom skydd mot olovlig insyn och avlyssning, samt beroende på riskerna även till exempel skydd mot diffus elektromagnetisk strålning.

Om terminalutrustningen används för behandling av såväl nationella som internationella säkerhetsklassificerade uppgifter ska det vid förvaring av terminalutrustning i säkerhetsklass III iakttas de internationella informationssäkerhetsskyldigheterna som kan helt förbjuda förvaring utanför skyddsområde.

BEHANDLING AV PAPPERSHANDLINGAR	
Delområde för säkerhet	**Miniminorm**
Principen om begränsning av behovsenlig behörighet	Uppgifter får behandlas om åtkomsten till säkerhetsklassificerade uppgifter har skyddats mot utomstående. Med utomstående avses alla personer som saknar fastställd behörighet till de säkerhetsklassificerade uppgifterna.
Åtgärder mot smygtittande	Om det föreligger en risk för att säkerhetsklassificerade uppgifter kan ses av obehöriga, även oavsiktligt, ska lämpliga åtgärder vidtas för att kontrollera risken.
Åtgärder mot teknisk underrättelseinhämtning (endast TL I och TL II)	Myndigheten ska inspektera alla elektroniska enheter innan de används på det område där behandlingen sker, om hotnivån mot uppgifterna anses vara hög. Området ska vid behov inspekteras regelbundet med fysiska och/eller tekniska metoder. Området bör också inspekteras vid eventuellt obehörigt intrång eller misstanke om intrång.

Tabell 5: Behandling av pappershandlingar

ELEKTRONISK BEHANDLING AV UPPGIFTER	
Delområde för säkerhet	**Miniminorm**
Principen om begränsning av behovsenlig behörighet	Uppgifter får behandlas om åtkomsten till säkerhetsklassificerade uppgifter har skyddats mot utomstående. Med utomstående avses alla personer som saknar fastställd behörighet till de säkerhetsklassificerade uppgifterna.
Åtgärder mot smygtittande	Om det föreligger en risk för att säkerhetsklassificerade uppgifter kan ses av obehöriga, även oavsiktligt, ska lämpliga åtgärder vidtas för att kontrollera risken.
Åtgärder mot teknisk underrättelseinhämtning (endast TL I och TL II)	Myndigheten ska inspektera alla elektroniska enheter innan de används på ett område där uppgifter behandlas, om hotnivån mot uppgifterna anses vara hög. Området ska vid behov inspekteras regelbundet med fysiska och/eller tekniska metoder. Området bör också inspekteras vid eventuellt obehörigt intrång eller misstanke om intrång.
Tempestrisker (endast TL I–III)	Vid elektronisk behandling av uppgifter i säkerhetsklass KONFIDENTIELL eller högre ska risker som hänför sig till diffus strålning och elektronisk underrättelseinhämtning reduceras i tillräcklig omfattning.

Tabell 6: Elektronisk behandling av uppgifter

MUNTLIG BEHANDLING AV UPPGIFTER	
Delområde för säkerhet	Miniminorm
Principen om begränsning av behovsenlig behörighet	Uppgifter får behandlas om utomstående inte kan höra diskussioner som gäller säkerhetsklassificerade uppgifter. Med utomstående avses alla personer som saknar fastställd behörighet till de säkerhetsklassificerade uppgifterna. Gällande ljudisolering bör det beaktas att det även inom området kan arbeta sådana personer som saknar behovsbehörighet till uppgifterna.
Åtgärder mot teknisk underrättelseinhämtning (endast TL I och TL II)	Behandlingsområdet ska ha intrångsdetekteringssystem och området ska vara låst då det inte används. Personer och material som kommer in på området ska övervakas. Området ska vid behov inspekteras regelbundet med fysiska eller tekniska metoder. Området bör också inspekteras vid eventuellt obehörigt intrång eller misstanke om intrång. På behandlingsområdet får inte finnas obehöriga - datakommunikationsförbindelser - telefoner andra kommunikationsenheter elektroniska enheter. Myndigheten ska inspektera alla elektroniska enheter innan de används på det område där behandlingen sker, om hotnivån mot uppgifterna anses vara hög.

Tabell 7: Muntlig behandling av uppgifter

6 Avskiljning av informationssystem (SäKIF 11.1 § punkt 1)

Informationssystem och datakommunikationsarrangemang som används för behandling av säkerhetsklassificerade handlingar ska genomföras så att

1) 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 i olika säkerhetsklasser kan ske med brandväggar och styrning av säkerhetskritiska tjänster i lägre säkerhetsklasser (t.ex. webbläsning och e-posttrafik via internet) via separata proxyservrar som filtrerar innehållet. Informationssystem och datakommunikationsarrangemang i säkerhetsklass IV får kopplas upp mot internet och andra opålitliga nät under förutsättning att de risker som hänför sig till uppkopplingen kan reduceras tillräckligt med andra skydd till den nivå som krävs för säkerhetsklass IV. Detta kräver speciellt att programvaran hålls uppdaterad, principen om lägsta behörighet ska gälla, systemen ska härdas samt incidenter ska detekteras och korrigeras. En vanlig behandlingsmiljö i säkerhetsklass IV är en del av informationshanteringsdelen i organisationens ”kontorsnät”, som kan bestå av exempelvis arbetsstationer och ärendehanteringssystem samt skyddsarrangemangen för dessa. Motsvarande avskiljning med brandvägg och andra filter kan också tillämpas för att skydda sekretessbelagda uppgifter som saknar säkerhetsklassificering samt för att skydda integriteten och användbarheten av offentliga uppgifter.

Från och med säkerhetsklass III kan avskiljningen i miljöer i olika säkerhetsklasser verkställas med tillräckligt säkra gatewaylösningar. De ska läggas upp med kraven ”No Read Up” ja ”No Write Down” enligt säkerhetsmodellen Bell-LaPadula. Gatewaylösningarna ska med andra ord på ett tillförlitligt sätt blockera att uppgifter i en högre säkerhetsklass förmedlas till en miljö i en lägre säkerhetsklass. Principerna för systemupplägget beskrivs mer detaljerat i Cybersäkerhetscentrets anvisning om gatewaylösningar.

Säkra gatewaylösningar är exempelvis datadioder som säkerställer ett enkelriktat informationsutbyte. Avskiljning av informationssystem och datakommunikationsarrangemang i säkerhetsklass II får i princip verkställas endast med ytterst säkra datadioder. Avskiljning i säkerhetsklass I ska i princip ske genom fullständig fysisk separering och endast i undantagsfall med datadioder. Praktiska utföranden av säkra gatewaylösningar beskrivs mer detaljerat i Cybersäkerhetscentrets anvisning om gatewaylösningar.

Då informationssystem och datakommunikationsarrangemang ansluts till system och arrangemang i en lägre säkerhetsklass bör det också tas hänsyn till internationella informationssäkerhetsåtaganden som eventuellt förbjuder anslutning. Statsförvaltningsmyndigheter kan med stöd av lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011) anlita Cybersäkerhetscentret för bedömning av informationssäkerheten i sina system eller arrangemang. Det rekommenderas att myndigheten ber om en bedömning speciellt av anslutning av informationssystem och datakommunikationsarrangemang i säkerhetsklass I och II till system och arrangemang i en lägre säkerhetsklass, för att den myndighet som ansvarar för säkerheten i dessa ska kunna fatta beslut om riskhanteringen med stöd av Cybersäkerhetscentrets expertbedömning av eventuella kvarstående risker.

6.1 Bestämmelser och tilläggsinformation

Anvisning Guide om planeringsprinciper och lösningsmodeller för gatewaylösningar (Cybersäkerhetscentret)

Anvisning Bedömnings- och godkännandeprocesser av informationssystem utförda av Transport- och kommunikationsverket Traficom (Cybersäkerhetscentret)

Katakri 2015 – verktyg för informationssäkerhetsauditering för myndigheter (Försvarsministeriet): 5. Delområde I Teknisk informationssäkerhet, Krav I 01

7 Krypteringslösningar (SäKlF 11.1 § punkt 7)

Informationssystem och datakommunikationsarrangemang som används för behandling av säkerhetsklassificerade handlingar ska genomföras så att

7) de krypteringslösningar som används är tillräckligt säkra med beaktande av säkerhetsklassen för de handlingar som behandlats i informationssystemen eller datakommunikationsarrangemangen.

Denna rekommendation är också avsedd att stödja genomförandet av följande normer:

14 § i informationshanteringslagen: Informationsöverföring i datanät

Om en myndighet överför sekretessbelagd information i det allmänna datanätet ska informationen överföras i ett krypterat eller på annat sätt skyddat format. 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.

I lagen om tillhandahållande av digitala tjänster (306/2019) föreskrivs om identifiering av användaren i samband med digitala tjänster som tillhandahålls allmänheten.

12 § i förordningen om säkerhetsklassificering: Överföring av en handling via datanätet

Bestämmelser om överföring av sekretessbelagd information i det allmänna datanätet finns i 14 § i informationshanteringslagen. Säkerhetsklassificerade handlingar får 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. 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.

Speciellt vid kommunikation över offentliga nät eller nät i en lägre säkerhetsklass är krypteringslösningar ofta det enda skyddet för sekretessbelagda uppgifters konfidentialitet och oftast även deras integritet. Eftersom det ofta är ytterst svårt att kompensera eventuella brister i krypteringslösningarna med andra skyddsmetoder krävs det särskild omsorg vid såväl valet av krypteringslösning som säker användning av den.

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. I praktiken används för kryptering exempelvis VPN-lösningar mellan användarnas terminalenheter och myndighetens informationssystem, kryptering mellan organisationers nätverk (LAN-2-LAN) samt olika lösningar för e-postkryptering och filkryptering som tillhandahålls slutanvändarna. Vid överföring av sekretessbelagda uppgifter mellan fysiskt skyddade områden och inom ett nät med åtminstone motsvarande skyddsnivå är det utifrån riskbedömning möjligt att använda överföring med lägre skyddsnivå eller utan kryptering.

Myndigheten ska använda sådana krypteringslösningar vars tillräckliga säkerhet har bestyrkts på ett tillförlitligt sätt. Bedömningen av krypteringslösningar bygger på flera olika faktorer. Utöver verifiering av krypteringsstyrkan och krypteringsproduktens funktionsriktighet ska man även beakta hotnivån i produktens driftsmiljö. Till exempel är hotnivån vid datatrafik över Internet annan än för kryptering vid överföring inom ett kontrollerat och fysiskt skyddat område (till exempel datatrafik mellan två skyddsområden via ett administrativt område). Andra faktorer som ska beaktas vid bedömningen av krypteringsprodukter är till exempel de krav som de specifika omständigheterna för användningen ställer på sekretesstiden och integriteten.

Olika slags informationsmaterial är föremål för olika slags risker. Exempelvis myndigheternas säkerhetsklassificerade uppgifter ska i regel skyddas med tanke på statens säkerhet (allmänintresset). Säkerhetsklassificerade uppgifter kan å andra sidan antas vara föremål för intresse från andra parter än de som intresserar sig till exempel för personuppgifter som saknar säkerhetsklassificering. Skillnaderna i riskexponeringen ska beaktas vid valet av krypteringslösning.

Den valda krypteringslösningen bör företrädesvis vara en lösning som bedömts och godkänts av den nationella myndigheten för informationssäkerhet (NCSA-verksamheten vid Cybersäkerhetscentret). Ett väsentligt element för godkännandet av

krypteringslösningarna är de policyer och inställningar för användningen med vilka lösningen ska ge ett fullgott skydd för uppgifter i den aktuella säkerhetsklassen.

Krypteringseffekten kan gå delvis eller helt förlorad i situationer där svagheter i nyckelförvaltningen kan utnyttjas av obehöriga. Därför ska det finnas planerade, implementerade och dokumenterade (genom beskrivningar eller anvisningar) processer för förvaltningen av krypteringsnycklarna. Endast behöriga användare och processer får ha åtkomst till krypterade nycklar. Av processerna ska krävas åtminstone a) kryptografiskt starka nycklar, b) säker nyckeldistribution, c) säker nyckelförvaring, d) nyckelutbyte med fastställda intervaller, e) utbyte av föråldrade eller avslöjade nycklar, och f) förhindrande av obehörigt nyckelutbyte.

Myndigheten ska vid riskbedömningen också ta hänsyn till säkerheten i leveranskedjorna speciellt i fråga om krypteringslösningar. Även om krypteringslösningen är tillräckligt säker då tillverkaren levererar den, kan bristande skydd i leveranskedjan möjliggöra manipulering av krypteringslösningen varigenom myndigheten sedan 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 har bland annat i användningspolicyerna för de krypteringslösningar som centret har godkänt för skydd av säkerhetsklassificerade uppgifter tagit ställning till användaridentifiering då krypteringslösningen används vid kommunikation med en person som befinner sig inom i en annan organisation (exempelvis krypterad e-post). Å andra sidan har många krypteringslösningar motpartsidentifiering som bygger på att nyckelförvaltningen är tillförlitlig (t.ex. symmetrisk kryptering mellan organisationens verksamhetsställen eller nätverksdatakryptering (LAN-2-LAN), eller filkryptering med delad nyckel).

Speciellt i samband med överföring av säkerhetsklassificerade uppgifter bör det dessutom beaktas att utan tillförlitligt bevis för nuläget gällande skyddet av informationshanteringsmiljöerna (t.ex. nätverk som förbinder flera myndigheter) tillhandahålls tillräcklig kryptering eller mottagarautentisering inte nödvändigtvis som en integrerad tjänst utan ska genomföras med en separat krypteringslösning.

Speciellt vid överföring av sekretessbelagda uppgifter som saknar säkerhetsklassificering ska hänsyn tas till att i lagen om tillhandahållande av digitala tjänster (306/2019) föreskrivs om identifiering av användaren i samband med digitala tjänster som tillhandahålls allmänheten.

7.1 Bestämmelser och tilläggsinformation

Tabeller över krypteringsstyrka (på finska): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf

Anvisning om bedömning och godkännande av krypteringsprodukter (på finska): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-salaustuotearvioinnit-ja-hyvaksynnat.pdf

Godkända krypteringslösningar (på finska): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

Mer information för utveckling av säkra krypteringslösningar:

- Säker utveckling – Med sikte på godkännande: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_10072019_SV.pdf

Om hantering av krypteringslösningar i bedömningskriterierna:
Katakri 2015 (i synnerhet punkterna I 12, I 01, I 15) (på finska): http://defmin.fi/katakri

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN 978-952-367-293-2 (pdf)

Mars 2020