VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri)

Rekommendation och kriterier

Nämnder

FINANSMINISTERIETS PUBLIKATIONER – 2023:47

Finansministeriets publikationer 2023:47

Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri)

Rekommendation och kriterier

Finansministeriet Helsingfors 2023

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: 978-952-367-462-2
ISSN pdf: 1797-9714

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2023

Presentationsblad
12.6.2023

Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri)

Rekommendation och kriterier

Finansministeriets publikationer 2023:47		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	svenska	**Sidantal**	173

Referat

I lagen om informationshantering inom den offentliga förvaltningen (906/2019) finns bestämmelser om ansvar i fråga om informationssäkerhetsåtgärder som gäller informationshanteringsenheter och myndigheter inom den offentliga förvaltningen samt privatpersoner, sammanslutningar och offentligrättsliga samfund som inte är myndigheter till den del som de sköter offentliga förvaltningsuppgifter. I lagen finns också bestämmelser om miniminivån för informationssäkerhetsåtgärder och om skyldigheten att följa upp informationssäkerheten i verksamhetsmiljön och försäkra sig om informationssäkerheten i informationsmaterial och informationssystem under hela deras livscykel. Organisationen ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Vid upphandlingar ska organisationen säkerställa att de aktuella informationssystemen har lämpliga informationssäkerhetsåtgärder.

Den här rekommendationen av informationshanteringsnämnden beskriver kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen och ger anvisningar om hur de används. Kriterierna för bedömning stödjer behoven av utveckling och bedömning av informationssäkerheten i hela den offentliga förvaltningen. De kan användas som hjälp vid bedömning av hur kraven på informationssäkerhet i informationshanteringslagen, säkerhetsklassificeringsförordningen och delvis i dataskyddsförordningen uppfylls.

Informationshanteringsnämnden godkände rekommendationerna vid sitt möte den 11 maj 2022.

Nyckelord nämnder, informationshanteringsnämnden, lag om informationshanteringslagen, offentlig förvaltning, säkerhet i förvaltningen, fysisk säkerhet, teknisk säkerhet, beredskap, hantering av kontinuiteten, informationssäkerhet, dataskydd, cybersäkerhet, riskhantering, informationssystem, informationshantering, bedömning

ISBN PDF	978-952-367-462-2	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-462-2		

Kuvailulehti
12.6.2023

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)
Suositus ja kriteeristö

Valtiovarainministeriön julkaisuja 2023:47		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	ruotsi	**Sivumäärä**	173

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) on säädetty tietoturvallisuustoimenpiteisiin liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää. Lisäksi laissa säädetään tietoturvallisuustoimenpiteiden vähimmäistasosta sekä velvoitteesta seurata toimintaympäristönsä tietoturvallisuuden tilaa ja varmistua tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta koko niiden elinkaaren ajan. Organisaation on tunnistettava olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Hankintojen osalta organisaation tulee varmistaa, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Tässä tiedonhallintolautakunnan antamassa suosituksessa kuvataan julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), ja ohjeistetaan sen käytöstä. Arviointikriteeristö tukee koko julkishallinnon tietoturvallisuuden kehittämisen ja arvioinnin tarpeita. Sitä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä.

Tiedonhallintalautakunta hyväksyi suosituskokoelman kokouksissaan 11.5.2022.

Asiasanat lautakunnat, tiedonhallintalautakunta, tiedonhallintalaki, julkinen hallinto, hallinnollinen turvallisuus, fyysinen turvallisuus, tekninen turvallisuus, varautuminen, jatkuvuuden hallinta, tietoturva, tietosuoja, kyberturvallisuus, riskienhallinta, tietojärjestelmät, tiedonhallinta, arviointi

ISBN PDF	978-952-367-462-2	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-462-2		

Description sheet
12 June 2023

Assessment criteria for information security in public administration (Julkri) Recommendation and criteria

Publications of the Ministry of Finance 2023:47		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	Swedish	**Pages**	173

Abstract

The Act on Information Management in Public Administration (906/2019) lays down obligations relating to information security measures that apply to information management units and authorities as well as to private individuals or corporations or to corporations subject to public law other than those serving as authorities insofar as they perform public administrative tasks. The Act also lays down provisions on a minimum level for information security measures and on an obligation for organisations to monitor the state of the data security of their operating environment and ensure the data security of their datasets and information systems over their entire lifecycle. Organisations shall determine the material risks related to data processing and scale their data security measures in accordance with a risk assessment. With respect to procurement, organisations shall ensure that appropriate data security measures have been implemented in the information system to be acquired.

The recommendation issued by the Information Management Board describes the assessment criteria for information security in public administration (Julkri) and provides instructions for using them. The assessment criteria support the development and assessment of information security in public administration as a whole. The criteria can be used to assess the fulfilment of the information security requirements laid down in the Information Management Act, Security Classification Decree and partly also in the General Data Protection Regulation.

The Information Management Board approved the collection of recommendations on 11 May 2022.

Keywords board, Information Management Board, Information Management Act, public administration, administrative security, physical security, technical security, preparedness, continuity management, information security, data protection, cyber security, risk management, data systems, information management, evaluation

ISBN PDF	978-952-367-462-2	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-462-2		

Innehåll

1 Inledning

Detta är informationshanteringsnämndens rekommendation om kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen, nedan *Julkri*, och användningen av kriterierna. Kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen stöder behoven av utveckling och bedömning av informationssäkerheten i hela den offentliga förvaltningen. De kan användas som hjälp vid bedömning av hur kraven på informationssäkerhet i informationshanteringslagen, säkerhetsklassificeringsförordningen och delvis även i dataskyddsförordningen uppfylls.

Rekommendationen och dess bilagor har beretts i sektionen för kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen som informationshanteringsnämnden tillsatt för perioden 1.5–31.12.2021 och i informationssäkerhetssektionen som tillsattes för perioden 1.1–31.12.2022. Specialsakkunnig Eelis Laine från finansministeriet har agerat som sektionens ordförande, och informationssäkerhetssakkunnig Hanna Heikkinen och ledande expert Tuula Seppo från Myndigheten för digitalisering och befolkningsdata har agerat som dess sekreterare. Informationshanteringsnämnden har utsett experter från olika informationshanteringsenheter till medlemmar av sektionen. Dessutom har sektionen i stor omfattning hört även experter utanför sektionen under sina möten, verkstäder och seminarier. Rekommendationsutkastet var öppen för kommentarer via den offentliga utlåtandetjänsten under perioden 28.03–19.04.2022.

Vad gäller dataskydd och tryggandet av personuppgifter har kriterierna utarbetats i samarbete med Dataombudsmannens byrå. Dataombudsmannens byrå ansvarar för dataskyddskriterierna (bilaga 1B) och de övriga delarna som är förknippade med dataskydd samt ger mer information om dessa. Vad gäller de övriga delarna fås information från Informationshanteringsnämnden.

I lagen om informationshantering inom den offentliga förvaltningen (906/2019), nedan *informationshanteringslagen*, finns bestämmelser om ansvar i fråga om informationssäkerhetsåtgärder som gäller informationshanteringsenheter och myndigheter inom den offentliga förvaltningen samt privatpersoner, sammanslutningar och offentligrättsliga samfund som inte är myndigheter till den del som de sköter offentliga förvaltningsuppgifter. Nedan används termen *organisation* om dessa objekt för datasäkerhetsreglering. I lagen finns också bestämmelser om miniminivån för informationssäkerhetsåtgärder och om skyldigheten att följa upp informationssäkerheten i verksamhetsmiljön och försäkra

sig om informationssäkerheten i informationsmaterial och informationssystem under hela deras livscykel. Organisationen ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Vid upphandlingar ska organisationen säkerställa att de aktuella informationssystemen har lämpliga informationssäkerhetsåtgärder.

I utarbetandet av rekommendationen har uppmärksamhet fästs vid Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019), nedan *säkerhetsklassificeringsförordningen*, lagen om offentlighet i myndigheternas verksamhet (621/1999), nedan *offentlighetslagen*, EU:s allmänna dataskyddsförordning ((EU) 2016/679), nedan *dataskyddsförordningen*, och dataskyddslagen (1050/2018). Dessutom har man beaktat verktyget för informationssäkerhetsauditering för myndigheter (Katakri) och säkerhetskriterierna för molntjänster (PiTuKri) för att säkerställa enhetligheten.

Säkerheten i myndigheternas informationssystem kan bedömas i enlighet med lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011), nedan *bedömningslagen*. Ytterligare information om bedömnings- och godkännandeprocessen finns i den finskspråkiga anvisningen ”Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit” (Bedömnings- och godkännandeprocesser av informationssystem utförda av Transport- och kommunikationsverket Traficom).

Organisationerna kan använda certifikat som gäller dataskydd enligt dataskyddsförordningen som ett sätt att visa att den personuppgiftsansvarige eller personuppgiftsbiträdet iakttar sina föreskrivna skyldigheter. Certifiering i enlighet med artikel 42 i den allmänna dataskyddsförordningen minskar inte den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar vad gäller iakttagandet av dataskyddsförordningen och begränsar inte Dataombudsmannens byrås uppgifter och befogenheter. Mer information om ansvarsskyldigheten som gäller behandlingen av personuppgifter finns i dataombudsmannens anvisning ”Visa att du iakttar dataskyddsbestämmelserna”.

I bedömningen av tillförlitligheten av tjänsteleverantörer som erbjuder tjänster åt myndigheter kan man utnyttja säkerhetsutredningar av företag i enlighet med säkerhetsutredningslagen (726/2014). Dessa utredningar riktas in på tjänster som produceras i Finland eller som produceras i framtiden och på tjänsteleverantören som erbjuder tjänsten i fråga. Ytterligare information finns i Skyddspolisens anvisning ”Säkerhetsutredning av företag”. Bedömningar av informationssystem som omfattas av internationella skyldigheter gällande informationssäkerhet genomförs enligt förfaranden som föreskrivs i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004). Utrikesministeriet agerar som Finlands nationella säkerhetsmyndighet i genomförandet av internationella förpliktelser som gäller informationssäkerhet. Ytterligare information finns i den nationella säkerhetsmyndighetens anvisningar.

2 Kriterier

I denna rekommendation och dess bilagor beskrivs kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen och rekommendationen för deras användning. Rekommendationen innehåller följande bilagor:

- bilaga 1A Julkri-kriterierna,
- bilaga 1B Dataskyddskriterier,
- bilaga 2 Julkri-verktyget (Excel),
- bilaga 3 Bruksanvisning för Julkri-verktyget och
- bilaga 4 Terminologi.

Kriterierna klassificeras på olika nivåer enligt konfidentialitet, tillgänglighet och integritet. Av dessa plockar verktyget de väsentliga och de valfria kriterierna utifrån säkerhetskraven för objektet som ska bedömas och utgående från det valda användningsfallet. I princip bör de väsentliga kriterierna inkluderas i bedömningen. Organisationen kan utifrån riskbedömningen och fallspecifik bedömning inkludera även valfria kriterier i bedömningen och besluta vilka valfria kriterier som ska inkluderas.

Kriterierna kan användas som hjälp vid bedömning av hur kraven på informationssäkerhet i informationshanteringslagen, säkerhetsklassificeringsförordningen och delvis även i dataskyddsförordningen uppfylls. Kriterierna är en rekommendation och lagstiftningens krav kan också uppfyllas på annat sätt än det som beskrivs i kriterierna. Utöver Katakri[1]- och PiTuKri[2]-kriterierna innehåller Julkri även kriterier gällande offentlig och sekretessbelagd information, dataskydd och hantering av beredskap och kontinuitet.

1 Katakri se Katakri – verktyg för informationssäkerhetsauditering för myndigheter - Utrikesministeriet (um.fi))

2 PiTuKri se https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_PiTuKri_2020_SE_210506_WEB.pdf

2.1 Syfte och fördelar

Användningen av kriterierna stöder organisationerna i planeringen, genomförandet och bedömningen av datasäkerheten och skyddet av personuppgifter. De kan utnyttjas i bedömningen av lagenlighet och som en del av ansvarsskyldigheten i enlighet med dataskyddsförordningen. Organisationen kan använda Julkri till exempel i följande situationer:

- **Planering av tjänsten och definition av kraven** innan utvecklingen eller upphandlingen med syfte att identifiera kraven som ska ställas på tjänsten.
- **Bedömning av leverantören** med syfte att identifiera kraven på leverantören i konkurrensutsättningen eller som en del av tjänsteavtalet och säkerställa att kraven uppfylls i leverantörens verksamhet.
- **Bedömning av tjänsten** i förhållande till upphandlingens och tjänsteavtalets krav.
- **Bedömning av uppfyllande av kraven gällande dataskydd.**

Kriterierna stöder organisationens riskbaserade säkerhetsledning. På förhand definierade användningsfall underlättar den situationsspecifika tillämpningen av kriterierna. Dessutom är det möjligt att i Julkri definiera även organisationsspecifika användningsfall för ofta återkommande bedömningssituationer. Användningsfallen behandlas i bruksanvisningen för Julkri-verktyget (bilaga 3).

Kriterierna kan användas i bedömningen av behandlingen av sekretessbelagda uppgifter, personuppgifter och säkerhetsklassificerade uppgifter. Vad gäller säkerhetsklass I (TL I – YTTERST HEMLIG) ska organisationen dessutom beakta fallspecifika behandlingskrav.

2.2 Avgränsningar

I det administrativa och tekniska delområdet i Julkri nämns tillgänglighet som ett av de allmänna kriterierna. Kriterierna innehåller inte mer detaljerade tillgänglighetskriterier, vilket innebär att organisationen ska beakta tillgänglighetsrelaterade krav separat. (Lagen om tillhandahållande av digitala tjänster 306/2019).

Julkri innehåller inte bedömning av datasäkerheten av internationella säkerhetsklassificerade uppgifter (588/2004). Den nationella säkerhetsmyndigheten (NSA) som är underställd utrikesministeriet ansvarar för anvisningar och bedömningskriterier förknippade med detta.

Åtgärder som gäller verksamhetens kontinuitet i undantagsförhållanden och som omfattas av beredskapslagen (1552/2011) omfattas inte av kriterierna. Den del av kriterierna som gäller beredskap och grundar sig på informationshanteringslagen (VAR)

stöder dock för sin del organisationen även i att uppfylla kraven gällande beredskap för undantagsförhållanden.

Kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen beaktar inte kraven inom branschspecifik lagstiftning, såsom inom social- och hälsovården eller finansbranschen. De beaktar inte heller kraven i enlighet med lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018).

Trots att kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen inte innehåller krav förknippade med internationell och branschspecifik lagstiftning, ska organisationen ändå identifiera och beakta sådana krav och krav förknippade med EU-reglering i sin egen verksamhet.

3 Kriteriernas struktur och delområden

Kriterierna har grupperats i fem **delområden**. Varje delområde har ett preciserande namn, och den första delen av identifieraren för kriterierna som hör till delområdet baserar sig på delområdets finska namn. Kriteriernas delområden och deras förkortningar är följande:

- administrativ säkerhet (HAL),
- fysisk säkerhet (FYY),
- teknisk säkerhet (TEK),
- beredskap och kontinuitetshantering (VAR),
- dataskydd (TSU).

Delområdena består av **huvudkriterier** och **underkriterier** som kompletterar huvudkriterierna. Det finns sammanlagt över tvåhundra kriterier. Strukturen huvudkriterium – underkriterium har utnyttjats till exempel i sådana fall där kraven som är förknippade med samma tema är strängare på högre säkerhetsnivåer. Till exempel kan ett huvudkriterium som gäller sekretessbelagda uppgifter kompletteras med ett underkriterium som preciserar genomförandesättet av ett krav som gäller uppgifter som hör till klass TL IV.

Varje kriterium har klassificerats på olika nivåer med tanke på konfidentialitet, integritet, tillgänglighet och dataskydd. Beroende på kriteriet kan det vara förknippat med ett eller flera av dessa synvinklar. Till exempel kan samma kriterium som gäller åtkomsträttigheter vara förknippat med både konfidentialitet, integritet och dataskydd.

Allmänna beskrivningar av kriteriernas olika delområden finns i de följande kapitlen. De enstaka kriterierna finns i bilagorna 1A och 1B.

3.1 Administrativ säkerhet

Delområdet administrativ säkerhet behandlar de metoder som används för att implementera hantering av informationssäkerheten som en del av hela organisationens verksamhet. Delområdet täcker allmänna kriterier för administrativ säkerhet, personalsäkerhet, informationssystem och deras upphandling samt användningssäkerhet. Med den administrativa säkerhetens kriterier strävar man efter att organisationen har ett hanteringssystem för informationssäkerhet som fungerar tillräckligt bra och förfaranden för att säkerställa

att personalen som behandlar uppgifterna agerar på korrekt sätt. Organisationen ska också säkerställa att förpliktelser gällande behandling av uppgifter iakttas i situationer där uppgifter behandlas på uppdrag av organisationen.

Många kriterier inom delområdet administrativ säkerhet fungerar som grund för de övriga delområdenas kriterier. Till exempel är kriterierna förknippade med identifiering av skyddade objekt, riskhantering och dokumentering allmänna och ska som standard utnyttjas i samband med tillämpningen av de övriga delområdenas kriterier.

Processer förknippade med administrativ säkerhet ska behandlas som helheter. Informationssäkerhetens hanteringsmetoder ska utifrån riskbedömningen relateras till uppgifterna som ska skyddas och till organisationens verksamhet.

Användningen av kriterierna förutsätter ändamålsenlig inriktning. Om vissa funktioner har bedömts redan tidigare kan de tidigare resultaten utnyttjas i tillämpliga delar. Till exempel om organisationens telekommunikationsmiljö har bedömts under det senaste året och inga betydande ändringar har gjorts i den, kan bedömningen i fråga eventuellt utnyttjas i bedömningen av ett nytt informationssystem som installeras i telekommunikationsmiljön.

Om man i organisationen behandlar uppgifter som klassificerats på olika nivåer i separata miljöer och processer, kan det vara ändamålsenligt att dela in bedömningen i separata logiska helheter. Till exempel vad gäller personalen som använder en behandlingsmiljö för uppgifter som säkerhetsklassificerats på en högre nivå skiljer sig innehållet i anvisningarna vanligen i betydande grad från de allmänna anvisningarna som gäller hela organisationen.

God riskhantering omfattar dokumentering av förfaringssätt och särskilt riskbedömningen. Planer och anvisningar förknippade med hantering av informationssäkerheten samt bedömningsresultaten och slutsatserna bör presenteras skriftligen. Handlingarna ska kompletteras med information om åtgärdernas genomförande. Med dokumentering avses här i stor omfattning olika slags inspelningar som kan omvandlas till skriftlig format, såsom Intranät-sidor och arbetsorder i ERP-system.

3.2 Fysisk säkerhet

Fysisk säkerhet (FYY) innehåller kriterier som är förknippade med lokaler och förvaringslösningar och som förhindrar eller begränsar olovlig åtkomst till uppgifter. Dessutom beskriver delområdet kriterier förknippade med behandling, förvaring, överföring, transport och förstöring av uppgifter. Det är möjligt att använda delområdet fysisk säkerhet i bedömning av åtgärder som vidtagits för att fysiskt skydda uppgifterna.

Delområdets innehåll grundar sig på Katakri-kriterierna. Innehållet av särskilt de kriterier som gäller behandling av säkerhetsklassificerade uppgifter har man försökt bevara som enhetliga med Katakri. De tydligaste skillnaderna i förhållande till Katakri är att kriterier som grundar sig på internationella skyldigheter gällande informationssäkerhet har lämnats bort från delområdet och att vissa kriterier klassificerats som möjliga att tillämpa även på andra än säkerhetsklassificerade uppgifter.

Delområdets struktur har planerats så att gemensamma kriterier som gäller säkerhetsområden på olika nivåer, kriterier som gäller endast administrativa områden och kriterier som gäller endast skyddsområden har samlats i var sitt underkapitel. Denna struktur avviker från strukturen i Katakri, där en del av kriterierna har repeterats med samma innehåll i säkerhetsområden på olika nivåer.

Myndigheternas informationsmaterial ska behandlas och förvaras i verksamhetslokaler som är tillräckligt säkra enligt kraven på tillförlitlighet, integritet och tillgänglighet (15 § 2 mom. i informationshanteringslagen). För att fysiskt skydda säkerhetsklassificerade uppgifter föreskriver säkerhetsklassificeringsförordningen om två typer av fysiskt skyddade säkerhetsområden: administrativa områden och skyddsområden. I Julkri används begreppen administrativt område och skyddsområde.

Rekommendationen är att datalager som innehåller sekretessbelagda uppgifter och de informationssystem som används till att behandla uppgifterna placeras i ett skyddat område som myndigheten har fastställt för detta syfte. Ett sådant område kan till exempel utgöras av ett administrativt område som beskrivs i säkerhetsklassificeringsförordningen, denna rekommendation och kriterierna som bifogats till rekommendationen.

Med ett administrativt område avses i praktiken ett sådant område definierat av organisationen som utomstående inte har okontrollerad åtkomst till och för vilken tillräckliga åtgärder vidtagits för att säkerställa säkerheten av de uppgifter som behandlas och förvaras i området. Inga detaljerade krav har ställts på områdets strukturer och andra åtgärder, utan organisationen kan planera dem genom att riskbaserat tillämpa det fysiska (FYY) delområdets kriterier.

Med fysisk säkerhet avses genomförande av fysiska och tekniska skyddsåtgärder så att man förhindrar olovlig åtkomst till uppgifterna genom att:

a) säkerställa att uppgifter behandlas och förvaras ändamålsenligt,
b) möjliggöra åtkomst till uppgifterna utifrån behov och vid behov utifrån säkerhetsutredningar,
c) förebygga, förhindra och upptäcka olovliga åtgärder och
d) förhindra eller fördröja olagligt intrång.

I lokaler där flera organisationer är verksamma ska varje organisation som behandlar uppgifter säkerställa att de gemensamma lokalernas säkerhet är tillräcklig i förhållande till de krav på fysisk säkerhet som riktas mot organisationen.

3.3 Teknisk säkerhet

Det tekniska delområdet omfattar kriterierna som är förknippade med informationssystemens och dataförbindelsernas tekniska egenskaper, säkra användning och verksamhetsmodeller. Kriterierna har som syfte att säkerställa att informationssystemen och deras användning uppfyller de allmänna kraven förknippade med teknisk informationssäkerhet och vid behov även med dataskydd. Det bör dock noteras att genomförandet av det tekniska delområdets kriterier i sig inte garanterar säkerheten av ett enskilt informationssystem, utan kriterierna för de övriga delområdena ska också beaktas.

Objekten som bedöms kan vara antingen enskilda informationssystem eller databehandlingsmiljöer eller flera informationssystem som bildar en större helhet. Vid bedömning av en helhet som består av flera informationssystem bör det beaktas att kraven uppfylls i varje enskilt system.

Det tekniska delområdet tar även i beaktande systemens placering i säkerhetsområdena och deras fjärranvändning utanför dessa områden. Närmare krav som gäller det administrativa området och skyddsområdet har fastställts i delområdet fysisk säkerhet.

I flera av kriterierna hänvisar man till att krypteringslösningen ska vara tillräckligt säker för användningsfallet i fråga. I bedömningen av krypteringslösningens säkerhet kan man utnyttja till exempel godkännanden som Cybersäkerhetscentrets NCSA-verksamhet beviljat för att skydda internationella säkerhetsklassificerade uppgifter. Ytterligare information finns på Cybersäkerhetscentrets webbplats.

3.4 Beredskap och kontinuitetshantering

Delområdet innehåller kriterier som gäller beredskap och kontinuitetshantering i normala förhållanden. Kriterierna grundar sig på hanteringsmetoder som beskriver informationssäkerhetens kontinuitet och som skildras i informationshanteringslagen (bland annat i 4 § 2 mom. 2 punkten, 13 § 1, 2 och 4 mom. och 15 §), anvisningar och informationssäkerhetsåtgärder som utarbetas för allmänna krav och standarden ISO/IEC 27002. Åtgärder som gäller verksamhetens kontinuitet i undantagsförhållanden och som omfattas av beredskapslagen omfattas inte av kriterierna. Kriterierna stöder dock för sin del organisationen även i att uppfylla kraven gällande beredskap för undantagsförhållanden.

Delområdets kriterier gäller huvudsakligen objekt som klassificerats som viktiga eller kritiska med tanke på tillgängligheten. Nivåerna av tillgänglighet beskrivs i kapitel 4.2 Klassificeringsnivåer. Kriterierna kan riskbaserat tillämpas även i objekt som hör till lägre tillgänglighetskategorier. Att reda ut kraven på kontinuitet och lagstiftningen som ligger till grund för dem gäller dock i princip alla organisationer.

Delområdets centrala kriterier utgörs av beredskapsåtgärder förknippade med olika slags allvarliga störningssituationer, planer för verksamhetens kontinuitet och informationssystemens återställning samt övning av dessa planer. Kontinuitetshanteringen är nära förknippad med processer för hantering av störningar och avvikande situationer. Kriterierna associerade med dessa beskrivs i delområdena administrativ säkerhet och teknisk säkerhet.

3.5 Dataskydd

Personuppgifter är uppgifter på grundval av vilka en person direkt eller indirekt kan identifieras till exempel genom att kombinera en enskild uppgift med någon annan uppgift som möjliggör identifiering. En person kan identifieras till exempel utifrån namn, personbeteckning, någon faktor som är kännetecknande för personen i fråga eller individualiserande tekniska uppgifter för de terminaler som personen använder.

Kraven i dataskyddsförordningen ska iakttas i behandlingen av personuppgifter då behandlingen helt eller delvis är automatiskt eller då uppgifterna bildar en del av ett register. Dataskyddsförordningen skyddar personuppgifter oberoende av vilken teknik som används i behandlingen av uppgifterna. Hur uppgifterna förvaras har heller ingen betydelse. Uppgifterna kan förvaras till exempel i informationssystem, kameraövervakningssystem eller pappersarkiv.

Till delområdet dataskydd har samlats kriterier som gäller enbart behandling av personuppgifter. Sådana är till exempel kriterier som gäller behandlingens lagenlighet, dataskyddsprinciperna och den registrerades rättigheter. Dessutom tillämpar man i Julkri på behandlingen av personuppgifter datasäkerhetskriterier som finns inom de andra delområdena. Datasäkerhetskriterierna som tillämpas i behandlingen av personuppgifter är i Julkri till största delen gemensamma med de andra kriterierna som används till att säkra uppgifterna. Varje kriterium som finns inom andra delområden har klassificerats enligt huruvida det tillämpas även inom behandlingen av personuppgifter och huruvida kriteriet i så fall gäller alla personuppgifter eller endast särskilda kategorier av personuppgifter. Kriterier gällande behandlingen av personuppgifter som finns inom andra delområden har i vissa enskilda fall preciserats med ett kriterium inom delområdet dataskydd.

4 Kriteriernas uppgifter

Bedömningskriteriet består av en identifierare, klassificeringar (konfidentialitet, integritet, tillgänglighet, personuppgift), innehåll (namn, krav, allmän beskrivning och exempel på genomförande) och hänvisningar till olika källor.

Tabell 1. Exempel på kriteriet Riskhantering.

Identifierare	HAL-06, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Riskhantering
Krav	Organisationen genomför hantering av informationssäkerhetsrisker och har bedömt de väsentliga riskerna för uppgifterna samt dimensionerat informationssäkerhetsåtgärderna enligt riskbedömningen.
Allmän beskrivning	Hanteringsprocessen gällande informationssäkerhetsrisker består av att definiera verksamhetsmiljön, bedöma riskerna (identifiera dem, analysera dem och bedöma deras betydelse), behandla riskerna, godkänna riskerna, kommunicera och dela och få information om riskerna, följa upp riskerna och granska riskerna. Hantering av informationssäkerhetsrisker är en del av organisationens verksamhet och övriga riskhantering. Med hjälp av hantering av informationssäkerhetsrisker säkerställer man tillräckligheten av informationssäkerhetsåtgärderna för att skydda uppgifternas konfidentialitet, integritet och tillgänglighet. Riskhanteringen påverkar de övriga delområdena inom hantering av informationssäkerhet. Riskhanteringen ska planeras och anvisningar om den ska ges på så sätt att man i riskhanteringen systematiskt och planmässigt behandlar olika slags risker förknippade med informationssäkerhet, såsom risker som beror på felaktigheter i informationsinnehållet, risker förknippade med avbrott i organisationens verksamhet och risker förknippade med personuppgiftsincidenter.
Exempel på genomförande	– Allmänt godkända metoder används i bedömningen och analysen av informationssäkerhetsrisker. – En schemalagd årsplan i vilken ansvar delegerats utarbetas utifrån bedömningen av informationssäkerhetsriskerna. – Tillräckligt många sakkunniga deltar i informationssäkerhetsriskernas hantering. – Risker som orsakas på grund av intressentgrupper och leveranskedjor har beaktats i hanteringen av informationssäkerhetsrisker. – Bedömningen av informationssäkerhetsrisker utnyttjas i andra processer inom hantering av informationssäkerheten.
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 6 §, 7 §
Referenser	Julkri: FYY-01, TEK-01, TEK-14, TEK-16; Katakri: T-03
Övrig tilläggsinformation	SFS-EN ISO/IEC 27001:2017 6.1 och 8–10, SFS-EN ISO/IEC 27005:2018 kapitel 6, SFS ISO 31000:2018, PiTuKri TJ-03; Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 kapitel 5.2; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 6

Ovan beskrivs som exempel det administrativa delområdets kriterium Riskhantering. Kriteriets identifierare är HAL-06. I detta fall är nivån av konfidentialitet (L) offentlig, integritet (E) ringa och tillgänglighet (S) ringa, och kriteriet i fråga kan också utnyttjas i bedömningen av behandlingen av personuppgifter (TS). Kriteriernas identifierare och deras nivåer beskrivs närmare i kapitlen 4.1–4.4.

4.1 Identifierare

Kriteriet har en unik identifierare som består av förkortningen av delområdets finskspråkiga namn, huvudkriteriets löpande nummer och underkriteriets löpande nummer. De unika identifierarnas förkortningar är administrativ (HAL, hallinnollinen), teknisk (TEK, tekninen), beredskap (VAR, varautuminen), fysisk (FYY, fyysinen) och dataskydd (TSU, tietosuoja). Huvudkriterierna har numrerats enligt delområde och underkriterierna enligt huvudkriterium. Till exempel innefattar delområdet för teknisk informationssäkerhet huvudkriteriet TEK-15 och dess underkriterier TEK-15.1 och TEK-15.2.

4.2 Klassificeringsnivåer

Kriterierna har klassificerats med tanke på konfidentialitet, integritet och tillgänglighet. Om kriteriet även gäller behandling av personuppgifter har det dessutom klassificerats ur en dataskyddssynvinkel. Kompletterande informationssäkerhetssynvinklar, såsom informationens obestridlighet eller autenticitet, har beaktats i kriteriernas innehåll.

Kriteriet kan anknyta till ett eller flera informationssäkerhetssynvinklar och väljs med i bedömningen om den är väsentliga ur någon av synvinklarna. Till exempel kan kriteriet vara antecknat på nivån Normal ur integritetens synvinkel, vilket innebär att kriteriet är väsentligt för alla de uppgifter som klassificerats på nivån Normal med tanke på integriteten.

Många av kriterierna är allmänna till sin karaktär och är förknippade i större utsträckning med hantering av informationssäkerheten. Sådana är till exempel kriterier som gäller definiering av uppgifter och ansvar, riskhantering och dokumentering.

4.2.1 Nivåer av konfidentialitet

Konfidentialitet är en egenskap som ger uttryck åt att informationen endast kan användas om man har rätt att använda den och att informationen inte avslöjas för utomstående. I denna rekommendation beskrivs nivåerna av konfidentialitet på skalan offentlig,

sekretessbelagd, säkerhetsklass IV, säkerhetsklass III, säkerhetsklass II och säkerhetsklass I. Dessa nivåer och exempel på dem beskrivs i tabellen nedan. Informationshanteringsnämndens rekommendation (2021:10) innehåller rekommendationer om säkerhetsklassificering, anteckningar i säkerhetsklassificerade handlingar och informationssäkerhetsåtgärder som gäller behandling av handlingar som säkerhetsklassificerats.

Tabell 2. Nivåer av konfidentialitet.

Nivå	Beskrivning	Exempel
Offentlig	Myndighetshandlingar är offentliga om inte något annat föreskrivs särskilt i lag. (1 § i lagen om offentlighet i myndigheternas verksamhet)	Kommunfullmäktiges protokoll till sina offentliga delar, organisationens offentliga internet-sidor.
Sekretessbelagd	En myndighetshandling ska sekretessbeläggas, om det i lagen föreskrivs eller en myndighet med stöd av lag har föreskrivit att den ska vara sekretessbelagd eller om handlingen innehåller uppgifter för vilka tystnadsplikt föreskrivs genom lag (22 § i offentlighetslagen).	Journalhandlingar, uppgifter om klienter inom socialvården, psykologiska tester och lämplighetsprov.
Säkerhetsklass IV (TL IV)	Obehörigt avslöjande eller obehörig användning av handlingens sekretessbelagda uppgifter kan orsaka **lindrig** skada för det intresse som skyddas enligt 18 § 1 mom. i informationshanteringslagen.	Dokumentation gällande säkerhetsarrangemang för informationssystem som är väsentliga för de intressen som ska skyddas som anges i 18 § i informationshanteringslagen, då dokumentationens avslöjande inte avbryter verksamheten men kan förutsätta ändringar i de avslöjade planerna.
Säkerhetsklass III (TL III)	Obehörigt avslöjande eller obehörig användning av handlingens sekretessbelagda uppgifter kan orsaka **skada** för det intresse som skyddas enligt 18 § 1 mom. i informationshanteringslagen.	Dokumentation gällande säkerhetsarrangemang för funktioner som är livsviktiga för de intressen som ska skyddas som anges i 18 § i informationshanteringslagen, då dokumentationens avslöjande leder till att verksamheten måste avbrytas.

Nivå	Beskrivning	Exempel
Säkerhetsklass II (TL II)	Obehörigt avslöjande eller obehörig användning av handlingens sekretessbelagda uppgifter kan orsaka **betydande skada** för det intresse som skyddas enligt 18 § 1 mom. i informationshanteringslagen.	Dokumentation gällande säkerhetsarrangemang för funktioner som är livsviktiga för de intressen som ska skyddas som anges i 18 § i informationshanteringslagen, då dokumentationens avslöjande leder till att säkerheten av en stor grupp människor inte kan garanteras och verksamheten måste avbrytas för en relativt lång tid.
Säkerhetsklass I (TL I)	Obehörigt avslöjande eller obehörig användning av handlingens sekretessbelagda uppgifter kan orsaka **särskilt stor skada** för det intresse som skyddas enligt 18 § 1 mom. i informationshanteringslagen.	Avslöjande av kritisk infrastruktur, information som gäller säkerhetsarrangemang för livsviktig verksamhet eller andra funktioner som är centrala för både samhällets verksamhetsförmåga och de intressen som ska skyddas som anges i 18 § i informationshanteringslagen, då avslöjandet leder till att verksamheten av en myndighet eller annan aktör inom kritisk infrastruktur sannolikt förhindras och skadan är storskalig.

Kriterierna har inte med tanke på konfidentialiteten klassificerats separat på nivån Ges enligt prövning. Organisationen ska utgående från riskerna överväga om kriterier gällande sekretessbelagda uppgifter ska inkluderas i bedömningen av uppgifter som ges utifrån behovsprövning. Detta lyckas genom att man i bedömningens förhandsvillkor definierar nivån av konfidentialitet som Offentlig, då Julkri-verktyget erbjuder kriterierna gällande sekretessbelagda uppgifter som valfria.

4.2.2 Nivåer av tillgänglighet

Med tillgänglighet avses hur information, ett informationssystem eller en tjänst kan utnyttjas vid önskad tidpunkt och på det sätt som krävs. I Julkri är nivåerna av tillgänglighet ringa, normal, viktig och kritisk. Tabellen innehåller beskrivningar av och exempel på de olika nivåerna av tillgänglighet.

Tabell 3. Nivåer av tillgänglighet.

Nivå	Beskrivning	Exempel
Ringa	Vad gäller informationens tillgänglighet kan man godkänna störningar som pågår i flera veckor.	Register för personalens parkeringsplatser, felregister för parkbänkar
Normal	Vad gäller informationens tillgänglighet kan man godkänna störningar som pågår i högst några dagar.	Arkivsystem
Viktig	Vad gäller informationens tillgänglighet kan man godkänna störningar som pågår i högst några timmar.	Patientdatasystem
Kritisk	Vad gäller informationens tillgänglighet kan man godkänna störningar som pågår i högst några minuter.	Centraliserade tjänster för identifiering av användare

4.2.3 Nivåer av integritet

Integritet är en egenskap hos information som innebär att informationen inte har ändrats utan lov eller att det inte ändrats av misstag och att eventuella ändringar kan verifieras. I tabellen nedan beskrivs de nivåer av integritet som används i Julkri. Dessa är ringa, normal, viktig och kritisk. Dessutom innehåller tabellen några exempel på varje nivå.

Tabell 4. Nivåer av integritet.

Nivå	Beskrivning	Exempel
Ringa	Att information försvinner eller ändras orsakar ingen väsentlig olägenhet.	Kontorsprogram, systemens felloggar.
Normal	Att information försvinner eller ändras orsakar rimlig olägenhet, men detta kan upptäckas och återhämtning är möjlig.	Personaladministrationens system.
Viktig	Att information försvinner eller ändras orsakar betydande olägenhet eller skada till anseendet och det kan vara svårt att upptäcka.	Integrationsplattformar som förmedlar laboratorieresultat där det kan vara svårt att upptäcka fel i enskilda mätningar. Logginformation som anknyter till behandlingen av personuppgifter.
Kritisk	Att information försvinner eller ändras är oacceptabelt i alla situationer.	Betalningssystem som är centrala för samhällets funktionalitet eller spårtrafikens styrsystem.

4.3 Innehåll

Kriteriernas innehåll består av namn, krav, en allmän beskrivning och ett exempel på genomförande.

- **Namnet** beskriver på rubriknivå vilket ärende kriteriet är kopplat till. Namnet utgörs av ett eller några ord som beskriver kriteriets ämnesområde. Underkriteriets namn består av namnet på huvudkriteriet och en identifierare som separerats med ett bindestreck. Ett exempel på detta är Användarrättigheter – aktualitet, som är ett underkriterium som gäller aktualitet och som preciserar huvudkriteriet användarrättigheter.
- **Kravet** beskriver målet som organisationen ska uppfylla. Kravet är en kort mening eller ett kort stycke. Kraven kan uppfyllas på många olika sätt. Kraven är unika, vilket innebär att ett krav inte består av flera olika krav. Om underkriteriet inte innehåller ett separat krav, preciserar det huvudkriteriet vad gäller antingen den allmänna beskrivningen eller exemplet på genomförande.
- **Den allmänna beskrivningen** innehåller ytterligare information som ger bakgrundsfakta till och motiverar kriteriet. Den är inte ett krav utan en grund för kriteriet. I den allmänna beskrivningen kan man till exempel beskriva hot som bekämpas med hjälp av de kriterieenliga hanteringsåtgärderna. Om flera

underkriterier är förknippade med en och samma helhet ska man utarbeta endast en gemensam allmän beskrivning av de olika kriterierna i samband med huvudkriteriet.
- **Exemplet på genomförande** beskriver hur organisationen kan uppfylla kravet. Exemplet är inte ett krav men kan agera som en riktgivande anvisning om nivån hur kravet kan uppfyllas.

4.4 Hänvisningar

Kriterierna kan innehålla hänvisningar till lagstiftning, anvisningar och standarder samt till Katakri- och PiTuKri-kriterierna och de övriga kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen. Strävan har varit att hänvisningarna specificeras så att motsvarande punkt är lätt att hitta i referensmaterialet.

- **Lagstiftningen** beskriver vilken lagstiftning kriteriet grundar sig på.
- **Övrig tilläggsinformation** innehåller hänvisningar till informationshanteringsnämndens rekommendationer, PiTuKri-bedömningskriterier och standarder som är förknippade med kriteriet.
- **Julkri-hänvisningen** innehåller en referens till ett eller flera andra Julkri-kriterier om kriteriet bildar en tillämplig helhet tillsammans med ett annat kriterium.
- **Katakri-hänvisningen** innehåller en referens till det motsvarande kriteriet i Katakri-bedömningskriterierna, om ett sådant kriterium existerar.

5 Användning av kriterierna

Kriterierna kan tillämpas på hela organisationens verksamhet, verksamheten av ett visst delområde eller bedömningen av en tjänst som upphandlas. Rekommendationen är att behandlingsmiljöer avsedda för informationens olika nivåer bedöms separat så att alltför stränga kriterier inte tillämpas på objekt på en lägre nivå vilket också skulle onödigt öka krångligheten och kostnaderna.

En precis definition och begränsning av objektet som ska bedömas är en av de viktigaste faserna i användningen av kriterierna. Bedömningen kan riktas på ett enskilt system, men dessutom bör man säkerställa att olika bedömningar tillsammans täcker hela organisationens verksamhet.

I organisationen behandlas uppgifter som med tanke på sin kritiskhet och konfidentialitet hör till många olika klasser, och många olika informationssystem och tjänster används i behandlingen. Dessutom utnyttjar man ofta gemensamma plattformtjänster i samband med olika informationssystem. På grund av dessa faktorer lönar det sig för organisationen att planera objekten som ska bedömas som logiska helheter och utnyttja bedömningar som genomförts tidigare.

Om man till exempel skaffar ett nytt informationssystem som ska användas på en gemensam plattform vars säkerhet redan har bedömts i ett tidigare skede, behöver bedömningen av informationssystemet inte inkludera de tidigare bedömda kriterierna som den gemensamma plattformen ansvarar för.

Med hjälp av användningsfall kan organisationen i förväg fastställa kriterier som är lämpliga för olika situationer och på så sätt underlätta användningen av kriterierna i liknande återkommande situationer. Utnyttjandet av användningsfall beskrivs närmare i den separata bilagan 3 Bruksanvisning för verktyget.

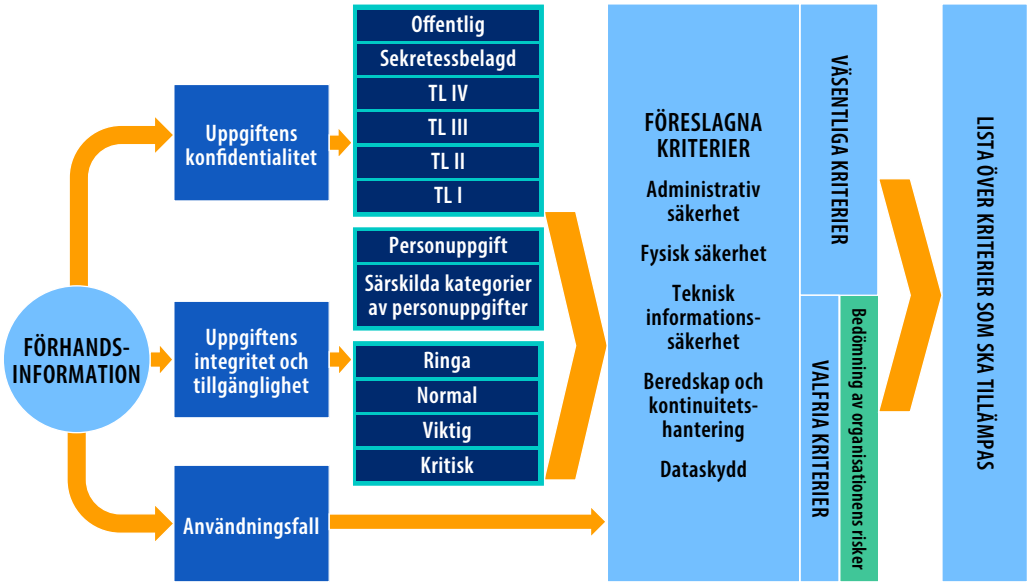
Innan kriterierna används ska organisationen definiera följande om föremålet för bedömningen:

- den konfidentialitet, integritet och tillgänglighet som förutsätts av objektet,
- huruvida objektet innefattar personuppgifter och huruvida dessa uppgifter hör till särskilda kategorier av personuppgifter,

- delområden som eventuellt inte ska beaktas i bedömningen,
- användningsfallet, om ett användningsfall som lämpar sig för bedömningen existerar.

Utifrån klassificeringen av objektet som ska bedömas är kriterierna väsentliga eller valfria, eller så lämnas de utanför bedömningen. Rekommendationen är att organisationen inkluderar de väsentliga kriterierna i bedömningen. Vad gäller de valfria kriterierna beslutar organisationen utgående från riskbedömningen och fallspecifik bedömning huruvida något av kriterierna används i bedömningen. Figur 1 visar processen för användningen av kriterierna.

Figur 1. Visualisering av användning av kriterierna.



Då Julkri-kriterierna utnyttjas i bedömningen av organisationens informationssäkerhet är utgångspunkten att kraven förknippade med de kriterier som ingår i bedömningen ska uppfyllas. Organisationen kan dock låta bli att uppfylla något av dessa krav om organisationen kan visa att det inte finns någon risk eller att risken acceptabel även om kriteriets krav inte uppfylls. Till exempel har riskerna kanske minskats tillräckligt med andra metoder med hjälp av kompenserande kontroller. Krav direkt förknippade med lagstiftningen ska dock uppfyllas på det sätt som lagstiftningen förutsätter.

Om organisationen behöver ett intyg om överensstämmelse med kraven som grundar sig på Julkri-kriterierna, ska varje kriterium som ingår i bedömningen uppfyllas i objektet som

bedöms. Om det dock inte är möjligt att uppfylla ett kriterium ska man specificera och motivera kompenserande förfaranden som säkerställer att risken är acceptabel även om kriteriet inte uppfylls.

Kriterierna kan användas som hjälp vid bedömning av hur kraven på informationssäkerhet i informationshanteringslagen, säkerhetsklassificeringsförordningen och delvis även i dataskyddsförordningen uppfylls. Kriterierna är en rekommendation och lagstiftningens krav kan också uppfyllas på annat sätt än det som beskrivs i kriterierna.

5.1 Åtgärder före bedömning

Innan bedömningen inleds lönar det sig att säkerställa upphandlingarnas säkerhet samt reda ut lagstiftningsrelaterade risker och avtalsvillkorens lämplighet för användningsändamålet. Detta gäller i första hand bedömningar av informationssystem eller tjänster. Här kan man utnyttja kriterierna HAL-06 och HAL-06.1 som gäller riskhantering och kriterierna HAL-16 och HAL-16.1 som är förknippade med upphandlingarnas säkerhet, båda delar av delområdet administrativ säkerhet. De nämnda åtgärderna beskrivs kort i följande stycken.

Ordnande av informationssäker databehandling

Organisationen ska säkerställa i sina upphandlingar att man har vidtagit ändamålsenliga informationssäkerhetsåtgärder vad gäller informationssystemen och tjänsterna som används. Organisationen ska på förhand försäkra sig om att uppgifternas sekretess och skydd genomförs ändamålsenligt.

Lagstiftningsrelaterade risker

Organisationen ska identifiera lagstiftningsrelaterade risker. Dessa hänvisar till möjligheterna inom olika länders lagstiftning att förplikta tjänsteleverantören att samarbeta med myndigheterna i landet i fråga och erbjuda till exempel direkt eller indirekt åtkomst till kundernas sekretessbelagda uppgifter i tjänsten eller systemet.

System- och tjänsteavtal

Vad gäller avtalsvillkoren för tjänstens eller systemets tjänsteleverantör ska man säkerställa att de inte begränsar lämpligheten av tjänsten eller systemet i fråga för användningsfallet under hela deras livscykel.

KÄLLOR

Författningar

Värnpliktslagen (1438/2007). https://www.finlex.fi/sv/laki/ajantasa/2007/20071438. Hämtad den 26 april 2022.
Europaparlamentets och rådets förordning (EU) 2016/679 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). https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=-CELEX:32016R0679&from=FI. Hämtad den 26 april 2022.
Lagen om tillhandahållande av digitala tjänster (306/2019). https://www.finlex.fi/sv/laki/ajantasa/2019/20190306. Hämtad den 26 april 2022.
Lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018). https://www.finlex.fi/sv/laki/ajantasa/2018/20181054. Hämtad den 26 april 2022.
Lagen om informationshantering inom den offentliga förvaltningen (906/2019). https://finlex.fi/sv/laki/ajantasa/2019/20190906. Hämtad den 26 april 2022.
Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004). https://www.finlex.fi/sv/laki/ajantasa/2004/20040588. Hämtad den 26 april 2022.
Lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011). https://www.finlex.fi/sv/laki/ajantasa/2011/20111406. Hämtad den 26 april 2022.
Lagen om offentlighet i myndigheternas verksamhet (621/1999). https://www.finlex.fi/sv/laki/ajantasa/1999/19990621. Hämtad den 26 april 2022.
Dataskyddslagen (1050/2018). https://www.finlex.fi/sv/laki/ajantasa/2018/20181050. Hämtad den 26 april 2022.
Säkerhetsutredningslagen (726/2014). https://www.finlex.fi/sv/laki/ajantasa/2014/20140726. Hämtad den 26 april 2022.
Arbetstidslagen (872/2019). https://www.finlex.fi/sv/laki/ajantasa/2019/20190872. Hämtad den 26 april 2022.
Lagen om statens tjänstekollektivavtal (664/1970). https://www.finlex.fi/sv/laki/ajantasa/1970/19700664. Hämtad den 26 april 2022.
Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019). https://www.finlex.fi/sv/laki/ajantasa/2019/20191101. Hämtad den 26 april 2022.
Beredskapslagen (1552/2011). https://www.finlex.fi/sv/laki/ajantasa/2011/20111552. Hämtad den 26 april 2022.

Informationshanteringsnämndens rekommendationer

Informationshanteringsnämndens rekommendation – Finansministeriet 2021:65. Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet. http://urn.fi/URN:ISBN:978-952-367-890-3.
Informationshanteringsnämndens rekommendation – Finansministeriet 2021:10. Rekommendation om behandling av säkerhetsklassificerade handlingar. http://urn.fi/URN:ISBN:978-952-367-520-9.
Informationshanteringsnämndens rekommendation – Finansministeriet 2022:6. Hantering av säkerhetsklassificerade handlingar i molntjänster. http://urn.fi/URN:ISBN:978-952-367-918-4.

Anvisningar och övrigt material

BSI IT-Grundschutz-Compendium 2021. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf. Hämtad den 26 april 2022.
CIS Critical Security Controls. https://www.cisecurity.org/controls. Hämtad den 26 april 2022.
Hansel. 2017. Hur ska dataskyddsförordningen beaktas vid konkurrensutsättning av offentlig upphandling? Version 1. dataskyddsforordning.pdf (hansel.fi). Hämtad den 28 april 2022.
Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246. Hämtad den 26 april 2022.
NIST SP 800-serien. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information. Hämtad den 26 april 2022.
NIST. Särskilt 800–53 (metoder för hantering av informationssäkerheten och dataskyddet), 800–37 (riskhantering), 800–63B (användaridentifiering och hantering av livscykeln). https://csrc.nist.gov/publications/sp800. Hämtad den 26 april 2022.

PiTuKri 2020 Säkerhetskriterier för molntjänster. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_PiTuKri_2020_SE_210506_WEB.pdf. Hämtad den 26 april 2022.
Skyddspolisen. Skyddspolisens anvisning: Säkerhetsutredning av företag. https://supo.fi/sv/sakerhetsutredningar-av-foretag. Hämtad den 26 april 2022.
Dataombudsmannens byrå. Visa att du iakttar dataskyddsbestämmelserna. https://tietosuoja.fi/sv/ansvarsskyldighet. Hämtad den 26 april 2022.
Säkerhetskommittén (2017). Säkerhetsstrategin för samhället. https://turvallisuuskomitea.fi/sv/sakerhetsstrategi-for-samhallet/. Hämtad den 26 april 2022.
Traficom 2021. Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit. Tilaajaorganisaation näkökulma. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf. Hämtad den 26 april 2022.
Traficom 2021. Krypteringslösningar som godkänns av Transport- och kommunikationsverket Traficoms NCSA-verksamhet. https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa/krypteringslosningar-som-godkanns-av-transport-och-kommunikationsverket. Hämtad den 26 april 2022.
Utrikesministeriet. Nationella säkerhetsmyndigheten. https://um.fi/nationella-sakerhetsmyndigheten. Hämtad den 26 april 2022.
Finansministeriet (2020:73). Pilvipalvelujen soveltamisohje – Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille. http://urn.fi/URN:ISBN:978-952-367-503-2. Hämtad den 26 april 2022.

Allmänna kontrollistor och anvisningar om skärpning

CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/. Hämtad den 26 april 2022.
DISA Security Technical Implementation Guides (STIGs). https://public.cyber.mil/stigs/. Hämtad den 26 april 2022.
NIST - National Checklist Program Repository. https://ncp.nist.gov/repository. Hämtad den 26 april 2022.

Bilagor

Bilaga 1A: Julkri-kriterierna

1 Kriteriernas struktur och delområden

Kriterierna har grupperats i fem **delområden**. Varje delområde har ett preciserande namn, och den första delen av identifieraren för kriterierna som hör till delområdet baserar sig på delområdets finska namn. Kriteriernas delområden och deras förkortningar är följande:

- administrativ säkerhet (HAL),
- fysisk säkerhet (FYY),
- teknisk säkerhet (TEK),
- beredskap och kontinuitetshantering (VAR) och
- dataskydd (TSU).

Delområdena består av **huvudkriterier** och **underkriterier** som kompletterar huvudkriterierna. Det finns sammanlagt över tvåhundra kriterier. Strukturen huvudkriterium – underkriterium har utnyttjats till exempel i sådana fall där kraven som är förknippade med samma tema är strängare på högre säkerhetsnivåer. Till exempel kan ett huvudkriterium som gäller sekretessbelagda uppgifter kompletteras med ett underkriterium som preciserar genomförandesättet av ett krav som gäller uppgifter som hör till klass TL IV.

Varje kriterium har klassificerats på olika nivåer med tanke på konfidentialitet, integritet, tillgänglighet och dataskydd. Beroende på kriteriet kan det vara förknippat med ett eller flera av dessa synvinklar. Till exempel kan samma kriterium som gäller åtkomsträttigheter vara förknippat med både konfidentialitet, integritet och dataskydd.

Allmänna beskrivningar av kriteriernas olika delområden och de kriterier som är inkluderade i delområdet i fråga finns i de följande kapitlen. Den allmänna beskrivningen av delområdet dataskydd och dess kriterier finns i bilaga 1B Dataskyddskriterier.

2 Administrativ säkerhet

Delområdet administrativ säkerhet behandlar de metoder som används för att implementera hantering av informationssäkerheten som en del av hela organisationens verksamhet. Delområdet täcker allmänna kriterier för administrativ säkerhet, personalsäkerhet, informationssystem och deras upphandling samt användningssäkerhet. Med den administrativa säkerhetens kriterier strävar man efter att organisationen har ett hanteringssystem för informationssäkerhet som fungerar tillräckligt bra och förfaranden för att säkerställa att personalen som behandlar uppgifterna agerar på korrekt sätt. Organisationen ska också säkerställa att förpliktelser gällande behandling av uppgifter iakttas i situationer där uppgifter behandlas på uppdrag av organisationen.

Många kriterier inom delområdet administrativ säkerhet fungerar som grund för de övriga delområdenas kriterier. Till exempel är kriterierna förknippade med identifiering av skyddade objekt, riskhantering och dokumentering allmänna och ska som standard utnyttjas i samband med tillämpningen av de övriga delområdenas kriterier.

Processer förknippade med administrativ säkerhet ska behandlas som helheter. Informationssäkerhetens hanteringsmetoder ska utifrån riskbedömningen relateras till uppgifterna som ska skyddas och till organisationens verksamhet.

Användningen av kriterierna förutsätter ändamålsenlig inriktning. Om vissa funktioner har bedömts redan tidigare kan de tidigare resultaten utnyttjas i tillämpliga delar. Till exempel om organisationens telekommunikationsmiljö har bedömts under det senaste året och inga betydande ändringar har gjorts i den, kan bedömningen i fråga eventuellt utnyttjas i bedömningen av ett nytt informationssystem som installeras i telekommunikationsmiljön.

Om man i organisationen behandlar uppgifter som klassificerats på olika nivåer i separata miljöer och processer, kan det vara ändamålsenligt att dela in bedömningen i separata logiska helheter. Till exempel vad gäller personalen som använder en behandlingsmiljö för uppgifter som säkerhetsklassificerats på en högre nivå skiljer sig innehållet i anvisningarna vanligen i betydande grad från de allmänna anvisningarna som gäller hela organisationen.

God riskhantering omfattar dokumentering av förfaringssätt och särskilt riskbedömningen. Planer och anvisningar förknippade med hantering av informationssäkerheten samt bedömningsresultaten och slutsatserna bör presenteras skriftligen. Handlingarna ska kompletteras med information om åtgärdernas genomförande. Med dokumentering avses här i stor omfattning olika slags inspelningar som kan omvandlas till skriftlig format, såsom Intranät-sidor och arbetsorder i ERP-system.

Identifierare	**HAL-01, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Principer
Krav	Organisationen har informationssäkerhetsprinciper som den högsta ledningen godkänt och som beskriver hur organisationens informationssäkerhetsåtgärder hänger samman med organisationens verksamhet. Principerna är täckande och ändamålsenliga med tanke på skydd av uppgifterna.
Allmän beskrivning	Med informationssäkerhetsprinciperna som den högsta ledningen godkänt visar man att ledningen har förbundit sig till organisationens informationssäkerhetsprinciper och att principerna representerar ledningens vilja och stöder organisationens verksamhet. Principerna kan beskrivas på många olika sätt, till exempel som ett enskilt dokument eller som en del av de allmänna verksamhetsprinciperna, politiken eller strategin.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 13 §
Referenser	Katakri: T-01
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01

Identifierare	**HAL-02, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Uppgifter och ansvar
Krav	Organisationen har definierat och dokumenterat uppgifterna och ansvaren som relaterar till att sköta om informationssäkerheten, inklusive de ansvar som hör till tjänsteproducenten.
Allmän beskrivning	Med definition av uppgifterna och ansvaren förknippade med informationssäkerhetsarbetet strävar man efter att säkerställa att aktörer har utsetts för de mest centrala delområdena och att aktörerna är medvetna om sina ansvar och befogenheter. Organisationens ledning har som uppgift att definiera de ansvar som gäller informationshantering. Det är inte fråga om att delegera informationshanteringsansvar utan att definiera dem. Ansvaren bör fastställas särskilt för upprätthållande av säkerhetsanvisningar, riskhantering, beredskap och de personer som bär det övergripande ansvaret för säkerheten. Informationssäkerhetens ansvarsområden definieras vanligen som en del av säkerhetens helhetsansvar. I fastställandet av ansvaren ska man även beakta de uppgifter för vilka leverantören bär ansvaret. Då molntjänster används bör man beakta olika slags servicemodeller och därtill relaterade skillnader i ansvarsfördelningen mellan kunden och tjänsteproducenten.

Exempel på genomförande	Organisationen har fastställt uppgifterna för att genomföra säkerheten och därtill relaterade ansvar till följande delar: a) säkerhetsledning b) fysisk säkerhet c) teknisk säkerhet d) beredskap och kontinuitetshantering e) dataskydd f) riskhantering g) säkerhetens övergripande ansvar
Lagstiftning	Informationshanteringslagen 4 § 2 mom.
Referenser	Katakri: T-02
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.2; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3; PiTuKri TJ-02; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, kapitel 3
Identifierare	**HAL-02.1, L:Sekretessbelagd, E:Viktig, S:Viktig, TS:Särskild kategori av personuppgifter**
Namn	Uppgifter och ansvar – uppgifternas differentiering
Krav	Organisationen ska säkerställa att personer inte har arbetskombinationer som är farliga med tanke på informationssäkerheten.
Allmän beskrivning	Organisationens uppgifter och ansvarsområden ska vara separerade för att minska risken för olovliga eller oavsiktliga ändringar eller olovligt eller oavsiktligt missbruk vad gäller egendomen som organisationen ska skydda. Sådana farliga kombinationer är till exempel att en person kan ändra både uppgifterna i ett informationssystem och loggdata som används i informationssystemets uppföljning. Farliga arbetskombinationer ska beaktas även i utkontrakterad verksamhet.
Exempel på genomförande	– Organisationen har definierat de farliga arbetskombinationerna – Farliga arbetskombinationer kontrolleras som en del av definitionen av uppgifterna – Farliga arbetskombinationer kontrolleras som en del av hanteringen av användarrättigheter särskilt vad gäller administratörs- och tillsynsroller
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 13 §
Referenser	Katakri: I-06
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.3
Identifierare	**HAL-03, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Resurser
Krav	Organisationen har tillgång till tillräckliga resurser och expertis för att säkerställa informationssäkerheten.
Allmän beskrivning	Med resursfördelning och expertis säkerställer man att informationssäkerhetsarbetet kan genomföras i enlighet med de fastställda principerna. Med informationssäkerhetsarbetets resurser avses både personalresurser och ekonomiska satsningar såsom investeringar i informationssystem. Som allmänna krav kan räknas att organisationen ska ha personer som sköter uppgifter som hanteringen av informationssäkerheten förutsätter och att personerna har kompetens och tid att utföra de krävda uppgifterna. Dessutom ska organisationen ha förmåga och vilja att göra sådana informationssäkerhetsrelaterade investeringar som utgående från informationssäkerhetskraven och riskbedömningen identifierats som nödvändiga.

Exempel på genomförande	– De som sköter informationssäkerhetsuppgifter har tillräcklig sakkunskap och bevis på denna kunskap. – Informationssäkerhetsarbetets resurser, uppgifter, ansvar och befogenheter har definierats på ett tillräckligt täckande sätt med tanke på organisationens verksamhet, storlek och risker. – Resurserna räcker till att skapa, genomföra, underhålla och kontinuerligt förbättra ett system för hantering av informationssäkerheten. – Resursernas tillräcklighet bedöms regelbundet. – Organisationen fattar nödvändiga beslut om utrustningsrelaterade och andra investeringar som informationssäkerheten förutsätter.
Lagstiftning	Informationshanteringslagen 4 § 2 mom.
Referenser	Katakri: T-05
Övrig tilläggsinformation	SFS-EN ISO/IEC 27001:2017 7.1, 7.2, 5.1
Identifierare	**HAL-04, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Objekt som ska skyddas
Krav	Organisationen identifierar objekt som ska skyddas och upprätthåller aktuell dokumentation om dem.
Allmän beskrivning	Inventering av objekt som ska skyddas är ett av de grundläggande kraven inom hantering av informationssäkerheten. Sådana här objekt är uppgifter, informationssystem, databehandlingsprocesser, lokaler och andra objekt som eventuellt påverkar organisationens informationssäkerhet. I moderna databehandlingsmiljöer kan objekt som ska skyddas också utgöras av andra än traditionella informationstekniska objekt, såsom olika slags sensor- och analysutrustning samt IoT- och automationsmiljöer. Inventering av objekt som ska skyddas är en ovillkorlig förutsättning för att genomföra planmässig och effektiv hantering av informationssäkerheten. Den uppdaterade förteckningen över egendom som ska skyddas utnyttjas som utgångsinformation inom många av delområdena inom hantering av informationssäkerheten.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 5 § 2 mom., 13 §
Referenser	
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.9; Rekommendation för en informationshanteringsmodell 2020:41
Identifierare	**HAL-04.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Objekt som ska skyddas – ansvar
Krav	Organisationen fastställer ansvaren hos objekten som ska skyddas.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 4 § 2 mom.
Referenser	
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.9; Rekommendation för en informationshanteringsmodell FM 2020:41

Identifierare	HAL-04.2, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Objekt som ska skyddas – klassificering
Krav	Organisationen ska klassificera informationen och därtill relaterade system och behandlingsprocesser utifrån kraven som riktas på dem.
Allmän beskrivning	Organisationen ska från lagstiftningen identifiera de offentliga, sekretessbelagda och säkerhetsklassificerade uppgifter och personuppgifter som organisationen behandlar samt uppgifternas skyddsbehov. Med klassificering avses behovet att skydda uppgifterna på olika nivåer som beror på olika slags behandlingskrav. Genom att klassificera databehandlingsmiljöerna enligt informationsmaterial kan man lättare visa och motivera informationssäkerhetsåtgärderna relaterade till varje enskild databehandlingsmiljö. Klassificeringen bör inkluderas i organisationens processer och vara konsekvent och enhetlig i hela organisationen. Klassificeringen fungerar som utgångsinformation för flera andra processer inom informationssäkerheten. Till exempel är systemens tillgänglighetskrav förknippade med planeringen av systemens feltolerans och beredskap och konfidentialitetskraven med definitionen av systemens informationssäkerhetskrav. Klassificeringen av ett informationssystem eller ett annat objekt som innehåller flera informationsmaterial fastställs i första hand enligt materialet med den högsta klassificeringen. Vid bedömning av informationssystemens klassificering bör man även beakta masseffekten på ett riskbaserat sätt. Informationssystem som består av en stor mängd information från en viss nivå av konfidentialitet kan sakhelheten stiga till en nivå som är högre än de enskilda uppgifterna. Mängden är dock inte den enda faktorn, utan ibland kan till exempel kombinationen av två olika informationskällor leda till att datalagrets klassificering höjs. Typiskt handlar anhopningen om information i klass IV (till exempel kan en stor mängd uppgifter i säkerhetsklass IV bilda ett datalager i säkerhetsklass III då uppgifterna kombineras).
Exempel på genomförande	– Organisationen definierar de nivåer som används i klassificeringen av uppgifterna och till dem relaterade informationssystem och behandlingsprocesser ur konfidentialitets-, tillgänglighets- och integritetssynvinkeln. Vid behov kan klassificeringen utvidgas så att den täcker även andra synvinklar, såsom huruvida informationen innehåller personuppgifter. – Organisationen definierar kriterierna enligt vilka uppgifterna och de övriga objekten klassificeras. – Klasserna och deras kriterier grundar sig på lagstadgade krav, men organisationerna ska precisera kriterierna så att de är ändamålsenliga för personerna som arbetar i organisationen. – Klassificeringen kan genomföras i samband med inventeringen av objekten som ska skyddas och inkluderas i förteckningen över dessa objekt – till exempel i en informationshanteringsmodell.
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 5 §, 13 §, 18 §; säkerhetsklassificeringsförordningen 3 §, 4 §; offentlighetslagen 24 §
Referenser	Katakri: T-08
Övrig tilläggsinformation	Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65, kapitel 4.1; Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10, kapitel 2, kapitel 5.3; ISO/IEC 27002:2022 5.9

Identifierare	HAL-04.3, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Objekt som ska skyddas – masseffekten
Krav	Masseffekten har beaktats i klassificeringen av objekt som ska skyddas.
Allmän beskrivning	Klassificeringen av ett informationssystem eller ett annat objekt som innehåller flera informationsmaterial fastställs i första hand enligt materialet med den högsta klassificeringen. Vid bedömning av informationssystemens klassificering bör man även beakta masseffekten på ett riskbaserat sätt. Informationssystem som består av en stor mängd information från en viss nivå av konfidentialitet kan sakhelheten stiga till en nivå som är högre än de enskilda uppgifterna. Mängden är dock inte den enda faktorn, utan ibland kan till exempel kombinationen av två olika informationskällor leda till att datalagrets klassificering höjs. Typiskt handlar anhopningen om information i klass IV (till exempel kan en stor mängd uppgifter i säkerhetsklass IV bilda ett datalager i säkerhetsklass III då uppgifterna kombineras), men masseffekten ska också beaktas i skyddet av sekretessbelagd information som inte säkerhetsklassificerats.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 5 § 2 mom., 13 § 1 mom.
Referenser	Julkri: HAL-06, TEK-06; Katakri: T-08
Övrig tilläggsinformation	
Identifierare	**HAL-04.4, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter**
Namn	Objekt som ska skyddas – anteckning
Krav	Organisationen ska anteckna uppgifterna i enlighet med lagstadgade krav och de klassificeringsprinciper som organisationen fastställt.
Allmän beskrivning	Sätten att anteckna information ska täcka både fysiska och elektroniska uppgifter och den egendom som ska skyddas och som är relaterad till uppgifterna, såsom datamedier. Anteckningarna bör följa de klassificeringsprinciper som organisationen fastställt och vara lätta att känna igen. Organisationen ska ge anvisningar om vart och hur anteckningarna ska fästas. I anvisningarna bör man beakta även utskrifter. För att minska mängden onödigt arbete lönar det sig dessutom att ge anvisningar om när anteckningar inte behövs. I vissa fall, såsom i anteckningar enligt offentlighetslagen som gäller sekretess, ska det också framgå till vilka delar handlingen är sekretessbelagd och vad sekretessen grundar sig på.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 18 §; säkerhetsklassificeringsförordningen 3 §, 4 §; offentlighetslagen 25 §
Referenser	Katakri: T-08
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10, kapitel 3; ISO/IEC 27002:2022 5.13
Identifierare	**HAL-04.5, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Objekt som ska skyddas – beroendeförhållanden
Krav	Organisationen har identifierat och dokumenterat beroendeförhållandena mellan objekten som ska skyddas.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 5 §
Referenser	
Övrig tilläggsinformation	

Identifierare	HAL-04.6, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Objekt som ska skyddas – intressentgrupper
Krav	Organisationen har identifierat och dokumenterat intressentgrupperna som är förknippade med objekten som ska skyddas.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 5 §
Referenser	
Övrig tilläggsinformation	

Identifierare	HAL-05, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Kraven
Krav	Organisationen identifierar informationssäkerhetskraven som beror på lagstiftningen, intressentgrupper och organisationens verksamhet.
Allmän beskrivning	Organisationen ska identifiera och specificera krav som gäller informationssäkerhet som har grund i lagstiftningen, avtal som ingåtts med olika intressentgrupper och organisationens verksamhet. Dessutom ska organisationen identifiera och beakta krav förknippade med branschspecifik lagstiftning, internationell lagstiftning och EU-reglering. De minimikrav på informationssäkerhet som grundar sig på informationshanteringslagen och som den offentliga förvaltningen ska iaktta samt rekommendationerna för uppfyllande av dessa krav definieras i kapitel 2 i informationshanteringsnämndens rekommendation 2021:65. Organisationens informationssäkerhetskrav bildas av ovan nämnda minimikrav och andra identifierade krav. Förfarandet för uppfyllandet av varje enskilt krav bedöms med hjälp av en riskbedömningsprocess.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 §
Referenser	
Övrig tilläggsinformation	SFS-EN ISO/IEC 27001:2017 4.2; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitlen 2 och 4

Identifierare	HAL-05.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Kraven – uppföljning
Krav	Organisationen följer upp ändringar i de ställda informationssäkerhetskraven och i verksamhetsmiljön samt vidtar nödvändiga åtgärder för att reagera på ändringar.
Allmän beskrivning	Lagstiftningen, avtalskraven och de föränderliga hoten mot informationssäkerheten förutsätter regelbunden uppföljning av kraven och hoten och att man reagerar på ändringar.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 13 § 1 mom.
Referenser	
Övrig tilläggsinformation	SFS-EN ISO/IEC 27001:2017 9.1; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 4.1

Identifierare	HAL-05.2, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Kraven – konsekvenser
Krav	Organisationen bedömer konsekvenserna av införandet av väsentliga administrativa reformer och informationssystem i förhållande till informationssäkerhetskraven och -åtgärderna.
Allmän beskrivning	I samband med väsentliga ändringar ska organisationen genomföra en konsekvensbedömning. Som en del av konsekvensbedömningen ska man bedöma ändringarnas konsekvenser i förhållande till informationssäkerhetskraven och -åtgärderna.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 5 §
Referenser	
Övrig tilläggsinformation	Rekommendation om bedömning av förändringar i informationshanteringen 2020:65; ISO/IEC 27002:2022 5.31

Identifierare	HAL-06, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Riskhantering
Krav	Organisationen genomför hantering av informationssäkerhetsrisker och har bedömt de väsentliga riskerna för uppgifterna samt dimensionerat informationssäkerhetsåtgärderna enligt riskbedömningen.
Allmän beskrivning	Hanteringsprocessen gällande informationssäkerhetsrisker består av att definiera verksamhetsmiljön, bedöma riskerna (identifiera dem, analysera dem och bedöma deras betydelse), behandla riskerna, godkänna riskerna, kommunicera och dela och få information om riskerna, följa upp riskerna och granska riskerna. Hantering av informationssäkerhetsrisker är en del av organisationens verksamhet och övriga riskhantering. Med hjälp av hantering av informationssäkerhetsrisker säkerställer man tillräckligheten av informationssäkerhetsåtgärderna för att skydda uppgifternas konfidentialitet, integritet och tillgänglighet. Riskhanteringen påverkar de övriga delområdena inom hantering av informationssäkerhet. Riskhanteringen ska planeras och anvisningar om den ska ges på så sätt att man i riskhanteringen systematiskt och planmässigt behandlar olika slags risker förknippade med informationssäkerhet, såsom risker som beror på felaktigheter i informationsinnehållet, risker förknippade med avbrott i organisationens verksamhet och risker förknippade med personuppgiftsincidenter.
Exempel på genomförande	– Allmänt godkända metoder används i bedömningen och analysen av informationssäkerhetsrisker. – En schemalagd årsplan i vilken ansvar delegerats utarbetas utifrån bedömningen av informationssäkerhetsriskerna. – Tillräckligt många sakkunniga deltar i informationssäkerhetsriskernas hantering. – Risker som orsakas på grund av intressentgrupper och leveranskedjor har beaktats i hanteringen av informationssäkerhetsrisker. – Bedömningen av informationssäkerhetsrisker utnyttjas i andra processer inom hantering av informationssäkerheten.
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 6 §, 7 §
Referenser	Julkri: FYY-01, TEK-01, TEK-14, TEK-16; Katakri: T-03
Övrig tilläggsinformation	SFS-EN ISO/IEC 27001:2017 6.1 och 8–10; SFS-EN ISO/IEC 27005:2018 kapitel 6; SFS ISO 31000:2018, PiTuKri TJ-03; Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 kapitel 5.2; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 6

Identifierare	HAL-06.1, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Riskhantering – lagstiftningsrelaterade risker
Krav	Lagstiftningsrelaterade risker förknippade med tjänsten har identifierats, bedömts och skötts.
Allmän beskrivning	Lagstiftningsrelaterade risker hänvisar till möjligheterna inom olika länders lagstiftning att förplikta tjänsteleverantören att samarbeta med myndigheterna i landet i fråga och erbjuda till exempel direkt eller indirekt åtkomst till kundernas sekretessbelagda uppgifter i tjänsten. Lagstiftningsrelaterade risker kan sträcka sig till både det fysiska läget av sekretessbelagda uppgifter och bland annat överlämnande av uppgifter från ett annat land via administrativ åtkomst. Det lagstiftningsrelaterade överlämnandet av uppgifter och forskningsrätten har i flera länder begränsats så att de gäller polisen och underrättelsemyndigheter. Organisationen ska säkerställa att de lagstiftningsrelaterade riskerna inte begränsar tjänstens lämplighet för dess användningsändamål. I bedömningen av lagstiftningsrelaterade risker har man beaktat hela leveranskedjan som används vid produktionen av tjänsten, bestämmelserna i de stater enligt vilka tjänsten produceras och riskerna för dessa staters myndigheter förknippade med uppgifternas olagliga avslöjande. I enlighet med rekommendationen om hantering av säkerhetsklassificerade handlingar i molntjänster (FM 2022:6) är rekommendationen att man i behandlingen av säkerhetsklassificerade informationsmaterial använder endast sådana molntjänster och leverantörer som myndigheter bedömt som tillförlitliga, detta för att ha kontroll över riskerna förknippade med molntjänster. Om säkerhetsklassificerat informationsmaterial behandlas i internationella molntjänster rekommenderas det dessutom att det säkerhetsklassificerade informationsmaterial som behandlas avgränsas och väljs noggrant utifrån användningsfallen och därtill relaterade myndighetsprocesser och på så sätt att de kan överlämnas till stater vars jurisdiktion molntjänstens leverantör och dess underleverantörer hör till.
Exempel på genomförande	Riskbedömningen bör täcka lagstiftningsrelaterade risker vad gäller minst följande faktorer: a) Det fysiska läget av information som behandlas i tjänsten under informationens hela livscykel, inklusive eventuella underleverantörs- och utkontrakteringskedjor. b) det fysiska läget av tjänstens olika funktioner (till exempel underhålls- och administrationslösningar, bekräftelser) och komponenter under informationens hela livscykel. c) Eventuella övriga aktörer som deltar i att producera tjänsten, till exempel eventuella underleverantörs- och utkontrakteringskedjor. d) Lagstiftning och forum som tillämpas på användning av tjänsten och de uppgifter som behandlas i tjänsten. e) Aktörer som på grund av lagstiftning som tillämpas kan ha åtkomst till de uppgifter som behandlas i tjänsten. För att bedöma de lagstiftningsrelaterade riskerna bör tjänsteleverantören förutsättas beskriva de lagstiftningsrelaterade risker som riktas mot uppgifter som behandlas i tjänsten i fråga. Beskrivningarna ska vara sådana att man utifrån dem kan pålitligt bedöma tjänstens allmänna lämplighet för användningsfallet i fråga. Beskrivningarna ska täcka användningen av tjänsten och hela livscykeln av uppgifterna som behandlas i tjänsten. Dessutom ska man beakta innehållet i underpunkterna a–e ovan. Rekommendationen är att man i bedömningen följer de allmänna principer om vidarebedömning som beskrivs i PiTuKri (EE-02 / Tabell 2). Vad gäller skyddet av sekretessbelagda uppgifter som inte säkerhetsklassificerats ska det tas i beaktande att man i skyddet av sådana uppgifter i större grad än med säkerhetsklassificerad information kan godkänna lagstiftningsrelaterade risker.
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 6 §, 7 §
Referenser	Julkri: FYY-01, TEK-01, TEK-14, TEK-16, TSU-18; Katakri: T-03
Övrig tilläggsinformation	SFS-EN ISO/IEC 27001:2017 6.1 och 8–10; SFS-EN ISO/IEC 27005:2018 kapitel 6; SFS ISO 31000:2018, PiTuKri TJ-03 och EE-02; Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 kapitel 5.2; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 6

Identifierare	HAL-07, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Uppföljning och tillsyn
Krav	Uppföljning och tillsyn har ordnats i organisationen vad gäller funktionaliteten av informationssäkerhetsrelaterade processer och uppfyllandet av krav.
Allmän beskrivning	Organisationen ska följa upp informationssäkerheten i sin verksamhetsmiljö och försäkra informationssäkerheten i informationsmaterial och informationssystem under hela deras livscykel. Informationens livscykel börjar då informationen produceras eller tas emot och slutar med att informationen förvaras permanent i ett arkiv eller förstörs. Informationens livscykel täcker varje skede av informationsbehandlingen. Dessa skeden är informationens produktion eller mottagning, förvaring, användning, delande, överföring och arkivering eller förstöring. Som indikatorer för informationssäkerhetens uppföljning kan användas indikatorer som grundar sig på såväl hanteringsåtgärdernas prestationsförmåga som effektivitet. Indikatorerna kan vara numeriska eller kvalitativa. Uppföljningen grundar sig på observerade avvikelser utifrån vilka man utarbetar förslag om hur informationssäkerheten kan utvecklas. Indikatorerna kan vara exempelvis numeriska gränsvärden (till exempel att tjänsternas tillgänglighet är minst 99 procent) eller gå ut på verifiering av kravenlighet (till exempel att bedömningar och granskningar enligt årsklockan har genomförts planenligt).
Exempel på genomförande	En organisation som behandlar många sekretessbelagda uppgifter har fastställt till exempel följande: a) vad som ska följas upp och mätas b) med vilka uppföljnings-, mätnings-, analys- eller bedömningsmetoder lämpliga resultat säkerställs c) när uppföljningen och mätningen ska genomföras d) vem som genomför uppföljningen och mätningen e) när uppföljnings- och mätningsresultaten ska analyseras och bedömas f) vem som analyserar och bedömer resultaten
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 13 § 1 mom.
Referenser	Katakri: T-01, I-19
Övrig tilläggsinformation	SFS-EN ISO/IEC 27001:2017 9.1; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18 kapitel 7
Identifierare	**HAL-07.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Uppföljning och tillsyn – uppgifternas användning och överlämnande
Krav	Organisationen har identifierat kraven förknippade med insamling av loggdata och säkerställt utifrån kraven att insamlingen och uppföljningen av loggdata är tillräcklig.
Allmän beskrivning	Loggdata är ett av de mest centrala sätten att följa upp användningen och överlämnandet av uppgifter. Enligt informationshanteringslagen ska loggdata samlas in om användningen av informationssystemet förutsätter identifiering eller annan inloggning. Dessutom förutsätter dataskyddsförordningens ansvarsskyldighet gällande säkerheten av behandlingen av personuppgifter ofta i praktiken att loggdata samlas in och följs upp. Loggdata ska samlas in om användningen av informationssystemet och överlämnandet av uppgifter, men insamlingen är bunden till nödvändighet. Om sekretessbelagda uppgifter eller personuppgifter överlämnas från informationssystemet via gränssnitt eller en elektronisk förbindelse, ska man i systemet varifrån uppgifterna överlämnas samla in loggdata om överlämnandet för att säkerställa att överlämnandet av uppgifterna haft en laglig grund. Dessutom ska loggdata om användningen samlas in åtminstone från sådana informationssystem där personuppgifter eller sekretessbelagda uppgifter behandlas.

Exempel på genomförande	En organisation som ofta behandlar sekretessbelagda uppgifter kan vidta till exempel följande åtgärder: – Som en del av upphandlingen av tjänster och informationssystem definierar organisationen kraven på insamling av loggdata förknippade med dessa tjänster och system samt säkerställer att kraven uppfylls. – Organisationen definierar behoven och förfarandena förknippade med användningen av uppgifter och uppföljningen av överlämnanden per informationssystem. – Uppföljningsförfaranden bedöms med regelbundna intervaller. – Organisationen definierar ansvaren förknippade med att förvara, förstöra och skydda loggdata och säkerställer att dessa ansvar genomförs. – Om loggdata används i stor omfattning kan organisationen överväga att övergå till centraliserad hantering av loggdata (SIEM).
Lagstiftning	Informationshanteringslagen 17 §
Referenser	Katakri: I-10
Övrig tilläggsinformation	Cybersäkerhetscentret, Så här samlar du in och använder loggdata; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 14; ISO/IEC 27002:2022 5.31, 8.15
Identifierare	**HAL-08, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Hantering av störningar
Krav	Organisationen har processer och anvisningar som definierats för informationssäkerhetsstörningar och avvikande situationer.
Allmän beskrivning	Med hantering av informationssäkerhetsstörningar strävar man efter att säkerställa att organisationen klarar av att fungera effektivt i icke-önskade, oförväntade situationer på ett sätt som minimerar skadorna och återställer situationen till det normala och garantera att en liknande störning inte är möjlig annanstans i organisationen. Organisationen ska ha en process för behandling av störningar som åtminstone tar ställning till att definiera situationens allvarlighet, förhindra ytterligare skador, samla in bevis, reda ut situationen, kommunicera om situationen, vidta korrigerande åtgärder och lära sig av situationen. Behandlingsprocessen ska beakta huruvida tjänsten är tidskritisk och vid planeringen ska man bedöma behoven vad gäller hanteringen av störningar som sker utanför tjänstetiden. Organisationen har också utrett vilka nationella och internationella författningar eller avtal som organisationen ingått förutsätter att informationssäkerhetsincidenter eller misstanke om sådana rapporteras till myndigheterna. Kriterier, ansvar, kontaktuppgifter och tidsfrister vad gäller denna rapportering har fastställts och dokumenterats.
Exempel på genomförande	Följande gäller för hanteringen av informationssäkerhetsstörningar: – hanteringen är planerad med beaktande av hela tjänstekedjan och störningar som sker utanför tjänstetiden, – anvisningar har getts om och personal har utbildats i hanteringen, – hanteringen har dokumenterats på en tillräcklig nivå, – hanteringen har övats och – dess kommunikationspraxis och ansvar har avtalats.
Lagstiftning	Informationshanteringslagen 4 § 2 mom. och 13 §; säkerhetsklassificeringsförordningen 7 §
Referenser	Katakri: T-07
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.24; PiTuKri TJ-04

Identifierare	HAL-09, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Dokumentering
Krav	Politik, processer och anvisningar förknippade med informationssäkerheten och resultat som uppstår då processerna genomförs har dokumenterats.
Allmän beskrivning	
Exempel på genomförande	– Organisationen har definierat de dokument som hanteringen av informationssäkerheten förutsätter och som uppstår inom de olika processerna för hanteringen av informationssäkerhet. – Underhålls- och distributionsprocesser har definierats för dokumentationen. – Dokumentationens rätter och skydd har definierats.
Lagstiftning	Informationshanteringslagen 5 §, 6 §, 13 § 1 mom.
Referenser	Katakri: T-01
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.37
Identifierare	**HAL-09.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Dokumentering – aktualitet
Krav	Dokumentationen förknippad med informationssäkerhet är aktuell.
Allmän beskrivning	
Exempel på genomförande	– Organisationen har en process med hjälp av vilken man följer upp dokumentationens omfattning och aktualitet. – Man reagerar på brister i dokumentationen.
Lagstiftning	Informationshanteringslagen 5 §, 6 §, 13 § 1 mom.
Referenser	
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.37
Identifierare	**HAL-10, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Bedömning av personalens pålitlighet
Krav	Organisationen identifierar de uppgifter vars genomförande förutsätter särskild pålitlighet från personer som är anställda av organisationen eller som agerar för den.
Allmän beskrivning	Uppgifter som förutsätter särskild pålitlighet kan identifieras till exempel genom att definiera situationer där en person behandlar säkerhetsklassificerade uppgifter eller sekretessbelagda uppgifter i betydande utsträckning och regelbundet eller arbetar i lokaler där personen annat än sporadiskt kan få kännedom om säkerhetsklassificerade eller sekretessbelagda uppgifter.
Exempel på genomförande	– Organisationen utarbetar en beskrivning av sådana uppgifter förknippade med – behandling av informationsmaterial som förutsätter särskild pålitlighet. – Man ansöker en säkerhetsutredning av personer som utses för dessa uppgifter om det finns en grund för detta enligt säkerhetsutredningslagen. – Dessutom upprätthåller informationshanteringsenheten en förteckning över dessa uppgifter.
Lagstiftning	Informationshanteringslagen 12 §
Referenser	Katakri: T-10
Övrig tilläggsinformation	Säkerhetsutredningslagen (726/2014); ISO/IEC 27002:2022 6.1

Identifierare	HAL-10.1, L:Sekretessbelagd, E:Kritisk, S:Kritisk, TS:Särskild kategori av personuppgifter
Namn	Bedömning av personalens pålitlighet – säkerhetsutredning
Krav	Organisationen bedömer behovet av en säkerhetsutredning, och om en utredning förutsätts beviljar organisationen inte personerna åtkomst till objekt som ska skyddas förrän säkerhetsutredningen genomförts.
Allmän beskrivning	Förutsättningarna gällande säkerhetsutredning av person föreskrivs i säkerhetsutredningslagen (726/2014). En säkerhetsutredning av person kan göras om personen i sitt arbete har åtkomst till exempel till en lokal som är viktig med tanke på säkerheten eller behandlar sekretessbelagda uppgifter. Säkerhetsutredningens omfattning beror på personens arbetsuppgift och nödvändiga rättigheter till exempel till behandling av sekretessbelagda uppgifter. Utredningens omfattning avgör vilka informationskällor som används i utredningen. Vid behov kan personen också intervjuas. Det är vanligen arbetsgivaren som ansöker om en säkerhetsutredning, och arbetstagaren fyller inledningsvis de blanketter som hör till säkerhetsutredningen.
Exempel på genomförande	– Huruvida uppgiften förutsätter en säkerhetsutredning kontrolleras i samband med rekryteringar, uppgiftsförändringar och externa tjänsteupphandlingar, – vid behov har organisationen definierat en process för ansökan om säkerhetsutredningar
Lagstiftning	Informationshanteringslagen 12 §; säkerhetsklassificeringsförordningen 9 §
Referenser	Katakri: T-10
Övrig tilläggsinformation	Statstjänstemannalagen (750/1994) 8 c §
Identifierare	**HAL-11, L:Sekretessbelagd, E:, S:, TS:Personuppgift**
Namn	Sekretess och tystnadsplikt
Krav	Personerna som behandlar uppgifter har gjorts medvetna om informationssäkerhetsprinciperna och -åtgärderna förknippade med skyddet av uppgifter och behandlingen av handlingar.
Allmän beskrivning	
Exempel på genomförande	– Personen görs medveten om principerna förknippade med skyddet av uppgifter innan hen får åtkomst till uppgifterna, – som intyg på att personen gjorts medveten om detta kan personen underteckna en skriftlig tystnadsförbindelse och underskriften förtecknas i ”förteckningen över tystnadsförbindelser” eller – det finns ett elektronisk förfarande för att avge förbindelse och detta sköts automatiskt i samband med den första inloggningen.
Lagstiftning	Informationshanteringslagen 4 § 2 mom.; säkerhetsklassificeringsförordningen 6 §, 8 §; offentlighetslagen 25 §, 26 § 3 mom.
Referenser	Katakri: T-11
Övrig tilläggsinformation	ISO/IEC 27002:2022 6.6; PiTuKri HT-03

Identifierare	HAL-12, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Anvisningar
Krav	Organisationen har aktuella och täckande anvisningar för att säkerställa informationssäkerheten.
Allmän beskrivning	Genom att ge anvisningar om ärenden som är centrala med tanke på informationssäkerheten strävar man efter att säkerställa att verksamheten inte är personberoende. Organisationen bör ha aktuella anvisningar om behandlingen av uppgifter, användningen av informationssystem, databehandlingsrättigheterna, genomförandet av ansvar inom informationshanteringen, genomförandet av rätten att få information och informationssäkerhetsåtgärderna. Anvisningarna omfattar informationsrelaterade processer och behandlingsmiljöer under informationens hela livscykel.
Exempel på genomförande	– Förfaranden och anvisningar som behövs för att skydda uppgifterna och säkerställa informationssäkerheten har dokumenterats. – Säkerhetsanvisningarna ges med beaktande av behoven förknippade med personalens arbetsuppgifter. – Säkerhetsanvisningarnas omfattning och aktualitet följs upp regelbundet och de är tillgängliga för nödvändiga aktörer.
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 13 § 1 mom.; säkerhetsklassificeringsförordningen 6 §, 8 §
Referenser	Julkri: TEK-17.2; Katakri: T-04
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.37; SFS-EN ISO/IEC 27001:2017 7.5; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, kapitel 4

Identifierare	HAL-13, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Utbildningar
Krav	Organisationen säkerställer med introduktioner, utbildningar och kommunikation att personalen och alla som agerar för organisationens räkning har kännedom om gällande bestämmelser och anvisningar om informationssäkerheten.
Allmän beskrivning	Ledningen ska sörja för att organisationen erbjuder utbildning som säkerställer att personalen och alla som agerar för organisationens räkning har kännedom om gällande författningar, bestämmelser och organisationens anvisningar förknippade med informationssäkerhet, informationshantering, informationsbehandling och uppgifternas offentlighet och sekretess samt om risker och hot riktade mot uppgifter som organisationen ansvarar för. Särskilt i utbildningar ska man beakta hot och anvisningar förknippade med fjärranvändning, administration av informationssystem och andra behandlingssituationer med högre risk.
Exempel på genomförande	– Personen som behandlar uppgifter har gjorts medveten om säkerhetsregler och -förfaranden som gäller skyddet av uppgifterna. – Utbildningen genomförs med beaktande av behoven förknippade med personalens arbetsuppgifter. – Utbildningens innehåll dokumenteras. – Vem som deltar i utbildningarna bokförs.
Lagstiftning	Informationshanteringslagen 4 § 2 mom.; säkerhetsklassificeringsförordningen 6 §, 8 §
Referenser	Katakri: T-12
Övrig tilläggsinformation	ISO/IEC 27002:2022 6.3; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, kapitel 5

Identifierare	HAL-14, L:Offentlig, E:Ringa, S:, TS:Personuppgift
Namn	Åtkomst- och behandlingsrätt
Krav	Organisationen säkerställer att informationssystemens åtkomsträttigheter och rätten att behandla informationen definieras enligt uppgiftsrelaterade behov och hålls uppdaterade.
Allmän beskrivning	Med hjälp av hantering av åtkomst- och behandlingsrättigheter möjliggörs en lovlig användning av informationen och olovlig användning förhindras. Användaren ges endast sådana användarrättigheter och -fullmakter för informationssystemen som är nödvändiga med tanke på arbetsuppgifterna. Åtkomsträtt till informationen kan ges endast sådana personer som på grund av sina arbetsuppgifter har ett behov av att få information eller i övrigt behandla informationen, har gjorts medveten om anvisningar om skyddet av informationen och känner till skyldigheterna som gäller behandlingen av informationen.
Exempel på genomförande	– Organisationen har definierat principer enligt vilka åtkomst- och behandlingsrättigheter beviljas – Ansvar och förfaranden har fastställts för beviljandet av dessa rättigheter – Ansvar och förfaranden har fastställts för genomförandet av dessa rättigheter – Beviljandet av åtkomsträttigheter har dokumenterats så att detta kan kontrolleras i efterhand
Lagstiftning	Informationshanteringslagen 4 § 2 mom. och 16 §; säkerhetsklassificeringsförordningen 8 §, 11 § 1 mom. 3 punkten
Referenser	Katakri: T-13, I-6
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.15, 5.18; PiTuKri HT-05; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65, kapitel 13; Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10, kapitel 7.6
Identifierare	**HAL-14.1, L:TL III, E:, S:, TS:**
Namn	Åtkomst- och behandlingsrätt – aktuell förteckning
Krav	Organisationen säkerställer att den har uppdaterade förteckningar över personernas åtkomst- och behandlingsrättigheter.
Allmän beskrivning	Statsförvaltningens myndighet ska föra en förteckning över personer som har rätt att behandla handlingar i säkerhetsklasserna I, II eller III. I förteckningen ska anges personens uppgift som behovet av behandling av säkerhetsklassificerad information grundar sig på.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 8 §
Referenser	Katakri: T-13
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.18; Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 kapitel 4.1

Identifierare	HAL-14.2, L:Sekretessbelagd, E:Kritisk, S:, TS:Särskild kategori av personuppgifter
Namn	Åtkomst- och behandlingsrätt – avslutande
Krav	Organisationen säkerställer att den som inte längre arbetar inom uppgifter som rätten att behandla information grundar sig på återlämnar informationen eller förstör den på ändamålsenligt sätt.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 21 § 2 mom.; säkerhetsklassificeringsförordningen 8 §
Referenser	Katakri: T-13
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.18; Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 kapitel 4.1
Identifierare	**HAL-15, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Arbetets informationssäkerhet under hela anställningsförhållandet
Krav	Organisationen sköter om arbetets informationssäkerhet under hela anställningsförhållandet.
Allmän beskrivning	Man ska särskilt beakta åtgärder vid rekrytering, ändringar i arbetsuppgifterna och då anställningsförhållandet avslutas. Förfaranden i början av och under anställningsförhållandet är till exempel säkerhetsutredningar av personer, behandlings-, användar- och åtkomsträttigheter, förståelse av sekretess och tystnadsplikt, säkerhetsutbildning, eventuell uppdatering av dessa vid förändringar och utbildning i förändringarna. Förfaranden förknippade med avslutandet av ett anställningsförhållande är till exempel att återlämna nycklar, koder och material samt radering av behandlings-, användar- och åtkomsträttigheter. Då anställningsförhållandet avslutas är det också väsentligt att påminna om sekretessen och tystnadsplikten.
Exempel på genomförande	Typiskt förutsätter åtgärderna anvisningar om förfarande som nödvändiga personalgrupper utbildats i och har tillgång till. Anvisningar om förfarande kan till exempel delas in i helheter enligt anställningsförhållandets livscykel. Anvisningshelheterna kan till exempel utgöras av anvisningar om rekrytering, introduktion, ändringar under anställningsförhållandet, anställningsförhållandets avslutande och mer detaljerade åtgärder, såsom anvisningar om ändringar i rättigheterna gällande behandling, användning och åtkomst.
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 12 §, 16 §; Säkerhetsklassificeringsförordningen 6 §, 8 §
Referenser	Katakri: T-09
Övrig tilläggsinformation	ISO/IEC 27002:2022 6.1, 6.2, 6.3, 6.5; PiTuKri HT-01; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65, kapitel 5; Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10

Identifierare	HAL-16, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Upphandlingarnas säkerhet
Krav	Organisationen säkerställer redan på förhand att informationssystem och tjänsterna som upphandlas är informationssäkra. Dessutom säkerställer organisationen deras säkerhet i förändringssituationer under systemets hela livscykel.
Allmän beskrivning	Man ska säkerställa i upphandlingarna att informationssystemen och tjänsterna som upphandlas uppfyller informationssäkerhetskraven i enlighet med det behandlade informationsmaterialet och att informationssystemen lämpar sig till att utföra myndighetens uppgifter resultatrikt och effektivt. Innan ett upphandlingsbeslut fattas är det tillrådligt att kartlägga alternativen och redan i ett tidigt skede gallra bort sådana alternativ som inta kan uppfylla de minimikrav som lagstiftningen ställer. En metod för sådan gallring på förhand är att bekanta sig med beskrivningar som tjänsteleverantörskandidaterna producerat och preliminärt bedöma systemet eller tjänsten som upphandlas utifrån dem med hänsyn till minimikraven. En allmänt använd metod för att säkerställa tjänsternas säkerhet är att bedöma informationssystemen och deras tjänsteleverantörer. Detta beskrivs närmare i kapitel 4 i rekommendationen ”Hantering av säkerhetsklassificerade handlingar i molntjänster”. En del tjänsteleverantörer erbjuder sina kunder en möjlighet att ta i bruk nya funktioner som är i förhandsgranskning- eller testningsfasen. Om man vill ta i bruk sådana funktioner i behandlingen av sekretessbelagda uppgifter är det tillrådligt att i riskbedömningen beakta bland annat ansvar förknippade med införandet. Genomförandet av nya funktioner kan ännu vara bristfälligt, och ersättningen av eventuella skador som dessa orsakar riktas ofta till kunden i avtalen.
Exempel på genomförande	Organisationen definierar informationssäkerhetskraven för upphandlings- och utvecklingsprocesserna och säkerställer att kraven uppfylls. För att garantera kravens tillräcklighet förutsätter organisationen att informationssäkerhetskraven definieras, granskas och godkänns innan upphandlingen går vidare och att informationssäkerhetstestningen genomförts med godkänt resultat innan informationssystemen tas i bruk. Leverantören av tjänsten eller systemet som upphandlas ska kunna reda ut minst följande: 1) Det finns en systembeskrivning av tjänsten. Det ska vara möjligt att utifrån tjänsteleverantörens beskrivning kunna bedöma tjänstens allmänna lämplighet för användningsfallet i fråga. Minst följande ska framgå av systembeskrivningen: a) Tjänstens service- och genomförandemodeller och deras servicenivåavtal (Service Level Agreements, SLAs). b) Principer, förfaranden och skyddsåtgärder förknippade med livscykeln för tjänstens tillhandahållande (utveckling, användning, tagande ur bruk), inklusive tillsynsåtgärder. c) Beskrivning av infrastrukturen, nätet och systemkomponenterna som används i utvecklingen, underhållet/hanteringen och användningen av tjänsten. d) Principer och praxis för förändringshantering, särskilt behandlingsprocesser förknippade med ändringar som påverkar säkerheten. e) Behandlingsprocesser för betydande incidenter som avviker från normal användning, till exempel verksamhetssätt vid betydande fel i systemen. f) Rollerna förknippade med leverans och användning av tjänsten och ansvarsfördelningen mellan kunden och tjänsteleverantören. Av beskrivningen ska tydligt framgå de åtgärder som kunden ansvarar för vad gäller att säkerställa tjänstens säkerhet. Tjänsteleverantörens ansvar ska inkludera samarbetsskyldighet särskilt vid utredning av avvikande situationer. g) Funktioner som överförts till underleverantörer eller utkontrakterats. Infrastruktur, nät och systemkomponenter ska beskrivas tillräckligt ingående så att man baserat på beskrivningen kan göra en allmän lämplighetsbedömning av tjänsten och en riskanalys med hänsyn till kundens användningsfall. Jfr PiTuKri KT-01 ((Systembeskrivning till stöd för kontinuitet och driftssäkerhet). Infrastruktur kan med vissa förbehåll beskrivas med hjälp av den programkod som används för infrastrukturen i fråga.
Lagstiftning	Informationshanteringslagen 13 § 4 mom.; säkerhetsklassificeringsförordningen 6 §; offentlighetslagen 26 §

Referenser	Katakri: I-13
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.19, 5.20, 5.21, 8.29, 8.30; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, kapitel 6; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65, kapitel 8; Rekommendation om hantering av säkerhetsklassificerade handlingar i molntjänster 2022:6 kapitel 4; PiTuKri EE-01 och KT-01
Identifierare	**HAL-16.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Upphandlingarnas säkerhet – avtal
Krav	Organisationen säkerställer att kraven som ingår i informationssäkerheten beaktas i avtalen och att avtalen dessutom beaktar att kraven bevaras under hela livscykeln. Avtalsvillkoren får inte heller begränsa tjänsten lämplighet för användningsfallet i fråga.
Allmän beskrivning	Särskilt molntjänster ändras ständigt. Utmärkande för molntjänster är en snabb och kraftig utveckling som förutsätter fortlöpande uppföljning och övervakning av avtalen och hantering av förändringar. Ändringar ökar risken för att tjänsten, dess leverantör eller någon ny egenskap förändras i strid med avtalet eller kraven eller att risker som är förenade med bestämmanderätt realiseras. Även tjänsteproducentens ägarbyte är förknippad med risker som i tillräckligt stor omfattning ska beaktas i avtalen. Dessutom bör det påpekas att det kan vara omöjligt att försäkra sig om att informationssäkerheten varar hela livscykeln tillsammans med sådana tjänsteleverantörer som i sina avtal förbehåller sig rätt att ensidigt ändra avtalsvillkoren. Riskbaserat ska man också bedöma avtalens tillförlitlighet och försäkra sig om att det som leverantören kommit överens om i avtalet faktiskt genomförts på det sätt som avtalats. Särskilt i avtal förknippade med molntjänster ska man tillräckligt tydligt definiera vilka uppgifter som tjänsteproducenten ansvarar för och vilka kunden ansvarar för. Behandlingen av personuppgifter kan ur dataskyddsregleringens synvinkel även förhindras om tjänsteleverantören inte kan erbjuda ett avtal som följer dataskyddsregleringen och som inte kan ändras ensidigt, det vill säga utan kundens samtycke. I bedömningen ska man beakta bestämmelserna i artikel 28.4 i EU:s allmänna dataskyddsförordning vid användning av underbiträden. Tjänsteleverantören (den personuppgiftsansvarige) ska ingå ett skriftligt avtal med personuppgiftsbiträdet. Tjänsternas avtal och användarvillkor kan också vara förknippade med olika slags leverantörspecifika sätt att definiera de länder där tjänsten eller en del av den är fysiskt belägen. Överföring av personuppgifter till länder utanför EU/EES ska alltid ske i enlighet med de förutsättningar som föreskrivs i EU:s allmänna dataskyddsförordning (kapitel V). Bland annat vad gäller lagstiftningsrelaterade risker, kontinuitet och beredskap ska det också beaktas att kundens uppgifter ska under hela sin livscykel vara belägna endast på sådana fysiska platser som beskrivs i avtalet. Undantag till detta utgörs av en situation där kunden skriftligen på förhand har godkänt överföring av uppgifterna eller behandling av dem på andra fysiska platser. Att fylla sådana behov är vanligen inte möjligt på ett rimligt sätt i situationer där tjänsteleverantören förbehåller sig möjligheten att ensidigt ändra sina avtalsvillkor, med andra ord utan kundens samtycke. Dessutom ska man beakta att myndigheten ska på förhand försäkra sig om att uppgifternas sekretess och skydd genomförs ändamålsenligt (26 § i offentlighetslagen). Myndigheten ska också på förhand säkerställa att en säkerhetsklassificerad handling skyddas på behörigt sätt om myndigheten lämnar ut den till någon annan än en statsförvaltningsmyndighet (6 § i säkerhetsklassificeringsförordningen).
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 §; säkerhetsklassificeringsförordningen 6 §; offentlighetslagen 26 §; dataskyddsförordningen artikel 28.4
Referenser	Katakri: I-13
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.20; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, kapitel 6; PiTuKri TJ-07;

Identifierare	HAL-17, L:, E:Viktig, S:Viktig, TS:
Namn	Informationssystemens funktionella användbarhet och feltolerans
Krav	Organisationen säkerställer feltoleransen och den funktionella användbarheten av informationssystem som är väsentliga med tanke på att sköta uppgifterna med regelbunden och tillräcklig testning.
Allmän beskrivning	Med väsentliga informationssystem avses sådana informationssystem som är kritiska med tanke på utförandet av myndigheternas lagstadgade uppgifter, särskilt då tjänster produceras för förvaltningskunder. Med funktionell användbarhet avses med tanke på användaren av informationssystemet att man säkerställer att informationssystemet är lätt att lära sig använda och dess funktionslogik är lätt att komma ihåg i användning, informationssystemets verksamhet stöder de arbetsuppgifter som användaren ska utföra med det och systemet främjar dess felfria användning.
Exempel på genomförande	– Organisationen identifierar och gör en förteckning över informationssystem som är väsentliga med tanke på att sköta uppgifterna, till exempel som en del av inventeringen av objekt som ska skyddas och informationens klassificering. – Organisationen definierar tillgänglighetskriterier för väsentliga informationssystem, mot vilka feltoleransen kan testas. Man kan utnyttja tillgänglighetsklassificering av informationssystemen vid definitionen av systemspecifika tillgänglighetskriterier. – Organisationen definierar kriterierna för funktionell användbarhet. – Organisationens upphandlingsprocesser och -anvisningar beaktar kraven förknippade med funktionell användbarhet och feltolerans. – Organisationen dokumenterar feltoleranstesterna.
Lagstiftning	Informationshanteringslagen 13 § 2 mom.
Referenser	
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.29; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 7

Identifierare	HAL-17.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Informationssystemens funktionella användbarhet och feltolerans – tillgänglighet
Krav	Organisationen ska säkerställa digitala tjänsters tillgänglighet i den omfattning som lagstiftningen förutsätter.
Allmän beskrivning	Tillgänglighet innebär att så många olika människor som möjligt kan använda webbplatser och mobila applikationer så enkelt som möjligt. Tillgänglighet handlar om att beakta olikheterna och mångfalden bland människor i planeringen och förverkligandet av webbplatser och mobila applikationer. Tre delområden ska beaktas i planeringen och genomförandet av en tillgänglig digital tjänst: det tekniska genomförandet, användarvänligheten och att innehållet är tydligt och begripligt. Eftersom tillgänglighet inte omfattas av informationshanteringsnämndens behörighet tas tillgänglighet upp i Julkri-kriterierna endast som ett säkerställande kriterium på övergripande nivå. Julkri-kriterierna används sålunda inte för bedömning av tillgängligheten, men kriteriet har tagits med för att påminna organisationerna om att även tillgängligheten ska säkerställas som en del av planeringen och genomförandet av digitala tjänster. Närmare anvisningar och krav finns på webbplatsen www.tillganglighetskrav.fi som drivs av Regionförvaltningsverket i Södra Finland.
Exempel på genomförande	
Lagstiftning	Lagen om tillhandahållande av digitala tjänster (306/2019)
Referenser	
Övrig tilläggsinformation	www.tillganglighetskrav.fi

Identifierare	HAL-18, L:Offentlig, E:, S:, TS:
Namn	Genomförande av handlingsoffentlighet
Krav	Organisationen säkerställer att informationssystem, datalagrens informationsstrukturer och relaterad informationsbehandling planeras så att handlingarnas offentlighet kan genomföras utan besvär.
Allmän beskrivning	Kravet riktas till myndigheter som i praktiken ansvarar för tillgängligheten av uppgifter i informationsmaterial. Kravet poängterar att man av de uppgifter som finns i myndighetens informationssystem och med sökfunktioner som finns i systemet ska kunna bilda myndighetens handlingar för att genomföra offentligheten av myndighetens verksamhet.
Exempel på genomförande	– Organisationerna definierar de informationsbehov som riktas till informationsmaterial som organisationen ansvarar för och beaktar särskilt de krav som gäller offentligheten av myndigheternas uppgifter. – Organisationerna beaktar kraven på att handlingsoffentligheten kan genomföras utan svårighet i genomförande- och upphandlingsprocesserna. – Organisationen följer upp behov förknippade med genomförandet av handlingsoffentligheten och underhåller gamla informationssystem enligt behov.
Lagstiftning	Informationshanteringslagen 13 § 3 mom.
Referenser	
Övrig tilläggsinformation	

Identifierare	HAL-19, L:Offentlig, E:, S:, TS:Personuppgift
Namn	Behandling av uppgifter
Krav	Organisationen säkerställer att uppgifter behandlas och förvaras på så sätt att åtkomst till dem skyddas från utomstående.
Allmän beskrivning	Informationssäkerheten av behandlingen och förvaringen av uppgifter påverkas bland annat av de fysiska lokalernas säkerhet, säkerheten av de informationssystem och terminaler som används i behandlingen av uppgifter och anvisningarna för och utbildningen av de personer som behandlar uppgifterna. Med hjälp av organisationens processer för säkerhetshantering ska man säkerställa att nödvändiga åtgärder vidtagits för varje delområde som nämnts ovan. Med detaljerade kriterier om behandlingen och lagringen av uppgifter klassificerade på olika säkerhetsnivåer presenteras i delområdena fysisk säkerhet och teknisk säkerhet.
Exempel på genomförande	Organisationen har säkerställt säkerheten av behandlingen av uppgifter till exempel med följande åtgärder: – Organisationen har säkerställt att lokalerna avsedda för behandling och lagring av uppgifter uppfyller de krav som ställts av informationssystemen och uppgifterna som behandlas och förvaras i lokalerna. Dessutom har organisationen fastställt nödvändiga administrativa områden och skyddsområden. – Organisationen har gett anvisningar om i vilka lokaler uppgifter klassificerade på olika säkerhetsnivåer får behandlas och förvaras. – Organisationen har gett anvisningar om hur åtkomsten till uppgifterna ska skyddas från utomstående i olika behandlingsmiljöer. – Organisationen har fastställt hur olika informationssystem avsedda för behandling av uppgifter ska förvaras. – Organisationen har fastställt kraven förknippade med terminaler som används i behandlingen av uppgifter.
Lagstiftning	Informationshanteringslagen 13 §, 15 § 2 mom.; säkerhetsklassificeringsförordningen 10 § 1 mom.
Referenser	Julkri: FYY-03, FYY-04, TEK-09; Katakri: I-17
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.15; Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 4;

3 Fysisk säkerhet

Fysisk säkerhet (FYY) innehåller kriterier som är förknippade med lokaler och förvaringslösningar och som förhindrar eller begränsar olovlig åtkomst till uppgifter. Dessutom beskriver delområdet kriterier förknippade med behandling, förvaring, överföring, transport och förstöring av uppgifter. Det är möjligt att använda delområdet fysisk säkerhet i bedömning av åtgärder som vidtagits för att fysiskt skydda uppgifterna.

Delområdets innehåll grundar sig på Katakri-kriterierna. Innehållet av särskilt de kriterier som gäller behandling av säkerhetsklassificerade uppgifter har man försökt bevara som enhetliga med Katakri. De tydligaste skillnaderna i förhållande till Katakri är att kriterier som grundar sig på internationella skyldigheter gällande informationssäkerhet har lämnats bort från delområdet och att vissa kriterier klassificerats som möjliga att tillämpa även på andra än säkerhetsklassificerade uppgifter.

Delområdets struktur har planerats så att gemensamma kriterier som gäller säkerhetsområden på olika nivåer, kriterier som gäller endast administrativa områden och kriterier som gäller endast skyddsområden har samlats i var sitt underkapitel. Denna struktur avviker från strukturen i Katakri, där en del av kriterierna har repeterats med samma innehåll i säkerhetsområden på olika nivåer.

Myndigheternas informationsmaterial ska behandlas och förvaras i verksamhetslokaler som är tillräckligt säkra enligt kraven på tillförlitlighet, integritet och tillgänglighet (15 § 2 mom. i informationshanteringslagen). För att fysiskt skydda säkerhetsklassificerade uppgifter föreskriver säkerhetsklassificeringsförordningen om två typer av fysiskt skyddade säkerhetsområden: administrativa områden och skyddsområden. I Julkri används begreppen administrativt område och skyddsområde.

Rekommendationen är att datalager som innehåller sekretessbelagda uppgifter och de informationssystem som används till att behandla uppgifterna placeras i ett skyddat område som myndigheten har fastställt för detta syfte. Ett sådant område kan till exempel utgöras av ett administrativt område som beskrivs i säkerhetsklassificeringsförordningen, denna rekommendation och kriterierna som bifogats till rekommendationen.

Med ett administrativt område avses i praktiken ett sådant område definierat av organisationen som utomstående inte har okontrollerad åtkomst till och för vilken tillräckliga

åtgärder vidtagits för att säkerställa säkerheten av de uppgifter som behandlas och förvaras i området. Inga detaljerade krav har ställts på områdets strukturer och andra åtgärder, utan organisationen kan planera dem genom att riskbaserat tillämpa det fysiska (FYY) delområdets kriterier.

Med fysisk säkerhet avses genomförande av fysiska och tekniska skyddsåtgärder så att man förhindrar olovlig åtkomst till uppgifterna genom att:

a) säkerställa att uppgifter behandlas och förvaras ändamålsenligt,
b) möjliggöra åtkomst till uppgifterna utifrån behov och vid behov utifrån säkerhetsutredningar,
c) förebygga, förhindra och upptäcka olovliga åtgärder och
d) förhindra eller fördröja olagligt intrång.

I lokaler där flera organisationer är verksamma ska varje organisation som behandlar uppgifter säkerställa att de gemensamma lokalernas säkerhet är tillräcklig i förhållande till de krav på fysisk säkerhet som riktas mot organisationen.

Identifierare	FYY-01, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Bedömningen av risker förknippade med fysisk säkerhet
Krav	Fysiska skyddsåtgärder ska dimensioneras i enlighet med riskbedömningen.
Allmän beskrivning	I riskbedömningen ska man beakta till exempel principerna om informationsbehov, uppgifternas differentiering och lägsta behörighet som inkluderas i processerna förknippade med hantering av åtkomsträtt och andra säkerhetsarrangemang. Riskbedömningen gällande fysiska skyddsåtgärder ska vara regelbunden och utgöra en del av organisationens riskhanteringshelhet. Bedömda risker har utsedda ägare. Risker förknippade med förändringar i godkända fysiska skyddsåtgärder bör bedömas i samband med förändringen. Särskilt vad gäller ersättande fysiska skyddsåtgärder bör man kunna motivera de valda åtgärderna.
Exempel på genomförande	Samtliga relevanta faktorer ska beaktas i riskbedömningen, särskilt följande: a) Uppgifternas säkerhetsklass och sekretessgrund b) Uppgifternas behandlings- och lagringssätt samt mängd med beaktande av att om det finns mycket information eller om informationen samlas ihop kan tillämpning av strängare riskhanteringsåtgärder förutsättas c) Uppgifternas behandlings- och lagringstid d) Miljön där uppgifterna behandlas och förvaras: byggnadens miljö, placering i byggnaden, lokalen eller en del av den e) Responstid vid larm f) Utkontrakterade funktioner, såsom underhålls-, städnings-, fastighets- och säkerhetstjänster g) Det bedömda hotet mot uppgifterna som underrättelsetjänster, brottslig verksamhet och den egna personalen utgör
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.
Referenser	Julkri: HAL-06; Katakri: F-02
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 36

Identifierare	FYY-01.1, L:TL III, E:, S:, TS:
Namn	Bedömningen av risker förknippade med fysisk säkerhet – TEMPEST
Krav	Vid bedömning av behandlingen av uppgifter i en terminal och läget av säkerhetsområden ska man i tillräckligt stor omfattning även beakta TEMPEST-risken.
Allmän beskrivning	Vid bedömning av behandlingen av uppgifter i en terminal och läget av säkerhetsområden ska man i tillräckligt stor omfattning även beakta TEMPEST-risken, det vill säga risken som orsakas av elektromagnetisk diffus strålning. TEMPEST-risken kan vanligen minskas genom att ändra placeringen av den plats där uppgifterna behandlas i fastigheten.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 2 mom.
Referenser	Julkri: TEK-15; Katakri: F-05.8, F-06.10
Övrig tilläggsinformation	

Identifierare	FYY-02, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Val av fysiska skyddsåtgärder (skydd på flera nivåer)
Krav	I säkerhetsområden och lokalerna som omger dem ska man vidta åtgärder som förebygger, förhindrar och begränsar handlingar som äventyrar skyddet av säkerhetsområdet, åtgärder för att upptäcka och spåra handlingar som äventyrar skyddet och åtgärder för att utan dröjsmål återställa den säkerhetsnivå som föregick handlingen som äventyrade skyddet genom att tillämpa principen om skydd på flera nivåer. Anordningar ska kontrolleras och underhållas regelbundet.
Allmän beskrivning	Datalager som innehåller sekretessbelagda uppgifter och handlingar samt de informationssystem som används till att behandla dessa ska placeras i ett skyddat område som myndigheten har fastställt för detta ändamål. Ett sådant område kan till exempel utgöras av ett administrativt område som beskrivs i säkerhetsklassificeringsförordningen. Om de inte placeras i ett sådant område ska uppgifterna skyddas riskbaserat med andra skyddskontroller. Rekommendationen är att den utrustning och de system som inkluderas i helheten som flernivåskyddet bildar följer europeiska standarder och deras minimikrav. Valet av rätt standardklass grundar sig alltid på en riskbedömning. I kolumnen Målnivå som placerats i anslutning till de enskilda kraven presenteras en standardenlig klass eller anvisning som är tillräcklig för de flesta lösningar gällande flernivåskydd. Förutsättningen för godkännande av enskilda skyddsåtgärder är dock inte att målnivån uppnås, eftersom bedömningen av fysiska skyddsåtgärder grundar sig på riskbedömning och den helhet som flernivåskyddet bildar. I vissa fall kan man med grund i riskbedömningen även förutsätta enskilda skyddsåtgärder som är på en högre nivå än målnivån. Vid bedömning av anordningar och system ska man säkerställa att de är funktionsdugliga och lämpliga för sitt användningsändamål. Anordningarnas och systemens leveransprover, kontroller som genomförts under användningen och det genomförda underhållet ska dokumenteras. Vid bedömning av systemrättigheter ska man fästa särskild uppmärksamhet vid att principen om lägsta behörighet och uppgifternas differentiering realiseras. Lokalen dit anordningarna och systemen placeras ska vara belägen i ett skyddat säkerhetsområde. Installation, kontroll, underhåll och städning av anordningar och system och de lokaler dit dessa placerats genomförs endast av personer som fått självständig åtkomsträtt till området eller i sådana personers övervakning. Fjärråtkomst till anordningar och system samt installation av dem ska genomföras utgående från riskbedömningen på ett tillräckligt datasäkert sätt så att utrustning och system endast är tillgängliga via auktoriserade terminaler och nät. Dessutom ska dataförbindelsernas, anordningarnas och systemens gränssnitt vara skyddade så att utomstående inte har tillgång till de överförda uppgifterna. Det är också möjligt att behandla sekretessbelagda uppgifter i gemensamma arbetsmiljöer där flera olika organisationer kan arbeta. I sådana fall kommer man vid behov överens om nivån på den fysiska säkerheten i förväg så att lokalerna möjliggör korrekt behandling och förvaring av sekretessbelagda uppgifter på ett sätt som beaktar behoven av varje organisation. Väsentligt i dessa fall är att den som behandlar uppgifter bär ansvaret för att behandla uppgifterna på så sätt att ingen som inte har rätt att komma åt uppgifterna kan få tillgång till dem.

Exempel på genomförande	Skydd på flera nivåer bildas av administrativa, funktionella och fysiska metoder, såsom: a) strukturella barriärer: ett fysiskt hinder med vilket säkerhetsområdena och de omgivande lokalerna avgränsas och olovligt intrång försvåras och fördröjs, b) passerkontroll: med passerkontroll begränsar man tillträde till säkerhetsområden och omgivande lokaler. Målet är att upptäcka obehöriga tillträdesförsök, förhindra att obehöriga får tillträde och kontrollera vem som rör sig i området. Passerkontroll kan riktas mot ett område, en eller flera byggnader i 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. Även bevakningspersonalen, receptionisten eller den egna personalen kan delta i kontrollerna. c) intrångsdetekteringssystem: ett system för att upptäcka intrång (inbrottslarm) kan användas till att förbättra den säkerhetsnivå som strukturella barriärer ger. Systemet kan också användas i stället för bevakningspersonal eller för att bistå denna. d) bevakningspersonal: bevakningspersonal som är utbildad, under tillsyn, utrustad och vid behov säkerhetsutredd på lämpligt sätt kan sättas in bland annat för att bistå passerkontrollen och för att upptäcka och förhindra personer med planer på intrång i säkerhetsområdet eller de omgivande lokalerna. e) kameraövervakning: kameraövervakning kan användas i säkerhetsområdet eller i dess omgivning särskilt till att förebygga olaglig underrättelse och till att förebygga incidenter, kontrollera larm och utreda incidenter. Bevakningspersonal kan använda kameraövervakningen för aktiv bildövervakning i realtid eller för passiv analys av bildmaterial i efterhand. f) 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 system. g) belysning: en eventuell inkräktare kan upptäckas med hjälp av belysning och bevakningspersonalen kan effektivt övervaka området antingen direkt eller indirekt via ett kameraövervakningssystem. h) andra lämpliga fysiska åtgärder vars syfte är att avskräcka från och upptäcka obehörigt tillträde eller förhindra att säkerhetsklassificerade uppgifter går förlorade eller skadas.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; Säkerhetsklassificeringsförordningen 7 §
Referenser	Katakri: F-03
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 33; ISO/IEC 27002:2022 7.1, 7.2, 7.3

Identifierare	FYY-03, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Behandling av uppgifter
Krav	Uppgifter ska behandlas så att åtkomst till dem skyddas från utomstående.
Allmän beskrivning	Med förhindrande avses skydd av uppgifter både från personer som inte har behov att ta del av uppgifterna i fråga (need-to-know) och från olaglig underrättelse. Skydd innebär i praktiken till exempel att man hindrar personer från att direkt se eller höra säkerhetsklassificerad information. Behandling av säkerhetsklassificerade uppgifter i säkerhetsområdena (administrativt område eller skyddsområde) är huvudregeln, men i vissa situationer – såsom vid distansarbete eller arbetsuppgifter utanför säkerhetsområdena – måste informationen även behandlas utanför de fastställda säkerhetsområdena. Uppgifter kan behandlas både i pappersformat och via terminaler som uppfyller kraven i skyddsområden, administrativa områden eller utanför dessa med den förutsättningen att åtkomst till uppgifterna har skyddats från utomstående. Behandling är tillåten upp till klass TL II, dock så att datalager som innehåller handlingar i säkerhetsklass II eller III och informationssystem som används för att behandla dessa handlingar ska placeras i ett skyddsområde.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 10 §
Referenser	Julkri: HAL-19; Katakri: F-04
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 29
Identifierare	**FYY-03.1, L:TL I, E:, S:, TS:**
Namn	Behandling av uppgifter – TL I
Krav	Handlingar inom säkerhetsklass I får behandlas endast i ett skyddsområde.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § 2 mom.
Referenser	Julkri: HAL-19; Katakri: F-04
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 29
Identifierare	**FYY-04, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter**
Namn	Lagring av uppgifter
Krav	Uppgifter ska förvaras så att åtkomst till dem skyddas från utomstående.
Allmän beskrivning	Skydd innebär i praktiken till exempel att uppgifterna eller en terminal som innehåller information förvaras på ett tillräckligt säkert sätt. I behandlingen av uppgifter ska man dessutom beakta verksamheten under pauser i arbetet då handlingarna och terminalerna ska placeras enligt säkerhetsklass i ett lämpligt säkerhetsområde och/eller i en förvaringsenhet för den tid man inte arbetar med dem. Med förvaring av uppgifter hänvisar man till en situation där den som behandlar uppgifterna inte övervakar informationen direkt.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 10 §
Referenser	Julkri: HAL-19; Katakri: F-04
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 28–29

Identifierare	FYY-04.1, L:TL IV, E:, S:, TS:
Namn	Förvaring av uppgifter – TL IV
Krav	Organisationen förvarar pappershandlingar och andra uppgifter som inte är i elektroniskt format – på ett skyddsområde eller administrativt område i kontorsmöbler som anses vara lämpliga för användningsändamålet eller – tillfälligt utanför säkerhetsområdena om den som behandlar uppgifterna har förbundit sig till att följa de ersättande åtgärder som fastställts i säkerhetsanvisningarna. – Organisationen förvarar uppgifter som är i elektroniskt format – på ett skyddsområde eller administrativt område i utrustning eller elektroniska datamedier som uppfyller kraven eller – utanför säkerhetsområdena i terminaler eller elektroniska datamedier som uppfyller kraven och som är placerade i en övervakad lokal eller i en lämplig, låst kontorsmöbel i en säkerhetspåse eller på motsvarande sätt.
Allmän beskrivning	
Exempel på genomförande	Om området saknar en förvaringslösning som anses adekvat för informationen, bör områdets väggar, golv, tak, fönster och dörrar uppnå minst ett skydd som motsvarar kategori RC3 i standarden SFS-EN-1627. Om en låst kontorsmöbel används som förvaringsenhet för den säkerhetsklassificerade informationen ska man säkerställa att intrång lämnar efter sig spår av inbrott.
Lagstiftning	Säkerhetsklassificeringsförordningen 10 §
Referenser	Katakri: F-04
Övrig tilläggsinformation	

Identifierare	FYY-04.2, L:TL IV, E:, S:, TS:
Namn	Förvaring av uppgifter – Datalager och informationssystem – TL IV
Krav	Datalager som innehåller handlingar i säkerhetsklass IV och informationssystem som används för att behandla dessa handlingar ska placeras i ett säkerhetsområde (administrativt område eller skyddsområde).
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § 3 mom. 3 punkten
Referenser	Julkri: HAL-19; Katakri: F-04
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 28–29

Identifierare	FYY-04.3, L:TL III, E:, S:, TS:
Namn	Förvaring av uppgifter – Datalager och informationssystem – TL III
Krav	Datalager som innehåller handlingar i säkerhetsklass II eller III och informationssystem som används för att behandla dessa handlingar ska placeras i ett skyddsområde.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § 3 mom. 2 punkten
Referenser	Julkri: HAL-19; Katakri: F-04
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 28–29

Identifierare	FYY-04.4, L:TL III, E:, S:, TS:
Namn	Förvaring av uppgifter – TL III
Krav	Organisationen förvarar pappershandlingar och andra uppgifter som inte är i elektroniskt format i ett skyddsområde i en förvaringslösning som bedömts vara lämplig. Organisationen förvarar uppgifter som är i elektroniskt format – på ett skyddsområde i utrustning eller elektroniska datamedier som uppfyller kraven eller – utanför skyddsområdena i en terminal som uppfyller kraven och som är placerad i en övervakad lokal eller i en lämplig, låst kontorsmöbel i en säkerhetspåse eller på motsvarande sätt.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 §
Referenser	Katakri: F-04
Övrig tilläggsinformation	

Identifierare	FYY-04.5, L:TL II, E:, S:, TS:
Namn	Förvaring av uppgifter – TL II
Krav	Organisationen förvarar pappershandlingar och andra uppgifter som inte är i elektroniskt format i ett skyddsområde i en förvaringslösning som bedömts vara lämplig. Organisationen förvarar uppgifter som är i elektroniskt format i ett skyddsområde i utrustning eller elektroniska datamedier som uppfyller kraven.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 §
Referenser	Katakri: F-04
Övrig tilläggsinformation	

Identifierare	FYY-04.6, L:TL I, E:, S:, TS:
Namn	Förvaring av uppgifter – TL I
Krav	Handlingar inom säkerhetsklass I får förvaras endast i ett skyddsområde.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § 2 mom.
Referenser	Julkri: HAL-19; Katakri: F-04
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 29

Identifierare	FYY-05, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Säkerhetsområde
Krav	Säkerhetsområden, det vill säga administrativa områden och skyddsområden, ska följa rekommendationerna i detta kriterium.
Allmän beskrivning	Många rekommendationer om fysisk säkerhet är gemensamma för både administrativa områden och skyddsområden. Detta kriterium innehåller de gemensamma rekommendationer som ska beaktas i bedömningen av såväl administrativa områden som skyddsområden.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 9 §
Referenser	Katakri: F-05.4, F-06.6
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 39

Identifierare	FYY-05.1, L:TL IV, E:, S:, TS:
Namn	Säkerhetsområde – Ljudisolering
Krav	Områdets ljudisolering ska göra det omöjligt för obehöriga att tydligt uppfatta diskussioner om skyddade uppgifter. Det ska också finnas ljudisolering inom området om man där diskuterar skyddade uppgifter som alla inte behöver ta del av.
Allmän beskrivning	Med förhindrande avses skydd av uppgifter både från personer som inte har behov att ta del av uppgifterna som diskuteras och från olaglig underrättelse. Kravet på ljudisolering gäller endast de lokaler i området där skyddade uppgifter diskuteras. Ljudisolering kan bedömas till exempel genom att lyssna på diskussionen utanför lokalen vid dörrar, väggar, ventilationskanaler och andra genomgående hål. Ljudisoleringen i lokalen kan vid behov också jämföras med det krav på luftljudsisolering som gäller för strukturerna.
Exempel på genomförande	Kravet kan definieras i enlighet med standarden SFS-EN-ISO 717-1. Luftljudsisoleringen kan konstateras med en mätning som utförs i enlighet med standarden SFS-EN-ISO 16283-1. I bedömningen ska man utöver luftljudsisoleringen även beakta stomljudisolering. Kravet på ljudisolering kan vid behov uppfyllas till exempel med att omplacera lokalen, förbättra strukturernas och de genomgående hålens isolering eller med bakgrundsbrus i lokalerna utanför den lokal som bedöms.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 10 § 1 mom.
Referenser	Katakri: F-05.4, F-06.6
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 39

Identifierare	FYY-05.2, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Säkerhetsområde – Åtgärder mot tjuvtittande
Krav	Om det finns en risk för avsiktligt eller oavsiktligt tjuvtittande på uppgifter ska lämpliga åtgärder vidtas för att avvärja risken.
Allmän beskrivning	
Exempel på genomförande	Risken för tjuvtittande kan reduceras till exempel genom arbetsplatsernas placering och avskärmning samt persienner, gardiner eller skydd för datorskärmar.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 10 § 1 mom.
Referenser	Julkri: HAL-19; Katakri: F-05.6, F-06.8
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sidorna 40 och 45
Identifierare	**FYY-05.3, L:TL II, E:, S:, TS:**
Namn	Säkerhetsområde – Inspektioner av lokaler och utrustning
Krav	Organisationen ska inspektera alla elektroniska apparater innan de används inom ett område där uppgifter i säkerhetsklass II behandlas om hotnivån bedöms som hög. Även 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.
Allmän beskrivning	Om det inte är möjligt att tillförlitligt inspektera berörda elektroniska apparater (till exempel mobiltelefoner, smartklockor osv.) ska de lämnas utanför lokalerna, exempelvis i en förvaringslösning för detta ändamål.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 7 §, 10 § 1 mom., 11 § 2 mom.
Referenser	Katakri: F-05.7, F-06.9
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sidorna 40 och 46

Identifierare	FYY-05.4, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Säkerhetsområde – Förfarandena i behörighets- och nyckelhanteringen
Krav	Organisationen ska fastställa förfarandena och rollerna i behörighets- och nyckelhanteringen för området.
Allmän beskrivning	Tillträdet till området kan begränsas med mekaniska eller elektroniska metoder eller genom personigenkänning. Det ska utses en områdesansvarig som hanterar förfarandena vad gäller behörigheter och nyckelhantering. Områdets reservnycklar förvaras säkert i ett förseglat förvaringskuvert som försetts med datum för förseglingen och kvittering eller alternativt i ett nyckelskåp i anslutning till passerkontrollen. Nycklarna överlämnas för arbetsuppgifter och mot kvittering. Förfarandet beskrivs säkerhetshanteringsanvisningarna. Det ska inte vara möjligt att komma in på området med en huvudnyckel som ger tillgång till en lokal som hör till en lägre klass. Rekommendationen är att den utrustning och de system som inkluderas i helheten som flernivåskyddet bildar följer europeiska standarder och deras minimikrav. Standarder som kan användas som referens vid bedömning av en lämplig lösning: Lås med hylsa: SFS 7020+5970, klasserna 1–4, målnivå 3; Elektroniska passersystem: SFS-EN 60839-11-1 och 2. Observera till exempel kraven i standarden SFS-EN 50131 om passersystemet är en del av intrångsdetekteringssystemet.
Exempel på genomförande	Man har utsett en områdesansvarig som hanterar följande förfaranden vad gäller behörigheter och nyckelhantering: – 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. – grunden för överlämnande av nycklar antecknas i en handling. – nycklarna överlämnas endast till personer som fått självständig tillträdesrätt till området. – ändringar i personalen överförs vid behov till nyckelhanteringsrätten.
Lagstiftning	Informationshanteringslagen 15 § 2 mom.; säkerhetsklassificeringsförordningen 9 §
Referenser	Katakri: F-05.2, F-06.3
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sidorna 39 och 44; ISO/IEC 27002:2022 7.2

Identifierare	FYY-05.5, L:TL IV, E:, S:, TS:
Namn	Säkerhetsområde – Besökare
Krav	Personer som inte har auktoriserats på behörigt sätt av organisationen (besökare) ska alltid ha en följeslagare.
Allmän beskrivning	Värden ska ha självständig tillträdesrätt till säkerhetsområdet som hen tar besökarna och rätt att vara värd för besökare. Med besöksförfaranden ska man säkerställa att besöket inte äventyrar konfidentialiteten av de uppgifter som behandlas eller förvaras i området. Serviceåtgärder inom området genomförs endast av personer som fått självständig tillträdesrätt till området eller i sådana personers övervakning. Behandling av uppgifter i området under service, installation och städning är förbjudet om det finns en risk för att personalen som genomför ovan nämnda åtgärder får kännedom om skyddade uppgifter. Det är möjligt att godkänna besök utan följeslagare (unescorted visitor) för de besökare i området som uppfyller kraven gällande beviljande av tillträdesrätt.

Exempel på genomförande	Organisationen har godkänt riktlinjer som gäller besökare. Besöksinstruktionerna kan omfatta bland annat följande: – Besökaren identifieras och förses med en besökarbricka. – Besöket registreras. – Besökare ska inte släppas in eller lämnas i områdena utan tillsyn, och 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. – Personalen har fått anvisningar om hur man ska reagera på personer som rör sig utan namnskylt.
Lagstiftning	Säkerhetsklassificeringsförordningen 9 §
Referenser	Katakri: F-05.3, F-06.4
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sidorna 39 och 44
Identifierare	**FYY-06, L:Sekretessbelagd, E:, S:, TS:**
Namn	Administrativt område
Krav	Det administrativa området ska uppfylla de rekommendationer som presenteras i detta avsnitt och de riskbaserat bedömda preciseringarna så att skyddsåtgärdernas mål uppnås.
Allmän beskrivning	Datalager som innehåller sekretessbelagda uppgifter och handlingar samt de informationssystem som används till att behandla dessa ska placeras i ett skyddat område som myndigheten har fastställt för detta ändamål. Ett sådant område kan till exempel utgöras av ett administrativt område som beskrivs i säkerhetsklassificeringsförordningen. Om de inte placeras i ett sådant område ska uppgifterna skyddas riskbaserat med andra skyddskontroller. Med ett administrativt område avses områden och lokaler som är avsedda för normalt arbete, såsom en kontorslokal eller en helhet som bildas av flera olika kontorslokaler. Det administrativa området ska uppfylla de minimikrav som presenteras i detta avsnitt. Utöver minimikraven ska man planera, genomföra, upprätthålla och fördela ansvar gällande övriga riskhanteringsåtgärder som grundar sig på riskbedömning och principen om flernivåskydd. Detta ska göras på så sätt att den kvarstående risken som riktas mot säkerhetsklassificerade uppgifter kan godkännas och skyddsåtgärdernas mål uppnås. Dessutom ska det administrativa området uppfylla samtliga gemensamma krav som gäller säkerhetsområden. Dessa beskrivs i kriteriet ”Säkerhetsområde”.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 9 §
Referenser	Julkri: FYY-05; Katakri: F-05
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 38

Identifierare	FYY-06.1, L:TL IV, E:, S:, TS:
Namn	Administrativt område – områdets gränser och strukturer
Krav	Området ska ha tydligt bestämda synliga gränser men det ställs inga specifika krav på den områdesavgränsande konstruktionen (väggar, dörrar, fönster, golv- och takkonstruktioner).
Allmän beskrivning	Målet med de fysiska skyddsåtgärderna ska uppnås innan säkerhetsområdena kan godkännas. Strukturerna i området kan vara vanliga kontorsstrukturer. Strukturerna som avgränsar området ska förstärkas om säkerhetsklassificerade uppgifter förvaras där och inbrottsrisken anses sannolik. Dessa förstärkningar ska bedömas i förhållande till det övriga skyddet som de omgivande lokalerna erbjuder och bevakningspersonalens responstid. Med tanke på ändamålsenlig passerkontroll ska det vara möjligt att låsa eller stänga alla öppningar till området som inte används för in- och utpassering. Om ett mekaniskt lås har använts vid det administrativa områdets gränser bör kopieringen av nycklarna till låset förhindras med patentskydd. Om möjligt får utrymningsvägar inte gå genom skyddsområdet. Rekommendationen är att de lösningar som inkluderas i helheten som flernivåskyddet bildar följer europeiska standarder och deras minimikrav.
Exempel på genomförande	Standarder som kan användas som referens vid bedömning av strukturer som avgränsar området: Väggar, dörrar och golv- och takkonstruktioner: SFS-EN 1627, RC1–RC6; Fönster (skyddsglas): SFS-EN 356, P4A-P5A och P6B-P8B
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 9 § 1 mom. 1 punkten
Referenser	Katakri: F-05.1
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 39

Identifierare	FYY-06.2, L:TL IV, E:, S:, TS:
Namn	Administrativt område – passerkontroll
Krav	Tillträde till området ska övervakas om detta utifrån riskbedömningen är ändamålsenligt.
Allmän beskrivning	Passerkontroll kan vara ändamålsenligt till exempel om man i området behandlar uppgifter från säkerhetsklass III eller högre.
Exempel på genomförande	Rekommendation om genomförande av passerkontroll: – Organisationen använder identitetskort med bild eller motsvarande synliga identifierare. – Personen har endast den passagerätt som hen behöver för att utföra sina arbetsuppgifter. – Grunden för beviljande av passagerätt antecknas i en handling och endast utsedda personer har passagerätt till området. – Ändringar i personalen förmedlas vid behov till passagerätten. – Hanteringen av passersystemet kan vara utkontrakterad om detta förvaltas väl.
Lagstiftning	Säkerhetsklassificeringsförordningen 7 §, 9 §
Referenser	Katakri: F-05.2
Övrig tilläggsinformation	

Identifierare	FYY-06.3, L:Sekretessbelagd, E:, S:, TS:
Namn	Administrativt område – beviljande av rätt till tillträde
Krav	Endast personer som auktoriserats på behörigt sätt har självständigt tillträde till området. Självständigt tillträde till området kan beviljas av organisationen som ansvarar för uppgifterna eller med avtalade förfaranden av tjänsteproducenten som ansvarar för hanteringen av den fysiska lokalen, till exempel molntjänsteleverantören.
Allmän beskrivning	Tillträdet till området kan begränsas med mekaniska eller elektroniska metoder eller genom personigenkänning.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 9 §
Referenser	Julkri: FYY-05.4; Katakri: F-05.2
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 39, PiTuKri FT-03
Identifierare	**FYY-06.4, L:TL IV, E:, S:, TS:**
Namn	Administrativt område – intrångsdetekteringssystem
Krav	Vid behov kan ett intrångsdetekteringssystem användas som en kompletterande riskhanteringsmetod inom flernivåskyddet.
Allmän beskrivning	Området eller dörrarna till området kan förses med ett intrångsdetekteringssystem (inbrottslarm) om säkerhetsklassificerade uppgifter förvaras i området i låsbara kontorsmöbler och inbrottsrisken anses sannolik. Området eller ingångarna till området kan förses med ett intrångsdetekteringssystem (inbrottslarm) om säkerhetsklassificerade uppgifter förvaras i området och inbrottsrisken anses sannolik. Vid bedömningen av områdets eventuella intrångsdetekteringssystem eller ersättande arrangemang ska man beakta bedömningen av responstid som behandlats i samband med kravet gällande områdets strukturer. Om området övervakas med ett intrångsdetekteringssystem rekommenderas övervakning med hjälp av systemet när ingen arbetar i området. Intrångsdetekteringssystemet bör placeras inom säkerhetsområdet som systemet skyddar.
Exempel på genomförande	Rekommendationen är att den utrustning och de system som inkluderas i helheten som flernivåskyddet bildar följer europeiska standarder och deras minimikrav. Standarder som kan användas som referens vid bedömning av en lämplig lösning: Intrångsdetekteringssystem: SFS-EN 50131 klasserna 1–4, målnivå 2; Intrångsdetekteringssystemets larmöverföring: SFS-EN 50136-1 klasserna DP1–DP4 och SP5–SP6; Bevakningsföretagets larmcentral: SFS-EN 50518
Lagstiftning	Säkerhetsklassificeringsförordningen 7 §
Referenser	Katakri: F-05.5
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 40

Identifierare	FYY-07, L:TL III, E:, S:, TS:
Namn	Skyddsområde
Krav	Skyddsområdet ska uppfylla de rekommendationer som presenteras i detta avsnitt och de riskbaserat bedömda ytterligare preciseringarna så att flernivåskyddets mål uppnås.
Allmän beskrivning	Med skyddsområde avses områden och lokaler där säkerhetsklassificerade uppgifter behandlas och förvaras och som är avsedda för organisationens arbete och är bättre skyddade än de administrativa områdena. Ett skyddsområde kan tillfälligt grundas inom ett administrativt område för ett säkerhetsklassificerat möte eller något annat liknande ändamål. Skyddsområdet ska uppfylla de rekommendationer som presenteras i detta avsnitt. Utöver rekommendationerna ska man planera, genomföra, upprätthålla och fördela ansvar gällande övriga riskhanteringsåtgärder som grundar sig på riskbedömning och principen om flernivåskydd. Detta ska göras på så sätt att den kvarstående risken som riktas mot säkerhetsklassificerade uppgifter kan godkännas och flernivåskyddets mål uppnås. Dessutom ska skyddsområdet beakta samtliga gemensamma rekommendationer som gäller säkerhetsområden. Dessa beskrivs i kriteriet ”Säkerhetsområde”.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 7 §, 9 §
Referenser	Julkri: FYY-05; Katakri: F-06
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 43
Identifierare	**FYY-07.1, L:TL III, E:, S:, TS:**
Namn	Skyddsområde – områdets gräns och strukturer
Krav	Området ska ha tydligt bestämda synliga gränser. Om området saknar en förvaringslösning som anses adekvat för informationen, ska områdets väggar, golv, tak, fönster och dörrar hålla den säkerhetsnivå som förvaringen förutsätter.
Allmän beskrivning	Med tanke på tillförlitlig passerkontroll ska det vara möjligt att låsa eller stänga alla öppningar till området som inte används för in- och utpassering med galler eventuellt av stål. Öppningar ska övervakas med intrångsdetekteringssystem om området inte har tjänstgörande personal dygnet runt eller om lokalerna inte inspekteras vid den normala arbetstidens slut och slumpvis utanför arbetstid. Strukturerna i området ska förstärkas om säkerhetsklassificerade uppgifter förvaras där och inbrottsrisken anses sannolik. Områdets gränser och strukturer ska då vara av betong, stål, tegel eller starkt trä. Bristfälliga strukturer, såsom normala kontorsstrukturer, ska förstärkas. Det ska inte vara möjligt att lösgöra väggelement som hela från utanför lokalen. Dessa förstärkningar ska bedömas i förhållande till det övriga skyddet som de omgivande lokalerna erbjuder och bevakningspersonalens responstid. Då dörrarnas strukturer kontrolleras ska man fästa uppmärksamhet vid karmens struktur, mellanrummet mellan dörren och karmen och hur karmarna fästs i väggstrukturen. Om området saknar en förvaringslösning som anses adekvat för informationen, bör områdets väggar, golv, tak, fönster och dörrar uppnå minst ett skydd som motsvarar kategori RC3 i standarden SFS-EN-1627. Skyddsglaset ska i första hand monteras som en del av den normala fönsterstrukturen. Lösningar som installeras i efterhand ska undvikas. Utrymningsvägar får inte gå genom skyddsområdet. Om det är nödvändigt för utrymningsvägen att gå genom skyddsområdet ska man säkerställa att den utrustats med ett intrångsdetekteringssystem. Ett skyddsområde med en utrymningsväg som går genom området kan inte godkännas om inträde till skyddsområdet i praktiken innebär direkt åtkomst till säkerhetsklassificerade uppgifter som förvaras där eller om området inte har en förvaringslösning som bedömts vara adekvat för förvaring av information.

Exempel på genomförande	Väggar, dörrar och golv- och takkonstruktioner: SFS-EN 1627, RC1–RC6, målnivå RC3; Fönster (skyddsglas): SFS-EN 356, P4A-P5A och P6B-P8B, målnivå P5A
Lagstiftning	Säkerhetsklassificeringsförordningen 9 § 1 mom. 2 punkten
Referenser	Katakri: F-06.1
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 43
Identifierare	**FYY-07.2, L:TL III, E:, S:, TS:**
Namn	Skyddsområde – passerkontroll
Krav	All in- och utpassering vid områdesgränsen ska kontrolleras genom att personerna har passerkort eller identifieras personligen.
Allmän beskrivning	Passerkontrollen kan utföras elektroniskt eller bygga på personlig identifiering. Dubbelsidig passerkontroll kan användas vid områdets gräns. Rekommendationen är att man använder tvåstegsverifiering vid in- och/eller utpassering. Fjärråtkomst till passersystemet och installation av läsare ska genomföras utgående från riskbedömningen på ett tillräckligt datasäkert sätt så att systemet endast är tillgängligt via auktoriserade terminaler och nät. Dessutom ska dataförbindelsen och passersystemets gränssnitt vara skyddade så att utomstående inte har tillgång till de överförda uppgifterna. Passersystemet bör placeras inom säkerhetsområdet som systemet skyddar.
Exempel på genomförande	Rekommendation om genomförande av passerkontroll: – Organisationen använder identitetskort med bild eller motsvarande synliga identifierare. – Passagerätt till skyddsområdet beviljas av en utsedd ansvarsperson i organisationen. – Anvisningar har getts om förfaringssätten i systemet för hantering av passerkontrollen och sätten har dokumenterats. • En handling utarbetas av beviljade passagerätter. Handlingen upprätthålls av en utsedd ansvarsperson. • Personen har endast den passagerätt som hen behöver för att utföra sina arbetsuppgifter. • Grunden för beviljande av passagerätt antecknas i en handling och endast utsedda personer har passagerätt till området. • Ändringar i personalen förmedlas vid behov till passagerätten. • Förteckningar över organisationens personal och utomstående personer hålls separat från varandra. • Passagerätten granskas med regelbundna mellanrum, till exempel var sjätte månad, av en ansvarig person som utsetts från organisationen. • Hanteringen av passersystemet kan vara utkontrakterad om detta förvaltas väl. • Det ska inte vara möjligt att öppna en dörr till skyddsområdet från en basanvändares arbetsstation. – Endast behöriga personer har passagerätt till skyddsområdet. Inpasseringar till området ska kunna verifieras efteråt. – Inpasseringar till lokalen ska kunna verifieras efteråt. – Identifierarna ska använda modern och krypterad läsningsteknik eller förutsätta tvåstegsverifiering. Rekommendationen är att den utrustning och de system som inkluderas i helheten som flernivåskyddet bildar följer europeiska standarder och deras minimikrav: Elektroniska passersystem: SFS-EN 60839-11-1 och 2, klasserna 1–4. Kameraövervakningssystem: SFS-EN 62676, planerad i enlighet med Finanssialas K-metod. Tiden för förvaringen av kameraövervakningssystemets inspelningar fastställs riskbaserat i enlighet med organisationens förmåga att upptäcka avvikelser och med beaktande av förebyggande och reagerande förfaranden. Den rekommenderade minimitiden för inspelningar är 1 månad. Dessutom kan kameraövervakningssystemet kopplas till intrångsdetekteringssystemet.
Lagstiftning	Säkerhetsklassificeringsförordningen 9 § 1 mom. 2 punkten
Referenser	Katakri: F-06.2
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 43

Identifierare	FYY-07.3, L:TL III, E:, S:, TS:
Namn	Skyddsområde – beviljande av rätt till tillträde
Krav	Självständig tillträdesrätt till området kan endast beviljas personer som på behörigt sätt auktoriserats av organisationen, vilkas pålitlighet har fastställts och som har ett särskilt tillstånd att få komma in på området.
Allmän beskrivning	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.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 9 § 1 mom. 2 punkten
Referenser	Julkri: FYY-05.4; Katakri: F-06.3
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 44

Identifierare	FYY-07.4, L:TL III, E:, S:, TS:
Namn	Skyddsområde – Besökare
Krav	Följande krav gäller om inträde till skyddsområdet i praktiken innebär direkt åtkomst till säkerhetsklassificerade uppgifter som förvaras där: – den högsta säkerhetsklassen för uppgifter som normalt förvaras i området ska anges tydligt och – varje besökare ska ha ett särskilt tillstånd att komma till området, de ska alltid ha en följeslagare och deras pålitlighet ska vara på ett lämpligt sätt säkerställt, utom om det har säkerställts att besökare inte har åtkomst till säkerhetsklassificerade uppgifter.
Allmän beskrivning	Kriteriet kompletterar kriteriet ”Säkerhetsområde – Besökare” som gäller alla säkerhetsområden.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 9 § 1 mom. 2 punkten, 10 § 1 mom.
Referenser	Julkri: FYY-05.5; Katakri: F-06.4
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 44

Identifierare	FYY-07.5, L:TL III, E:, S:, TS:
Namn	Skyddsområde – säkerhetsanvisningar
Krav	För varje skyddsområde ska det tas fram anvisningar om säkerhetsförfaranden i området.
Allmän beskrivning	Säkerhetsanvisningarna täcker processer och säkerhetsområden förknippade med säkerhetsklassificerade uppgifter för uppgifternas hela livscykel. Efterlevnaden av säkerhetsanvisningarna övervakas och anvisningarnas förändringsbehov bedöms regelbundet. Säkerhetsanvisningarnas aktualitet och förankring säkerställs regelbundet, minst en gång om året.
Exempel på genomförande	För varje skyddsområde ska det tas fram säkerhetsförfaranden med anvisningar om följande: a) Förvaring och behandling av uppgifter i området: säkerhetsklassen för de uppgifter som får behandlas och förvaras i området. b) Övervaknings- och skyddsåtgärder som tillämpas. c) Beviljande av tillträdesrätt till området: personer som har tillträde till området utan följeslagare grundat på särskilt tillstånd och fastställd pålitlighet. d) Besökare: vid behov förfaranden för användning av följeslagare eller skydd av säkerhetsklassificerade uppgifter när andra personer beviljas tillträde till området. e) Övriga relevanta åtgärder och förfaranden.
Lagstiftning	Informationshanteringslagen 4 § 2 mom.; säkerhetsklassificeringsförordningen 10 § 1 mom.
Referenser	Julkri: HAL-12; Katakri: F-06.5
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 45

Identifierare	FYY-07.6, L:TL III, E:, S:, TS:
Namn	Skyddsområde – intrångsdetekteringssystem
Krav	Områden som inte har tjänstgörande personal dygnet runt ska efter behov inspekteras vid den normala arbetstidens slut och slumpvis utanför arbetstid, utom när intrångsdetekteringssystem (inbrottslarm) har installerats i området.
Allmän beskrivning	Områdets gränser och strukturer (väggar, dörrar, fönster, golv- och takkonstruktioner) och/eller ingångarna till området kan förses med ett intrångsdetekteringssystem (inbrottslarm) om säkerhetsklassificerade uppgifter förvaras i området och inbrottsrisken anses sannolik. Vid bedömningen av områdets eventuella intrångsdetekteringssystem eller ersättande arrangemang ska man beakta bedömningen av responstid som behandlats i samband med kravet gällande områdets strukturer. Om området övervakas med ett intrångsdetekteringssystem rekommenderas övervakning med hjälp av systemet när ingen arbetar i området. Larmöverföringen bör genomföras övervakat eller som två anslutningar. Med hjälp av larmöverföringsapparaten ska man överföra minst följande uppgifter till bevakningsföretaget eller någon annan säkerhetstjänst: inbrott, på/av, sabotage, fel. Systemet ska opereras med hjälp av en personlig kod. Fjärråtkomst till systemet och installation av reglage ska genomföras utgående från riskbedömningen på ett tillräckligt datasäkert sätt så att systemet endast är tillgängligt via auktoriserade terminaler och nät. Dessutom ska dataförbindelsen och intrångsdetekteringssystemets gränssnitt vara skyddade så att utomstående inte har tillgång till de överförda uppgifterna. Intrångsdetekteringssystemet bör placeras inom säkerhetsområdet som systemet skyddar. Organisationen ska ha kontroll över hanteringen av områdets intrångsdetekteringssystem. Hanteringen kan utkontrakteras utgående från riskbedömningen och uppgifternas differentiering. Förfarandena förknippade med hanteringen av systemet, systemets larm och responsverksamheten ska bedömas. Testningen av larmöverföringen (1 gång/månad) och responstiden (1 gång/år) ska vara regelbunden och dokumenteras. Bevakningspersonalen ska vara ändamålsenligt utbildad i att agera i området. Bevakningspersonalens kompetens och arbetsredskap ska vara adekvata i förhållande till riskerna i verksamhetsmiljön. Det kan förutsättas att två personer kommer till området samtidigt vid larm om inträde till skyddsområdet i praktiken innebär direkt åtkomst till säkerhetsklassificerade uppgifter som förvaras där eller om området inte har en förvaringslösning som bedömts vara adekvat för förvaring av information.
Exempel på genomförande	Rekommendationen är att den utrustning och de system som inkluderas i helheten som flernivåskyddet bildar följer europeiska standarder och deras minimikrav: Intrångsdetekteringssystem: SFS-EN 50131 klasserna 1–4, målnivå 3; Intrångsdetekteringssystemets larmöverföring: SFS-EN 50136-1, klasserna DP1–DP4 och SP5–SP6, målnivå DP3–DP4 (dual path) eller SP5–SP6 (single path); Bevakningsföretagets larmcentral: SFS-EN 50518. Företaget ska vara kompetent i enlighet med standarden och dessutom upprätthålla ett certifierat kvalitetshanteringssystem i enlighet med SFS-EN ISO 9001, eller anses motsvara standarden till tillämpliga delar.
Lagstiftning	Säkerhetsklassificeringsförordningen 7 §, 9 § 1 mom. 2 punkten
Referenser	Katakri: F-06.7
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 45

Identifierare	FYY-07.7, L:TL III, E:, S:, TS:
Namn	Skyddsområde – nycklar och lösenkoder till förvaringsenheter
Krav	Nycklar eller lösenkoder till förvaringsenheter innehas av sådana personer som har behov av att ta del av uppgifterna som förvaras i förvaringsenheten. Dessa personer ska memorera kombinationerna. Kombinationerna till förvaringslösningar som innehåller säkerhetsklassificerade uppgifter ska bytas ut – vid mottagande av ett nytt säkert förvaringsställe vad gäller fabrikskoderna. – vid varje byte av personal som känner till kombinationen. – vid inträffade eller misstänkta fall av röjande. – när ett lås har genomgått underhållsarbete eller reparation.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 8 §, 9 § 1 mom. 2 punkten, 10 § 1 mom.
Referenser	Katakri: F-06.10
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 46
Identifierare	**FYY-08, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter**
Namn	Transport av uppgifter
Krav	1. Uppgifterna ska transporteras enligt organisationens anvisningar som beaktar skyddet av uppgifterna i tillräckligt hög grad. 2. Uppgifterna ska förpackas så att de har skyddats från olovligt uppdagande. 3. Uppgifter får transporteras utanför säkerhetsområden om man skyddar de elektroniska datamedierna med tillräckligt säker kryptering. 4. Uppgifter som inte krypterats kan transporteras med hjälp av posttjänster.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; Säkerhetsklassificeringsförordningen 13 §
Referenser	Julkri: TEK-16, FYY-02; Katakri: F-08.1
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 26–28

Identifierare	FYY-08.1, L:TL IV, E:, S:, TS:
Namn	Transport av uppgifter – TL IV
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Vad gäller uppgifter i säkerhetsklass IV kan kravet uppfyllas på så sätt att man vidtar följande åtgärder: 1) Uppgifterna förpackas i ett slutet kuvert eller något motsvarande. Förpackningens ytterkuvert får inte ha anteckningar om säkerhetsklass, och förpackningen får inte utvärtes på annat sätt avslöja att den innehåller säkerhetsklassificerade uppgifter (kuvertet eller motsvarande ska inte vara genomskinligt). 2) Uppgifterna levereras i hemlandet som vanlig post, rekommenderat brev eller i enlighet med ett förfarande som godkänts för säkerhetsklassen i fråga. Till utlandet levereras uppgifterna med post endast med grund i myndighetens separata godkännande. 3) Endast godkänd personal ingår i behandlingskedjan för organisationens interna post. 4) Kraven har identifierats i organisationen och förfaranden för förmedling av specialskyddade uppgifter (till exempel krypteringsnycklar) har genomförts.
Lagstiftning	Säkerhetsklassificeringsförordningen 13 §
Referenser	Katakri: F-08.1
Övrig tilläggsinformation	

Identifierare	FYY-08.2, L:TL III, E:, S:, TS:
Namn	Transport av uppgifter – TL III
Krav	Okrypterad information i säkerhetsklass II–III ska för transportering förpackas på ett lämpligt sätt och övervakas hela tiden medan den transporteras till mottagaren. Nämnda uppgifter får också transporteras till mottagaren på något annat säkert sätt om uppgifternas konfidentialitet och integritet säkerställs enligt vad som säkerhetsklassen i fråga kräver.
Allmän beskrivning	
Exempel på genomförande	Vad gäller uppgifter i säkerhetsklass III kan kravet uppfyllas på så sätt att man dessutom vidtar följande åtgärder: 5) Uppgifterna förpackas i ett slutet, dubbelt kuvert eller något motsvarande. Förpackningens ytterkuvert får inte ha anteckningar om säkerhetsklass, och förpackningen får inte utvärtes på annat sätt avslöja att den innehåller säkerhetsklassificerade uppgifter (kuverten eller motsvarande får inte vara genomskinliga). 6) Uppgifterna levereras till mottagaren under ständig övervakning av en person från organisationen som är berättigad till den säkerhetsklassificerade informationen i fråga. Alternativt kan uppgifterna levereras i enlighet med ett förfarande som godkänts för säkerhetsklassen i fråga. 7) Endast godkänd och säkerhetsutredd personal ingår i behandlingskedjan för organisationens interna post.
Lagstiftning	Säkerhetsklassificeringsförordningen 13 §
Referenser	Katakri: F-08.1
Övrig tilläggsinformation	

Identifierare	FYY-08.3, L:TL II, E:, S:, TS:
Namn	Transport av uppgifter – TL II
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Vad gäller uppgifter i säkerhetsklass II kan kravet uppfyllas på så sätt att man dessutom vidtar följande åtgärder: 8) Uppgifterna förpackas i ett slutet, dubbelt kuvert eller något motsvarande. Förpackningens ytterkuvert får inte ha anteckningar om säkerhetsklass, och förpackningen får inte utvärtes på annat sätt avslöja att den innehåller säkerhetsklassificerade uppgifter (kuverten eller motsvarande får inte vara genomskinliga). Det inre kuvertet ska vara förseglat. Mottagaren ska ges anvisningar om att kontrollera att förseglingen är obruten och anmäla omedelbart om det finns misstanke om att förseglingen äventyrats.
Lagstiftning	Säkerhetsklassificeringsförordningen 13 §
Referenser	Katakri: F-08.1
Övrig tilläggsinformation	

Identifierare	FYY-09, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Kopiering av uppgifter
Krav	Skyddsåtgärder som gäller de ursprungliga uppgifterna tillämpas även på kopior och översättningar.
Allmän beskrivning	Skrivare och kopieringsmaskiner tolkas som informationssystem och de ska sålunda uppfylla kraven vad gäller teknisk, fysisk och administrativ informationssäkerhet. De tekniska kraven kan uppfyllas bland annat med separat utrustning.
Exempel på genomförande	Kravet kan uppfyllas på så sätt att man vidtar följande åtgärder: 1) Kopior behandlas på samma sätt som ursprungliga uppgifter. 2) Kopian kan överlåtas vidare endast till en person som har rätt att behandla uppgifterna och behov av informationsinnehållet. 3) Kopian/utskriften får endast tas med en maskin som uppfyller kraven på säkerhetsnivån i fråga.
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 2 § 2 mom.
Referenser	Katakri: F-08.2
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 28

Identifierare	FYY-09.1, L:TL II, E:, S:, TS:
Namn	Kopiering av uppgifter – TL II
Krav	Uppgifternas kopior och vem som behandlar dem ska förtecknas. Kopiering av uppgifter kräver tillstånd från myndigheten som utarbetat uppgifterna.
Allmän beskrivning	
Exempel på genomförande	Kravet kan uppfyllas på så sätt att man dessutom vidtar följande åtgärd: 4) Kopieringen och hanterarna införs i diarium/register eller förtecknas på annat motsvarande sätt.
Lagstiftning	Säkerhetsklassificeringsförordningen 14 § 1 mom. 3 och 4 punkten
Referenser	Katakri: F-08.2
Övrig tilläggsinformation	

Identifierare	FYY-10, L:TL III, E:, S:, TS:
Namn	Registrering av uppgifter
Krav	Mottagning och avsändning av uppgifter i säkerhetsklass III eller högre ska registreras. Behandling av uppgifter i säkerhetsklass III eller högre registreras i en elektronisk logg, ett informationssystem, ett ärendehanteringssystem, ett ärenderegister eller för kännedom (till exempel som en del av en handling).
Allmän beskrivning	Med registrering avses tillämpning av sådana förfaranden som används för att registrera uppgifternas livscykel, inklusive distribution och förstöring. Om det är fråga om ett informationssystem kan registreringen genomföras med hjälp av systemets egna processer. Praktiskt genomförande av registrering av uppgifternas livscykel förutsätter vanligen bland annat att man säkerställer att händelser kan spåras.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 14 § 1 mom. 1 och 2 punkten
Referenser	Katakri: F-08.3
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 19–23
Identifierare	**FYY-11, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter**
Namn	Fysisk förstöring av uppgifter
Krav	Förstöring av uppgifter som inte är i elektroniskt format har ordnats på ett tillförlitligt sätt. Man använder metoder som förhindrar att informationen helt eller delvis sammanställs på nytt.
Allmän beskrivning	Informationen måste skyddas ända till slutet av livscykeln. Detta ska beaktas i synnerhet då tredjepartstjänster används för att förstöra informationen. Det vanligaste förfaringssättet är att den organisation som ansvarar för informationen övervakar förstöringsprocessen till slutet av informationslivscykeln. Rekommendationen är att den utrustning och de system som inkluderas i helheten som flernivåskyddet bildar följer europeiska standarder och deras minimikrav. Vid användning av godkända storlekar på partiklar kan strimlingsavfall förstöras på samma sätt som vanligt kontorsavfall. Andra metoder som ersätter eller kompletterar strimlingsskyddet kan användas om metoden tillförlitligt förhindrar återskapande av uppgifterna (till exempel att bränna pappersstrimlor). Förstöring av elektroniskt material beskrivs separat i kriteriet TEK-21.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 21 §; säkerhetsklassificeringsförordningen 15 §
Referenser	Julkri: TEK-21; Katakri: F-08.4
Övrig tilläggsinformation	Rekommendation om behandling av säkerhetsklassificerade handlingar 2021:10 sid 29–31

Identifierare	FYY-11.1, L:TL IV, E:, S:, TS:
Namn	Fysisk förstöring av uppgifter – TL IV
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	– 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). – Högst 10 mm2 stora partiklar av optiska medier (DIN 66399 / O-5).
Lagstiftning	Säkerhetsklassificeringsförordningen 15 §
Referenser	Katakri: F-08.4
Övrig tilläggsinformation	

Identifierare	FYY-11.2, L:TL III, E:, S:, TS:
Namn	Fysisk förstöring av uppgifter – TL III
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	– 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). – Högst 5 mm2 stora partiklar av optiska medier (DIN 66399 / O-6).
Lagstiftning	Säkerhetsklassificeringsförordningen 15 §
Referenser	Katakri: F-08.4
Övrig tilläggsinformation	

Identifierare	FYY-11.3, L:TL II, E:, S:, TS:
Namn	Fysisk förstöring av uppgifter – TL II
Krav	Om uppgifterna har utarbetats av en annan myndighet ska denna myndighet anmälas om förstöringen av onödig information om informationen inte återlämnas till myndigheten i fråga. Uppgifterna får endast förstöras av en person som myndigheten utsett för detta. Beredningsskedets versioner kan förstöras av personen som utarbetat dem.
Allmän beskrivning	
Exempel på genomförande	– 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). – Högst 5 mm2 stora partiklar av optiska medier (DIN 66399 / O-6).
Lagstiftning	Säkerhetsklassificeringsförordningen 15 §
Referenser	Katakri: F-08.4
Övrig tilläggsinformation	

4 Teknisk säkerhet

Det tekniska delområdet omfattar kriterierna som är förknippade med informationssystemens och dataförbindelsernas tekniska egenskaper, säkra användning och verksamhetsmodeller. Kriterierna har som syfte att säkerställa att informationssystemen och deras användning uppfyller de allmänna kraven förknippade med teknisk informationssäkerhet och vid behov även med dataskydd. Det bör dock noteras att genomförandet av det tekniska delområdets kriterier i sig inte garanterar säkerheten av ett enskilt informationssystem, utan kriterierna för de övriga delområdena ska också beaktas.

Objekten som bedöms kan vara antingen enskilda informationssystem eller databehandlingsmiljöer eller flera informationssystem som bildar en större helhet. Vid bedömning av en helhet som består av flera informationssystem bör det beaktas att kraven uppfylls i varje enskilt system.

Det tekniska delområdet tar även i beaktande systemens placering i säkerhetsområdena och deras fjärranvändning utanför dessa områden. Närmare krav som gäller det administrativa området och skyddsområdet har fastställts i delområdet fysisk säkerhet.

I flera av kriterierna hänvisar man till att krypteringslösningen ska vara tillräckligt säker för användningsfallet i fråga. I bedömningen av krypteringslösningens säkerhet kan man utnyttja till exempel godkännanden som Cybersäkerhetscentrets NCSA-verksamhet beviljat för att skydda internationella säkerhetsklassificerade uppgifter. Ytterligare information finns på Cybersäkerhetscentrets webbplats.

Identifierare	TEK-01, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Nätets strukturella säkerhet
Krav	Databehandlingsmiljön har separerats från offentliga datanät och andra miljöer med lägre säkerhetsnivå på ett tillräckligt säkert sätt.
Allmän beskrivning	Avskiljning av informationssystem är en av de effektivaste faktorerna i skyddet av sekretessbelagda uppgifter. Målet med avskiljningen är att begränsa miljön där sekretessbelagda uppgifter behandlas till en helhet som kan kontrolleras och särskilt att kunna begränsa denna behandling till enbart sådana miljöer som är tillräckligt säkra. I en behandlingsmiljö i högre säkerhetsklass är det möjligt att även behandla uppgifter som hör till en lägre klass, med förutsättningen att behandlingen genomförs i sin helhet enligt de skydd som den högre säkerhetsklassen kräver. Avskiljningen kan genomföras till exempel med hjälp av en brandvägg. Internet, MPLS-nät som operatören erbjuder och till exempel så kallade svartfibrer (dark fiber) tolkas som offentliga nät.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 1 punkten
Referenser	Katakri: I-01
Övrig tilläggsinformation	Traficom: Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista (2.12.2021); ISO/IEC 27002:2022 8.20, 8.22; Informationshanteringsnämnden: Rekommendation om behandling av säkerhetsklassificerade handlingar (2020:19, kapitel 6); PiTuKri TT-01

Identifierare	TEK-01.1, L:Sekretessbelagd, E:Kritisk, S:, TS:Personuppgift
Namn	Nätets strukturella säkerhet – kryptering i allmänna datanät
Krav	Datatrafik som innehåller sekretessbelagda uppgifter krypteras i allmänna datanät med en lösning som inte har några kända sårbarheter och som enligt tillverkaren stöder modern krypteringsstyrka och moderna krypteringsinställningar. Alternativt kan överföringen genomföras med en skyddad dataförbindelse eller ett annat skyddat dataöverföringssätt.
Allmän beskrivning	Vid valet av krypteringsstyrka och -inställningar kan man i regel utnyttja styrkor och inställningar i enlighet med säkerhetsklass IV.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 14 §; Säkerhetsklassificeringsförordningen 12 § och 11 § 1 mom. 7 punkten
Referenser	Julkri: FYY-7.1; Katakri: I-01, I-12, I-15
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.24

Identifierare	TEK-01.2, L:Sekretessbelagd, E:Viktig, S:, TS:Särskild kategori av personuppgifter
Namn	Nätets strukturella säkerhet – brandvägg
Krav	Att koppla databehandlingsmiljön till miljöer på andra säkerhetsnivåer förutsätter användning av åtminstone brandväggar.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 1 och 2 punkten
Referenser	Katakri: I-01
Övrig tilläggsinformation	PiTuKri TT-01
Identifierare	**TEK-01.3, L:TL IV, E:, S:, TS:**
Namn	Nätets strukturella säkerhet – avskiljning av behandlingsmiljöer
Krav	Databehandlingsmiljön har avskilts från andra miljöer.
Allmän beskrivning	
Exempel på genomförande	Databehandlingsmiljöer för sekretessbelagda uppgifter som inte säkerhetsklassificerats och även miljöer med säkerhetsklass IV kan kopplas till miljöer med en annan säkerhetsklass med brandväggar och styrning av trafiken i säkerhetskritiska tjänster med lägre säkerhetsklass (webbsidor, routning av e-post via internet o.d.) via proxyservrar som filtrerar innehållet. Behandlingsmiljöer för sekretessbelagda uppgifter som inte säkerhetsklassificerats och även miljöer med säkerhetsklass IV kan anslutas till internet och andra icke betrodda nätverk under förutsättning att riskerna med anslutningen kan reduceras tillräckligt genom andra skydd. Att reducera riskerna förknippade med anslutning till internet för sekretessbelagda uppgifter som inte säkerhetsklassificerats och för säkerhetsklass IV förutsätter i synnerhet att man sköter programuppdateringarna, tillämpar principen om lägsta behörighet, minimerar systemets sårbarhetsyta och har förmåga att upptäcka incidenter och vidta korrigerande åtgärder. En vanlig behandlingsmiljö för sekretessbelagda uppgifter som inte säkerhetsklassificerats och/eller med säkerhetsklass IV är en begränsad del av organisationens databehandlingsmiljö som kan bildas till exempel av terminaltjänster, applikationstjänster, datatrafiktjänster och arrangemang förknippade med att skydda dessa.
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 1 och 2 punkten
Referenser	Katakri: I-01, I-06, I-08, I-11, I-19
Övrig tilläggsinformation	
Identifierare	**TEK-01.4, L:TL IV, E:, S:, TS:**
Namn	Nätets strukturella säkerhet – kryptering utanför skyddsområden
Krav	Trafik som lämnar ett kontrollerat fysiskt säkerhetsområde krypteras på ett tillräckligt säkert sätt.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Katakri: I-01
Övrig tilläggsinformation	

Identifierare	TEK-01.5, L:TL III, E:, S:, TS:
Namn	Nätets strukturella säkerhet – användningen av gatewaylösningar
Krav	Säkerhetsklasserna III–II: Koppling av en databehandlingsmiljö till miljöer med andra säkerhetsklasser förutsätter användningen av en tillräckligt säker gatewaylösning.
Allmän beskrivning	Databehandlingsmiljöer antas i princip vara icke betrodda till varandra även i situationer där man kopplar databehandlingsmiljöer som administreras av olika organisationer till varandra. Databehandlingsmiljöer med samma säkerhetsklass kan kopplas till varandra med hjälp av en krypteringslösning som är tillräckligt säker för säkerhetsklassen i fråga (till exempel sammankoppling av behandlingsmiljöer med samma säkerhetsklass i organisationens olika verksamhetsställen via det offentliga nätet). Obs. Att överskrida säkerhetsklassen vad gäller administrativ trafik förutsätter användning av en gatewaylösning som är tillräckligt säker för säkerhetsklassen i fråga. I praktiken begränsas den administrativa trafiken nästan utan undantag enligt säkerhetsklass. Skyddsprinciperna för administrativ trafik behandlas närmare i TEK-04.

Exempel på genomförande	Från och med säkerhetsklass III kan anslutningen till miljöer med olika säkerhetsklasser ske genom tillräckligt säkra gatewaylösningar. Lösningarna ska på ett tillförlitligt sätt hindra att uppgifter i en högre säkerhetsklass förmedlas till en miljö med lägre säkerhetsklass. Planeringsprinciperna och allmänna lösningsmodeller för säkra gatewaylösningar som kan godkännas beskrivs närmare på finska i Cybersäkerhetscentrets anvisning om gatewaylösningar (www.ncsa.fi > ”Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista”). Behandlingsmiljöer i säkerhetsklass III är helheter som isolerats i flera faser och på ett logiskt eller fysiskt sätt från icke betrodda nät/system. Med fysisk isolering avses avskiljning som sker på OSI-modellens fysiska lager. Behandlingsmiljöer med säkerhetsklass III kopplas i regel inte till andra nät eller system. Om slutanvändarens arbetsuppgifter förutsätter tillgång till internet eller andra system eller nät med olika säkerhetsklass, är det vanligen bäst att ordna detta på en separat dator som inte kopplas till ett nät med säkerhetsklass III. I vissa fall kan det vara möjligt att godkänna att även en behandlingsmiljö med säkerhetsklass III kopplas fysiskt till ett separat kontrollerat och godkänt nät eller system. Sådana separat godkända nät eller system delas vanligen in i fyra användningsfall: A. Dataöverföringssystem Ett system/nät med säkerhetsklass III kan vara ett dataöverföringssystem mellan två eller flera fysiska punkter. Då bör varje kopplad punkt vara på motsvarande säkerhetsnivå. Nätnivåns gränssnitt är vanligen av formen [fysiskt avskilt nät/fysiskt avskild arbetsstation] – [brandväggsutrustning/-program] – [krypteringsapparat som godkänts för säkerhetsklassen] – [brandväggsutrustning/-program] – [internet] – [brandväggsutrustning/-program] – [krypteringsapparat som godkänts för säkerhetsklassen] – [brandväggsutrustning/-program] – [fysiskt avskilt nät/fysiskt avskild arbetsstation]. Med motsvarande arrangemang kan man även genomföra lösningar i enlighet med säkerhetsklass II. B. Tjänstesystem Ett system/nät med säkerhetsklass III kan vara till exempel en databastjänsst som används från flera fysiska punkter. Nätnivåns gränssnitt är då likadan som i fall A. C. Gatewaylösningar C1. Uppgifter från en miljö med lägre säkerhetsklass kan överföras till en behandlingsmiljö för uppgifter i säkerhetsklass III via en gatewaylösning som tillåter enkelriktad kommunikation (till exempel datadioder). Med motsvarande arrangemang kan man även genomföra lösningar i enlighet med säkerhetsklass II. I kommunikation mellan säkerhetsklasserna IV och III kan man även utnyttja innehållsfiltrering som grundar sig på elementidentifiering (jfr punkt C2 nedan). C2. Uppgifter i en lägre säkerhetsklass kan överföras från en behandlingsmiljö för uppgifter i säkerhetsklass III till en miljö med lägre säkerhetsklass via innehållsfiltrering som grundar sig på elementidentifiering. Användningen av innehållsfiltrering förutsätter att informationen identifieras i en miljö på högre nivå och att endast uppgifter på lägre nivå får överföras från en miljö med högre säkerhetsklass till en miljö med lägre säkerhetsklass. D. Övriga behandlingsmiljöer Andra behandlingsmiljöer med säkerhetsklass III är vanligen organisationens produktutvecklingsnät eller andra behandlingsmiljöer för uppgifter i säkerhetsklass III. Till sådana system kan kopplas till exempel en uppdateringsserver som betjänar endast denna miljö. Centraliserad distribution av skyddsuppdateringar och signaturer som identifierar skadeprogram kan tillåtas från uppdateringsservern med vissa begränsningar. Uppdateringarna som distribueras och signaturbaserna kan flyttas till uppdateringsservern över ett luftgap eller alternativt till exempel genom en datadiod.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 1 och 2 punkten
Referenser	Julkri: TEK-04; Katakri: I-01
Övrig tilläggsinformation	

Identifierare	TEK-01.6, L:TL II, E:, S:, TS:
Namn	Nätets strukturella säkerhet – TL II behandling
Krav	Behandlingsmiljöer med säkerhetsklass II är i princip fysiskt avskilda helheter.
Allmän beskrivning	
Exempel på genomförande	Kommunikation som överskrider säkerhetsklassen kan tillåtas endast via datadioder eller motsvarande enkelriktade gatewaylösningar som fungerar med OSI-modellens fysiska lager.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 1 och 2 punkten
Referenser	Katakri: I-01
Övrig tilläggsinformation	

Identifierare	TEK-01.7, L:TL I, E:, S:, TS:
Namn	Nätets strukturella säkerhet – TL I behandling
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	I princip är rekommendationen att databehandlingsmiljöer med säkerhetsklass I hålls fysiskt isolerade från alla andra miljöer. Ett vanligt genomförandesätt är behandling av uppgifter med en terminal som reserverats för detta syfte inom ett fysiskt skyddsområde i en lokal som skyddats från diffus strålning och avskilts fysiskt från alla andra miljöer. Genomförandesättet kan också vara en databehandlingsmiljö som består av terminaler som fysiskt placerats i en lokal inom skyddsområdet som skyddats från diffus strålning och avskilts fysiskt från andra miljöer, ett lokalt nät som kopplar terminalerna till varandra och en separat skrivare som reserverats för detta syfte. Informationsöverföring till fysiskt avskilda miljöer ska genomföras så att risken att uppgifter i säkerhetsklass I hamnar i en miljö med lägre säkerhetsklass är så liten som möjligt. Ett vanligt genomförandesätt är utnyttjande av optiska medier för engångsbruk i informationsöverföringen från en miljö med lägre säkerhetsklass till en miljö med högre säkerhetsklass. Om det med tanke på de funktionella behoven är absolut nödvändigt att koppla en databehandlingsmiljö med säkerhetsklass I till en miljö med lägre säkerhetsklass, bör detta ske via en gatewaylösning som godkänts för säkerhetsklass I. Det finns ett begränsat antal gatewaylösningar som godkänts för avskiljning av databehandlingsmiljöer med säkerhetsklass I, med fokus vanligen endast på lösningsmodeller med flera faser för datadiodlösningar som möjliggör enkelriktad kommunikation (TL II --> TL I). Gatewaylösningar beskrivs närmare i Cybersäkerhetscentrets anvisning om gatewaylösningar.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 1 och 2 punkten
Referenser	Katakri: I-01
Övrig tilläggsinformation	

Identifierare	TEK-02, L:Sekretessbelagd, E:Viktig, S:Viktig, TS:Särskild kategori av personuppgifter
Namn	Telekommunikationsnätets indelning i zoner
Krav	Telekommunikationsnätets indelning i zoner och dess filtreringsregelverk ska genomföras i enlighet med principen om skydd på flera nivåer.
Allmän beskrivning	Att dela telekommunikationsnätet inom en säkerhetsklass till separata domäner (zoner och segment) kan till exempel ur informationsskyddets synvinkel innebära ändamålsenlig avskiljning av arbetsstationer och servrar och även omfatta eventuella projektspecifika avskiljningsbehov. Alla kopplade informationstekniska system bör i princip behandlas som otillförlitliga och man ska vara beredd på allmänna nätangrepp. Att vara beredd på allmänna nätangrepp omfattar till exempel att man håller endast nödvändiga funktioner aktiverade. Med andra ord ska det finnas ett motiverat funktionellt behov av varje aktiv funktion. Funktionaliteten bör begränsas till den minsta delgruppen som uppfyller de funktionella kraven (till exempel begränsning av funktionernas synlighet). Dessutom ska man beakta till exempel förfalskning av adresser (spoofing), blockering och begränsning av nätens synlighet.
Exempel på genomförande	Kravet kan uppfyllas på så sätt att man vidtar följande åtgärder: 1) Telekommunikationsnätet har delats inom säkerhetsklassen i fråga i separata domäner (zoner, segment). 2) Trafiken mellan domänerna begränsas och default-deny-regeln tillämpas på trafiken in i miljön. 3) Databehandlingsmiljön är beredd på allmänna nätangrepp.
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 1 och 2 punkten
Referenser	Katakri: I-02
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02

Identifierare	TEK-02.1, L:TL IV, E:, S:, TS:
Namn	Telekommunikationsnätets indelning i zoner – principen om lägsta behörighet
Krav	Telekommunikationsnätets indelning i zoner och dess filtreringsregelverk ska genomföras i enlighet med principen om lägsta behörighet inom säkerhetsklassen i fråga.
Allmän beskrivning	Övervakning och begränsning av trafiken mellan domäner kan genomföras på yttre gränsen av ett nät med säkerhetsklass IV till exempel så att alla försök att öppna en förbindelse som skickas till nätet blockeras och förbindelser från nätet begränsas till bläddring av webbsidor som kommer via en proxyserver och till e-posttrafik. Att i tillräckligt stor grad beakta principen om lägsta behörighet i nät med alla säkerhetsklasser förutsätter vanligen också att endast nödvändiga förbindelser tillåts mellan domäner inom säkerhetsklassen (källa-objekt-protokoll) och att andra förbindelseförsök upptäcks. Inom en miljö med klassen i fråga kan skyddet också kompletteras och stödas med ett så kallat Zero Trust-tillvägagångssätt som innebär att olika aktörers verksamhetsmöjligheter kan begränsas och övervakas med särskild grund i identifiering och verifiering av aktörerna och funktionerna. Man ska dock beakta att Zero Trust inte ersätter kravet på tillräckligt tillförlitlig avskiljning av databehandlingsmiljöer med olika skyddsbehov/säkerhetsklass. TEK-01.3 och TEK-01.5). Identifiering och verifiering av databehandlingsmiljöns aktörer (användare och anordningar) spelar en central roll i genomförandet av Zero Trust. Även adekvat kryptering i datatrafiken mellan aktörer är viktig. Man ska försäkra sig regelbundet om kopplingarnas och konfigurationernas säkra funktion, jfr TEK-03. Vad gäller säkerhetsklass IV bör man också beakta hotet av överbelastningsangrepp om systemet ansluts till ett icke betrott nät. Filtreringen bör grunda sig på principen om lägsta behörighet och tillåta endast separat godkänd kommunikation (default-deny). Filtreringen bör också beakta funktionerna av olika protokoll (till exempel IPv4, IPv6, GRE, IPSec-tunnlar, routningsprotokoll och även protokoll i övre lager, till exempel HTTP, SSH, FTP och SMTP). Onödiga protokoll bör tas ur bruk i alla sådana system (arbetsstationer, servrar, närverksenheter osv.) där de inte behövs, och man ska säkerställa att trafik blockeras med filtreringsregler för brandväggar (på nätverks-, arbetsstations- och servernivå). Om till exempel IPv6-funktionen används i arbetsstationer, servrar, nätverksenheter eller andra motsvarande system, bör man beakta dess inverkan särskilt vad gäller filtrering av trafiken (brandväggarna ska täcka även IPv6-trafik) och routning. Även effekterna av kombination och parallell användning av olika protokoll (till exempel IPv4-IPv6, NAT-64, Teredo) bör beaktas i helhetsplaneringen av nätets/systemets säkerhet.
Exempel på genomförande	I behandlingsmiljöer med säkerhetsklass IV–II kan kravet uppfyllas på så sätt att man vidtar följande åtgärder utöver de åtgärder som nämnts tidigare: 4) Trafiken mellan domäner övervakas och begränsas så att endast separat godkänd trafik som är nödvändig för funktionen tillåts (default-deny).
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 1 och 2 punkten
Referenser	Julkri: TEK-03; Katakri: I-02
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02

Identifierare	TEK-03, L:Sekretessbelagd, E:Viktig, S:Viktig, TS:Särskild kategori av personuppgifter
Namn	Administration av filtrerings- och övervakningssystem
Krav	Man sköter om den ändamålsenliga funktionen av filtrerings- och övervakningssystem under databehandlingsmiljöns hela livscykel.
Allmän beskrivning	System som filtrerar och/eller övervakar trafik är vanligen brandväggar, routrar, IDS- och IPS-system och nätverksenheter, servrar och applikationer som innehåller motsvarande funktioner. Genomförande av adekvat dokumentation förutsätter vanligen till exempel att nätets struktur inklusive domäner (zoner och segment) beskrivs så noggrant att man utifrån dokumentationen kan kontrollera att nätet motsvarar den tillräckligt säkra struktur som dokumenterats. Med tanke på användbarheten och säkerställandet av adekvat dokumentation är den ändamålsenliga lösningen ofta att säkerhetskopiera filtrerings- och övervakningssystemens inställningar (konfigurationer, inklusive till exempel brandväggsregelverk) och förvara säkerhetskopiorna i enlighet med säkerhetsklassen. Den godtagbara granskningsfrekvensen för inställningar och önskade funktioner beror i synnerhet på hur ofta ändringar sker i objektet och hur omfattande objektet är. Till exempel kan regelverket gällande brandväggar för organisationens databehandlingsmiljö med säkerhetsklass IV vara omfattande, och ändringar kan behövas ofta. I sådana miljöer kan en tillräcklig granskningsfrekvens vara till exempel varje kvartal eller halvårsvis. Å andra sidan kan det räcka med kontroller som görs en gång om året om miljön är begränsad och dess filtreringsregelverk kräver ändringar mycket sällan. Filtrerings- eller övervakningssystemens funktioner kan ändras eller nya egenskaper introduceras även i regelbundna programuppdateringar. Det är motiverat att säkerställa korrektheten av filtreringsregelverket och de övriga funktionerna även i samband med programuppdateringar som installeras regelbundet. Möjligheterna att utnyttja och ta i bruk nya egenskaper (till exempel bättre filtrering) ska bedömas som en del av förändringshanteringen (jfr I-16).
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; Säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Katakri: I-03
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.21, 8.23
Identifierare	**TEK-03.1, L:Sekretessbelagd, E:Viktig, S:Viktig, TS:Särskild kategori av personuppgifter**
Namn	Administration av filtrerings- och övervakningssystem – ansvarsfördelning och organisering
Krav	Tillägg, ändring, radering och övervakning av inställningar i system som filtrerar eller övervakar trafiken har organiserats och ansvaret för dem delegerats.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 4 § 2 mom. 1 punkten; Säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Katakri: I-03, I-16
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.35, PiTuKri MH-01

Identifierare	TEK-03.2, L:Sekretessbelagd, E:Viktig, S:Viktig, TS:Särskild kategori av personuppgifter
Namn	Administration av filtrerings- och övervakningssystem – dokumentering
Krav	Dokumenteringen av nätet och därtill relaterade filtrerings- och övervakningssystem upprätthålls under nätets livscykel som en oskiljaktig del av hanteringsprocessen för ändringar och inställningar.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 5 § 2 mom.; Säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Julkri: HAL-09; Katakri: I-03
Övrig tilläggsinformation	

Identifierare	TEK-03.3, L:Sekretessbelagd, E:Viktig, S:Viktig, TS:Särskild kategori av personuppgifter
Namn	Administration av filtrerings- och övervakningssystem – kontroller
Krav	Inställningar och den önskade verksamheten i system som filtrerar eller övervakar trafiken kontrolleras med regelbundna intervaller under databehandlingsmiljöns funktion och service samt då avvikande situationer uppkommer.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; Säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Katakri: I-03
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.32

Identifierare	TEK-04, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Administrativa anslutningar
Krav	Administrativ åtkomst sker via avgränsade, kontrollerade och övervakade punkter.
Allmän beskrivning	Med anordningar/anslutningar avses i genomförandeexemplen nedan sådana system som endast administratörer eller motsvarande bör ha hanteringsrätt till. Sådana är vanligen till exempel brandväggar, routrar, växlar, trådlösa basstationer, servrar, arbetsstationer, separata konsolanslutningar (till exempel iLO, iDrac) och förvaltningsanslutningar för Blade-stommar. En särskild fråga att beakta då man utvärderar skyddet av en administrativ anslutning är i vilken mån sekretessbelagda uppgifter är sårbara via anslutningen i fråga. De flesta administrativa anslutningar ger åtkomst till sekretessbelagd information antingen direkt (exempel: den som administrerar en databas kommer vid behov oftast åt innehållet i databasen) eller indirekt (exempel: den som administrerar nätverksenheter kan oftast ändra brandväggsreglerna som skyddar informationssystemet), vilket gör dessa ett särskilt lockande objekt för illvilliga aktörer. När en administrativ anslutning ger direkt eller indirekt åtkomst till säkerhetsklassificerade uppgifter är det särskilt viktigt att anslutningen och de använda terminalerna begränsas till en säkerhetsklass som i princip är samma som databehandlingsmiljön i fråga. Hantering av en miljö med lägre säkerhetsnivå kan i vissa fall vara möjligt från en hanteringsmiljö med högre säkerhetsklass med den förutsättningen att säkerhetsklassernas gränser har en tillräckligt säker gatewaylösning som förhindrar att uppgifter i en högre säkerhetsklass hamnar i en miljö med lägre säkerhetsklass. Särskilt på grund av programsårbarheter i förbindelseprotokoll begränsas hanteringsmöjligheterna i miljöer med lägre säkerhetsnivå riskbaserat vanligen endast till hantering av miljöer med lägre säkerhetsklass från miljöer med säkerhetsklass IV. På grund av den administrativa trafikens säkerhetskritiska natur är det i princip inte möjligt att administrera en miljö med högre säkerhetsklass från miljöer med svagare skydd. Man kan via en tillräckligt säker gatewaylösning i vissa fall (read-only) erbjuda övervakningsåtkomst från en miljö med högre säkerhetsklass till en miljö vars säkerhetsklass är en klass lägre. I genomförandet av adekvat spårbarhet kan man inom säkerhetsklassen i fråga utnyttja till exempel så kallad hoppmaskinpraxis där alla hanteringsåtgärder genomförs via ytterst härdade, system- och rollspecifika hoppmaskiner, vilket samtidigt möjliggör täckande spårbarhet (loggföring, jfr TEK-12). Att observera särskilt vid genomförande som utnyttjar molnteknik: – I molntjänstmiljöer är fjärradministration vanligtvis den mest typiska administrationsmetoden, både för själva molnplattformen och för kundens system. Som fjärradministration räknas till exempel underhåll utfört av molnleverantören när det sker från utsidan av en fysiskt skyddad datorhall. Som fjärradministration räknas också underhåll som utförs av en kund hos molntjänsten på de systemdelar som kunden ansvarar för. – En särskild fråga att beakta då man utvärderar skyddet av en administrativ anslutning är i vilken mån informationen som behandlas i molntjänsten är sårbar via anslutningen i fråga. De flesta administrativa anslutningar ger åtkomst till information, antingen direkt (exempel: den som administrerar en databas kommer vid behov oftast åt innehållet i databasen) eller indirekt (exempel: den som administrerar nätverksenheter kan oftast ändra brandväggsreglerna som skyddar datasystemet). Som administrativa anslutningar räknas i princip alla anslutningar genom vilka det går att påverka skyddet av sekretessbelagd information. Administrativa anslutningar innefattar i typiska fall även webbkonsoler/-portaler och motsvarande administrativa fjärranslutningar som molntjänsten erbjuder sina kunder. – När en administrativ anslutning ger direkt eller indirekt åtkomst till sekretessbelagda uppgifter är det särskilt viktigt att anslutningen och de använda terminalerna begränsas till att användas på en skyddsnivå som i princip är samma som databehandlingsmiljön i fråga. På grund av den administrativa trafikens säkerhetskritiska natur är det i princip inte möjligt att administrera en miljö som används för behandling av säkerhetsklassificerad information från miljöer eller terminaler med svagare skydd. Administrativ åtkomst till en molnplattform som innehåller säkerhetsklassificerade uppgifter ska begränsas till terminaler som uppfyller säkerhetsklassens krav. Observera att även administrationslösningar för terminaler och andra bakgrundssystem som är kopplade till dem ska uppfylla kraven för säkerhetsklassen i fråga, liksom även fysiska lokaler/områden där hanteringen utförs. – Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

Exempel på genomförande	Begränsad åtkomst ska genomföras med till exempel hoppmaskiner, kontrollportaler och motsvarande förfaranden.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 14 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom.
Referenser	Julkri: TEK-12; Katakri: I-04
Övrig tilläggsinformation	Traficom: Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista (2.12.2021); ISO/IEC 27002:2022 8.2, 8.20, 8.21, 8.22; PiTuKri IP-03, TT-01
Identifierare	**TEK-04.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Administrativa anslutningar – stark autentisering i offentligt nät
Krav	Administrativ åtkomst från offentligt nät eller annan fjärradministrationslösning som används ska förutsätta stark autentisering som baserar sig på minst tvåfaktorsverifiering.
Allmän beskrivning	Skyddet av administrativa anslutningar är en av de mest kritiska faktorerna som påverkar informationssystemens säkerhet. Det kan dock vara motiverat att också kunna administrera särskilt sekretessbelagda system som inte säkerhetsklassificerats och system med säkerhetsklass IV från utanför fysiskt skyddade säkerhetsområden. I situationer där fjärradministration anses motiverat är rekommendationen att den skyddas med skyddsåtgärder som är mer täckande än fjärranvändningens. Till exempel kan fjärradministrationsförbindelser i system med säkerhetsklass IV begränsas till enstaka fysiska och logiska punkter.
Exempel på genomförande	Administrativa anslutningar från offentligt nät förutsätter till exempel en VPN-anslutning där åtminstone antingen användaren eller enheten verifieras starkt.
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 5 punkten
Referenser	Katakri: I-04
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.2; PiTuKri IP-03
Identifierare	**TEK-04.2, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Administrativa anslutningar – kryptering av administrativa anslutningar
Krav	Den administrativa trafiken i offentligt nät har krypterats med en metod som lämpar sig för användningsfallet och gynnar krypteringslösningar/-protokoll som verifierats (validerats) och standardiserats med tanke på korrekt funktion.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 4 och 7 punkten
Referenser	Katakri: I-04
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.24

Identifierare	TEK-04.3, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Administrativa anslutningar – lägsta behörighet
Krav	De administrativa anslutningarna har begränsats enligt principen om lägsta behörighet.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 16 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 3 punkten
Referenser	Julkri: HAL-2.1; Katakri: I-04
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.20

Identifierare	TEK-04.4, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Administrativa anslutningar – personliga koder
Krav	Administratörskoderna för systemen och applikationerna är personliga.
Allmän beskrivning	
Exempel på genomförande	Om det inte är tekniskt möjligt att använda personliga koder i alla system eller applikationer måste det finnas överenskommen och dokumenterad hanteringspraxis som gör det möjligt att identifiera användaren för gemensamma användar-ID.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 16 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 3 och 5 punkten
Referenser	Katakri: I-04
Övrig tilläggsinformation	PiTuKri IP-02

Identifierare	TEK-04.5, L:TL IV, E:, S:, TS:
Namn	Administrativa anslutningar – begränsning av anslutningar enligt säkerhetsklass
Krav	De administrativa anslutningarna har begränsats enligt säkerhetsklass om man inte använder en gatewaylösning som är tillräckligt säker med beaktande av säkerhetsklassen.
Allmän beskrivning	
Exempel på genomförande	Det finns ingen sammanlänkning till databehandlingsmiljön för administrativa anslutningar från miljöer med andra säkerhetsklasser utan en gatewaylösning som är tillräckligt säker med beaktande av säkerhetsklassen.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 1 punkten
Referenser	Julkri: TEK-01; Katakri: I-04
Övrig tilläggsinformation	

Identifierare	TEK-04.6, L:TL IV, E:, S:, TS:
Namn	Administrativa anslutningar – administrativa anslutningar som innehåller säkerhetsklassificerade uppgifter
Krav	Då den administrativa trafiken innehåller säkerhetsklassificerade uppgifter och då den går via en miljö med lägre säkerhetsklass har säkerhetsklassificerade uppgifter krypterats med en tillräckligt säker krypteringsprodukt.
Allmän beskrivning	
Exempel på genomförande	Den administrativa arbetsstationen för säkerhetsklassen i fråga kopplas till anordningen/anslutningen endast via en tillräckligt säker krypteringslösning i situationer där den administrativa trafiken går via en miljö med lägre säkerhetsklass.
Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Katakri: I-04, I-12
Övrig tilläggsinformation	

Identifierare	TEK-04.7, L:TL IV, E:, S:, TS:
Namn	Administrativa anslutningar – kryptering inom säkerhetsklass
Krav	När administrativ trafik går inom en säkerhetsklass kan kryptering på en lägre nivå eller okrypterad överföring användas enligt riskhanteringsprocessens resultat.
Allmän beskrivning	
Exempel på genomförande	Något av följande gäller i situationer där den administrativa trafiken går inom en säkerhetsklass (inom kryptering som är adekvat för säkerhetsklassen i fråga och/eller inom ett nät som fysiskt avskilts från andra miljöer och som befinner sig inom ett säkerhetsområde som godkänts för förvaring av uppgifter i säkerhetsklassen i fråga): a) den administrativa arbetsstationen i säkerhetsklassen i fråga kopplas fysiskt till anordningen/anslutningen (till exempel konsolkabel) eller b) den administrativa anslutningens kommunikationskanal i säkerhetsklassen i fråga har skyddats fysiskt på annat pålitligt sätt (till exempel kablar inom skyddsområdet) eller c) den administrativa arbetsstationen i säkerhetsklassen i fråga kopplas till anordningen/anslutningen med en förbindelse som skyddats med kryptering på lägre nivå (till exempel SSH, HTTPS, SCP). 4) Administrativ kontakt till anordningarna/anslutningarna tillåts i enlighet med principen om lägsta behörighet enbart från godkända källor och med definierade användarrättigheter.
Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Katakri: I-04
Övrig tilläggsinformation	

Identifierare	TEK-04.8, L:TL III, E:, S:, TS:
Namn	Administrativa anslutningar – TL III
Krav	Fjärradministration av behandlingsmiljöer med säkerhetsklass III ska genomföras från ett skyddsområde.
Allmän beskrivning	I behandlingsmiljöer med säkerhetsklass III och i andra kritiska behandlingsmiljöer förutsätter man att fjärradministration binds tekniskt till godkänd fjärradministrationsutrustning (till exempel enhetsidentifiering).
Exempel på genomförande	Fjärradministration har hindrats tekniskt med hjälp av anordningar som inte godkänts.
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § 3 mom. 1 punkten
Referenser	Katakri: I-18
Övrig tilläggsinformation	

Identifierare	TEK-05, L:Sekretessbelagd, E:, S:, TS:Personuppgift
Namn	Trådlös informationsöverföring
Krav	Datatrafik inom trådlös informationsöverföring krypteras med en lösning som inte har några kända sårbarheter och som enligt tillverkaren stöder modern krypteringsstyrka och moderna krypteringsinställningar.
Allmän beskrivning	Användningen av radiogränssnitt i trådlös informationsöverföring (till exempel WLAN, Bluetooth) tolkas som att man lämnar ett fysiskt skyddat område. Med andra ord jämställs användningen av radiogränssnitt med trafik via allmänt nät, vilket bör beaktas särskilt i trafikens kryptering och genomförandet av den fysiska säkerheten. Flera trådlösa gränssnitt är också förknippade med brister i genomförandet av protokoll och program som kan utnyttjas av utomstående. Motsvarande skyddsprincip tillämpas även på trådlös kringutrustning (till exempel mus, tangentbord, hörlurar och system för bildöverföring). Undantag till detta är situationer där risker förknippade med användningen av trådlösa gränssnitt kan minskas på ett pålitligt sätt med hjälp av förfaranden inom fysisk säkerhet (till exempel användning av trådlös mus inom ett skyddsområde i ett rum som endast personer som auktoriserats att behandla uppgifterna i fråga kan komma nära). Vad gäller trådlösa enheter ska man även beakta smarttelefoner och motsvarande utrustning med lägre säkerhetsnivå som inte ska kopplas till databehandlingsmiljön till exempel för att ladda batteriet. Produkterna och algoritmerna som används får inte innehålla kända sårbarheter eller svagheter som inte har korrigerats och som äventyrar informationssäkerheten. Dessutom ska tillverkaren av de använda produkterna erbjuda säkerhetsuppdateringar för produkterna.
Exempel på genomförande	1) Trådlös informationsöverföring som sträcker sig utanför ett fysiskt skyddat område krypteras i enlighet med kraven. 2) Trådlös informationsöverföring som sker innanför ett fysiskt skyddat område men vars skydd är svagare än vad kraven förutsätter (till exempel trådlös kringutrustning) kan godkännas om man kan säkerställa att informationens konfidentialitet inte äventyras via dessa anslutningar. 3) Anordningar med lägre säkerhetsnivå och med trådlösa anslutningar kopplas inte till miljön.
Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Katakri: I-05, I-08, I-09, I-12, I-15, I-16
Övrig tilläggsinformation	PiTuKri SA-01; ISO/IEC 27002:2022 8.22

Identifierare	TEK-05.1, L:TL IV, E:, S:, TS:
Namn	Trådlös informationsöverföring – kryptering
Krav	I trådlös informationsöverföring krypteras datatrafiken med en lösning som är tillräckligt säker för säkerhetsklassen i fråga.
Allmän beskrivning	
Exempel på genomförande	I klass TL IV kan kravet genomföras till exempel genom att tunnla trafiken med en tillräckligt säker VPN-lösning eller använda en godkänd krypteringslösning på applikationsnivån.
Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Katakri: I-05
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.24; PiTuKri SA-01

Identifierare	TEK-06, L:Sekretessbelagd, E:, S:, TS:Personuppgift
Namn	Masseffekten
Krav	Masseffekten har beaktats i skyddet av databehandlingsmiljön.
Allmän beskrivning	När säkerhetsklassen av objektets centrala datalager tolkas som högre än nivån på enskilda informationselement på grund av den kumulativa effekten ska datalagrets fastställda skyddsmetoder genomföras i enlighet med kraven som en högre nivå ställer. Med fastställda skyddsmetoder avses metoder som används för att begränsa åtkomsten till den enskilda eller begränsade del av informationsinnehållet som behövs i uppgiften och med vilka försök att utan behörighet komma åt en större del av informationsinnehållet upptäcks. Då Julkri används som bedömningsverktyg bör den kumulativa effekten tolkas så att man av datalagrets skydd förväntar utöver datalagrets fysiska säkerhet även punkterna TEK-14 (applikationslagrets säkerhet), TEK-12 och TEK-13 (spårbarhet och observationsförmåga), HAL-02.1 (Uppgifter och ansvar – uppgifternas differentiering) och TEK-07 (Administration av åtkomsträtt), alla i enlighet med en högre säkerhetsnivå. Man ska beakta att datalagrets säkerhetsklass som stigit med en klass till följd av den kumulativa effekten förutsätter inte en acceptabel gatewaylösning mellan datalagret (till exempel TL III) och terminalerna (till exempel TL IV). Till följd av den kumulativa effekten ska man i administrativa lösningar förknippade med datalager med säkerhetsklass III dessutom ägna särskild uppmärksamhet åt att terminalerna som används för hanteringen avskilts på ett pålitligt sätt från nät kopplade till internet.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 15 § 2 mom., 13 § 1 mom.
Referenser	Julkri: HAL-04.3
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01

Identifierare	TEK-07, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Administration av åtkomsträtt
Krav	Informationssystemens åtkomsträttigheter har definierats.
Allmän beskrivning	Det centrala målet för hanteringen av åtkomsträttigheter är att kunna försäkra sig om att endast berättigade användare har åtkomst till databehandlingsmiljön och de skyddade uppgifter som miljön innehåller.
Exempel på genomförande	1) Ansvariga personer har utsetts för hanteringen av systemens åtkomsträttigheter. 2) Det finns en förteckning över systemanvändarna.
Lagstiftning	Informationshanteringslagen 16 §; säkerhetsklassificeringsförordningen 8 §, 11 § 1 mom. 3 punkten
Referenser	Julkri: HAL-14, HAL-14.1, HAL-19; Katakri: I-06
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01

Identifierare	TEK-07.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Administration av åtkomsträtt – beviljande av åtkomsträtt
Krav	Åtkomsträtt till informationssystem kan endast beviljas till personer vars användningsbehov säkerställts.
Allmän beskrivning	Det rekommenderas att åtkomsträttigheterna grundar sig på ett avtal eller annan dokumenterad grund som kan verifieras (till exempel anställningsförhållande, avtal om arbete som ska utföras i miljön).
Exempel på genomförande	3) Man kontrollerar i samband med beviljande av åtkomsträtt att den som får rätten hör till personalen eller annars är berättigad till den. 4) Det finns anvisningar om behandlingen och beviljandet av åtkomsträttigheter. 5) Det finns en handling om varje beviljad åtkomsträtt (papper eller elektronisk).
Lagstiftning	Informationshanteringslagen 16 §; säkerhetsklassificeringsförordningen 8 §, 11 § 1 mom. 3 punkten
Referenser	Julkri: HAL-14, HAL-10.1; Katakri: I-06
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01
Identifierare	**TEK-07.2, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Administration av åtkomsträtt – begränsning av åtkomsträtt
Krav	Databehandlingsmiljöns användare och automatiska processer ges endast de uppgifter, rättigheter eller behörigheter som är nödvändiga med tanke på utförandet av deras uppgifter.

Allmän beskrivning

Åtkomsträtt begränsas endast till den delmängd som det funktionella behovet förutsätter. Onödigt omfattande rättigheter ger användaren, processen eller en attackerare som får tag på det ovan nämnda onödigt omfattande verksamhetsmöjligheter. Genom att begränsa åtkomsträtten så att den följer principen om lägsta behörighet kan man reducera riskerna förknippade med både avsiktliga och oavsiktliga handlingar och riskerna som till exempel sabotageprogram medför. Man ska särskilt se till att underhållsrättigheter endast används för underhållsåtgärder. Ett användarkonto med underhållskoder ska inte användas till exempel för att bläddra på nätet eller kontrollera e-posten.

Ägare av säkerhetsklassificerade uppgifter förbehåller sig ofta rätten att granska alla nät/system i vilka uppgifterna de äger behandlas. I granskningarna förutsätter man ofta fysisk och logisk åtkomst till objektet som ska granskas, och sålunda har de som genomför granskningen ofta tekniskt sett en möjlighet att komma åt de uppgifter som behandlas i objektet. Särskilt i nät för flera projekt och andra motsvarande miljöer där man behandlar uppgifter från flera olika ägare ska man försäkra sig om att nätets/systemets struktur möjliggör granskningar där ägarna inte kommer åt varandras uppgifter i samband med granskningen. Obs.: Kravet på avskiljning av uppgifter i säkerhetsklass IV tillämpas inte på arbetsstationer eller andra motsvarande begränsade datalager, med den förutsättningen att tillförlitliga metoder används för att förebygga den kumulativa effekten. Uppgifterna från ägare som förbehåller sig rätten till granskning behöver inte heller avskiljas i situationer då ett separat skriftligt godkännande har mottagits från varje ägare om att ägarna godkänner de risker som granskningsrätten kan leda till eller om uppgifternas ägare förbinder sig att inte använda den tekniska granskningsrätten i databehandlingsmiljön i fråga.

Olika ägares metoder för avskiljning av uppgifter delas in i tre huvudkategorier.
a) Metoder som grundar sig på avskiljning på logisk nivå (till exempel virtualisering av servrar och mappar på nätverksdiskar som begränsats med åtkomsträttigheter) är lämpliga för uppgifter i säkerhetsklass IV.
b) Metoder som grundar sig på tillförlitlig logisk avskiljning (till exempel på ett acceptabelt sätt krypterade virtuella maskiner på skivsystemets fysiska diskar som reserverats kundspecifikt och godkänd kryptering av uppgifter/datatrafik i nätverksenheter som används gemensamt) är lämpliga för säkerhetsklasserna IV och III för avskiljning inom respektive säkerhetsklass.
c) Metoder som grundar sig på avskiljning på fysisk nivå (ägarspecifikt reserverade fysiska apparater) är lämpliga för säkerhetsklasserna IV, III, II och I.

Att observera särskilt vid genomförande som utnyttjar molnteknik:

- Ansvarsfördelningen mellan molnleverantören och kunden ska beaktas i tillämpningen av kravet. Vanligen är det molnleverantören som ansvarar för behörighetshanteringen av systemhelheten som är förknippad med molntjänstens produktion, medan kunden ansvarar för behörighetshanteringen av den del som byggs på tjänsteleverantörens tjänstehelhet (IaaS, PaaS eller SaaS). Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.
- Följande ska beaktas då avskiljning genomförs med hjälp av molnteknik:
  - Sekretessbelagda uppgifter ska avskiljas tillräckligt pålitligt, med hjälp av logisk och/eller fysisk avskiljning. En vanlig avskiljningslösning för till exempel gemensamma nätverksenheter och lagringssystem är kryptering. Kryptering av datatrafik (data-in-transit) och kryptering vid lagring (data-at-rest) utförs med kundspecifika nycklar och är ett pålitligt skydd också för andra ändamål, till exempel säker förstöring av enheter.
  - Om samma maskinvara används för att behandla flera kunders information samtidigt ska man försäkra sig om att uppgifternas fysiska och logiska avskiljning är tillräckligt säker. Om tillräcklig säkerhet inte kan säkerställas ska separata fysiska enheter användas för behandlingen av uppgifterna. Till exempel kan säkerhetsklassificerade uppgifter förvaras fysiskt på en egen virtualiseringsplattform där endast personer som har behörighet att behandla säkerhetsklassificerad information har tillgång exempelvis till gränssnitt där processorsårbarheter kan förekomma.
  - Om samma enheter används för att behandla flera kunders uppgifter så att behandlingen inte sker samtidigt måste man även säkerställa att den föregående kundens uppgifter har tagits bort på ett tillräckligt säkert sätt (inbegripet alla delar, BIOS, cacheminnen i andra enheter). Om tillräcklig säkerhet inte kan säkerställas ska separata fysiska enheter användas för behandlingen av uppgifterna. Jfr PiTuKri / SI-02 (Förstöring av informationsmaterial).
    –– Ägare av säkerhetsklassificerade, sekretessbelagda uppgifter kan förbehålla sig rätten att granska alla nät/system i vilka uppgifterna de äger behandlas. I granskningarna förutsätter man ofta fysisk och logisk åtkomst till objektet som ska granskas, och sålunda har de som genomför granskningen ofta tekniskt sett en möjlighet att komma åt de uppgifter som behandlas i objektet. Särskilt i miljöer där man behandlar uppgifter från flera olika ägare ska man försäkra sig om att nätets/systemets genomförandesätt möjliggör granskningar där ägarna inte kommer åt varandras uppgifter i samband med granskningen. Särskilt i leveransformerna IaaS och PaaS ska avskiljningen av den säkerhetsklassificerade informationen säkerställas med hjälp av fysiskt separata nätverk eller virtuella eller programbaserade lokala nätverk som krypteras. Jfr PiTuKri / SA-03 (Kryptering innanför ett fysiskt skyddat säkerhetsområde).

Exempel på genomförande	6) I informationssystem har säkerhetsklassificerade uppgifter specificerats med behörighetsdefinitioner och systemets behandlingsregler eller på något annat motsvarande sätt i enlighet med principen om lägsta behörighet. 7) Uppgifter från ägare som förbehåller sig rätten till granskning förvaras i informationssystem åtskilda från varandra. Avskiljningen genomförs på ett sätt som är tillräckligt säkert för säkerhetsklassen i fråga.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom. 1 punkten, 16 §; säkerhetsklassificeringsförordningen 8 §, 11 § 1 mom. 3 och 4 punkten
Referenser	Katakri: I-06
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01, SA-03, KT-03
Identifierare	**TEK-07.3, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Administration av åtkomsträtt – åtkomsträttens aktualitet
Krav	Åtkomsträttigheterna ska hållas aktuella.
Allmän beskrivning	
Exempel på genomförande	8) Det finns en tydlig och fungerande metod att omedelbart anmäla ändringar i personalen till relevanta aktörer och ett fungerande sätt att genomföra nödvändiga ändringar. 9) Åtkomsträttigheterna granskas regelbundet.
Lagstiftning	Informationshanteringslagen 16 §
Referenser	Julkri: HAL-14.1; Katakri: I-06
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01
Identifierare	**TEK-07.4, L:TL IV, E:, S:, TS:**
Namn	Administration av åtkomsträtt – avskiljning av säkerhetsklassificerade uppgifter
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	1) Uppgifterna i varje enskild säkerhetsklass hålls separat från offentliga uppgifter och uppgifter i andra säkerhetsklasser, eller så behandlas uppgifter på olika nivåer i enlighet med den högsta säkerhetsklassen. 2) Säkerhetsklassificerade uppgifter förvaras i servrar, arbetsstationer och andra lagringsmedier tillräckligt säkert krypterade om krypteringen används för avskiljning av olika uppgifter vars ägare förbehåller sig rätten till granskning och/eller om lagringsmedier under sin livscykel exporteras utanför säkerhetsområdet som godkänts för förvaring av uppgifter i säkerhetsklassen i fråga.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 1 punkten
Referenser	Katakri: I-06
Övrig tilläggsinformation	

Identifierare	TEK-07.5, L:TL III, E:, S:, TS:
Namn	Administration av åtkomsträtt – TL III
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	En tillräckligt bra avskiljning av uppgifter beror i betydande grad på användningsfallen i systemet i fråga. I de flesta system kan adekvat avskiljning uppnås genom att åtskilja systemets administrationsroller (och personer) och de roller (och personer) som deltar i övervakning av loggarna. En annan vanlig övervakningsmekanism är att kritiska underhållsåtgärder och motsvarande åtgärder kräver godkännande från två eller flera personer.
Exempel på genomförande	Uppgifterna och ansvarsområdena ska till den mån det är möjligt vara separerade för att minska risken för olovliga eller oavsiktliga ändringar eller olovligt eller oavsiktligt missbruk vad gäller objekten som ska skyddas. Det ska finnas en övervakningsmekanism för farliga arbetskombinationer som eventuellt kan uppstå.
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 3 punkten
Referenser	Julkri: HAL-2.1; Katakri: I-06, I-12
Övrig tilläggsinformation	

Identifierare	TEK-08, L:Sekretessbelagd, E:Normal, S:, TS:Personuppgift
Namn	Identifiering av aktörer inom databehandlingsmiljön
Krav	Personer, apparater och informationssystem som använder databehandlingsmiljön identifieras på ett tillräckligt tillförlitligt sätt.
Allmän beskrivning	

Exempel på genomförande	Kravet kan uppfyllas på så sätt att man vidtar följande åtgärder: Identifiering av personer: 1) Alla användare har individuella och personliga användar-ID:n. 2) Alla användare identifieras och verifieras. 3) Identifieringen och verifieringen ska ske enligt en betrodd, pålitlig teknik eller ordnas på annat pålitligt sätt. 4) Användar-ID:n låser sig om identifieringen misslyckas för många gånger efter varandra. 5) Administratörskoderna för systemen och applikationerna är personliga. Om detta inte är tekniskt möjligt i alla system eller applikationer måste det finnas överenskommen och dokumenterad hanteringspraxis som gör det möjligt att identifiera användaren för gemensamma användar-ID. 6) Verifieringen kräver minst lösenord. Om autentisering sker med lösenord ska följande villkor uppfyllas: a) användarna har fått anvisningar om vad som utgör ett säkert lösenord och hur man använder det säkert och b) det övervakande programmet ställer vissa minimisäkerhetskrav på lösenorden och tvingar användaren att byta lösenord med lämpliga mellanrum. Detta lämpliga mellanrum ska väljas enligt klassificeringen av organisationens verksamhetsmiljö och de säkerhetsklassificerade uppgifter som behandlas och förvaras i apparaten, med beaktande av andra säkerhetslösningar. Identifiering av informationssystem: 7) Informationssystem som utbyter information med varandra identifieras med teknik som lämpar sig för användningsfallet, såsom lösenord, nycklar (till exempel API-nyckel), informationsbärare (token, till exempel oAuth) eller motsvarande. Identifiering görs med krypterade förbindelser. Att observera En pålitlig identifiering och autentisering innebär följande: i) autentiseringsmetoden är skyddad mot man-i-mitten-attacker (man-in-the-middle), ii) ingen onödig information avslöjas vid inloggning, före autentisering, iii) de identifierande uppgifter som används för autentisering är alltid krypterade om de sänds över nätet, iv) autentiseringsmetoden är skyddad mot återuppspelningsattacker (replay attacks), och v) autentiseringsmetoden är skyddad mot uttömmande attacker (brute force attacks). Att observera särskilt vid genomförande som utnyttjar molnteknik: – Molntjänster som är tillgängliga i offentligt nät tolkas användningssättet som fjärranvändning. Sålunda ska man beakta till exempel kraven på stark autentisering som baserar sig på flerfaktorautentisering. – I situationer där man vid identifiering i molntjänsten utnyttjar federerad identitetshantering och/eller identitets- och åtkomsthanteringssystem (organisationens egna system eller till exempel system som produceras av molnleverantören) ska särskild uppmärksamhet fästas vid tillförlitligheten hos identifieringstjänsten och attributens förmedlingskedja. För behandling av sekretessbelagda uppgifter lämpar sig endast sådana identifieringstjänster som erbjuder en identitet som grundar sig på stark första identifiering och vars attribut kan förmedlas på ett tillräckligt säkert sätt till en tjänst som stöder sig på identifiering. – Eftersom skyddet av sekretessbelagda uppgifter i allmänhet är direkt beroende av identifieringstjänstens tillförlitlighet, hör det nästan utan undantag till bedömningen av molntjänstens säkerhet att se till att identifieringstjänsten är säker. Till exempel är det vanligen skäl att bedöma det krypteringstekniska skyddet vid förmedling av attribut i samma riktning som förmedlingen av nycklarna till krypteringslösningen som tillämpas på skyddet av datatypen i fråga. – Av identitetshanteringsmodellerna lämpar sig en organisationsorienterad modell (organization-centric identity management) i allmänhet bättre än till exempel en användarcentrerad modell (user-centric) för att skydda sekretessbelagda uppgifter, där man också ska beakta att användaren är bunden till en viss organisation och att säkerhetsutförandet är tillförlitligt. – Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.
Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 5 punkten
Referenser	Julkri: HAL-19; Katakri: I-07
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02, SA-01, SA-02 och SA-03.

Identifierare	TEK-08.1, L:Sekretessbelagd, E:Normal, S:, TS:Personuppgift
Namn	Identifiering av aktörer inom databehandlingsmiljön
Krav	Alla användare identifieras och verifieras med individuella och personliga användar-ID:n.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 16 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 3 och 5 punkten
Referenser	Katakri: I-07
Övrig tilläggsinformation	PiTuKri IP-02
Identifierare	**TEK-08.2, L:Sekretessbelagd, E:Normal, S:, TS:Personuppgift**
Namn	Identifiering av aktörer inom databehandlingsmiljön
Krav	Identifieringen och verifieringen ska ske enligt en betrodd, pålitlig teknik eller ordnas på annat pålitligt sätt.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 14 §, 16 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 3 och 5 punkten
Referenser	Katakri: I-07
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.5; PiTuKri IP-02
Identifierare	**TEK-08.3, L:Sekretessbelagd, E:Normal, S:, TS:Personuppgift**
Namn	Identifiering av aktörer inom databehandlingsmiljön
Krav	Användar-ID:na låser sig om identifieringen misslyckas alltför många gånger efter varandra.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 7 §
Referenser	Katakri: I-07
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.5; PiTuKri IP-02

Identifierare	TEK-08.4, L:TL IV, E:Kritisk, S:, TS:
Namn	Identifiering av aktörer inom databehandlingsmiljön – TL IV
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Identifiering av enheter: Man använder endast sådana terminaler som organisationen erbjuder och administrerar och som godkänts för säkerhetsklassen i fråga för behandlingen av säkerhetsklassificerad information. Att koppla andra enheter än dessa till behandlingsmiljöer för säkerhetsklassificerade uppgifter är entydigt förbjudet. Personalen har fått anvisningar om detta och ålagts att agera enligt anvisningarna. Identifiering av informationssystem: Informationssystem som utbyter information med varandra identifieras med teknik som lämpar sig för användningsfallet, såsom lösenord, nycklar (till exempel API-nyckel), informationsbärare (token, till exempel oAuth) eller motsvarande. Identifiering görs med krypterade förbindelser. Att observera: I behandlingsmiljöer med säkerhetsklass IV där hotet av överbelastningsangrepp (låsande av koder till exempel i identifieringstjänster kopplade till internet) anses vara betydande kan låsandet av koder ersättas med ett förfarande som minskar risken (till exempel förfaranden som grundar sig i fördröjda svar, filtrering eller tillfälligt låsande). I behandlingsmiljöer med säkerhetsklass IV förutsätter man vanligen inte att terminalen identifieras tekniskt om användarna identifieras.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 5 punkten
Referenser	Katakri: I-07
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02
Identifierare	**TEK-08.5, L:TL III, E:Kritisk, S:, TS:**
Namn	Identifiering av aktörer inom databehandlingsmiljön – TL III
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	För säkerhetsklasserna III–II vidtar man även följande åtgärder: 1) Man förutsätter stark autentisering som baserar sig på minst tvåfaktorsverifiering. 2) Terminaler identifieras tekniskt (enhetsidentifiering, 802.1X, eller motsvarande) innan åtkomst till nätet eller tjänsten tillåts om inte anslutningen till nätet begränsats med hjälp av fysisk säkerhet (till exempel genom att placera servrar i låsta skåp inom skyddsområdet). Att observera Stark identifiering av användare och terminaler som används i behandlingsmiljöer med säkerhetsklasserna III och II kan i vissa fall genomföras så att det endast är möjligt att komma åt informationssystemet i ett mycket begränsat, fysiskt skyddat område (vanligen ett skyddsområde, ett låst skåp eller motsvarande) och åtkomstövervakningen använder stark autentisering som grundar sig på minst två faktorer. Då kan identifieringen ordnas i informationssystemet med användarnamn och lösenord. I situationer då identifieringen av användare grundar sig på metoder inom fysisk säkerhet ska även dessa metoder uppfylla kraven på spårbarhet, särskilt vad gäller förvaringstiden för logguppgifter och motsvarande uppteckningar.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 5 punkten
Referenser	Katakri: I-07
Övrig tilläggsinformation	

Identifierare	TEK-09, L:Sekretessbelagd, E:Kritisk, S:, TS:Särskild kategori av personuppgifter
Namn	Informationssystemens fysiska säkerhet
Krav	Informationsmaterial ska behandlas och förvaras i verksamhetslokaler som är tillräckligt säkra enligt kraven på tillförlitlighet, integritet och tillgänglighet.
Allmän beskrivning	Kraven för administrativa områden, skyddsområden och till exempel förvaringsenheter beskrivs i delarna om fysisk säkerhet. Användning utanför säkerhetsområdet är fjärranvändning, och på det tillämpas kraven i punkten i fråga. I situationer där uppgifter behandlas tillfälligt i en lokal med en lägre säkerhetsnivå än uppgifternas klass ska man även beakta till exempel verksamheten under pauser i arbetet (till exempel att flytta uppgifterna till ett kassaskåp i skyddsområdet för pausen), begränsning av hur bra man kan se in i lokalen (till exempel att täcka eventuella fönster) och begränsning av tillträde till behandlingslokalen så att endast godkända personer kan komma in. Man ska kunna säkerställa terminalens integritet på en tillräcklig nivå så att uppgifternas konfidentialitet inte äventyras till följd av att terminalens integritet förloras. Det vanligaste sättet att säkerställa informationssystemets integritet är att skydda det med säkerhetsområdets metoder för fysisk åtkomsthantering, inklusive till exempel alla fysiska servrar, nätverksenheter, terminaler och kablar anslutna till informationssystemet.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 15 § 2 mom.; säkerhetsklassificeringsförordningen 10 §
Referenser	Julkri: FYY-7.1, HAL-19; Katakri: I-17
Övrig tilläggsinformation	ISO/IEC 27002:2022 7.1, 7.3, 7.6, 7.8; Informationshanteringsnämnden: Rekommendation om behandling av säkerhetsklassificerade handlingar (2020:19, kapitel 5); PiTuKri FT-02; CPNI: Physical Security Advice

Identifierare	TEK-10, L:Sekretessbelagd, E:Viktig, S:, TS:Särskild kategori av personuppgifter
Namn	Systemhärdning
Krav	Detta tillvägagångssätt innebär att systemen installeras enligt ett systematiskt mönster så att slutresultatet är en härdad installation.
Allmän beskrivning	Systemen har ofta funktionaliteter som vanligen är förinställt aktiverade och lätta att ta i bruk. Dessa förinställningar brukar vara alltför osäkra. Genom att låta onödiga funktionaliteter vara kvar gör man dem tillgängliga för illvilliga aktörer. Om tjänster som är nödvändiga tillåts ha sårbara förinställningar blir också dessa tillgängliga för illvilliga aktörer. Förinställningarna i ett system inbegriper ofta till exempel administratörslösenord som definierats på förhand, färdigt installerade onödiga program och onödiga användarkonton. Att härda ett system betyder allmänt att inställningarna ändras så att systemet blir mindre sårbart. Den allmänna regeln är att endast funktioner, enheter och tjänster som är väsentliga med tanke på användningskraven ska vara aktiverade i systemet och att till exempel tjänsternas synlighet ska göras så liten som möjligt. På motsvarande sätt ska man till exempel till automatiska processer endast ge de uppgifter, rättigheter eller behörigheter som är nödvändiga för att de ska kunna utföra sin uppgift. På så sätt begränsas den möjliga skadan av olyckor, fel eller obehörig användning av systemets resurser. Systemets eventuellt oskyddade förinställningar och till exempel onödiga förinställda användarkonton ska ändras eller raderas. Med system avses nätets aktiva utrustning, servrar, arbetsstationer, mobila enheter, skrivare, kringutrustning och andra apparater som kan uppfattas som informationssystem. Tillräcklig härdning av servrar, arbetsstationer och motsvarande kan genomföras till exempel följa DISA STIG, CIS eller någon motsvarande nivå. Om man vid behandlingen av säkerhetsklassificerade uppgifter använder nätverksskrivare, telefonsystem eller motsvarande, bör principerna ovan tillämpas även på dessa system. Ofta går det att använda verktyg för konfigurationshantering för härdning och underhåll av den härdade installationen. Väsentligt om härdning 1) Förinställda lösenord har bytts till lösenord av hög kvalitet som följer organisationens lösenordspolitik. Lösenorden förvaras så att de är båda skyddade och tillgängliga. 2) Överflödiga tjänster, applikationer, förbindelser (även på BIOS-nivå) och utrustning har tagits bort. 3) Användare, gränssnitt och apparater identifieras (jfr I-07). 4) Aktiva nödvändiga tjänster är tillgängliga endast för nödvändiga nät, apparater och användar-ID:n. 5) Program (till exempel fast programvara, applikationer) är alltid uppdaterade (jfr I-19). 6) Objektets förbindelser, inklusive administrativa anslutningar, är begränsade, härdade, använder användar-ID:n och tidsbegränsade (timeout av sessioner). 7) Applikationer, gränssnitt och motsvarande som används har härdats och begränsats och deras egenskaper följer principen om lägsta behörighet. 8) Programvara, såsom operativsystem, applikationer och fast programvara, samlar in nödvändig loggdata för upptäckt av missbruk (jfr I-10). 9) Det går inte att starta informationssystem från okända (andra än primära) apparater. Ersättande metoder Om det inte är tekniskt möjligt att hantera till exempel nätverksenheter med användar-ID som preciserar användaren, kan preciserande identifiering genomföras med regler om användning. Ett exempel på detta är att tillgång till lösenordet förutsätter deltagande av två personer. Om miljön är relativt stor finns det skäl att ordna verifieringen med hjälp av speglade AAA-servrar (särskilt TACACS+, RADIUS eller Kerberos). Att observera särskilt vid genomförande som utnyttjar molnteknik: Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

Exempel på genomförande	1) Objekt som ska härdas har identifierats. 2) Genomförandet av härdningen har definierats. 3) Objekten har härdats enligt definitionerna. 4) Man säkerställer regelbundet att härdningarna är aktiva, särskilt efter uppdateringar under hela informationssystemets livscykel. Särskilt att observera: a) Härdningarna riktas till alla enheter i databehandlingsmiljön. Sådana enheter är bland annat nätets aktiva utrustning, servrar, arbetsstationer, mobila enheter, skrivare, kringutrustning och andra apparater som kan uppfattas som informationssystem. b) För att begränsa ytan som kan attackeras är endast nödvändiga tjänster, gränssnitt, förbindelser och kanaler aktiva, och dessa fungerar enligt principen om lägsta behörighet. c) Enhetens fasta programvara (firmware, BIOS och motsvarande), operativsystem, applikationer och andra motsvarande komponenter härdas åtminstone enligt tillverkarens rekommendation och/eller enligt allmänt kända anvisningar om härdning. Utöver detta skräddarsys härdningarna systemspecifikt utifrån användningsändamål och risker. Om det inte finns anvisningar om härdning för komponenten som används ska man tillämpa anvisningar avsedda för en motsvarande produkt.
Lagstiftning	Informationshanteringslagen 13 § 1 och 4 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 6 punkten
Referenser	Katakri: I-08
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.27; The United States Government Configuration Baseline (USGCB); DISA Security Technical Implementation Guides (STIGs); NIST - National Checklist Program Repository; Microsoft DSC Environment Analyzer; Microsoft Baseline Management; CIS benchmarks; PiTuKri JT-02
Identifierare	**TEK-10.1, L:Sekretessbelagd, E:Viktig, S:, TS:Särskild kategori av personuppgifter**
Namn	Systemhärdning – minimering av tjänster som används
Krav	Endast funktioner, enheter och tjänster som är väsentliga med tanke på användningskraven och behandlingen av uppgifter är aktiverade.
Allmän beskrivning	En härdad installation innehåller endast sådana komponenter, tjänster, användarrättigheter och processrättigheter som är nödvändiga för att driftskraven ska uppfyllas och säkerheten kunna garanteras.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 6 punkten
Referenser	Katakri: I-08
Övrig tilläggsinformation	
Identifierare	**TEK-10.2, L:Sekretessbelagd, E:Viktig, S:, TS:Särskild kategori av personuppgifter**
Namn	Systemhärdning – säkerställande av härdning under hela livscykeln
Krav	Härdningens giltighet och effektivitet ombesörjs under informationssystemets hela livscykel.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 och 4 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 6 punkten
Referenser	Katakri: I-08
Övrig tilläggsinformation	

Identifierare	TEK-10.3, L:TL III, E:Kritisk, S:, TS:
Namn	Systemhärdning – säkerhetsklassificerade miljöer
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	Särskilt i miljöer med högre säkerhetsklasser är det ofta motiverat att blockera användningen av onödiga komponenter genom att fysiskt ta loss dessa komponenter (till exempel trådlösa nätverkskort, kameror, mikrofoner) från enheten. I situationer där komponenten i fråga inte kan tas fysiskt loss kan man i vissa fall till exempel tejpa kameror och ta anordningar programmässigt ur bruk som ersättande skydd. Dessutom kan ersättande skydd också uppnås på användarinställnings-, operativsystems- och fast programvarunivå. I vissa operativsystem kan skyddet också kompletteras genom att ta bort programdelar (kernel module) som är förknippade med användningen av enheten i fråga. I behandlingsmiljöer med säkerhetsklass III–II ska kravet beakta härdningsanvisningarnas eventuella nivåer och utnyttjandet av flera olika anvisningar, till exempel tillverkarspecifika anvisningar, CIS Benchmark och DISA STIG, i säkerställandet av härdningens omfattning.
Exempel på genomförande	I behandlingsmiljöer med säkerhetsklass III–II kan kravet uppfyllas på så sätt att man utöver punkterna 1–4 även använder flera härdningsanvisningar för härdningen och genom att göra genomförandet av anvisningarna strängare.
Lagstiftning	Informationshanteringslagen 13 § 1 och 4 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 6 punkten
Referenser	Katakri: I-08
Övrig tilläggsinformation	

Identifierare	TEK-11, L:Sekretessbelagd, E:Normal, S:Normal, TS:Särskild kategori av personuppgifter
Namn	Skydd mot skadeprogram
Krav	Databehandlingsmiljön förses med tillförlitliga lösningar för förebyggande, förhindrande och upptäckt av samt försvar mot skadlig programvara, och för återställande av systemet.
Allmän beskrivning	Systemen kan skyddas mot skadeprogram till exempel genom härdning, med avgränsningar av användarrättigheter, genom att hålla systemen på nivån för säkerhetsuppdateringarna, med kapacitet att observera avvikelser, genom att se till att personalen har säkerhetsmedvetenhet och även genom att använda program för bekämpning av skadliga program. Riskerna kan också minskas genom att sårbara miljöer skiljs åt från produktionsmiljöerna och regler definieras för användning av bland annat flyttbar media (till exempel USB-minnen). Man kan låta bli att installera bekämpningsprogram i miljöer som på andra sätt gjorts otillgängliga för skadeprogram (till exempel system utan anslutningar för import/export av information eller system där man i noggrant begränsade anslutningar genomför tillförlitlig validering/sanitering av uppgifterna som ska överföras).
Exempel på genomförande	Kravet kan uppfyllas på så sätt att man vidtar följande åtgärder: 1) Systemets användarrättigheter har begränsats enligt principen om lägsta behörighet. 2) Systemen hålls på nivån för säkerhetsuppdateringarna. 3) Systemen har härdats så att endast nödvändiga funktioner och programkomponenter används. 4) Man har försäkrat sig om att personalen har säkerhetsmedvetenhet. Användarna har fått anvisningar om skadeprogram och verksamhet som följer organisationens informationssäkerhetsprinciper. 5) Program för bekämpning av skadeprogram har installerats i alla sådana system som är känsliga för skadeprogram. Sådana är vanligen bland annat nätslussar i det offentliga nätet (till exempel e-post- och WWW-trafik) och terminaler kopplade till yttre gränssnitt (övriga nät, USB-medier och motsvarande). 6) Bekämpningsprogrammen är fungerande och har aktiverats. 7) Bekämpningsprogrammen producerar logguppgifter och larm om sina observationer. 8) Signaturerna som identifierar skadeprogram (och motsvarande) uppdateras regelbundet. 9) Observationer av och larm om skadliga program följs upp regelbundet och man reagerar på dem.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 2 och 3 punkten
Referenser	Katakri: I-09
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.7; PiTuKri JT-04
Identifierare	**TEK-11.1, L:TL IV, E:, S:, TS:**
Namn	Skydd mot skadeprogram – TL IV
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Vad gäller behandlingsmiljöer med säkerhetsklass IV kan kravet uppfyllas på så sätt att man dessutom vidtar följande åtgärder: 1) Man har identifierat systemen som får extra skydd från program för bekämpning av skadeprogram.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Katakri: I-09
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.7; PiTuKri JT-04

Identifierare	TEK-11.2, L:TL III, E:, S:, TS:
Namn	Skydd mot skadeprogram – TL III
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	Miljöer som isolerats från offentliga nät I system som inte kopplas till offentliga nät kan uppdateringen av signaturerna som identifierar skadeprogram ordnas till exempel genom att använda en kontrollerad, skyddad server för sökning av uppdateringar. Denna servers signaturbas hålls uppdaterad till exempel genom att manuellt överföra signaturer från ett separat system som kopplats till internet (till exempel 1–3 gånger om veckan) eller genom att överföra signaturerna via en godkänd gatewaylösning. Bedömningen av huruvida signaturerna uppdateras tillräckligt ofta ska i riskbedömningen ställas i relation till miljöns särdrag, med särskilt beaktande av hur ofta annan informationsöverföring utförs i miljön. Obs.: Det ska finnas ett tillvägagångssätt för att säkerställa uppdateringarnas integritet (källa, kontrollsummor, underskrifter osv.). De fallspecifika villkoren för användning av USB-portar och motsvarande anslutningar kan inkludera till exempel att endast separat definierade USB-minnen (och motsvarande) som verifierats som tillförlitliga och som inte kopplas till andra system kan kopplas till systemet i fråga. De fallspecifika villkoren kan innehålla till exempel ett arrangemang där endast minnesenheter som delats ut av organisationens dataadministration (eller motsvarande) kan kopplas till organisationens system och att koppling av alla andra minnesenheter är förbjudet och/eller förhindras med tekniska medel. I situationer där det finns behov av att hämta information med hjälp av en minnesenhet från system som inte är betrodda, innefattar de fallspecifika villkoren också definitioner om vilka metoder som ska användas för att minska risken som detta orsakar. Som metod kan man till exempel använda koppling av en minnesenhet från en icke betrodd källa till ett isolerat kontrollsystem. Informationen överförs till systemet, och sedan överförs den vidare från systemet till det betrodda systemet med hjälp av en separat minnesenhet.
Exempel på genomförande	I behandlingsmiljöer med säkerhetsklass III–II kan kravet uppfyllas på så sätt att man dessutom vidtar följande åtgärder: Alla användningsfall för import och export av information har identifierats. Säkra verksamhetssätt har definierats, anvisningar har getts om dem och de övervakas. De säkra verksamhetssätten omfattar bedömning av behovet att använda systemets USB-portar och motsvarande anslutningar. a) I situationer där det inte finns en sådan grund för användningen av anslutningar som tål kritisk granskning ska anslutningarna tas ur bruk. b) I situationer där det finns sådan grund för användningen av anslutningar som tål kritisk granskning ska man fallspecifikt bedöma de förutsättningar och villkor som fastställer hurdana anordningar och verktyg (till exempel USB-minnen) som man kan koppla till systemet. I situationer där det finns behov av att importera information med hjälp av en minnesenhet från system som inte är betrodda ska man dessutom för säkerhetsklass III vanligen åtminstone beakta granskning av minnesområdet.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Katakri: I-09
Övrig tilläggsinformation	

Identifierare	TEK-11.3, L:TL II, E:, S:, TS:
Namn	Skydd mot skadeprogram – TL II
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	

Exempel på genomförande	I situationer där det finns behov av att importera information med hjälp av en minnesenhet från system som inte är betrodda beaktar man dessutom för säkerhetsklass II och högre vanligen även hot förknippade med att skräddarsy minnesenhetens kontrollernivå.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 2 och 5 punkten
Referenser	Katakri: I-09
Övrig tilläggsinformation	
Identifierare	**TEK-12, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Spårbarhet av säkerhetsrelaterade händelser
Krav	Pålitliga metoder för att upptäcka olovlig ändring av uppgifter och annan olovlig eller obehörig behandling av uppgifter i databehandlingsmiljön genomförs i miljön för att säkerställa spårbarheten av säkerhetsrelaterade händelser.
Allmän beskrivning	Med spårbarhet avses att händelser i systemmiljön dokumenteras så att man i händelse av en incident kan utreda vad som gjorts i miljön, vem som gjort det och vilka konsekvenserna har varit. Utöver inloggningsuppgifter är logguppgifterna för viktiga nätverksenheter och servrar typiskt viktiga dokument. Samma gäller väldigt ofta logguppgifterna för till exempel arbetsstationer och motsvarande. Omfattningen kan i de flesta fall tillgodoses så att man säkerställer att loggföringen är aktiverad åtminstone i arbetsstationer, servrar, nätverksenheter (särskilt brandväggar, medräknat arbetsstationernas programbrandväggar) och motsvarande enheter. Viktigt är också att man med hjälp av loggarna för nätverksenheterna i efterhand kan utreda vilka administrativa åtgärder som har utförts på enheterna, när de har utförts och vem som har utfört dem. Det bör föras händelseloggar över systemets funktion, användaraktivitet, händelser av säkerhetsrelevans och incidenter. Ett rekommenderat sätt att säkra loggarna är att viktig logginformation styrs till en centraliserad och starkt skyddad loggserver som säkerhetskopieras dagligen till en separat miljö med minst samma säkerhetsklass. Man ska försöka genomföra insamlingen och lagringen av logguppgifter på så sätt att radering och ändring av logguppgifter kan upptäckas även i situationer då till exempel en nätförbindelse mellan loggkällan och loggsamlaren inte är tillgänglig. På motsvarande sätt förutsätter till exempel logginsamling i arbetsstationer som permanent kopplats loss från nätet och bekräftelser av de insamlade logguppgifterna en regelbunden process. En rekommendation med tanke på administratörernas rättskydd och undersökningen av misstänkta dataintrång är att funktionen att administrera logguppgifter åtskiljs från övriga administrationsfunktioner. I genomförandet av spårbarheten ska man också beakta situationer där den som loggat in i systemet har en möjlighet att genomföra funktioner med ett annat konto (user impersonation). Det är också viktigt att programvaran som lagrar och övervakar logguppgifter övervakas, och det ska vara möjligt att snabbt upptäcka eventuella störningar (till exempel inom ett dygn efter att loggkällan slutat skicka in logguppgifter). Behoven i användningsfallet i fråga ska beaktas i förvaringstiderna för logguppgifterna. Till exempel kan det vara motiverat att förutsätta olika lagringstider för loggdata om behandling och överlämnande än för logguppgifter som samlas in för att utreda incidenter. Till exempel i myndighetsverksamhet kan straffrättsliga preskriptionstider vanligen leda till förvaringstider på minst fem år. En vanlig praxis är att logguppgifterna för sex månader är tillgängliga i realtid och logguppgifter för en längre tidsperiod finns tillgängliga vid behov med ett dröjsmål på några arbetsdagar. Olika användningsfall för logguppgifter behandlas också i Informationshanteringsnämndens rekommendation (2020:21, kapitel 7). Genomförandet förutsätter också att man tar i beaktande att logguppgifternas förvaringsutrymme och -tid är tillräckligt omfattande. Rekommendation: tillräckligt mycket plats reserveras för loggdata i miljön. Hur mycket tid som är tillräcklig kan definieras till exempel genom att utifrån logguppgifterna som samlats in under en månad bedöma hur mycket plats den krävda förvaringsperioden behöver. Obs: det lönar sig att i stället reservera en tillräcklig ”buffert” eftersom incidenter och även vissa typer av attacker ökar loggmängden på ett betydande sätt.

Exempel på genomförande	Kravet kan uppfyllas på så sätt att man vidtar följande åtgärder: 1) I verksamheten har förankrats en skriftlig politik/anvisning om insamling, överlämnande och uppföljning av och larm om loggar. Denna har utarbetats med beaktande av verksamhetens krav. 2) De dokument som uppstår är tillräckligt omfattande för verifiering i efterhand av utförda dataintrång eller försök till sådana. 3) Viktiga dokument förvaras i minst 6 månader såvida inte lagstiftningen eller avtalen kräver en längre förvaringstid. Vad gäller behandlingsloggar och dokument för vilka till exempel myndighetsverksamhetens straffrättsliga preskriptionstider gäller är förvaringstiden minst fem år. 4) Logguppgifter och inloggningstjänster skyddas från obehörig åtkomst (administration av användarrättigheter, logisk åtkomstkontroll).
Lagstiftning	Informationshanteringslagen 17 §, 15 §; säkerhetsklassificeringsförordningen 7 §, 14 §
Referenser	Julkri: HAL-7.1; Katakri: I-10
Övrig tilläggsinformation	The United States Government Configuration Baseline (USGCB); ISO/IEC 27002:2022 5.33, 8.15, 8.17; Informationshanteringsnämnden: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, kapitel 7); PiTuKri JT-01
Identifierare	**TEK-12.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Spårbarhet av säkerhetsrelaterade händelser – överlämnande av uppgifter
Krav	Om användningen av informationssystemet förutsätter identifiering eller annan inloggning ska nödvändiga logguppgifter samlas in om användningen av informationssystemet och om överlämnandet av uppgifter från det.
Allmän beskrivning	Användningsändamålet för logguppgifterna är att följa upp hur uppgifterna i informationssystemet används och överlämnas samt att utreda tekniska fel i informationssystemet.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 17 §, 15 §; säkerhetsklassificeringsförordningen 7 §, 14 §
Referenser	Julkri: HAL-07.1, TSU-18; Katakri: I-10
Övrig tilläggsinformation	

Identifierare	TEK-12.2, L:TL III, E:, S:, TS:
Namn	Spårbarhet av säkerhetsrelaterade händelser – TL III
Krav	Behandlingen av uppgifter i säkerhetsklass II–III ska registreras i en elektronisk logg, ett informationssystem, ett ärenderegister eller för kännedom (till exempel som en del av en handling).
Allmän beskrivning	Rekommendationen FM 2021:10: ”Rekommendation om behandling av säkerhetsklassificerade handlingar” har utarbetats om lagringen av logguppgifter förknippade med behandlingen av säkerhetsklassificerade handlingar.
Exempel på genomförande	I behandlingsmiljöer med säkerhetsklass III–II kan kravet uppfyllas på så sätt att man utöver punkterna 1–4 även vidtar följande åtgärder: 5) Viktiga dokument förvaras i minst fem år såvida inte lagstiftningen, rekommendationerna eller avtalen förutsätter en längre förvaringstid. Dokument som är av mycket ringa betydelse till exempel med tanke på straffrättslig utredning av incidenter eller myndighetsverksamhet kan förvaras en kortare tid, till exempel 2–5 år. 6) Logguppgifterna säkerhetskopieras regelbundet. 7) Klockorna i väsentliga databehandlingssystem som är placerade i samma säkerhetsområde är synkroniserade med en överenskommen tidskälla. 8) Det finns en metod för att säkerställa loggarnas integritet (att de inte ändras). 9) Det uppstår anteckningar om användningen och behandlingen av bildade logguppgifter.
Lagstiftning	Informationshanteringslagen 17 §, 15 §; säkerhetsklassificeringsförordningen 7 §, 14 §
Referenser	Katakri: I-10
Övrig tilläggsinformation	Finansministeriet: Rekommendation om behandling av säkerhetsklassificerade handlingar (2021:10) 7.9.
Identifierare	**TEK-12.3, L:TL I, E:, S:, TS:**
Namn	Spårbarhet av säkerhetsrelaterade händelser – TL I
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Riskbaserat rekommenderas det att man i behandlingen av uppgifter i säkerhetsklass I använder sådana lagringstider för logguppgifter som är längre än i säkerhetsklass II (till exempel minst 10 år). Databehandlingsmiljöer med säkerhetsklass I är vanligen begränsade och består till exempel av terminaler som permanent kopplats loss från alla nät. Å andra sidan är det utmanande att på ett pålitligt sätt och enbart med terminaler realisera hållbarheten av loggdata som samlats in under 10 år. Därför förutsätter logginsamlingen i sådana terminaler och bekräftelserna av de insamlade logguppgifterna vanligen en planerad, regelbunden process. Praktiskt kan detta genomföras till exempel genom att regelbundet samla logguppgifterna på ett separat medium som behandlas och förvaras under dess livscykel på samma sätt som uppgifter i säkerhetsklass I. Dessutom ska man observera att om informationssystemets åtkomstkontroll eller till exempel åtgärdernas spårbarhet stöder sig på metoder inom fysisk säkerhet, kan det också vara skäl att förvara och administrera dokument som uppstår om dessa metoder som om de hörde till säkerhetsklass I.
Lagstiftning	Informationshanteringslagen 17 §, 15 §; säkerhetsklassificeringsförordningen 7 §, 14 §
Referenser	Katakri: I-10
Övrig tilläggsinformation	

Identifierare	TEK-13, L:Sekretessbelagd, E:Viktig, S:Viktig, TS:Särskild kategori av personuppgifter
Namn	Förmåga att upptäcka avvikelser och återhämtning
Krav	I databehandlingsmiljön genomförs pålitliga metoder vars syfte är att upptäcka attacker mor databehandlingsmiljön, begränsa attackens effekter så att de påverkar en så liten del av uppgifterna eller databehandlingsmiljöns resurser som möjligt, förhindra andra skador och återställa databehandlingsmiljöns skyddade läge utan dröjsmål.
Allmän beskrivning	Förmågan att upptäcka tekniska avvikelser grundar sig vanligen på tre källor: 1) Händelser som syns i nätdatatrafiken, 2) insamlade uppgifter (loggdata) och 3) händelser som syns vid objekten (hosts). Tillräcklig teknisk observationsförmåga kan vanligen genomföras genom att kombinera observationskällorna ovan. Ju bättre man känner till databehandlingsmiljön i fråga och dess normala verksamhet, desto bättre kan man också upptäcka händelser som avviker från den normala verksamheten. Upptäckt av händelser som avviker från den normala verksamheten stöder också upptäckten av attacker för vilka identifierande uppgifter (IoC, Indicator of Compromise) inte är tillgängliga. Databehandlingsmiljöns normala verksamhet ska vara känd för hela livscykeln, från de första stunderna till stunden då miljön tas ur bruk. Även förändringshanteringen (TEK-17) stöder förmågan att upptäcka avvikelser, bland annat med hjälp av regelbunden granskning av ändringar i maskinvaru- och programvarukonfigurationer. Det finns flera sätt som lämpar sig till kontroller och begränsning av effekterna av upptäckta attacker, från granskning på de centrala nätnodernas nivå till arbetsstations-/serverspecifika sensorer och kombinationer av dessa. Oberoende av nätverksenheterna och leverantörerna som används förutsätter det praktiska genomförandet av observationsförmåga på nätnivån vanligen att man känner till nätdatatrafikens normala tillstånd. I behandlingsmiljöer med säkerhetsklass IV bör observationsförmågan på nätdatatrafiknivån omfatta särskilt nätets/objektets yttre gräns, och från och med klass III även den yttre gränsens gatewaylösning och kommunikationen inuti nätet/objektet. Upptäckt av en attack eller ett missbruksförsök förutsätter i de flesta miljöerna i praktiken att man använder automatiserade verktyg för upptäckt och larm. I vissa fall är det också möjligt och även nödvändigt att behandla logguppgifter manuellt om en avvikelse inte till exempel inte har upptäckts med automatiska metoder och incidenten kräver närmare utredning. Man ska också komma ihåg att man i loggarna endast får samla uppgifter som är nödvändiga för informationssäkerhetsrelaterade åtgärder och att man då åtgärderna vidtas inte får begränsa yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet. Allmänt ska man observera att observationsförmågan förutsätter kännedom om särdragen för varje enskild databehandlingsmiljö. Dessutom förutsätter förmågan att man definierar och skräddarsyr bland annat kritiska objekt händelser som ska uppföljas i enlighet med databehandlingsmiljön i fråga och att observationsförmågan kontinuerligt upprätthålls. Att återställa databehandlingsmiljön till ett skyddat läge inom en skälig tid förutsätter vanligen planerade, beskrivna, utlärda och övade processer och tekniska metoder. Utvecklingen och upprätthållandet av förmågan att upptäcka avvikelser ska också beakta hela personalens roll. Till exempel kan observationer som slutanvändarna anmält ge värdefull information för upptäckt av attacker och attackförsök.
Exempel på genomförande	Det finns kännedom om nätdatatrafikens normalläge (trafikmängd, protokoll och anslutningar). Det finns ett förfarande för att upptäcka händelser som avviker från normalläget (till exempel avvikande anslutningar eller anslutningsförsök).
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom., 17 §; säkerhetsklassificeringsförordningen 7 §, 11 § 1 mom. 2 punkten
Referenser	Julkri: TEK-17; Katakri: I-11, T-07, T-12
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.25, 5.26, 8.15, 8.16; PiTuKri TT-02, JT-01, TJ-05

Identifierare	TEK-13.1, L:Sekretessbelagd, E:Viktig, S:, TS:Särskild kategori av personuppgifter
Namn	Förmåga att upptäcka avvikelser och återhämtning – upptäckt av avvikelser via logguppgifter
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Rekommendationen är att det finns ett förfarande för att upptäcka avvikelser i insamlade loggar och statusinformation (till exempel förändringar i loggmängden). Framförallt ska försök till obehörig användning av informationssystemet kunna upptäckas.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom., 17 §; säkerhetsklassificeringsförordningen 7 §, 11 § 1 mom. 2 punkten
Referenser	Katakri: I-11
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05
Identifierare	**TEK-13.2, L:TL IV, E:Viktig, S:, TS:**
Namn	Förmåga att upptäcka avvikelser och återhämtning – TL IV
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	1) Det finns ett förfarande för att upptäcka avvikelser i insamlade loggar och statusinformation (till exempel förändringar i loggmängden). Framförallt ska försök till obehörig användning av informationssystemet kunna upptäckas. 2) Det finns ett förfarande för att upptäcka avvikelser hos objekt i databehandlingsmiljön (hosts, till exempel arbetsstationer och servrar). 3) Det finns ett förfarande för återhämtning från upptäckta avvikelser.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom., 17 §; säkerhetsklassificeringsförordningen 7 §, 11 § 1 mom. 2 punkten
Referenser	Katakri: I-11
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05
Identifierare	**TEK-13.3, L:TL I, E:, S:, TS:**
Namn	Förmåga att upptäcka avvikelser och återhämtning – TL I
Krav	Användarnas och administratörernas verksamhet följs för att upptäcka ovanlig verksamhet.
Allmän beskrivning	
Exempel på genomförande	Vad gäller behandlingen av uppgifter i säkerhetsklass I rekommenderas det effektiviserad förmåga att upptäcka avvikelser, med betoning på bland annat uppföljning av användarnas och administratörernas verksamhet i databehandlingsmiljön.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom., 17 §; säkerhetsklassificeringsförordningen 7 §, 11 § 1 mom. 2 punkten
Referenser	Katakri: I-11
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.16; PiTuKri JT-01, TJ-05

Identifierare	TEK-14, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Säkerställande av programmens säkerhet
Krav	Applikationer och gränssnitt för applikationsprogrammering (API) planeras, utvecklas, testas och tas i bruk i enlighet med branschens goda säkerhetspraxis. Applikationer och gränssnitt ska tåla allmänna attackmetoder som kan användas mot dem utan att konfidentialiteten, integriteten eller tillgängligheten av de behandlade uppgifterna äventyras.
Allmän beskrivning	Programvaror och deras användningsändamål i olika databehandlingsmiljöer skiljer sig från varandra på ett betydande sätt. På motsvarande sätt finns det också stora skillnader i behoven av säkert genomförande och ibruktagande av program i olika databehandlingsmiljöer och användningsändamål. Till exempel skiljer sig säkerhetsbehoven förknippade med ett kontorsprogram som används i en arbetsstation som avskilts fysiskt från alla nät från behoven riktade på ett ärendehanteringssystem som är tillgängligt för flera användare. Programvarurelaterade risker och säkerhetsbehov kan bedömas till exempel med hjälp av programmets användningsändamål, dess eventuella säkerhetsroll, ytan som kan attackeras och de behandlade uppgifternas karaktär och säkerhetsklass. Om programvarans användningsändamål och roll är att agera till exempel som en mekanism som begränsar åtkomsten vid behandling av säkerhetsklassificerade uppgifter, bör man kunna försäkra sig om att programmet fungerar på ett tillförlitligt sätt. Ytan som kan attackeras i programvara kan väsentligt påverka säkerhetsbehoven förknippade med programvaran. Vanligen kan till exempel tjänster med säkerhetsklass IV vara tillgängliga i större grad och tack vare en mer heterogen grupp än till exempel tjänster med säkerhetsklass III eller II. Säkerhetskraven som ställs på programvarorna kan i system med säkerhetsklass IV till vissa delar vara striktare än till exempel i sådana strikt isolerade och begränsade system med högre säkerhetsklass där varje användare har behov av att ta del av all den information som behandlas i systemet (need-to-know). Säkerhetsklassen för uppgifterna som behandlas och huruvida uppgifterna kan förmodas vara intressanta för utomstående aktörer kan påverka risken och skyddsbehovet som riktas på programvaran. Till exempel kan uppgifter som är politiskt mycket intressanta för utomstående eller uppgifter med hög säkerhetsklassificering påverka riskerna och säkerhetsbehoven förknippade med programvaran i betydande grad, även vad gäller beredskapen för de mest avancerade attacker. Då man tar i bruk färdig programvara eller beställer skräddarsydd eller själv producerad programvara ska beställaren redan i planeringsfasen ägna uppmärksamhet åt den informationssäkra utvecklingen av programvaran och dess kringkomponenter. Även andra faktorer som täcker hela programvarans livscykel ska beaktas. Sådana faktorer är till exempel kraven vid tidpunkten för ibruktagning, avtalsteknik, uppdateringspraxis och förändringshantering. Programvaror som väsentligt påverkar skyddet av säkerhetsklassificerade uppgifter ska genomföras med stöd i praxis gällande säker programutveckling, inklusive både kvaliteten på programvarukoden och programutvecklingens processer. Definieringen av programvarans krav ska redan i upphandlingsfasen beakta lagstiftningsbaserade krav. Särskilt helheter förknippade med kryptering (I-12), förvaltningsanslutningar (I-04), användarhantering och -identifiering (I-06, I-07), härdning (I-08) och spårbarhet (loggföring, I-10) ska beaktas även i genomförandet av programvarorna. Genomförandet av program får inte äventyra genomförandet av behovet av att ta del av information (need-to-know) eller ge utomstående aktörer åtkomst till den skyddade databehandlingsmiljön eller dess delhelheter. Man ska vid livscykelns olika skeden säkerställa i synnerhet att ansvaret vad gäller utförandet av programreparationer har fördelats och möjliggöra upprätthållande av programvarans säkerhet även mot nya attacktekniker. Man kan även sträva efter att försäkra sig om den tillräckligt bra kvaliteten av färdigprogram genom att följa motsvarande principer. Ibland kan det uppstå behov av att använda tjänster vars programkod och dess utvecklingspraxis har dålig eller till och med obefintlig synlighet. Man kan försöka få bevis på pålitligheten av sådana program till exempel genom att undersöka uppdateringsfrekvensen, dokumentationen och eventuell annan synlighet, såsom existerande testrapporter. I sådana situationer kan man utöver säker konfigurering även utnyttja ersättande skydd. I säker konfigurering och som ersättande skydd kan man med vissa begränsningar utnyttja till exempel effektiviserad observationsförmåga, härdning, begränsning av koden vid genomförande (till exempel AppLocker, SELinux, AppArmor), applikationsbrandväggar (WAF) och logisk differentiering av hela programvaran, till exempel med hjälp av virtualisering. Anvisningar och standarder som preciserar ämnesområdet ska utnyttjas i säkerställandet av programvarornas säkerhet. Sådana är till exempel VAHTI Sovelluskehityksen tietoturvaohje (VAHTI 1/2013), OWASP Application Security Verification Standard (ASVS) och Cybersäkerhetscentrets anvisning ”Säker utveckling: med sikte på godkännande”.

Exempel på genomförande	1) Programvarornas (applikationer, tjänster, system) användningsändamål och programvarornas eventuella säkerhetsroller har identifierats. 2) Programvarornas (applikationer, tjänster, system) säkerhetsbehov har bedömts, med särskilt beaktande av programvarans användningsändamål, dess eventuella säkerhetsroll, ytan som kan attackeras och de behandlade uppgifternas karaktär och säkerhetsklass. 3) Programvarornas (applikationer, tjänster, system) beroendeförhållanden och gränssnitt har identifierats. Krav som motsvarar kraven på programvaran gäller även beroendeförhållandena och gränssnitten, med beaktande av till exempel använda bibliotek, gränssnitt (API) och utrustningsbindningar. Kraven beaktar både serversidans och kundsidans andelar. 4) Kritiska programvaror (applikationer, tjänster, system) genomförs eller genomförandet kontrolleras i den mån det är möjligt mot en pålitlig standard och/eller med hjälp av en anvisning om säker programmering. 5) Man har säkerställt att upprätthållandet, utvecklingen och förändringshanteringen av kvaliteten på programvarornas (applikationer, tjänster, system) programkod motsvarar behoven under hela livscykeln. 6) Man har säkerställt att programvarorna (applikationer, tjänster, system) uppfyller de lagstiftningsbaserade kraven. Man ska särskilt beakta helheter förknippade med kryptering, förvaltningsanslutningar, användarhantering och -identifiering, härdning och spårbarhet.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom.; säkerhetsklassificeringsförordningen 11 § 1 mom. 2, 3, 4, 5 och 6 punkten
Referenser	Julkri: HAL-16; Katakri: I-13
Övrig tilläggsinformation	OWASP Application Security Verification Standard (ASVS); CWE TOP 25 Most Dangerous Software Errors; The Building Security In Maturity Model; Software Assurance Maturity Model; ISO/IEC 27002:2022 5.8, 8.26, 8.27, 8.28, 8.29; Traficom: Säker utveckling: med sikte på godkännande; PiTuKri MH-02
Identifierare	**TEK-15, L:TL III, E:, S:, TS:**
Namn	Diffus strålning (TEMPEST) och elektronisk underrättelse
Krav	Skyddsåtgärder vidtas i databehandlingsmiljöer förknippade med säkerhetsklassificerade uppgifter med tillräckligt säkra metoder på så sätt att oavsiktligt elektromagnetiskt läckage inte äventyrar uppgifterna (TEMPEST-skyddsåtgärder). Dessa skyddsåtgärder ska ställas i relation till risken att information exploateras och till informationens säkerhetsklass. Vid elektronisk behandling av uppgifter i säkerhetsklass III eller II ska man se till att risker förknippade med elektronisk underrättelse har minskats i tillräckligt stor grad.
Allmän beskrivning	Vad gäller diffus strålning som överskrider gränsvärdena i behandlingsmiljöer med säkerhetsklasserna III–II genomförs skyddet med förfaranden som är tillräckligt säkra för säkerhetsklassen i fråga. Vad gäller uppgifter i säkerhetsklass III har man större möjligheter att godkänna ersättande förfaranden för att uppnå adekvat skydd.
Exempel på genomförande	1) Riskerna förknippade med diffus strålning har identifierats och bedömts. 2) Skyddsåtgärderna eller de ersättande förfarandena har dimensionerats för riskerna, uppgifternas säkerhetsklass och den kvarstående riskens godtagbara nivå.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 2 mom.
Referenser	Julkri: FYY-5.6; Katakri: I-14
Övrig tilläggsinformation	Traficom: Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet; ISO/IEC 27002:2022 7.12

Identifierare	TEK-15.1, L:TL II, E:, S:, TS:
Namn	Diffus strålning (TEMPEST) och elektronisk underrättelse – TL II
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Man har vidtagit skyddsåtgärder som har dimensionerats efter riskerna och uppgifternas säkerhetsklass. Tillräckligheten av svarsåtgärderna gällande objektets diffusa strålning kan verifieras med zonmätning eller mätning av den skyddade lokalen.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 2 mom.
Referenser	Katakri: I-14
Övrig tilläggsinformation	

Identifierare	TEK-15.2, L:TL I, E:, S:, TS:
Namn	Diffus strålning (TEMPEST) och elektronisk underrättelse – TL I
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Vid skyddet av uppgifter i säkerhetsklass I ska man beakta riskerna som skiljer sig från uppgifterna i säkerhetsklass II och ställa dem i relation till skyddsåtgärderna som vidtas. Diffus strålning och principerna om skydd mot den beskrivs närmare i Cybersäkerhetscentrets anvisning om skydd mot diffus strålning.
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 2 mom.
Referenser	Katakri: I-14
Övrig tilläggsinformation	

Identifierare	TEK-16, L:Sekretessbelagd, E:Viktig, S:, TS:Särskild kategori av personuppgifter
Namn	Kryptering av information
Krav	När sekretessbelagda uppgifter överförs i allmänna datanät, krypteras informationen med en lösning som inte har några kända sårbarheter och som enligt tillverkaren stöder modern krypteringsstyrka och moderna krypteringsinställningar. Dessutom ska informationsöverföringen ordnas så att mottagaren säkerställs eller identifieras på ett tillräckligt datasäkert sätt innan mottagaren kan behandla överförda sekretessbelagda uppgifter som inte har säkerhetsklassificerats.
Allmän beskrivning	Elektronisk överföring av sekretessbelagda uppgifter är förknippad med många risker. Att minska riskerna till en acceptabel nivå förutsätter att faktorer förknippade med såväl personalen som det tekniska genomförandet beaktas. I situationer där det finns behov av att överföra sekretessbelagda uppgifter till exempel mellan två organisationer via ett offentligt nät förutsätter säker överföring säkra krypteringslösningar och säker nyckelhanteringspraxis samt en personal som fått övning i deras användning. I situationer där användningen av en krypteringslösning förutsätter åtgärder från personalen (till exempel förmedling av en sekretessbelagd handling till en annan organisation som en krypterad bilaga till ett e-postmeddelande), ska man ägna särskilt uppmärksamhet åt att säker användning av krypteringslösningen förankras bland personalen. En tekniskt säker krypteringslösning producerar inte ett tillräckligt skydd för sekretessbelagd information till exempel i situationer där nyckelhanteringspraxis är bristfällig eller där personalen inte använder krypteringslösningen i enlighet med principerna om säker användning förknippade med lösningen. Tillräckligt säkert säkerställande av mottagaren beror i stor grad på krypteringslösningen som används. Till exempel i användningspolitiken för krypteringslösningar som Transport- och kommunikationsverkets Cybersäkerhetscenter har godkänt för skydd av säkerhetsklassificerade uppgifter tar man ofta även ställning till användarnas identifiering när krypteringslösningen i fråga används till exempel vid kommunikation med en person i en annan organisation. Å andra sidan stöder identifieringen av motparten i flera krypteringslösningar på att nyckelhanteringen är tillförlitlig (till exempel (LAN-2-LAN) kryptering av nät mellan organisationens verksamhetsställen eller två olika organisationer som grundar sig på delad hemlighet eller filkryptering som grundar sig på delad hemlighet). Vid valet av krypteringsstyrka och -inställningar kan man i regel utnyttja styrkor och inställningar i enlighet med säkerhetsklass IV. Internet, MPLS-nät som operatören erbjuder och till exempel så kallade svartfibrer tolkas som offentliga nät. Detta täcker telefon, telefax (fax), e-post, meddelandetjänster och andra motsvarande informationsöverföringsmetoder som fungerar via datanät.
Exempel på genomförande	1) Då man överför sekretessbelagda uppgifter via nät utanför fysiskt skyddade områden som godkänts för informationen i fråga ska man i synnerhet beakta krypteringens roll som centralt skydd. a) Personalen har i bruk arbetsredskap och metoder för att skydda sekretessbelagda uppgifter som inte säkerhetsklassificerats med en krypteringslösning som inte har några kända sårbarheter och som enligt tillverkaren stöder modern krypteringsstyrka och moderna krypteringsinställningar. b) Personalens kompetens i säker användning av krypteringslösningen har säkerställts (till exempel anvisningar, utbildning och tillsyn). 2) Hemliga nycklar är tillgängliga endast för auktoriserade användare och processer. Processerna och praxis inom hanteringen av krypteringsnycklar har dokumenterats och genomförts på ett ändamålsenligt sätt. Processerna förutsätter åtminstone följande: a) kryptografiskt starka nycklar, b) säker fördelning av nycklar, c) säker förvaring av nycklar, d) regelbundet byte av nycklar, e) byte av gamla eller avslöjade nycklar, f) förhindrande av icke auktoriserade byten av nycklar. 3) Säkerheten av krypteringslösningens leveranskedja har säkerställts på en tillräckligt hög nivå. Man har i synnerhet säkerställt krypteringslösningens leveranskedja från en pålitlig tillverkare till objektets databehandlingsmiljö.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Julkri: TEK-01; Katakri: I-01, I-12, I-15, I-18
Övrig tilläggsinformation	Traficom: Krypteringslösningar som godkänns av Transport- och kommunikationsverket Traficoms NCSA-verksamhet; Traficom: Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat; Traficom: Säker utveckling: med sikte på godkännande; Informationshanteringsnämnden: Rekommendation om behandling av säkerhetsklassificerade handlingar (2020:19, kapitel 7); ISO/IEC 27002:2022 5.14, 5.31, 8.24; PiTuKri JT-05, SA-01, SA-02, SA-03

Identifierare	TEK-16.1, L:Sekretessbelagd, E:Viktig, S:, TS:Särskild kategori av personuppgifter
Namn	Kryptering av information – kryptering inom ett säkerhetsområde
Krav	Då sekretessbelagda uppgifter överförs inom myndighetens interna nät kan man använda kryptering för en lägre nivå eller okrypterad informationsöverföring enligt riskhanteringsprocessens resultat.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Julkri: FYY-7.1; Katakri: I-15
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03
Identifierare	**TEK-16.2, L:TL IV, E:, S:, TS:**
Namn	Kryptering av information – överföring av säkerhetsklassificerade uppgifter utanför säkerhetsområden
Krav	När säkerhetsklassificerade uppgifter överförs utanför godkända, fysiskt skyddade säkerhetsområden, ska uppgifterna/datatrafiken krypteras på ett tillräckligt säkert sätt. Dessutom ska informationsöverföringen ordnas så att mottagaren säkerställs eller identifieras på ett tillräckligt datasäkert sätt innan mottagaren kan behandla överförda säkerhetsklassificerade uppgifter.
Allmän beskrivning	Särskilt inom skyddet av säkerhetsklassificerade uppgifter betonas behovet av att använda krypteringslösningar vars adekvata säkerhet det finns pålitliga bevis på. Flera olika faktorer beaktas i bedömningen av krypteringslösningar. Utöver att säkerställa krypteringsstyrkan och krypteringslösningens korrekta funktion beaktar man dessutom bland annat hotnivån i krypteringslösningens användningsmiljö. Till exempel vid kommunikation över internet skiljer sig hotnivån betydligt från en situation då krypteringen används för kommunikation inom ett kontrollerat, fysiskt skyddat område (till exempel kommunikation mellan två skyddsområden via ett administrativt område). Andra faktorer som ska beaktas vid bedömningen av krypteringslösningar är till exempel kraven som användningsfallet i fråga ställer på informationens sekretesstid och kryptografiska integritet. Rent programbaserade krypteringslösningar är vanligen acceptabla för klass IV och i vissa situationer och med särskilda villkor även för klass III. Vad gäller klass II och oftast även klass III förutsätter man vanligen mer av plattformens tillförlitlighet. Krypteringslösningarnas godkännandeprocess beskrivs närmare i Cybersäkerhetscentrets anvisning om bedömning och godkännande av krypteringsprodukter. Krypteringslösningens minimikrav behandlas även i beskrivningen av krypteringsstyrka som upprätthålls av Cybersäkerhetscentret och i anvisningen om säker produktutveckling.
Exempel på genomförande	1) Organisationen har identifierats användningsfallen där krypteringslösningar behövs för att skydda säkerhetsklassificerade uppgifter. De identifierade användningsfallen täcker alla situationer där skyddet av säkerhetsklassificerad information stöder helt eller delvis på en krypteringslösning. Man har i synnerhet beaktat kommunikation via offentliga nät eller nät med lägre säkerhetsklass, förmedling av information till en annan organisation och terminaler som tas utanför säkerhetsområdena. 2) Man har skaffat följande för säkerhetsklassen i fråga: a) krypteringslösningar som godkänts av en behörig myndighet och som används i enlighet med den användningspolitik och de -inställningar som fastställts i samband med godkännandet, eller b) fallspecifika godkännanden och användningspolitik/-inställningar från en behörig myndighet för krypteringslösningar som inte godkänts redan tidigare. 3) Då man överför säkerhetsklassificerade uppgifter via nät utanför fysiskt skyddade säkerhetsområden som godkänts för säkerhetsklassen i fråga ska man i synnerhet beakta krypteringens roll som centralt skydd. a) Personalen har i bruk arbetsredskap och metoder för skydd av säkerhetsklassificerade uppgifter med en krypteringslösning som godkänts av en behörig myndighet. b) Personalens kompetens i säker användning av en tillräckligt säker krypteringslösning har säkerställts (till exempel anvisningar, utbildning och tillsyn).

Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Julkri: FYY-7.1; Katakri: I-01, I-12, I-15, I-18, F-08.1
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03
Identifierare	**TEK-16.3, L:TL IV, E:, S:, TS:**
Namn	Kryptering av information – överföring av säkerhetsklassificerade uppgifter inuti säkerhetsområden
Krav	När säkerhetsklassificerade uppgifter överförs innanför godkända, fysiskt skyddade säkerhetsområden, kan kryptering på en lägre nivå eller okrypterad överföring användas enligt riskhanteringsprocessens resultat med grund i separat godkännande från en behörig myndighet.
Allmän beskrivning	
Exempel på genomförande	2) Någondera av följande gäller i situationer där säkerhetsklassificerade uppgifter överförs innanför fysiskt skyddade säkerhetsområden: a) säkerhetsklassens kommunikationskanal är fysiskt skyddad (till exempel kablar som till sin helhet är belägna inom ett begränsat, fysiskt skyddat säkerhetsområde som täcker till exempel endast ett rum och som godkänts för förvaring av uppgifter i säkerhetsklassen i fråga), eller b) informationen skyddas med tillräckligt säker kryptering för en lägre nivå (till exempel HTTPS inom intern kommunikation i säkerhetsklassens nät).
Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Julkri: FYY-7.1; Katakri: I-15
Övrig tilläggsinformation	
Identifierare	**TEK-16.4, L:TL III, E:, S:, TS:**
Namn	Kryptering av information – TL III
Krav	Endast elektroniska uppgifter i säkerhetsklass III kan förvaras utanför skyddsområdet i en terminal som följer säkerhetsklassen i fråga, med den förutsättningen att a) uppgifterna har skyddats med en krypteringslösning som är adekvat för säkerhetsklassen i fråga och b) terminalens informationssäkerhet har säkerställts med adekvata förfaranden, i synnerhet vad gäller konfidentialiteten och integriteten som förutsätts för säkerhetsklassen i fråga.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 §
Referenser	Julkri: FYY-7.1; Katakri: F-04, I-12, I-17, I-18
Övrig tilläggsinformation	
Identifierare	**TEK-16.5, L:TL I, E:, S:, TS:**
Namn	Kryptering av information – TL I
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	I andra situationer där man använder krypteringslösningar för att skydda uppgifter i säkerhetsklass I, till exempel kryptering av terminalernas hårddiskar eller avskiljning av uppgifter med olika ägare, är det skäl att beakta att det finns ett ytterst begränsat antal krypteringslösningar som är tillräckligt pålitliga och godkända för skydd av uppgifter i säkerhetsklass I. I sådana situationer är utgångspunkten att krypteringslösningarna stöder andra skyddsåtgärder, särskilt fysisk åtkomsthantering.

Exempel på genomförande	Man ska särskilt beakta att det finns ett ytterst begränsat antal krypteringslösningar som är tillräckligt pålitliga och godkända för skydd av uppgifter i säkerhetsklass I. Detta förutsätter vanligen att uppgifter i säkerhetsklass I överförs med ett kurirförfarande som godkänts för säkerhetsklass I i situationer där det finns ett behov av att flytta uppgifter i säkerhetsklass I mellan fysiska skyddsområden.
Lagstiftning	Informationshanteringslagen 14 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 7 punkten, 12 §
Referenser	Katakri: I-15
Övrig tilläggsinformation	
Identifierare	**TEK-17, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Förändringshanteringsförfaranden
Krav	Ett förändringshanteringsförfarande som beaktar säkerheten används för ändringar i databehandlingsmiljön.
Allmän beskrivning	Pålitlig hantering av databehandlingsmiljöns informationssäkerhet och ändringar förutsätter att miljöns tekniska struktur och till exempel alla anordningar och programvaror som hör till den är kända. Ändringar i informationssystemens inställningar och verksamhet ska övervakas och upptäckta ändringar ska leda till att deras korrekthet kontrolleras. Med aktuell bokföring kan nödvändiga ändringar inriktas på ett exakt sätt under hela livscykeln, ändringarnas effekter är lättare att förutse och det är möjligt att granska miljöns säkerhet. Man kan i genomförandet av bokföringen utnyttja till exempel nätbilder, förteckningar över anordningar och programkomponenter och konfigurationsdatabaser. Man ska kunna säkerställa databehandlingsmiljöns informationssäkerhet under dess hela livscykel. Detta förutsätter kontinuerlig uppföljning av förändringsbehov och regelbundna ändringar. Förändringsbehov kan till exempel följas upp gällande slutet av livscykeln av databehandlingsmiljöns system eller det nuvarande skyddets oförmåga att svara på nya attackmetoder. Till exempel kan programuppdateringar orsaka oförväntade följder, såsom ändringar i säkerhetsinställningarna och användarrättigheterna eller inträde av nya osäkra tjänster i databehandlingsmiljön. Man kan försöka förebygga skadliga följder till exempel med omfattande testning och granskning av ändringsloggar (vanligen till exempel changelog, readme). Man kan sträva efter att upptäcka skadliga följder till exempel granskning av konfigurationer efter uppdateringar (som installerats i en testmiljö) och bland annat med automatiserad skanning och konfigurationsjämförelser. I skyddet av utrustning mot koppling av olovliga anordningar kan man utnyttja till exempel följande: a) placering av anordningar i en säkerhetsbur eller motsvarande som förseglats och/eller försetts med en larmanordning, b) användning av anordningar som skyddats mot manipulering, eller c) något annat motsvarande förfarande (till exempel försegling av anordningarna som används). Då man använder en metod som grundar sig på försegling bör det finnas en regelbunden process för kontroll av sigillens integritet. Granskningsfrekvensen som är acceptabel för kontroll av olovliga ändringar eller utrustning beror på metoderna som används i objektet i fråga för att begränsa och övervaka åtkomst till objektet (informationssystem, fysisk lokal). I de flesta miljöer kan det räcka med kontroller till exempel halvårsvis eller en gång om året. Skyddet mot koppling av olovlig utrustning ska också beakta anvisningarna till personalen. Man ska beakta att det endast är tillåtet att koppla sådan kringutrustning (till exempel skärm, tangentbord, mus) och sådana medier (till exempel USB-minne som godkänts endast för miljön i fråga)till terminalerna som godkänts för en databehandlingsmiljö med säkerhetsklassen i fråga. Särskilt i situationer där terminalen används i en fysisk lokal med lägre säkerhetsklassificering är det vanligen inte möjligt att använda kringutrustning eller medier som förvaras i lokalen i fråga.
Exempel på genomförande	1) Det finns aktuell bokföring om databehandlingsmiljöns sammansättning. Med bokföring avses anordnings- och programvarubokföring samt information om konfigurationer och förfaranden som påverkas säkerheten. 2) Det finns ett förändringshanteringsförfarande för ändringar förknippade med behandlingen av information och databehandlingsmiljön. Ändringarna kan spåras. 3) Det finns metoder med vilka man säkerställer att databehandlingsmiljöns säkerhetsnivå bevaras i samband med genomförda ändringar.

Lagstiftning	Informationshanteringslagen 13 §, 15 §
Referenser	Katakri: I-03, I-05, I-16, I-17, I-18, T-04, T-12
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.9, 5.36, 5.37, 8.19, 8.29, 8.32; Informationshanteringsnämnden: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, kapitel 5); PiTuKri MH-01
Identifierare	**TEK-17.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Förändringshanteringsförfaranden – omvärdering
Krav	Granskningar och översyn som gäller informationssäkerheten genomförs med regelbundna intervaller under databehandlingsmiljöns funktion och service samt då avvikande situationer uppkommer.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 13 § 1 mom.
Referenser	Katakri: I-16
Övrig tilläggsinformation	
Identifierare	**TEK-17.2, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift**
Namn	Förändringshanteringsförfaranden – dokumentering
Krav	Databehandlingsmiljöns säkerhetshandlingar utvecklas under miljöns livscykel som en oskiljaktig del av hanteringsprocessen för ändringar och inställningar.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 5 § 2 mom.
Referenser	Katakri: I-16
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.9, 8.32
Identifierare	**TEK-17.3, L:TL IV, E:Viktig, S:Viktig, TS:**
Namn	Förändringshanteringsförfaranden – TL IV
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	1) Databehandlingsmiljön har dokumenterats på en sådan nivå att man från dokumentationen kan reda ut de anordningar och program som använts i databehandlingsmiljön, inklusive versionsuppgifter (enhets-, operativsystems- och applikationsprogram). Dokumentationen stöder också hanteringen av sårbarheter. 2) Databehandlingsmiljöer övervakas för att upptäcka olovliga ändringar eller anordningar. Databehandlingsmiljöns bokföring hålls uppdaterad under hela livscykeln. 3) Klassificerings- och skyddsbehoven gällande material förknippat med genomförandet av databehandlingsmiljöns säkerhet (dokumentation, elektronisk bokföring och motsvarande) har fastställts.
Lagstiftning	Informationshanteringslagen 5 § 2 mom., 13 § 1 mom.
Referenser	Katakri: I-16
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.9, 8.8

Identifierare	TEK-17.4, L:TL II, E:Kritisk, S:Kritisk, TS:
Namn	Förändringshanteringsförfaranden – TL II
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	1) Utrustningen skyddas mot anslutning av olovliga anordningar (apparater som spelar in tangenttryckningar, trådlösa sändare inkl. mobila enheter och motsvarande).
Lagstiftning	Säkerhetsklassificeringsförordningen 11 § 1 mom. 2 och 5 punkten
Referenser	Katakri: I-16
Övrig tilläggsinformation	

Identifierare	TEK-18, L:Sekretessbelagd, E:Normal, S:, TS:Personuppgift
Namn	Fjärranvändning
Krav	Användarna har fått anvisningar om fjärranvändning och identifieras på ett tillräckligt tillförlitligt sätt under fjärranvändningen.
Allmän beskrivning	Med fjärranvändning och -fjärrhantering avses traditionellt sådan användning/hantering av informationssystem som sker utanför organisationens verksamhetslokaler med en terminal som skaffats för detta syfte. Vanligen är terminalen en bärbar dator som organisationen lånat till personen. Vad gäller säkerhetsklassificerade uppgifter lämpar sig fjärranvändning i sin traditionella betydelse endast för uppgifter i säkerhetsklass IV. Utbildningen av personalen och de anvisningar som personalen ska erbjudas ska beakta skyddet av särskilt sekretessbelagda uppgifter från utomstående. Skyddet från utomstående omfattar bland annat val av eventuella behandlingsplatser och begränsning av behandlingen i olika typer av platser (förhindrande av olovlig observation och avlyssning), skydd av terminaler och andra arbetsredskap mot stöld och manipulering (förvaring endast i låsta utrymmen, kryptering av minnesområden alltid aktiverad och användning av till exempel skyddsförpackningar och -fodral) och andra förfaranden förknippade med säker användning av terminaler och andra arbetsredskap.
Exempel på genomförande	1) Vid fjärranvändning identifieras användarna på ett tillförlitligt sätt. 2) Det finns anvisningar om fjärranvändning och fjärranvändning övervakas.
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 13 § 1 mom.; säkerhetsklassificeringsförordningen 10 § 1 mom.
Referenser	Julkri: HAL-12, HAL-13, HAL-19; Katakri: I-17, I-18
Övrig tilläggsinformation	CPNI: Personnel Security in Remote Working; CPNI: Configuring and managing Remote Access for Industrial Control Systems; CPNI: Physical Security Advice; ISO/IEC 27002:2022 5.10, 5.37, 6.3, 6.7, 7.1, 7.8, 7.9, 7.10, 8.1; PiTuKri IP-03, JT-05, SA-02

Identifierare	TEK-18.1, L:Sekretessbelagd, E:Viktig, S:, TS:Särskild kategori av personuppgifter
Namn	Fjärranvändning – kryptering av uppgifter och datatrafik
Krav	Terminaler, minnesenheter och dataförbindelser i fjärranvändning utanför säkerhetsområden har skyddats med sådana krypteringslösningar som inte har några kända sårbarheter och som enligt tillverkaren stöder modern krypteringsstyrka och moderna krypteringsinställningar.
Allmän beskrivning	Vad gäller mobila datamedier (hårddiskar, USB-minnen och motsvarande) kan man tillåta användningen av okrypterade anordningar i de fall då datamedierna aldrig lämnas utan tillsyn utanför godkända säkerhetsområden.
Exempel på genomförande	1) Uppgifterna i en terminal ska skyddas med en krypteringslösning som inte har några kända sårbarheter och som enligt tillverkaren stöder modern krypteringsstyrka och moderna krypteringsinställningar. 2) Fjärranvändning av system förutsätter en sådan krypteringslösning för datatrafik som inte har några kända sårbarheter och som enligt tillverkaren stöder modern krypteringsstyrka och moderna krypteringsinställningar. 3) Datamedier (hårddiskar, USB-minnen och motsvarande) som innehåller sekretessbelagda uppgifter får inte lämnas utan tillsyn utanför säkerhetsområden om datamedierna inte har krypterats med en lösning som inte har några kända sårbarheter och som enligt tillverkaren stöder modern krypteringsstyrka och moderna krypteringsinställningar.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 10 §, 11 §, 12 §, 13 §
Referenser	Julkri: FYY-7.1; Katakri: I-18
Övrig tilläggsinformation	ISO/IEC 27002:2022 7.9, 7.10, 8.1
Identifierare	**TEK-18.2, L:TL IV, E:, S:, TS:**
Namn	Fjärranvändning – kryptering av säkerhetsklassificerade uppgifter och datatrafik
Krav	Terminaler, minnesenheter och dataförbindelser i fjärranvändning utanför säkerhetsområden har skyddats med sådana krypteringslösningar som är tillräckligt säkra med beaktande av säkerhetsklassen i fråga.
Allmän beskrivning	Vad gäller mobila datamedier (hårddiskar, USB-minnen och motsvarande) kan man tillåta användningen av okrypterade anordningar i de fall då datamedierna aldrig lämnas utan tillsyn utanför godkända skyddsområden.
Exempel på genomförande	1) Uppgifter som finns på terminalen ska skyddas med en krypteringslösning som är tillräckligt säker för säkerhetsklassen i fråga. Dessutom ska man se till att terminalens integritet är på en nivå som är tillräcklig för säkerhetsklassen. 2) Fjärranvändning av system förutsätter att uppgifterna i säkerhetsklassen i fråga skyddas med tillräckligt säker trafikkryptering. 3) Om datamedier (hårddiskar, USB-minnen och motsvarande) som innehåller säkerhetsklassificerade uppgifter och som förs utanför säkerhetsområden inte har krypterats med en metod som är tillräckligt säker för säkerhetsklassen i fråga, får datamedierna inte lämnas utan tillsyn.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 2 mom.; säkerhetsklassificeringsförordningen 10 §, 11 §, 12 §, 13 §
Referenser	Julkri: FYY-7.1; Katakri: I-18
Övrig tilläggsinformation	ISO/IEC 27002:2022 7.9, 7.10, 8.1

Identifierare	TEK-18.3, L:TL IV, E:Viktig, S:, TS:
Namn	Fjärranvändning – stark autentisering av användare
Krav	Vid fjärranvändning identifieras systemanvändarna med stark autentisering som baserar sig på minst tvåfaktorsverifiering.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 §, 11 § 1 mom. 5 punkten
Referenser	Katakri: F-04, I-18
Övrig tilläggsinformation	

Identifierare	TEK-18.4, L:TL IV, E:Kritisk, S:, TS:
Namn	Fjärranvändning – godkända anordningar
Krav	Vid fjärranvändning använder man endast sådana identifierade anordningar som godkänts för användningsmiljön.
Allmän beskrivning	
Exempel på genomförande	Man använder endast anordningar och fjärråtkomst som godkänts för användningsmiljön.
Lagstiftning	Säkerhetsklassificeringsförordningen 10 §, 11 § 1 mom. 5 punkten
Referenser	Katakri: F-04, I-18
Övrig tilläggsinformation	

Identifierare	TEK-18.5, L:TL III, E:, S:, TS:
Namn	Fjärranvändning – användning av säkerhetsklassificerad information på en offentlig plats
Krav	Säkerhetsklassificerade uppgifter ska inte läsas eller behandlas på annat sätt när man reser eller på offentliga platser.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § 1 mom., 13 §
Referenser	Julkri: FYY-7.1; Katakri: I-18
Övrig tilläggsinformation	

Identifierare	TEK-18.6, L:TL III, E:Kritisk, S:, TS:
Namn	Fjärranvändning – enhetsidentifiering
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	I behandlingsmiljöer med säkerhetsklass III eller II och i andra kritiska behandlingsmiljöer förutsätter man att användningen binds tekniskt till godkänd fjärranvändningsutrustning (till exempel enhetsidentifiering).
Exempel på genomförande	Fjärranvändning har hindrats tekniskt med hjälp av anordningar som inte godkänts.
Lagstiftning	Säkerhetsklassificeringsförordningen 10 §, 11 § 1 mom. 5 punkten
Referenser	Katakri: I-18
Övrig tilläggsinformation	

Identifierare	TEK-18.7, L:TL III, E:Kritisk, S:, TS:
Namn	Fjärranvändning – TL III
Krav	Fjärranvändning (behandling) och förvaring av elektroniska uppgifter i säkerhetsklass III är möjlig utanför skyddsområden i en terminal som följer säkerhetsklassen i fråga, med den förutsättningen att a) uppgifterna har skyddats med en krypteringslösning som är adekvat för säkerhetsklassen i fråga och b) terminalens informationssäkerhet har säkerställts med adekvata förfaranden, i synnerhet vad gäller konfidentialiteten och integriteten som förutsätts för säkerhetsklassen i fråga.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § (TL III)
Referenser	Katakri: I-18
Övrig tilläggsinformation	

Identifierare	TEK-18.8, L:TL II, E:, S:, TS:
Namn	Fjärranvändning – fjärranvändning inom ett säkerhetsområde
Krav	Fjärranvändning av system begränsas till ett säkerhetsområde som godkänts av en behörig myndighet.
Allmän beskrivning	Behandling av uppgifter förutsätter ett fysiskt skyddat säkerhetsområde eller ersättande förfaranden med vilka man uppnår motsvarande fysiskt säkra förhållanden.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § (TL II)
Referenser	Katakri: I-18
Övrig tilläggsinformation	

Identifierare	TEK-18.9, L:TL I, E:, S:, TS:
Namn	Fjärranvändning – TL I
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	Uppgifter i säkerhetsklass I kan förvaras eller på annat sätt behandlas endast i skyddsområden (10 § i säkerhetsklassificeringsförordningen), vilket också begränsar möjligheterna till fjärranvändning.
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 10 § (TL I)
Referenser	Katakri: I-18
Övrig tilläggsinformation	

Identifierare	TEK-19, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Hantering av sårbarheter i program
Krav	Databehandlingsmiljön förses med tillförlitliga metoder för hantering av programsårbarheter som överspänner tjänstens hela livscykel.
Allmän beskrivning	Utnyttjandet av programsårbarheter är en del av många olika typer av attacker. Man ska beakta att sårbar källkod finns i såväl operativsystemsprogram, serverapplikationer och slutanvändarapplikationer som till exempel applikationer och drivrutiner på fast programvarunivå (firmware), BIOS och separata förvaltningsanslutningar (till exempel iLo, iDrac). Utöver programfel orsakar sårbarheter av konfigurationsfel och gammal praxis, till exempel användning av föråldrade krypteringsalgoritmer. Ansvarsfulla leverantörer korrigerar sårbarheter som upptäcks i deras programvaror. Risker kan minskas genom att installera korrigeringar. Då sårbarhetshantering genomföras ska man se till att sårbarhetsskannern, CMDB och andra system är uppdaterade. Även informationssäkerheten ska säkerställas. Hanteringen av sårbarheter bör sikta på noggranna lägesbilder så att kontinuerlig uppföljning och utveckling av program- och systemmiljön utgör en del av verksamheten. Risken som orsakas av brister och olika slags sårbarheter som upptäckts som en del av upprätthållandet av lägesbilden bör bedömas i förhållande till användningsmiljön, och korrigerande åtgärder ska vidtas med grund i hur kritisk bedömningen är. Korrigerande åtgärder är bland annat programvaruleverantörernas sårbarhetskorrigeringar, uppdateringar och konfigurationsändringar som siktar på att eliminera eller begränsa risken. Dessutom lönar det sig att följa upp det stöd som leverantörerna kommer med för de programversioner som används. För föråldrade programversioner publiceras inga regelbundna uppdateringar vilket kan göra det omöjligt att åtgärda sårbarheter i programvaran. Effektiv processliknande hantering av sårbarheter förutsätter en organiserad verksamhetsmodell där ansvaret fördelats och vanligen också samarbete mellan organisationens interna och externa intressentgrupper. Att observera särskilt vid genomförande som utnyttjar molnteknik: – Säkerhetsuppdateringar kan också köras baserat på en gyllene kopia (golden image) som är en tillförlitlig skivavbildning av till exempel de virtuella datorerna försedd med alla de senaste säkerhetsuppdateringarna. Avbildningen används i detta fall regelbundet för att helt återskapa de virtuella datorerna. I denna lösning är det särskilt viktigt att det finns ordentliga rutiner för att säkra att skivavbildningen bibehåller sin integritet. – Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.
Exempel på genomförande	Kravet kan uppfyllas så att det finns en process för hanteringen av sårbarheter som innefattar minst följande åtgärder: 1) Man följer aktivt med myndigheternas, maskin- och programtillverkarnas och motsvarande aktörers informationsbrev om säkerhet och utför kontrollerad installation av de säkerhetsuppdateringar som bedöms vara nödvändiga. 2) Huruvida installeringen av uppdateringar lyckas granskas regelbundet, minst en gång per månad. 3) Nätet och dess tjänster, servrar och arbetsstationer, bärbara datorer, skrivare, mobila enheter och motsvarande som kopplats till nätet granskas på ett omfattande sätt minst en gång om året (sårbarhetsskanning) och alltid efter betydande ändringar för att hitta sådant som ska korrigeras i uppdateringsförfarandena. 4) Behandlingen av sårbarheter och brister i uppdateringsförfarandena som upptäckts har ordnats så att svagheter som väsentligt påverkar skyddet av databehandlingsmiljön tas bort, korrigeras eller på annat sätt begränsas så att behandlingen av säkerhetsklassificerade uppgifter inte äventyras i onödan.
Lagstiftning	Informationshanteringslagen 13 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Julkri: HAL-16, HAL-16.1; Katakri: I-19
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.8; Informationshanteringsnämndens rekommendation (2020:21, kapitel 5); PiTuKri KT-04

Identifierare	TEK-19.1, L:TL IV, E:Viktig, S:Viktig, TS:
Namn	Hantering av sårbarheter i program – TL IV
Krav	Anordningarna i databehandlingsmiljön kontrolleras på ett övergripande sätt för programsårbarheter minst en gång om året och i samband med betydande ändringar.
Allmän beskrivning	
Exempel på genomförande	1) Nätet och dess tjänster, servrar och arbetsstationer, bärbara datorer, skrivare, mobila enheter och motsvarande som kopplats till nätet granskas på ett omfattande sätt minst en gång om året (sårbarhetsskanning, CMDB osv.) och alltid efter betydande ändringar för att hitta sådant som ska korrigeras i uppdateringsförfarandena. 2) Aktualiteten och informationssäkerheten av anordnings- och programvarubokföringen (inkl. CMDB) och skannings-programmet har säkerställts.
Lagstiftning	Informationshanteringslagen 13 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Katakri: I-19
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.8; Informationshanteringsnämndens rekommendation (2020:21, kapitel 5); PiTuKri KT-04

Identifierare	TEK-19.2, L:TL III, E:Kritisk, S:Kritisk, TS:
Namn	Hantering av sårbarheter i program – TL III
Krav	Anordningarna i databehandlingsmiljön kontrolleras på ett övergripande sätt för programsårbarheter minst halvårsvis och i samband med betydande ändringar.
Allmän beskrivning	
Exempel på genomförande	Nätet och dess tjänster, servrar och arbetsstationer, bärbara datorer, skrivare, mobila enheter och motsvarande som kopplats till nätet granskas på ett omfattande sätt minst halvårsvis (sårbarhetsskanning, CMDB osv.) och alltid efter betydande ändringar för att hitta sådant som ska korrigeras i uppdateringsförfarandena. ”Betydande ändringar” kan omfatta till exempel ändringar i nätverkstopologin, ibruktagande av nya system och/eller uppdateringar av gamla på service pack-nivå, betydande ändringar i brandväggar och motsvarande filtreringsregler osv.
Lagstiftning	Informationshanteringslagen 13 §; säkerhetsklassificeringsförordningen 11 § 1 mom. 2 punkten
Referenser	Katakri: I-19
Övrig tilläggsinformation	

Identifierare	TEK-20, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Säkerhetskopiering
Krav	Backup- och återställningsprocesserna har planerats, implementerats, testats och beskrivits så att de motsvarar kraven som lagstiftningen och verksamheten ställer.
Allmän beskrivning	Rekommendationen är att säkerhetskopiering alltid dimensioneras för verksamhetskraven. Säkerhetskopiering som är adekvat i förhållande till verksamhetskraven bör beakta åtminstone följande: 1) Backupfrekvensen är tillräcklig för hur kritisk informationen bedöms vara. Förutsätter utredning av mängden data som kan förloras (recovery point objective, RPO). 2) Säkerhetskopiorna omfattar all information som är väsentlig med tanke på kontinuiteten av systemets verksamhet. 3) Återställningsprocessen är tillräckligt snabb för verksamhetens krav. Förutsätter utredning av hur lång tid en återställning kan ta (recovery time objective, RTO). 4) Backup- och återställningsprocessens korrekthet testas regelbundet. 5) Återställningsprocessens dokumentering är på tillräckligt hög nivå. 6) Den fysiska platsen för säkerhetskopiorna är tillräckligt avskild från systemet (har inte samma ras- eller brandutrymme, avstånd mellan lokalen där säkerhetskopian förvaras och lokalen där systemet förvaras osv.). Obs. Säkerhetskopiorna ska skyddas med metoder för fysisk och logisk åtkomsthantering på minst samma nivå som uppgifternas säkerhetsklass (som eventuellt höjts av den kumulativa effekten).
Exempel på genomförande	Kravet kan uppfyllas på så sätt att man vidtar följande åtgärder: 1) Säkerhetskopiorna behandlas och förvaras under deras livscykel i system med minst motsvarande säkerhetsnivå. 2) Om säkerhetskopior överförs utanför ett fysiskt skyddat säkerhetsområde för säkerhetsklassen i fråga ska förfarandena genomföras enligt punkterna TEK-16 (elektronisk förmedling) och/eller FYY-08 (post/kurir) samt TEK-18 (transport utanför ett fysiskt skyddat område). 3) Backupmedier förstörs tillförlitligt. 4) Återställning av systemet och informationen testas regelbundet till exempel automatiserat så att uppgifterna kan återställas till rätt läge för att säkerställa integriteten.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom.; säkerhetsklassificeringsförordningen 2 § 2 mom., 7 §, 11 § 1 mom. 4 punkten
Referenser	Julkri: VAR-09; Katakri: I-20
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.13; Informationshanteringsnämnden: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, kapitel 5); PiTuKri KT-03

Identifierare	TEK-20.1, L:TL IV, E:, S:, TS:
Namn	Säkerhetskopiering – TL IV
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	Då man behandlar uppgifter från olika ägare med ett och samma backupsystem ska avskiljningsförfarandena som möjliggör granskningsrätt genomföras för backupsystemets anslutningar och lagringsmedier (till exempel ägar-/projektspecifika band som krypterats med olika nycklar och som förvaras i kundspecifika kassaskåp).
Exempel på genomförande	Då man behandlar uppgifter från olika ägare som förbehåller sig rätten till granskning med ett och samma backupsystem ska avskiljningsförfarandena som möjliggör granskningsrätt genomföras i enlighet med säkerhetsklassen i fråga för backupsystemets anslutningar och lagringsmedier.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 16 §; säkerhetsklassificeringsförordningen 7 §, 10 § 1 mom., 11 § 1 mom. 3 punkten
Referenser	Katakri: I-06, I-20
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.13; Informationshanteringsnämnden: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, kapitel 5); PiTuKri KT-03

Identifierare	TEK-20.2, L:TL III, E:, S:, TS:
Namn	Säkerhetskopiering – registrering av säkerhetskopior och uppföljning av behandling
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Det finns register över säkerhetskopiorna och behandlingen av säkerhetskopior registreras i en elektronisk logg, ett informationssystem, ett ärendehanteringssystem, ett manuellt diarium eller för kännedom (till exempel som en del av en handling).
Lagstiftning	Säkerhetsklassificeringsförordningen 14 §
Referenser	Katakri: F-08.3, I-20
Övrig tilläggsinformation	

Identifierare	TEK-21, L:Sekretessbelagd, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Förstöring av uppgifter i elektroniskt format
Krav	Förstöring av uppgifter i elektroniskt format har ordnats på ett tillförlitligt sätt. Man använder sådana metoder i förstöringen av sekretessbelagda uppgifter som förhindrar att informationen helt eller delvis kan sammanställas på nytt.
Allmän beskrivning	Informationen måste skyddas ända till slutet av livscykeln. Detta ska beaktas i synnerhet då tredjepartstjänster används för att förstöra informationen till exempel genom smältning av hårddiskar. Det vanligaste förfaringssättet är att den organisation som ansvarar för informationen övervakar förstöringsprocessen till slutet av informationslivscykeln. Säker förstöring av uppgifter ska beaktas även i hanteringen av anordningarnas livscykel och i deras förstöring, inklusive kringutrustning och olika typer av minnesenheter. Det är skäl att beakta även personalens roll i förstöringsprocessen. Organisationen ska välja ett entydigt sätt på vilket personalen kan förstöra uppgifter. +N79
Exempel på genomförande	Kombination av metoder vid förstöring Andra metoder som ersätter eller kompletterar strimlingsskyddet kan användas om metoden tillförlitligt förhindrar återskapande av uppgifterna (till exempel smältning av partiklarna från en hårddisk). Kryptering av information kan också minska riskerna avsevärt i olika skeden av informationens och utrustningens livscykel. Att observera vid förstöring av uppgifter i elektroniskt format Förfarandena för tillförlitlig förstöring av uppgifter i elektroniskt format bör omfatta all utrustning som någon gång under sin livscykel haft sparad säkerhetsklassificerad information. Särskilt när delar av utrustningen (hårddiskar, minnen, minneskort osv.) tas ur bruk, skickas för underhåll eller går till återanvändning ska säkerhetsklassificerade uppgifter förstöras på ett tillförlitligt sätt. Om en tillförlitlig radering (till exempel tillräckligt säker överskrivning) inte är möjlig, ska delar som innehåller säkerhetsklassificerade uppgifter 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.
Lagstiftning	Informationshanteringslagen 21 § 2 mom.; säkerhetsklassificeringsförordningen 15 §
Referenser	Julkri: FYY-11, FYY-11.1, FYY-11.2, FYY-11.3; Katakri: T-12, F-08.3, F-08.4, I-21
Övrig tilläggsinformation	Traficom: Kiintolevyjen elinkaaren hallinta (26.10.2016); CPNI: Secure destruction of sensitive items (2017); ISO/IEC 27002:2022 7.10, 7.14; Informationshanteringsnämnden: Suosituskokoelma tiettyjen tietoturvallisuussäädösten sovel-tamisesta (2020:21, kapitel 4); PiTuKri SI-02

Identifierare	TEK-21.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Förstöring av uppgifter i elektroniskt format – arkivering
Krav	Skyldigheten att arkivera uppgifterna har beaktats i hanteringen av informationens livscykel.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 21 §
Referenser	
Övrig tilläggsinformation	

Identifierare	TEK-21.2, L:Sekretessbelagd, E:, S:, TS:Personuppgift
Namn	Förstöring av uppgifter i elektroniskt format – förstöring av uppgifter i molntjänster
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	Att observera särskilt vid genomförande som utnyttjar molnteknik: – Om sekretessbelagda uppgifter som inte säkerhetsklassificerats har lagrats i en molntjänst endast i en krypterad form som bedömts vara tillräckligt säker kan den kvarstående risken vara acceptabel om nycklarna som använts i krypteringen kan förstöras på ett tillförlitligt sätt. Förfarandet kan också lämpa sig för förstöring av personuppgifter efter deras lagstadgade lagringstid.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 21 § 2 mom.
Referenser	
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.23; PiTuKri SA-03

Identifierare	TEK-21.3, L:TL IV, E:, S:, TS:
Namn	Förstöring av uppgifter i elektroniskt format – TL IV
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Förstöring genom överskrivning Då man förstör säkerhetsklassificerat material genom överskrivning är rekommendationen att man följer de krav på överskrivning och återanvändning av minnesenheter som anges i Cybersäkerhetscentrets anvisning ”Kiintolevyjen elinkaaren hallinta”. Förstöring genom strimling Då säkerhetsklassificerat material förstörs genom strimling ska man följa strimlingskraven för material i säkerhetsklassen i fråga enligt rekommendationen ”FM 2021:10 Rekommendation om behandling av säkerhetsklassificerade handlingar”.
Lagstiftning	Informationshanteringslagen 21 § 2 mom.; säkerhetsklassificeringsförordningen 15 §
Referenser	Julkri: FYY-11.1, FYY-11.2, FYY-11.3; Katakri: I-21
Övrig tilläggsinformation	Traficom: Kiintolevyjen elinkaaren hallinta (26.10.2016); Informationshanteringsnämnden: Rekommendation om behandling av säkerhetsklassificerade handlingar (2021:10)

Identifierare	TEK-21.4, L:TL II, E:, S:, TS:
Namn	Förstöring av uppgifter i elektroniskt format – uppgifter som utarbetats av en annan myndighet
Krav	Om uppgifterna har utarbetats av en annan myndighet ska denna myndighet anmälas om förstöringen av onödig information om informationen inte återlämnas till myndigheten i fråga.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 15 § 2 mom.
Referenser	Katakri: I-21
Övrig tilläggsinformation	

Identifierare	TEK-21.5, L:TL II, E:, S:, TS:
Namn	Förstöring av uppgifter i elektroniskt format – den som utför förstöringen
Krav	Uppgifterna får endast förstöras av en person som myndigheten utsett för detta. Beredningsskedets versioner kan förstöras av personen som utarbetat dem.
Allmän beskrivning	
Exempel på genomförande	
Lagstiftning	Säkerhetsklassificeringsförordningen 15 § 2 mom.
Referenser	Katakri: I-21
Övrig tilläggsinformation	

Identifierare	TEK-21.6, L:TL I, E:, S:, TS:
Namn	Förstöring av uppgifter i elektroniskt format – TL I
Krav	Underkriteriet preciserar huvudkriteriets krav.
Allmän beskrivning	
Exempel på genomförande	Strimlingskraven för säkerhetsklass II som anges i ”FM 2021:10 Rekommendation om behandling av säkerhetsklassificerade handlingar” kan användas då elektronisk information i säkerhetsklass I förstörs om skyddet kompletteras med myndighetsgodkända förfaranden. Vanliga förfaranden är bland annat efterbehandling där man bränner eller smälter partiklarna under övervakning.
Lagstiftning	Säkerhetsklassificeringsförordningen 15 §
Referenser	Katakri: I-21
Övrig tilläggsinformation	

Identifierare	TEK-22, L:, E:, S:Normal, TS:
Namn	Informationssystemens tillgänglighet
Krav	Myndigheten ska säkerställa informationssystemens tillgänglighet under systemets hela livscykel.
Allmän beskrivning	Genomförandet av tillgänglighetskraven ska beakta belastningens längd, feltoleransen och återhämtningstiden som förutsätts av informationssystemet.
Exempel på genomförande	Tillgänglighetskraven har identifierats. Man har identifierat åtminstone den längsta tid som systemet kan vara ur bruk, målet för återställningstiden och målet för återhämtningspunkten.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom. 4 punkten
Referenser	Julkri: VAR-02
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.6, 8.14
Identifierare	**TEK-22.1, L:, E:, S:Normal, TS:**
Namn	Informationssystemens tillgänglighet – förfaranden som skyddar tillgängligheten
Krav	Genomförandet av förfaranden som skyddar tillgängligheten har ställts i förhållande till målet för återställningstiden.
Allmän beskrivning	
Exempel på genomförande	Förfaranden som skyddar tillgängligheten har genomförts med systemspecifikt skräddarsydda skydd. Skyddet kan innefatta till exempel duplicering av körmiljöerna för centrala nätförbindelser, anordningar och applikationer.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom. 4 punkten
Referenser	Julkri: VAR-02, VAR-06, VAR-07, VAR-08
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.30
Identifierare	**TEK-22.2, L:, E:, S:Normal, TS:**
Namn	Informationssystemens tillgänglighet – övervakning av tjänsterna
Krav	Tillgängligheten av tjänsterna och informationssystemen följs upp och övervakas på den nivå som deras kritikalitet förutsätter.
Allmän beskrivning	
Exempel på genomförande	1) Om tjänsten har tillgänglighetskrav följer man upp tillgängligheten med ett övervakningssystem. 2) Övervakningssystemet ska ge larm om upptäckta avvikelser i tillgängligheten.
Lagstiftning	Informationshanteringslagen 13 § 1 mom., 15 § 1 mom. 4 punkten
Referenser	Julkri: HAL-07
Övrig tilläggsinformation	ISO/IEC 27002:2022 8.16

Identifierare	TEK-23, L:, E:Viktig, S:Viktig, TS:
Namn	Informationssystemens funktionella användbarhet
Krav	Myndigheten har säkerställt feltoleransen och den funktionella användbarheten av informationssystem som är väsentliga med tanke på att sköta uppgifterna.
Allmän beskrivning	Det rekommenderas att man vid säkerställandet av funktionell användbarhet använder såväl tekniska användbarhetstester som användbarhetstester som genomförs av användarna eller heuristiska expertbedömningar. I skräddarsydda system bör användbarheten fastställas och planeras enligt metoder som godkänts i organisationen. Användbarheten bör kontinuerligt testas under utvecklingen. Användbarheten av färdig programvara bör testas i samband med godkännandetestningen. Testningen bör genomföras ur olika användargruppers synvinkel. Användbarheten kan testas redan under upphandlingsfasen och sålunda på ett bättre sätt säkerställa att systemet som upphandlas är lämpligt för användningsbehovet. Uppfyllandet av informationshanteringslagen kan också stödas med förfaranden i enlighet med lagen om tillhandahållande av digitala tjänster (306/2019), förknippade med tillgängligheten av tjänster som tillhandahålls till publiken.
Exempel på genomförande	1) Informationssystem som är väsentliga för utförande av myndigheternas uppgifter har identifierats. Det finns en förteckning över de informationssystem som identifierats som väsentliga. 2) Feltoleransen och den funktionella användbarheten av informationssystem som identifierats som väsentliga säkerställs med hjälp av testning i både upphandlingsskedet och i samband med betydande underhållsåtgärder. Vid säkerställandet beaktar man särskilt att a) det är enkelt att lära sig använda informationssystemet, b) informationssystemets funktionslogik är lätt att komma ihåg, c) informationssystemets funktion stöder de arbetsuppgifter som användaren utnyttjar systemet för och d) informationssystemet främjar dess felfria användning.
Lagstiftning	Informationshanteringslagen 13 § 2 mom.
Referenser	Julkri: HAL-17, HAL-17.1
Övrig tilläggsinformation	

5 Beredskap och kontinuitetshantering

Delområdet innehåller kriterier som gäller beredskap och kontinuitetshantering i normala förhållanden. Kriterierna grundar sig på hanteringsmetoder som beskriver informationssäkerhetens kontinuitet och som skildras i informationshanteringslagen (bland annat i 4 § 2 mom. 2 punkten, 13 § 1, 2 och 4 mom. och 15 §), anvisningar och informationssäkerhetsåtgärder som utarbetas för allmänna krav och standarden ISO/IEC 27002. Åtgärder som gäller verksamhetens kontinuitet i undantagsförhållanden och som omfattas av beredskapslagen omfattas inte av kriterierna. Kriterierna stöder dock för sin del organisationen även i att uppfylla kraven gällande beredskap för undantagsförhållanden.

Delområdets kriterier gäller huvudsakligen objekt som klassificerats som viktiga eller kritiska med tanke på tillgängligheten. Nivåerna av tillgänglighet beskrivs i kapitel 4.2 Klassificeringsnivåer. Kriterierna kan riskbaserat tillämpas även i objekt som hör till lägre tillgänglighetskategorier. Att reda ut kraven på kontinuitet och lagstiftningen som ligger till grund för dem gäller dock i princip alla organisationer.

Delområdets centrala kriterier utgörs av beredskapsåtgärder förknippade med olika slags allvarliga störningssituationer, planer för verksamhetens kontinuitet och informationssystemens återställning samt övning av dessa planer. Kontinuitetshanteringen är nära förknippad med processer för hantering av störningar och avvikande situationer. Kriterierna associerade med dessa beskrivs i delområdena administrativ säkerhet och teknisk säkerhet.

Identifierare	VAR-01, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Lagstiftning som styr beredskapen
Krav	Organisationen har identifierat den nationella och EU-lagstiftningen som styr IKT-beredskapen i anslutning till organisationens verksamhet och tjänster samt de övriga normerna förknippade med IKT-beredskap.
Allmän beskrivning	Lagstiftningen och normerna definierar en miniminivå för genomförandet av IKT-beredskapen. Utöver detta ska organisationen beakta behoven som uppstår från särdragen i organisationens egen verksamhet. Att förstå funktionernas interna och externa beroendeförhållanden är en grundläggande förutsättning för kostnadseffektiv ledning av beredskapen.
Exempel på genomförande	Man utreder i organisationen lagstiftningen, bestämmelserna, anvisningarna, standarderna, avtalen och alla eventuella internationella skyldigheter som är förknippade med IKT-beredskap och kontinuitetshantering. Det är särskilt viktigt att både organisationen som skaffar tjänsten och organisationen som producerar tjänsten känner till de bestämmelser som påverkar tjänsten och säkerställer att den andra också är medveten om dem. Lagstiftningen som styr organisationens verksamhet och andra styrande handlingar har oftast identifierats och listats i informationssäkerhets- och riskhanteringspolitikens grunder. Strategierna, principerna och verksamhetsplaneringen beaktar riktlinjerna som styr IKT-beredskapen och som ställts i styrhandlingar på statsrådsnivå.
Lagstiftning	Informationshanteringslagen 4 § 2 mom. 2 punkten, 13 § 1 mom.
Referenser	Julkri: HAL-05
Övrig tilläggsinformation	PiTuKri TJ-07, PiTuKri EE-02

Identifierare	VAR-02, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Fastställande av kraven på kontinuitet
Krav	Kraven på kontinuitet gällande verksamheten och dess väsentliga tjänster och informationssystem har fastställts.
Allmän beskrivning	Målen för tjänstens eller systemets återhämtningstid ska definieras enligt hur länge systemet kan som längst vara ur bruk med tanke på organisationens verksamhet. Ur verksamhetens synvinkel ska man fastställa hur mycket information som kan förloras eller från en hur lång period information kan förloras.
Exempel på genomförande	Organisationen ska definiera kontinuitetskraven i samarbete med riskhanteringen, informationssäkerheten, dataskyddet, verksamheten och arkitekturen. Kärnfunktionernas och -processernas tjänster och system som ska skyddas har identifierats och tillgänglighetsmål har ställts för dem i enlighet med kärnfunktionernas eller -processernas krav. Förmågan att starta återhämtningsåtgärder har fastställts per tjänst.
Lagstiftning	Informationshanteringslagen 4 § 2 mom. 1 punkten, 13 § 1 och 2 mom., 15 § 1 mom.
Referenser	Julkri: HAL-05
Övrig tilläggsinformation	Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 6 och kapitel 11; ISO/IEC 27002:2022 5.30

Identifierare	VAR-02.1, L:Offentlig, E:Ringa, S:Ringa, TS:Personuppgift
Namn	Fastställande av kraven på kontinuitet – överföring av tjänster
Krav	Kontinuitetskraven beaktar tjänsternas hemtagning och överföring till en annan tjänsteleverantör.
Allmän beskrivning	Vid upphandling av tjänsten ska man beakta att det kan vara svårt att förankra tjänsten och att det i vissa fall kan vara besvärligt att överföra en tjänst till en annan tjänsteleverantör på grund av leverantörsinlåsning. Kravet ska beaktas särskilt vid upphandling av molntjänster.
Exempel på genomförande	
Lagstiftning	Informationshanteringslagen 4 § 2 mom. 1 punkten, 13 § 1, 2 och 4 mom., 15 § 1 mom.
Referenser	Julkri: HAL-05
Övrig tilläggsinformation	Pilvipalveluiden soveltamisohje 2020:73; ISO/IEC 27002:2022 5.23
Identifierare	**VAR-03, L:, E:, S:Viktig, TS:**
Namn	Kontinuitetsplaner
Krav	Kontinuitetsplanerna har utarbetats och tagits i bruk.
Allmän beskrivning	Organisationens kontinuitetsplan innehåller principerna om hur verksamheten ordnas på ett planmässigt sätt i olika situationer. De tjänster som organisationens kärnfunktioner är beroende av identifieras i organisationens kontinuitetsplanering. Dessutom innehåller planeringen bedömningar av vilka effekter som avbrott av olika längd i IKT-tjänsterna har på organisationens kärnfunktioner. Kontinuitetsplanerna ska också beakta bevarandet av informationssäkerhetens krävda nivå i undantagssituationer.
Exempel på genomförande	I kontinuitetsplanen ingår anteckningar om den tillgängliga personalen, nyckelpersoner och reservpersoner samt en bedömning av deras tillgänglighet. Kontinuitetsplanerna innehåller beskrivningar om hur man ska agera under störningssituationer och hur man övergår tillbaka till normal verksamhet efter sådana situationer. Organisationen har vid behov en plan för överföring av IKT-tjänsternas produktion till andra lokaler om de nuvarande lokalerna blir oanvändbara. Kontinuitetsplanerna samordnas med intressentgrupper i en tillräckligt omfattande grad i hela verksamhetskedjan. Planering av kommunikationen i störningssituationer utgör en del av kontinuitetsplanen.
Lagstiftning	Informationshanteringslagen 4 § 2 mom. 2 punkten, 15 §
Referenser	
Övrig tilläggsinformation	Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 11; ISO/IEC 27002:2022 5.23

Identifierare	VAR-03.1, L:, E:, S:Viktig, TS:
Namn	Testning och övning av kontinuitetsplaner
Krav	Kontinuitetsplaner testas och övas regelbundet.
Allmän beskrivning	Med övning testar man hur planerna fungerar i olika slags situationer. Observationerna används för att utveckla planerna.
Exempel på genomförande	Organisationerna ansvarar för sin egen övningsverksamhet och definierar praxis för testning av kontinuitetsplanerna. Organisationen över internt i nationella, regionala och lokala övningar i den omfattning som verksamheten förutsätter.
Lagstiftning	Informationshanteringslagen 4 § 2 mom., 13 § 2 mom., 15 §
Referenser	Katakri: I-13
Övrig tilläggsinformation	ISO/IEC 27002:2022 5.23

Identifierare	VAR-04, L:, E:, S:Viktig, TS:
Namn	Resurser och kompetens
Krav	Personerna känner till kontinuitets- och återhämtningsplanerna förknippade med den egna verksamheten och kan agera i enlighet med dem. Reservpersonerna har utsetts och deras förmåga att sköta uppgifterna i normala situationer har säkerställts.
Allmän beskrivning	
Exempel på genomförande	Varje utbildad person känner till principerna om organisationens beredskap och vet hur olika situationsmodeller påverkar den egna uppgiften. De uppmuntras att delta i olika slags samarbetsgrupper som stöder beredskapen.
Lagstiftning	Informationshanteringslagen 4 § 2 mom.
Referenser	Julkri: HAL-03; Katakri: T-04
Övrig tilläggsinformation	

Identifierare	VAR-05, L:, E:, S:Viktig, TS:
Namn	Personalens tillgänglighet och reservarrangemang
Krav	För att utföra kritiska uppgifter har man planerat och berett alternativa verksamhetssätt, personalens tillgänglighet och reservarrangemang för särskilda situationer.
Allmän beskrivning	
Exempel på genomförande	Åtgärder som lagstiftningen möjliggör har identifierats och vidtagits i nödvändig omfattning till exempel vad gäller upphävande av strejkrätter, användning av nödfallsarbete och personreservering (VAP).
Lagstiftning	Informationshanteringslagen 4 § 2 mom. 2 punkten, 13 § 1 mom., 15 § 1 mom. 4 punkten
Referenser	
Övrig tilläggsinformation	Arbetstidslagen 872/2019, 19 §; lagen om statens tjänstekollektivavtal 664/1970, 11 §; värnpliktslagen 1438/2007, 89 §

Identifierare	VAR-06, L:, E:, S:Viktig, TS:
Namn	Säkerställande av datatrafiken
Krav	Tillgängligheten under störningar av tjänster som är viktiga med tanke på verksamheten har beaktats i datatrafiktjänster och -avtal.
Allmän beskrivning	
Exempel på genomförande	Nätmiljöerna för viktiga tjänster och datatrafiktjänster verifieras till exempel genom duplicering. Datatrafiken kan dupliceras fysiskt via två olika rutter av två olika operatörer. I viktiga miljöer säkerställer man att fel i enstaka datatrafikkomponenter inte avbryter tjänstens verksamhet. I särskilt valda arbetsstationer kan man till exempel installera en separat dataförbindelse via vilken man kan ha åtkomst till det allmänna datanätet. I avtalsfasen bör man också beakta feltoleransen i förbindelser utanför Finland.
Lagstiftning	Informationshanteringslagen 13 § 1, 2 och 4 mom., 15 §
Referenser	Julkri: HAL-16.1
Övrig tilläggsinformation	Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 11

Identifierare	VAR-07, L:, E:, S:Viktig, TS:
Namn	Verifiering av informationstekniska miljöer
Krav	Tillgängligheten under störningar av tjänster som är viktiga med tanke på verksamheten har beaktats i informationstekniska miljöer och därtill relaterade avtal.
Allmän beskrivning	
Exempel på genomförande	Viktiga tjänsters informationstekniska miljöer verifieras till exempel genom duplicering så att fel i enstaka komponenter inte orsakar avbrott som varar längre än vad verksamhetens servicenivå förutsätter. Informationstekniska miljöer kan verifieras med reservkraft eller reservkraftsanslutningar så att eldistributionen kan startas tillräckligt snabbt och upprätthållas en tillräckligt lång tid i förhållande till verksamhetens krav.
Lagstiftning	Informationshanteringslagen 13 § 1, 2 och 4 mom., 15 §
Referenser	Julkri: HAL-16.1
Övrig tilläggsinformation	Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 11

Identifierare	VAR-08, L:, E:, S:Kritisk, TS:
Namn	Feltolerans
Krav	IKT-infrastrukturen och de väsentliga informationssystemen har genomförts utifrån riskbedömningen på ett sätt som säkerställer deras adekvata feltolerans och driftsäkerhet.
Allmän beskrivning	Man har förberett sig för störningar i informationssystemen för att säkerställa snabb återställning. I återställningen utnyttjar man mekanismer som strävar efter feltolerans i realtid eller nästan realtid för att upprätthålla tillgängligheten av kritiska system.
Exempel på genomförande	De kritiska tjänsternas nät-, server- och enhetsmiljöer verifieras till exempel genom duplicering. Utöver backup tar man i organisationen även skyddskopior av systemen. Dessa kopior förvaras minst i ett annat brandutrymme än de egentliga uppgifterna. Informationsmaterial har utifrån riskbedömningen decentraliserats geografiskt till åtminstone två olika platser och tillräckligt långt bort från varandra innanför Finlands gränser. Den offentliga förvaltningens mest kritiska tjänster och deras informationsöverföring genomförs i den mån det är möjligt i enlighet med säkerhetsnätets krav.
Lagstiftning	Informationshanteringslagen 13 § 1 och 2 mom., 15 §
Referenser	
Övrig tilläggsinformation	Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet 2021:65 kapitel 6
Identifierare	**VAR-08.1, L:, E:, S:Kritisk, TS:**
Namn	Feltolerans – beroendeförhållanden
Krav	Beroendeförhållandena mellan olika tjänster och mellan tjänster och andra aktörer har beaktats i hela planeringen av databehandlingsmiljön och dess feltolerans.
Allmän beskrivning	
Exempel på genomförande	Organisationen har identifierat de kritiska tjänsterna och deras hela tjänstekedja. Hela tjänstekedjan har genomförts med hjälp av tjänster med tillräcklig feltolerans. Plattformslösningar med tillräcklig feltolerans, till exempel säkerhetsnät, utnyttjas i genomförandet av feltoleransen.
Lagstiftning	Informationshanteringslagen 13 § 1 och 2 mom., 15 §
Referenser	
Övrig tilläggsinformation	Säkerhetsstrategi för samhället 2017

Identifierare	VAR-09, L:, E:, S:Viktig, TS:
Namn	Planer för informationssystemens återställning
Krav	Planerna för informationssystemens återställning ska utarbetas, tas i bruk och samordnas sinsemellan.
Allmän beskrivning	Återställningsplaner har definierats för återställning från störningssituationer i informationssystem som är viktiga med tanke på organisationens verksamhet.
Exempel på genomförande	De miniminivåer som IKT-tjänsterna behöver kan fastställas i SLA-avtalet som ingåtts om tjänsten och i återställningsplanen. Miniminivåerna kan ställas som tidskrav, anordningsplattformer eller datatrafikskapacitet som åtminstone krävs. Det är alltid den som beställer tjänsten som ansvarar för existensen av återställningsplaner. I utkontrakterade tjänster är det tjänsteleverantören som ansvarar för beredningen av systemspecifika återställningsplaner. Beställaren säkerställer att tjänsteleverantören testar återställningsplanerna regelbundet.
Lagstiftning	Informationshanteringslagen 4 § 2 mom. 2 punkten, 13 § 1 och 2 mom., 15 § 1 mom.
Referenser	Julkri: VAR-02
Övrig tilläggsinformation	

Bilaga 1B: Dataskyddskriterier

Personuppgifter är uppgifter på grundval av vilka en person direkt eller indirekt kan identifieras till exempel genom att kombinera en enskild uppgift med någon annan uppgift som möjliggör identifiering. En person kan identifieras till exempel utifrån namn, personbeteckning, någon faktor som är kännetecknande för personen i fråga eller individualiserande tekniska uppgifter för de terminaler som personen använder.

Kraven i dataskyddsförordningen ska iakttas i behandlingen av personuppgifter då behandlingen helt eller delvis är automatiskt eller då uppgifterna bildar en del av ett register. Dataskyddsförordningen skyddar personuppgifter oberoende av vilken teknik som används i behandlingen av uppgifterna. Hur uppgifterna förvaras har heller ingen betydelse. Uppgifterna kan förvaras till exempel i informationssystem, kameraövervakningssystem eller pappersarkiv.

Vid skydd av personuppgifter kan man använda informationssäkerhetskriterierna för ovan beskrivna delområden. Varje kriterium som finns i delområden har klassificerats enligt huruvida det tillämpas även inom behandlingen av personuppgifter och huruvida kriteriet i så fall gäller alla personuppgifter eller endast särskilda kategorier av personuppgifter.

Identifierare	TSU-01, L:, E:, S:, TS:Personuppgift
Namn	Identifiering av personuppgifter som behandlas
Krav	Organisationen identifierar alla personuppgifter som den behandlar.
Allmän beskrivning	Identifiering av personuppgifter som behandlas är en nödvändig förutsättning för skydd av personuppgifter och har en nära anknytning till utarbetandet av organisationens informationshanteringsmodell samt den identifiering av organisationens datalager som görs i samband med detta.
Exempel på genomförande	Identifiering och dokumentation av personuppgifter som behandlas kan göras som en del av identifiering av organisationens objekt som ska skyddas, då register förs över behandling eller då en informationshanteringsmodell skapas.
Lagstiftning	Informationshanteringslagen 5 §; Dataskyddsförordningen art 5 (1) (c)
Referenser	Julkri: HAL-04
Övrig tilläggsinformation	

Identifierare	TSU-01.1, L:, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Identifiering av personuppgifter som behandlas – Särskilda kategorier av personuppgifter eller uppgifter om fällande domar i brottmål och överträdelser
Krav	Organisationen identifierar de uppgifter som hör till särskilda kategorier av personuppgifter eller uppgifter om fällande domar i brottmål och överträdelser som den behandlar.
Allmän beskrivning	Till uppgifter som hör till särskilda kategorier av personuppgifter hör sådana personuppgifter som avslöjar personens ras eller etniska ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och biometriska uppgifter (för att entydigt identifiera en fysisk person), uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Ovan nämnda särskilda kategorier av personuppgifter är till stor del uppgifter som enligt lagen om offentlighet i myndigheternas verksamhet är sekretessbelagda uppgifter och som omfattas av större sekretesskrav än vanliga personuppgifter. Därför ska organisationen identifiera om behandlingen gäller särskilda kategorier av personuppgifter samt klassificera uppgifterna som särskilda kategorier av personuppgifter. Personuppgifter som gäller fällande domar i brottmål och överträdelser är också sekretessbelagda och på dem tillämpas högre säkerhetskrav än på vanliga personuppgifter samt separata krav som gäller behandlingens lagenlighet, varför de ska identifieras och klassificeras separat.
Exempel på genomförande	Identifiering och dokumentation av personuppgifter som hör till dessa kategorier av personuppgifter kan göras som en del av identifiering av organisationens objekt som ska skyddas, då register förs över behandling eller då en informationshanteringsmodell skapas.
Lagstiftning	Dataskyddsförordningen art 9 och 10
Referenser	Julkri: HAL-04.2
Övrig tilläggsinformation	

Identifierare	TSU-02, L:, E:, S:, TS:Personuppgift
Namn	Organisationens roller
Krav	Organisationen definierar utifrån de personuppgifter som den behandlar om organisationen är personuppgiftsansvarig, gemensamt personuppgiftsansvarig eller personuppgiftsbiträde.
Allmän beskrivning	En fysisk eller juridisk person, ett företag, myndighet eller sammanslutning som fastställer ändamålen med och medlen för behandlingen av personuppgifter kallas personuppgiftsansvarig. Vanligen är själva organisationen personuppgiftsansvarig, inte en person som tillhör organisationen. Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. En instans som är en utomstående part i förhållande till den personuppgiftsansvarige och som behandlar personuppgifter för den personuppgiftsansvariges räkning enligt den personuppgiftsansvariges anvisningar kallas personuppgiftsbiträde. OBS! Organisationen kan ha olika roller i vart och ett behandlingsfall, eftersom den är beroende av vem som fastställer ändamålen med och medlen för behandlingen. En organisation kan behandla personuppgifter för någon annans räkning som biträde. Den är dock personuppgiftsansvarig vad gäller behandling av personuppgifter för egen räkning, inte för personuppgiftsansvariga som utgör kunder. En organisation är personuppgiftsansvarig till exempel då den behandlar personuppgifter som gäller organisationens egen personal. Ett personuppgiftsbiträde kan behandla personuppgifter enbart för de syften som fastställts av den personuppgiftsansvarige. Ett personuppgiftsbiträde kan inte börja behandla uppgifter som det ska behandla för den personuppgiftsansvariges räkning för egna syften genom att fastställa syftena och metoderna för behandlingen av personuppgifter.
Exempel på genomförande	Organisationens roll kan dokumenteras som en utgångsuppgift i den dokumentation som beskriver behandlingen av personuppgifter, till exempel i registren över behandling och informationshanteringsmodellen.
Lagstiftning	Dataskyddsförordningen art 4 (7–8), 26 och 28
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-03, L:, E:, S:, TS:Personuppgift
Namn	Gemensamt personuppgiftsansvariga
Krav	Då organisationen är gemensamt personuppgiftsansvarig fastställer den genom ett öppet förfarande tillsammans med andra gemensamt personuppgiftsansvariga efterlevnad av personuppgiftsansvarigas skyldigheter samt tillhandahållande av information till de registrerade.
Allmän beskrivning	Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses. Arrangemanget ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade. Oavsett formerna för arrangemanget får den registrerade utöva sina rättigheter enligt denna förordning med avseende på och emot var och en av de personuppgiftsansvariga.
Exempel på genomförande	Organisationen kan till exempel ingå ett avtal med gemensamt personuppgiftsansvariga eller skriftligt dokumentera de arrangemang som har en anknytning till uppgiften som gemensamt personuppgiftsansvariga samt ge ut dem på nätet och göra dem tillgängliga på verksamhetsställen.
Lagstiftning	Dataskyddsförordningen art 26
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-04, L:, E:, S:, TS:Personuppgift
Namn	Personuppgiftsbiträde
Krav	Organisationen anlitar endast personuppgiftsbiträden som genomför tillräckliga skyddsåtgärder.
Allmän beskrivning	Den personuppgiftsansvarige ska endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. Befattningen för personuppgiftsbiträden kan vara väldigt noggrant avgränsad, såsom utkontraktering av sändning av post. Uppgifterna kan också vara omfattande och allmänna och de kan vara kopplade till hantering av en viss tjänst för en annan organisations räkning, till exempel uppgifter som relaterar till utbetalning av lön till ett företags arbetstagare. Den reglering som gäller för personuppgiftsbiträden omfattar till exempel följande tjänstetillhandahållare: – IT-tjänstetillhandahållare, programvaruintegrerare, cybersäkerhetsföretag och IT-konsultföretag, med tillträde till den personuppgiftsansvariges personuppgifter. – Ett hälsovårdslaboratorium som behandlar prover för den personuppgiftsansvariges räkning. – Marknadsförings- och kommunikationsbyråer som behandlar personuppgifter för sina kunders räkning. – Mer generellt, alla organisationer vars tjänster omfattar behandling av personuppgifter för en annan organisations räkning. – Också en offentlig myndighet eller organisation kan ses som ett personuppgiftsbiträde. Programvaruutgivare och apparattillverkare, till exempel tillverkare av apparater för tidsuppföljning, biometriska apparater eller medicinska apparater, ses inte som personuppgiftsbiträden, om de inte har tillgång till personuppgifter, och inte behandlar personuppgifter.
Exempel på genomförande	En organisation kan bedöma biträdets förmåga till exempel med hjälp av dokumentation, godkända uppförandekoder eller certifieringar som biträdet lämnar in.
Lagstiftning	Dataskyddsförordningen art 28
Referenser	Julkri: HAL-16
Övrig tilläggsinformation	

Identifierare	TSU-04.1, L:, E:, S:, TS:Personuppgift
Namn	Personuppgiftsbiträde – Avtal
Krav	Organisationen upprättar tillsammans med personuppgiftsbiträden avtal som uppfyller kraven i dataskyddsförordningen.
Allmän beskrivning	När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges. Mer detaljerade krav på avtalets innehåll fastställs i artikel 28 i dataskyddsförordningen.
Exempel på genomförande	Organisationen kan upprätta ett avtal som gäller behandling av personuppgifter till exempel genom att utnyttja dokumentet: Beaktande av dataskyddsförordningen vid konkurrensutsättning av offentliga upphandlingar (genomförs av: Hansel, Kommunförbundet, Kuntahankinnat, upphandling.fi) som en del av avtalet. Förutom avtalsvillkoren ska den personuppgiftsansvarige dessutom lämna in till personuppgiftsbiträdet eller i övrigt avtala med personuppgiftsbiträdet om de anvisningar som ska iakttas vid behandlingen av personuppgifter. Personuppgiftsbiträdet kan använda en annan personuppgiftsansvarigs (underbiträdets) tjänster endast med skriftligt tillstånd av den personuppgiftsansvarige. Tillståndet kan ha beviljats endast för ett visst personuppgiftsbiträde eller vara ett allmänt tillstånd, varvid den personuppgiftsansvarige ska meddelas om ändringar som gäller personuppgiftsbiträden och ges möjligheten att göra invändningar mot sådana ändringar.
Lagstiftning	Dataskyddsförordningen art 28
Referenser	Julkri: HAL-16.1
Övrig tilläggsinformation	

Identifierare	TSU-05, L:, E:, S:, TS:Personuppgift
Namn	Uppgifter och ansvar
Krav	Organisationen fastställer uppgifter och ansvar i anknytning till behandling av personuppgifter.
Allmän beskrivning	Organisationens ledning har som uppgift att definiera de ansvar som gäller behandling av personuppgifter. Ansvar för skyddet av uppgifter anknyter till fastställandet av ansvar för informationssäkerhet bland annat i fråga om åtgärder som gäller säkerhet i samband med behandlingen som i många situationer är gemensamma för personuppgifter och andra uppgifter som organisationen behandlar.
Exempel på genomförande	Uppgifter och ansvar skrivs in i arbetsordningar, befattningsbeskrivningar, anvisningar eller ansvarsmatriser. Uppgifterna kan också beskrivas rollbaserat, men då måste man säkerställa att de personer som är relaterade till rollerna kan hittas enkelt också utifrån dokumentationen. Omfattningen av de uppgifter som har en anknytning till dataskydd varierar beroende på organisation. I personuppgiftsintensiva organisationer kan man till exempel handla så att organisationen utser en eller flera personer som har ansvaret för utveckling, genomförande, upprätthållande och uppföljning av ett förvaltnings- och dataskyddsprogram som omfattar hela organisationen, så att man kan säkerställa kravenlighet i förhållande till alla tillämpliga lagar och myndighetskrav som gäller behandling av personuppgifter. I en del organisationer kan också ha ett behov av att separat utse personer som besvarar begäranden som gäller de registrerades rättigheter. Även om man skulle utse en viss fysisk person för att säkerställa efterlevnad av dataskyddsbestämmelser, är denna person inte personuppgiftsansvarig utan agerar på den juridiska persons vägnar som i sista hand i egenskap av personuppgiftsansvarig ansvarar för överträdelser av bestämmelser. På motsvarande sätt även om en viss avdelning eller enhet skulle ha operativt ansvar för säkerställande av att vissa behandlingsåtgärder iakttas, betyder detta inte att avdelningen eller enheten i fråga skulle bli personuppgiftsansvarig (i stället för hela organisationen).
Lagstiftning	Dataskyddsförordningen art 12, 24
Referenser	Julkri: HAL-02
Övrig tilläggsinformation	

Identifierare	TSU-05.1, L:, E:, S:, TS:Personuppgift
Namn	Uppgifter och ansvar – Dataskyddsombud
Krav	Organisationen utser ett dataskyddsombud som är lämpligt för uppgiften och ger ut dennes kontaktuppgifter.
Allmän beskrivning	Myndigheter ska utse ett dataskyddsombud förutom när detta sker som en del av domstolarnas dömande verksamhet. Flera myndigheter kan ha ett gemensamt dataskyddsombud. Den person som utses till dataskyddsombud ska ha expertis inom dataskyddslagstiftningen samt förmågan att sköta de uppgifter som fastställs för dataskyddsombudet i förordningen. Dataskyddsombudet kan höra till personalen eller sköter uppgifter utgående från ett tjänsteavtal. Organisationen ska offentliggöra dataskyddsombudets kontaktuppgifter samt ange dem till tillsynsmyndigheten.
Exempel på genomförande	
Lagstiftning	Dataskyddsförordningen art 37–39
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-05.2, L:, E:, S:, TS:Personuppgift
Namn	Uppgifter och ansvar – Dataskyddsombudets ställning och uppgifter
Krav	Organisationen definierar dataskyddsombudets ställning, resurser och befogenheter så att denne har förutsättningar att sköta de uppgifter som hör till dataskyddsombudet.
Allmän beskrivning	Dataskyddsombudet har följande uppgifter: – följer efterlevnaden av dataskyddsbestämmelserna i hela organisationen och lyfter fram brister som det upptäckt – ger information och råd om skyldigheterna enligt dataskyddsbestämmelserna till ledningen och arbetstagare som behandlar personuppgifter – ger på begäran råd om hur konsekvensbedömningen ska göras och övervakar genomförandet av denna – är kontaktperson för de registrerade i ärenden som gäller behandling av personuppgifter – är kontaktperson gentemot dataombudsmannens byrå och samarbetar med dataombudsmannens byrå För att säkerställa dataskyddsombudets ställning och verksamhetsförutsättningar ska organisationen – se till att dataskyddsombudet inkluderas i behandlingen av frågor som gäller dataskydd – säkerställa dataskyddsombudets resurser och tillgång till nödvändiga uppgifter – säkerställa dataskyddsombudets oberoende i utförandet av uppgifter Dataskyddsombudet omfattas av skyldighet att iaktta sekretess (lagen om offentlighet 621/1999 22–23 §)
Exempel på genomförande	Genomförandet av dataskyddsombudets uppgifter kan variera mycket beroende på hur omfattande behandlingen av personuppgifter är och vilken karaktär de har i organisationen. Dataskyddsombudet kan genomföra andra uppgifter förutsatt att de inte leder till intressekonflikter med uppgifterna. I stora organisationer kan dataskyddsombudets uppgifter fördelas mellan flera personer.
Lagstiftning	Dataskyddsförordningen art 37–39; lagen om offentlighet 22–23 §
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-06, L:, E:, S:, TS:Personuppgift
Namn	Anvisningar för behandling av personuppgifter
Krav	Organisationen tar fram anvisningar för behandling av personuppgifter och säkerställer att personuppgifterna behandlas enligt dessa anvisningar.
Allmän beskrivning	Personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, får endast behandla dessa på instruktion från den personuppgiftsansvarige. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige.
Exempel på genomförande	Organisationen kan skapa allmänna anvisningar för behandling av personuppgifter samt vid behov komplettera dem med processpecifika ytterligare anvisningar. Organisationen ska även säkerställa med hjälp av distribution av anvisningar, handledningar, utbildningar och kommunikation att aktuella anvisningar för behandling av personuppgifter är tillgängliga för alla som behöver dem och att det finns information om dem.
Lagstiftning	Dataskyddsförordningen art 29, 32(4)
Referenser	Julkri: HAL-12
Övrig tilläggsinformation	

Identifierare	TSU-07, L:, E:, S:, TS:Personuppgift
Namn	Laglig behandling av personuppgifter
Krav	Organisationen identifierar de lagenliga behandlingsgrunderna för de personuppgifter som den behandlar och dokumenterar dem.
Allmän beskrivning	Behandling av personuppgifter förutsätter alltid en grund för behandling som finns i lagen. Behandlingen är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt: a) den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål; b) behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås; c) behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige; d) behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person; e) behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning; f) behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn. (Led f ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.) Om behandlingen gäller personbeteckning, särskilda kategorier av personuppgifter, fällande domar i brottmål och därmed sammanhängande säkerhetsåtgärder eller grundar sig på samtycke, beaktar organisationen ytterligare krav i anknytning till dem.
Exempel på genomförande	Organisationen fastställer alla grunder för behandling av personuppgifter innan behandlingar inleds. När behandlingen av personuppgifter knyts till en grund för behandling, kan grunden inte längre bytas till en annan. Organisationen dokumenterar grunderna för behandling.
Lagstiftning	Dataskyddsförordningen art 5 (1)(a), 6, 7, 8, 10; Dataskyddslagen 4 §, 5 §, 7 § 29 §
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-07.1, L:, E:, S:,TS: Personuppgift
Namn	Laglig behandling av personuppgifter – Samtycke
Krav	Om behandlingen av personuppgifter utgår exceptionellt från samtycke, säkerställer organisationen att de förutsättningar som föreskrivs för samtycke i dataskyddsförordningen uppfylls.
Allmän beskrivning	Samtycket ska vara frivilligt, specifikt, informerat och otvetydigt medgivande för att vara giltigt. Särskild vikt ska läggas vid bedömning av huruvida samtycket är frivilligt. Myndigheter kan endast exceptionellt använda samtycke som gäller behandling av uppgifter som grund för behandling, eftersom det ofta förekommer en tydlig maktobalans mellan den registrerade och den personuppgiftsansvarige. I de flesta fallen är det också uppenbart att den registrerade inte har andra realistiska alternativ än att godkänna myndighetens behandling av uppgifter. I dataskyddsförordningen föreskrivs följande förutsättningar för begäran om samtycke: 1. Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter. 2. Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande. 3. De registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke. 4. Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.
Exempel på genomförande	Organisationen fastställer processer för att både begära om och återkalla samtycke, och i processerna säkerställs att alla förutsättningar för begäran uppfylls. I processerna ska man beakta dokumentation, så att förutsättningarna för samtycket uppfylls kan påvisas i efterhand. Då man säkerställer att förutsättningarna för samtycket uppfylls kan organisationen använda de anvisningar som finns på dataombudsmannens webbplats.
Lagstiftning	Dataskyddsförordningen art 4(1)(11), art 7
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-07.2, L:, E:, S:, TS:Personuppgift
Namn	Laglig behandling av personuppgifter – Personbeteckning
Krav	Organisationen identifierar de lagenliga behandlingsgrunderna för personbeteckning och dokumenterar dem.
Allmän beskrivning	En personbeteckning får behandlas med den registrerades samtycke eller när behandlingen regleras i lag. Dessutom får en personbeteckning behandlas, om det är viktigt att entydigt identifiera den registrerade: 1) för att utföra en i lag angiven uppgift; 2) för att tillgodose den registrerades eller den personuppgiftsansvariges rättigheter och uppfylla den registrerades eller den personuppgiftsskyldiges skyldigheter; eller 3) för historisk eller vetenskaplig forskning eller för statistikföring. En personbeteckning får behandlas vid kreditgivning och indrivning av fordringar, i försäkrings-, kreditinstituts-, betaltjänst-, uthyrnings- och utlåningsverksamhet, i kreditupplysningsverksamhet, inom hälso- och sjukvården, inom socialvården och inom annan verksamhet för att tillförsäkra social trygghet samt i ärenden som gäller tjänste- och arbetsavtalsförhållanden och andra anställningsförhållanden och förmåner som har samband med dessa. Utöver detta får en personbeteckning lämnas ut för sådan databehandling som sker i syfte att uppdatera adressuppgifter eller undvika mångfaldig postning, om mottagaren redan har tillgång till personbeteckningen.
Exempel på genomförande	Organisationen kan till exempel separat fastställa alla de behandlingsåtgärder där personbeteckning används och säkerställa vid varje åtgärd att det finns en grund som godkänns i lagen för användningen av personbeteckning.
Lagstiftning	Dataskyddslagen 29 §
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-07.3, L:, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Laglig behandling av personuppgifter – Särskilda kategorier av personuppgifter
Krav	Organisationen identifierar de lagenliga behandlingsgrunderna för de särskilda kategorier av personuppgifter som den behandlar och dokumenterar dem.
Allmän beskrivning	Behandling av uppgifter som gäller särskilda kategorier av personuppgifter, såsom etniskt ursprung eller hälsorelaterade uppgifter, är i princip förbjuden. Det är dock möjligt att behandla sådana uppgifter, då ett undantag till behandlingsförbudet föreskrivits i dataskyddsförordningen eller i den nationella lagstiftningen.
Exempel på genomförande	Innan behandling av särskilda kategorier av personuppgifter inleds kan organisationen till exempel handla enligt följande: – Organisationen utreder och dokumenterar grunderna för behandlingen och säkerställer att de utgår från ett undantag som fastställs i dataskyddsförordningen eller i den nationella lagstiftningen.
Lagstiftning	Dataskyddsförordningen art 9; Dataskyddslagen 6 § 1 mom.
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-07.4, L:, E:, S:, TS:Personuppgift
Namn	Laglig behandling av personuppgifter – Personuppgifter som gäller fällande domar i brottmål och överträdelser
Krav	Organisationen identifierar de lagenliga behandlingsgrunderna för personuppgifter som gäller fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder som den behandlar och dokumenterar dem.
Allmän beskrivning	Behandling av personuppgifter om gäller fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder med en lagenlig grund för behandling är möjlig endast under kontroll av myndighet eller om a. behandlingen behövs för utredning, fastställande, utövande, försvar eller avgörande av rättsliga anspråk; b. på sådan behandling av uppgifter som regleras i lag eller som föranleds av en uppgift som direkt har ålagts den personuppgiftsansvarige i lag; eller c. uppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.
Exempel på genomförande	Innan behandling av personuppgifter som gäller fällande domar i brottmål och överträdelser inleds kan organisationen till exempel handla enligt följande: – Organisationen utreder och dokumenterar grunderna för behandlingen och säkerställer deras ändamålsenlighet.
Lagstiftning	Dataskyddsförordningen art 10; Dataskyddslagen 7 §
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-08, L:, E:, S:, TS:Personuppgift
Namn	Nödvändighet och proportionalitet
Krav	Organisationen säkerställer att behandlingen av personuppgifter är nödvändig och proportionell för att uppnå berättigade ändamål för behandlingen.
Allmän beskrivning	Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel.
Exempel på genomförande	Innan behandling av personuppgifter inleds utreder och dokumenterar organisationen om syftet med behandlingen rimligen kan uppnås utan behandling av personuppgifter. Om syftet med behandlingen, till exempel genomförande av tjänsten, kan göras så att vissa uppgifter inte behandlas, är behandling av personuppgifter i de avseenden inte nödvändig och därmed ska personuppgifter inte behandlas.
Lagstiftning	Dataskyddsförordningen art 5
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-09, L:, E:, S:, TS:Personuppgift
Namn	Ändamålsbegränsning
Krav	Organisationen samlar in personuppgifter endast i ett specifikt, uttryckligt och legitimt syfte, och behandlar inte senare personuppgifter på ett sätt som strider mot det ursprungliga sättet.
Allmän beskrivning	Syftet eller syftena med behandlingen av personuppgifter ska planeras och fastställas tydligt innan behandlingen inleds. Personuppgifter får endast samlas in och behandlas för ett visst, uttryckligt och lagligt syfte. Uppgifter får inte behandlas senare på ett sätt som strider mot det ursprungliga sättet. Behandlingen av personuppgifter kan vid sidan av det fastställda ändamålet även vara möjlig för sådana ändamål som anses vara förenlig med det ursprungliga ändamålet. Behandlingen ska vara lagenlig även ur synvinkeln för andra dataskyddsbestämmelser; ett kompatibelt användningsändamål berättigar inte den personuppgiftsansvarige att avvika från övriga dataskyddsbestämmelser. Behandling av personuppgifter i följande syften är kompatibelt om skyddsåtgärderna i dataskyddsförordningen följs på behörigt sätt. – för arkivändamål av allmänt intresse – vetenskapliga eller historiska forskningsändamål – statistiska ändamål
Exempel på genomförande	Organisationen kan säkerställa iakttagandet av andamålsbegränsning till exempel: – noggrant dokumentera alla ändamål och behandlingsprocesser för personuppgifter, – regelbundet kontrollera att personuppgifter inte används för andra ändamål samt – informera om principen för ändamålsbegränsning i anvisningar och utbildningar.
Lagstiftning	Dataskyddsförordningen art 5(1)(b), 6(4)
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-10, L:, E:, S:, TS:Personuppgift
Namn	Uppgiftsminimering
Krav	Organisationen behandlar personuppgifter endast i den omfattning som det är nödvändigt med tanke på behandlingens syfte.
Allmän beskrivning	Med uppgiftsminimering avses minimering av de uppgifter som samlas in om de registrerade och som behandlas. De personuppgifter som behandlas ska vara – korrekta, det vill säga att de insamlade uppgifterna ska vara sådana med vilka det fastställda användningsändamålet kan uppfyllas – väsentliga, det vill säga att de insamlade personuppgifterna ska ha ett tydligt samband med det definierade användningsändamålet och – avgränsade, det vill säga nödvändiga för det fastställda användningsändamålet för personuppgifterna. För att bedöma den rätta mängden personuppgifter, ska orsaken till att personuppgifterna i fråga behövs tydligt kunna identifieras. Med användningsändamålet är det möjligt att definiera vilka personuppgifter som är nödvändiga för att uppnå syftet med behandlingen. Organisationen säkerställer att personbeteckning inte i onödan antecknas i handlingar som skrivs ut eller utarbetas med personregistret som utgångspunkt.
Exempel på genomförande	Bedömningen av behovet av personuppgifter kan definieras som en del av processer i anknytning till inledande av behandling av personuppgifter och ändringssituationer. I bedömningen ska man gå igenom alla enskilda personuppgiftsgrupper och bedöma om de är nödvändiga i förhållande till ändamålen för behandlingen. Innan behandling av personuppgifter inleds kan organisationen till exempel handla enligt följande: – Pseudonymisera eller anonymisera uppgifter när det är möjligt. – Säkerställa att onödiga personuppgifter inte syns på systemvyer samt i handlingar som skrivs ut och utarbetas (i synnerhet personbeteckning och särskilda kategorier av personuppgifter) till exempel genom planering av systemvyer, ge anvisningar, ta upp frågan i handledningar och utbildningar eller genom att utföra kontroller av handlingar som innehåller personuppgifter. – Säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.
Lagstiftning	Dataskyddsförordningen art 51(c), 25(2); Dataskyddslagen 29.4 §
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-11, L:, E:, S:, TS:Personuppgift
Namn	Lagringsminimering
Krav	Organisationen lagrar personuppgifter i en form som möjliggör identifiering av den registrerade endast så länge som är nödvändigt för de syften för vilka personuppgifterna behandlas.
Allmän beskrivning	Den personuppgiftsansvarige ska kunna planera och motivera längden på den period under vilken personuppgifterna kommer att lagras. Tiderna för lagring av personuppgifter ska även dokumenteras. Den personuppgiftsansvarige ska uppskatta lagringstiden för personuppgifter och nödvändigheten för ändamålet i fråga. Personuppgifter får lagras enbart så länge som det är nödvändigt med tanke på användningsändamålet för personuppgifterna. Lagringstiden för personuppgifter kan påverkas också av den nationella lagstiftningen, som innehåller bestämmelser om lagringstiden, till exempel bokföringslagen. Den personuppgiftsansvarige ska själv beakta de lagringstider som följer av lagstiftningen. När personuppgifter inte längre behövs, ska de anonymiseras eller raderas. Den personuppgiftsansvarige ska säkerställa att de datasystem som är i dess användning (inklusive molntjänster) och övriga behandlingsprocesser främjar iakttagandet av lagringstider och regelbunden bedömning. Också en registrerad kan begära att den personuppgiftsansvarige raderar personuppgifter då de inte längre behövs för de syften, för vilka de samlats in eller för vilka de behandlats. Personuppgifter får lagras längre än det ursprungliga användningsändamålet enbart då personuppgifter behandlas för arkivering enligt ett allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, om skyddsåtgärderna i dataskyddsförordningen följs på behörigt sätt. Skyddsåtgärderna ska täcka såväl tekniska som organisatoriska åtgärder, med vilka i synnerhet principen om uppgiftsminimering efterlevs. Principen om minimering förutsätter också en maximalt kort lagringstid. Personuppgifter får inte behandlas, om användningsändamålen kan uppnås med anonyma uppgifter.
Exempel på genomförande	Organisationen kan fastställa lagringstiden för personuppgifter som en del av den process som inleder behandling av personuppgifter eller grunden för fastställandet samt den process enligt vilken personuppgifter raderas när lagringstiden upphör. Organisationen säkerställer att även säkerhetskopior raderas då personuppgifter raderas.
Lagstiftning	Dataskyddsförordningen art 5(1) (e), 25(2)
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-12, L:, E:, S:, TS:Personuppgift
Namn	Korrekthet
Krav	Organisationen säkerställer att personuppgifterna är korrekta och om nödvändigt uppdaterade samt vidtar alla rimliga åtgärder för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.
Allmän beskrivning	Organisationen ska säkerställa att de uppgifter som den innehar är korrekta och om nödvändigt uppdaterade. Det är särskilt viktigt att säkerställa att uppgifterna är korrekta då beslut som är väsentliga för en enskild person fattas utifrån personuppgifter. Inexakta och felaktiga uppgifter kan på allvarligt sätt äventyra den registrerades rättigheter. Till exempel felaktiga hälsouppgifter i ett patientregister kan leda till felaktiga vårdåtgärder. Organisationen ska vidta alla rimliga åtgärder för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål. Ju viktigare att en uppgift är exakt, desto mer ska den personuppgiftsansvarige göra för att säkerställa att uppgiften är korrekt. Den personuppgiftsansvarige ska till sitt förfogande ha metoder för regelbunden bedömning av att uppgiften är exakt och korrekt och för att göra nödvändiga uppdateringar. Också den registrerade har i allmänhet rätt att bedöma de personuppgifter som den personuppgiftsansvarige använt och vid behov göra en begäran om korrigering av inexakta eller felaktiga uppgifter samt en begäran om radering av onödiga uppgifter. Om en personuppgiftsansvarig vidare överlåter personuppgifter i dess besittning, finns det skäl att föra bok över mottagarna. Den personuppgiftsansvarige har en skyldighet att underrätta varje mottagare av personuppgifter om korrigering av personuppgifter. Det är möjligt att avvika från anmälningsskyldigheten enbart då detta visar sig vara omöjligt eller då detta kräver oproportionell ansträngning. Den registrerade har också rätt att begära information om mottagarna av personuppgifter. När personuppgifter fås av en annan personuppgiftsansvarig, antecknas informationskällan vid sidan om personuppgiften. I så fall kan information om fel i personuppgifter vid behov förmedlas också till den ursprungliga informationskällan.
Exempel på genomförande	Den personuppgiftsansvarige kan till exempel fastställa processer för regelbunden bedömning av exakthet och korrekthet, utförande av nödvändiga uppdateringar samt underrättelse av korrigering av personuppgifter till varje mottagare, till vilka personuppgifter har överlåtit och till den informationskälla, varifrån den korrigerade uppgiften har fåtts.
Lagstiftning	Dataskyddsförordningen art 5(1)(d)
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-13, L:, E:, S:, TS:Personuppgift
Namn	Säkerhet i samband med behandlingen
Krav	Organisationen säkerställer säkerhet för personuppgifter genom lämpliga tekniska och organisatoriska åtgärder.
Allmän beskrivning	Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt a) pseudonymisering och kryptering av personuppgifter; b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna; c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident; d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet. Vid bedömning av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Personuppgiftsbiträdets anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism kan användas som ett sätt att påvisa att den personuppgiftsansvarige fullgör sina skyldigheter.
Exempel på genomförande	Säkerställande av säkerhet i samband med behandlingen av personuppgifter kan genomföras som en del av fastställandet och genomförandet av organisationens övriga informationssäkerhetskontroller genom att inkludera risker som gäller personuppgifter som en del av riskbedömning då man fattar beslut om nivån för tekniska och organisatoriska skyddsåtgärder riktas till uppgifter som ligger på organisationens ansvar. Organisationen kan säkerställa säkerhet i samband med behandling till exempel genom att uppfylla kriterier enligt fastställda kriterier och särskilt fästa vikt vid riskbaserat val av kriterier som kompletterar minimikriterierna.
Lagstiftning	Dataskyddsförordningen art 5, 32
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-13.1, L:, E:, S:, TS:Särskild kategori av personuppgifter
Namn	Säkerhet i samband med behandlingen – Särskilda kategorier av personuppgifter eller uppgifter om fällande domar i brottmål och överträdelser
Krav	Då organisationen behandlar särskilda kategorier av personuppgifter eller uppgifter om fällande domar i brottmål och överträdelser genomför den lämpliga och specifika åtgärder för att skydda den registrerades rättigheter.
Allmän beskrivning	Sådana särskilda åtgärder är: 1) åtgärder för att det i efterhand ska kunna säkerställas och bevisas vem som har registrerat, ändrat eller överfört personuppgifter; 2) åtgärder för att höja kompetensen hos den personal som behandlar personuppgifter; 3) utnämning av ett dataskyddsombud; 4) den personuppgiftsansvariges och personuppgiftsbiträdets interna åtgärder för att förhindra tillträde till personuppgifter; 5) pseudonymisering av personuppgifter; 6) kryptering av personuppgifter; 7) åtgärder för att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna i anknytning till behandlingen av personuppgifterna, inbegripet förmåga att återställa tillgängligheten och tillgången till uppgifterna i rimlig tid vid en fysisk eller teknisk incident; 8) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet; 9) särskilda förfaranderegler för att säkerställa att dataskyddsförordningen och denna lag iakttas när personuppgifter överförs eller behandlas för något annat ändamål; 10) utförande av en konsekvensbedömning avseende dataskydd enligt artikel 35 i dataskyddsförordningen; 11) andra tekniska, förfarandemässiga och organisatoriska åtgärder.
Exempel på genomförande	Då organisationen behandlar särskilda kategorier av personuppgifter eller uppgifter om fällande domar i brottmål och överträdelser ska den: – säkerställer säkerhet i samband med behandlingen av personuppgifter med beaktande att det är fråga om personuppgifter som kanske är sekretessbelagda, och vars integritet och konfidentialitet omfattas av högre krav och större risker. – bedömer behovet av särskilda åtgärder för att skydda den registrerades rättigheter och genomför utifrån riskbedömning de som är nödvändiga.
Lagstiftning	Dataskyddsförordningen art 5, 32; Dataskyddslagen 6 § 2 mom. och 7 § 2 §
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-14, L:, E:, S:, TS:Personuppgift
Namn	Personuppgiftsincidenter
Krav	Organisationen dokumenterar alla personuppgiftsincidenter samt fastställer verksamhetssätt för att informera tillsynsmyndigheten och den registrerade om dem.
Allmän beskrivning	Med en personuppgiftsincident avses en händelse som leder till att personuppgifter förstörs, försvinner, ändras, olovligen överlåts eller hamnar i händerna på en aktör som saknar rätt att behandla dem. I samband med personuppgiftsincidenter ska alla omständigheter, deras konsekvenser samt vidtagna korrigerande åtgärder dokumenteras. En personuppgiftsincident ska anmälas till dataombudsmannens byrå utan oskäligt dröjsmål och i den omfattning som möjligt inom 72 timmar från det att personuppgiftsincidenten har observerats, om det är sannolikt att personuppgiftsincidenten medför en risk för personers rättigheter och friheter. Om personuppgiftsincidenten kan medför en hög risk för personer, ska de informeras om personuppgiftsincidenten personligen utan onödigt dröjsmål. Om organisationen är personuppgiftsbiträde, ska den informera den personuppgiftsansvarige om personuppgiftsincidenten utan onödigt dröjsmål efter att ha fått kännedom om den.
Exempel på genomförande	Organisationen kan till exempel fastställa som bedömning och behandling av personuppgiftsincidenter som en del av den allmänna incidenthanteringsprocessen. I den ingår anvisningar och ansvar för bedömning av personuppgiftsincidenter, behandling, insamling av uppgifter som gäller personuppgiftsincidenter samt anmälan av personuppgiftsincident till dataombudsmannen och de registrerade. Organisationen samlar in och lagrar om den personuppgiftsincident som har ägt rum bland annat en beskrivning av personuppgiftsincidenten (såsom dess karaktär och de uppgifter som den gäller), logguppgifter under incidentstiden, uppgifter som behövs för att uppfylla anmälningsskyldigheterna, uppgifter om incidentens konsekvenser och följder, en riskbedömning samt genomförda åtgärder och beslut som gäller personuppgiftsincidenten.
Lagstiftning	Dataskyddsförordningen art 33
Referenser	Julkri: HAL-08, HAL-09
Övrig tilläggsinformation	

Identifierare	TSU-15, L:, E:, S:, TS:Personuppgift
Namn	Ansvarsskyldighet
Krav	Organisationen kan visa att den iakttar kraven i den allmänna dataskyddsförordningen.
Allmän beskrivning	Kraven i dataskyddsförordningen ska iakttas i behandlingen av personuppgifter. Skyldigheten innebär att den personuppgiftsansvarige ska även kunna visa att dataskyddslagstiftningen iakttas av den personuppgiftsansvarige. Den personuppgiftsansvarige ska vidta nödvändiga tekniska och organisatoriska åtgärder för att uppfylla kraven enligt ansvarsskyldigheten. Ansvarsskyldigheten innebär också en dokumentationsskyldighet, i praktiken en skyldighet att vidta och anteckna vissa åtgärder. Dessa åtgärder ska kontrolleras och vid behov uppdateras. Dataskyddsförordningen innehåller krav som gäller ansvarsskyldigheten, vars åläggande karaktär ska analyseras från fall till fall. Omfattningen på ansvarsskyldigheten beror bland annat på organisationens storlek, antalet anställda och hurudana personuppgifter den personuppgiftsansvarige behandlar. Den personuppgiftsansvarige ska beakta ansvarsskyldigheten redan i den fas då behandlingen av personuppgifter planeras.
Exempel på genomförande	För att uppfylla ansvarsskyldigheten kan organisationen till exempel fastställa och skriftligt dokumentera alla processer i anknytning till genomförande av dataskyddet samt säkerställa att resultatet av dessa processer är dokumentation som kan användas till att visa att processerna har följts.
Lagstiftning	Dataskyddsförordningen art 5(2), 24
Referenser	Julkri: HAL-09
Övrig tilläggsinformation	

Identifierare	TSU-16, L:, E:, S:, TS:Personuppgift
Namn	Hantering av dataskyddsrisker
Krav	Organisationen bedömer centrala risker för behandlingen av personuppgifter samt genomför nödvändiga tekniska och organisatoriska åtgärder enligt riskbedömningen.
Allmän beskrivning	Med hantering av dataskyddsrisker avses en systematisk, samordnad och fortlöpande verksamhet som används till att identifiera, analysera, bedöma, behandla och följa upp risker för den registrerades rättigheter och friheter. Bedömning av dataskyddsrisker ska göras ur den registrerades synvinkel, dvs. organisationen ska bedöma – vilka av den registrerades rättigheter och friheter hanteringen kan äventyra och – de skador (fysiska, materiella eller immateriella) som kan orsakas för den registrerade på grund av den planerade behandlingen av personuppgifter. Vid bedömning av dataskyddsrisker ska följande faktorer beaktas: a) behandlingens art (till exempel särskilda kategorier av personuppgifter, den registrerades svårighet att utöva sina rättigheter beroende till exempel på att hanteringen är oförutsägbar eller inte är transparent, ny teknik och innovationer, den registrerades svaga ställning), b) behandlingens omfattning (antalet registrerade, informationsmängden, lagringstid, geografisk omfattning), c) behandlingens sammanhang (till exempel konfidentialitet, hemfrid, sammanställning av uppgifter som har samlats in i olika sammanhang), d) ändamål för behandlingen (till exempel övervakning, uppföljning och kontroll av de registrerade, bedömning och poängsättning av personer, automatiskt beslutsfattande som har konsekvenser för den registrerade, samt e) risker för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar. Betydelsen av att identifiera en risk betonas i synnerhet då den personuppgiftsansvarige fastställer tekniska och organisatoriska åtgärder för att säkerställa genomförandet av dataskydd i behandlingen av personuppgifter. Med tekniska och organisatoriska åtgärder avses till exempel anvisningar som getts till personalen för att genomföra dataskyddet, användningskontroll som sker genom egenkontroll, informationssystemens informationssäkerhet, kryptering av uppgifter och andra skyddsåtgärder. Riskbedömning är kontinuerlig verksamhet: huruvida åtgärderna ligger på en adekvat nivå i förhållande till den risk som är förknippad med behandlingen ska bedömas oavbrutet och uppdateras vid behov. Den personuppgiftsansvarige har också en skyldighet att visa att en riskbaserad approach använts.
Exempel på genomförande	Hantering av dataskyddsrisker är en del av organisationens verksamhet och övriga riskhantering. Organisationen använder kontrollmedel enligt dessa kriterier och fäster särskilt vikt vid riskbaserat val av kriterier som kompletterar minimikriterierna. Risker som orsakas på grund av intressentgrupper och leveranskedjor har beaktats i hanteringen av informationssäkerhetsrisker. Bedömning av dataskyddskonsekvenser (TSU-17) samt särskild bedömning av dataskyddsrisker som ingår i denna är obligatorisk om den planerade behandlingen kan medföra en hög risk för människors rättigheter och friheter.
Lagstiftning	Dataskyddsförordningen art 24, 25, 32–34, 35
Referenser	Julkri: HAL-06
Övrig tilläggsinformation	

Identifierare	TSU-17, L:, E:, S:, TS:Personuppgift
Namn	Konsekvensbedömning avseende dataskydd
Krav	Organisationen genomför före behandling av personuppgifter en bedömning av vilka konsekvenser de planerade behandlingsåtgärderna har för skyddet av personuppgifter, då behandlingen av personuppgifter medför höga risker för de registrerade.
Allmän beskrivning	Syftet med en konsekvensbedömning är att hjälpa att identifiera, bedöma och hantera de risker som är förknippade med behandlingen av personuppgifter. Konsekvensbedömningen omfattar en beskrivning av behandlingen av personuppgifter, en bedömning av nödvändigheten av behandlingen, dess proportionalitet och de risker som orsakas av behandlingen av personuppgifter och nödvändiga åtgärder för att ingripa mot risker. Målet är att bedöma om den återstående risken är berättigad och godtagbar i rådande förhållanden. En konsekvensbedömning hjälper den personuppgiftsansvarige att iaktta kraven i dataskyddslagstiftningen och att dokumentera och bevisa efterlevnaden. En konsekvensbedömning ska göras åtminstone då en planerad behandling sannolikt orsakar en hög risk för den registrerades rättigheter och friheter. En konsekvensbedömning ska göras innan behandling inleds och den ska vid behov uppdateras. En konsekvensbedömning ska göras i synnerhet då – ny teknologi används i behandlingen av personuppgifter – behandlingen i hög grad omfattar brottmålsdomar, förseelser eller särskilda kategorier av personuppgifter såsom hälsouppgifter, etniskt ursprung, politiska åsikter, religiös övertygelse eller sexuell läggning – en enskild persons personliga egenskaper bedöms med automatisk behandling, systematiskt och på omfattande sätt, och bedömningen leder till beslut, som kan ha rättsverkningar eller som i övrigt har betydande konsekvenser för personen – ett område som är öppet för allmänheten övervakas systematiskt och på omfattande sätt. Dataombudsmannens byrå har gett ut på sin webbplats en lista över olika typer av behandlingsåtgärder, i samband av vilka den personuppgiftsansvarige ska göra en konsekvensbedömning vad gäller dataskydd. Dessutom kan den nationella speciallagstiftningen förutsätta en bedömning av dataskyddets konsekvenser. Krav som gäller genomförande av konsekvensbedömning tillämpas även på pågående behandlingsåtgärder som har inletts före 25.5.2018.
Exempel på genomförande	Organisationen kan fastställa en process, enligt vilken man bedömer om en konsekvensbedömning är nödvändig för olika åtgärder för behandling av personuppgifter som organisationen utför. Organisationen kan även ta fram för genomförandet av konsekvensbedömningen anvisningar och dokumentationsförfaranden som säkerställer rätt slags och enhetligt genomförande av konsekvensbedömningar. Organisationen ska begära om råd av dataskyddsombud då konsekvensbedömningen genomförs, om den personuppgiftsansvarige har utsett ett dataskyddsombud. Om personuppgifter behandlas helt eller delvis av personuppgiftsbiträdet, ska denne hjälpa till att genomföra konsekvensbedömningen. Då organisationen tar fram anvisningar och mallar för konsekvensbedömningen kan den använda de anvisningar som finns på dataombudsmannens webbplats. Obs! Huvuddelen av de uppgifter som insamlas och åtgärder som genomförs i konsekvensbedömningen är sådana som ska göras för alla åtgärder för behandling av personuppgifter oberoende av om det behövs en konsekvensbedömning eller inte. Det lönar sig för organisationen att säkerställa att sådan utgångsinformation är tillgänglig och att den använder den i konsekvensbedömningen.
Lagstiftning	Dataskyddsförordningen art 35
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-17.1, L:, E:, S:, TS:Personuppgift
Namn	Bedömning av dataskyddskonsekvenser – Förhandssamråd
Krav	Vid behov håller organisationen samråd med dataombudsmannens byrå innan behandlingen av personuppgifter inleds.
Allmän beskrivning	Organisationen ska hålla ett samråd med dataombudsmannen innan behandling av personuppgifter inleds om konsekvensbedömningen visar att behandlingen skulle orsaka en hög risk för de registrerade, och den personuppgiftsansvarige inte med egna åtgärder kunnat sänka risken till en lägre nivå. Dataskyddsmyndigheten ska höras till exempel då de registrerade kan drabbas av betydande eller oåterkalleliga konsekvenser, som de nödvändigtvis inte kan bekämpa. Med anledning av ett förhandssamråd ger dataombudsmannen den personuppgiftsansvarige eller personuppgiftsbiträdet skriftliga anvisningar om de åtgärder som ska vidtas för att sänka risken. Vid behov kan dataombudsmannen i samband med ett förhandssamråd använda de behörigheter som tilldelats den i dataskyddsförordningen, såsom en varning. Den personuppgiftsansvarige och biträdet ska vidta tilläggåtgärder enligt anvisningen innan behandlingen av personuppgifter påbörjas, så att behandlingen kan anses vara lagenlig.
Exempel på genomförande	Organisationen kan fastställa kontroll av behovet av förhandssamråd och genomförandet av föregående samråd till exempel som en del av processerna för konsekvensbedömning och inledning av behandling av personuppgifter.
Lagstiftning	Dataskyddsförordningen art 36
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-18, L:, E:, S:, TS:Personuppgift
Namn	Överföring av personuppgifter till länder utanför EES
Krav	Organisationen har identifierat internationella överföringar av personuppgifter till länder utanför EES-området i anknytning till dess verksamhet och de överföringsgrunder som används, samt säkerställt fallspecifikt att de personuppgifter som överförs garanteras i tredjelandets lagstiftning och praxis en sådan skyddsnivå för personuppgifter som i väsentliga delar svarar mot nivån i EES-området.
Allmän beskrivning	Organisationen kan överföra personuppgifter till offentliga organ i tredjeländer eller internationella organisationer på grundval av ett beslut om adekvat skyddsnivå som godkänts av Europeiska kommissionen (art. 45). Om det inte finns något beslut om att dataskyddet är adekvat som skulle vara tillämpligt för överföringen, kan uppgifter överföras antingen – med stöd av internationella avtal mellan offentliga organ (art. 46 (2)(a), – genom administrativa överenskommelser mellan offentliga organ (art. 46 (3)(b), – genom tillämpning av andra lämpliga skyddsåtgärder (art. 46), eller – i sista hand genom tillämpning av undantag i särskilda situationer och restriktivt tolkat, om det inte är möjligt att använda lämpliga skyddsåtgärder (art. 49); användning av undantag ska i regel gälla tillfälliga behandlingsåtgärder som inte är återkommande. Organisationen har fallspecifikt bedömt om den använda överföringsmekanismen är tillräcklig för att i väsentliga delar garantera samma dataskyddsnivå som i EES-området och har vid behov infört kompletterande skyddsåtgärder. OBS. Organisationen har även beaktat i fråga om personuppgiftsbiträden (till exempel leverantörer av molntjänster) var personuppgifterna finns fysiskt. Till exempel anses tillgång för personuppgiftsbiträden som är tjänsteleverantörer via fjärranslutning till personuppgifter utanför EES innebära överföring av personuppgifter till länder utanför EES-området. OBS. I princip har molntjänstleverantören alltid tillgång till uppgifter som behandlas i tjänsten, om uppgiften under sin livscykel är i vanlig läsbar form (till exempel som en bild som visas för kunden) i tjänsten eller om tjänsteleverantören har tillgång till de kryptonycklar som används till att kryptera uppgifter. OBS. Om inga förutsättningar för överföringsgrunden uppfylls, kan personuppgifter inte överföras till länder utanför EES.

Exempel på genomförande	Identifiering och dokumentation av personuppgifter som överförs till tredjeländer, de överföringsgrunder som används, mottagare av överföringar och identifiering av dem som genomför överföringar kan göras som en del av identifiering av organisationens objekt som ska skyddas, då register förs över behandling eller då en informationshanteringsmodell skapas. Organisationen kan säkerställa att de personuppgifter som överförs ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas, genom att till exempel följa de processer och den praxis som har fastställts för bedömning av att uppgifterna är korrekta (TSU-13). Organisationen kan utnyttja i ett tidigt skede de anvisningar som finns på dataombudsmannens och Europeiska dataskyddsstyrelsens webbplatser (i synnerhet dataskyddsstyrelsens Riktlinjer 2/2020 för överföringar av personuppgifter mellan offentliga myndigheter och organ i EES-länder och länder utanför EES) då den säkerställer att den allmänna dataskyddsförordningen följs i rättsligt bindande instrument eller administrativa arrangemang (internationella avtal). Organisationen kan vid fallspecifik bedömning av om personuppgifter som överförs garanteras i tredjelandets lagstiftning och/eller i dess praxis sådan skyddsnivå för personuppgifter som till väsentliga delar motsvarar nivån för EES-området, samt vid val av eventuellt nödvändiga kompletterande skyddsåtgärder använda Europeiska dataskyddsstyrelsens Rekommendationer 1/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, samt Rekommendationer 2/2020 om europeiska nödvändiga garantier för övervakningsåtgärder. Organisationen utreder lämpliga processuella krav, om den överför personuppgifter till ett tredjeland eller en internationell organisation och tillämpar någon av de följande skyddsåtgärderna: standardavtalsklausuler (art. 46 (2)(c) och (d) GDPR), administrativa överenskommelser mellan offentliga myndigheter (art. 46(3)(b) GDPR), godkänd uppförandekod (art. 46 (2)(e), godkänd certifieringsmekanism (art. 46(2)(f) GDPR) eller ad hoc-avtalsklausuler (art. 46.3(a) GDPR). Vid bedömning av lämpliga processuella krav kan du använda Europeiska dataskyddsstyrelsens Rekommendationer 1/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter. Organisationen bedömer med jämna mellanrum tillsammans med överföringens mottagare om det sker ändringar av skyddsnivån för personuppgifter i tredjelandet eller europeiska dataskyddsmyndigheters anvisningar och uppdaterar vid behov praxisen.
Lagstiftning	Dataskyddsförordningen kapitel V
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-19, L:, E:, S:, TS:Personuppgift
Namn	Den registrerades rättigheter
Krav	Organisation genomför den registrerades rättigheter.
Allmän beskrivning	När den personuppgiftsansvarige behandlar personuppgifter ska den utföra ändamålsenliga åtgärder för att förverkliga de registrerades rättigheter samt underlätta utövandet av deras rättigheter. Organisationen ska kontrollera identiteten på en registrerad som framför en begäran och följa de tidsfrister som fastställs i dataskyddsförordningen för tillmötesgående av begäran. Enligt dataskyddsförordningen har den registrerade rätt att – få information om behandlingen av sina personuppgifter – få åtkomst till uppgifterna – rätta uppgifter – radera uppgifter och bli bortglömd – begränsa behandlingen av uppgifter – överföra uppgifter från ett system till ett annat – göra invändning i samband med behandling av personuppgifter – inte bli föremål för automatiserat beslutsfattande.
Exempel på genomförande	För att genomföra de registrerades rättigheter kan organisationen genomföra och dokumentera processer som används till att säkerställa och påvisa att de registrerades rättigheter förverkligas. Det är viktigt att planera processer som gäller de registrerades rättigheter särskilt i sådana fall där man vet att de registrerade i stor omfattning utövar sina rättigheter.
Lagstiftning	Dataskyddsförordningen art 12–21
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-19.1, L:, E:, S:, TS:Personuppgift
Namn	Den registrerades rättigheter – Identifiering av de rättigheter som är tillgängliga för den registrerade
Krav	Organisationen har fastställt enligt den lagenliga grunden för behandling som den har identifierat, vilka av den registrerades rättigheter som han en koppling till behandlingen i fråga.
Allmän beskrivning	En registrerad kan inte utöva alla sina rättigheter i alla situationer. Vilka rättigheter den registrerade i varje enskilt fall kan använda påverkas av på vilken grund personuppgifterna i fråga behandlas. Organisationen kan använda det material på dataombudsmannens byrås webbplats som handlar om på vilket sätt behandlingsgrunden påverkar de tillgängliga rättigheterna. Det är möjligt att vägra tillgodoseendet av varje rättighet i enskilda fall. En vägran är möjlig om en relevant grund för vägran är aktuell för en viss rättighet eller om förutsättningar för tillgodoseende av en rättighet inte i övrigt är uppfyllda. Dessutom är det möjligt att speciallagstiftningen om organisationen i fråga innehåller bestämmelser om undantag till rättigheterna.
Exempel på genomförande	Organisationen fastställer enligt den lagenliga grunden för behandling vilka dataskyddsrättigheter som han en koppling till behandlingen i fråga. Organisationen beskriver hur rättigheterna beaktas vid behandlingen av personuppgifter samt hur begäranden som gäller rättigheter behandlas och genomförs.
Lagstiftning	Dataskyddsförordningen art 14 (5)(b-d), 17 (3), 20 (1) ja (3), 21 (1) och (6), 22 (2), 23, 85, 89; Dataskyddslagen 31–34 §
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-19.2, L:, E:, S:, TS:Personuppgift
Namn	Den registrerades rättigheter – Klar och tydlig information
Krav	Organisationen informerar de registrerade om behandlingen av personuppgifter enligt föreskrivet sätt.
Allmän beskrivning	Personuppgifter ska behandlas på ett sätt som ur den registrerades synvinkel är transparent. Det finns undantag från sådan allmän information. Syftet med informationen är att den registrerade får en omfattande och tydlig bild av helheten för behandling av personuppgifter. Den personuppgiftsansvarige ska bedöma om den givna informationen är begriplig med tanke på språk och konsekvens ur målgruppens synvinkel. De närmare kraven på informationen beror delvis på om uppgifter insamlas från personen eller från någon annan instans. De mer specifika kraven på information är: – informationsinnehållet – krav som gäller framförandesättet – krav som gäller distribution och leveranssättet – krav som gäller tidpunkten Information ska ges i samband med insamling av uppgifter eller inom en rimlig tid (minst en månad) efter att personuppgifter har mottagits, om uppgifterna inte har fåtts från den registrerade. Information ska ges senast när den registrerade kontaktas för första gången eller om uppgifter utlämnas för första gången i situationer, där uppgifter fås från andra än den registrerade och de används till kommunikation med den registrerade eller de ska utlämnas till en annan mottagare.
Exempel på genomförande	I samband med insamling av uppgifter som sker elektroniskt kan informationen ges till exempel med en dataskyddsbeskrivning som det finns en direkt länk till på den blankett som används till insamlingen av uppgifter. Man berättar om dataskyddsbeskrivningen med synliga meddelanden. Om insamlingen av uppgifter sker när den registrerade är fysiskt närvarande, kan information ges skriftligt eller på begäran även muntligt. Det väsentliga är att den registrerade får enkelt information om behandlingen av personuppgifter i en koncis, transparent, begriplig och tillgänglig form.
Lagstiftning	Dataskyddsförordningen art 5, 13–14
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-19.3, L:, E:, S:, TS:Personuppgift
Namn	Den registrerades rättigheter – Den registrerades rätt till tillgång
Krav	Organisationen sänder på begäran till den registrerade en kopia över de personuppgifter som behandlas samt information om behandlingen av personuppgifter.
Allmän beskrivning	Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna samt information som gäller behandlingen av personuppgifter, såsom till exempel ändamålen med behandlingen, kategorier av personuppgifter, mottagare och perioder under vilka personuppgifterna kommer att lagras. Om personuppgifterna överförs till ett tredjeland eller till en internationell organisation, ska den registrerade ha rätt till information om de lämpliga skyddsåtgärder som i har vidtagits vid överföringen. Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.
Exempel på genomförande	Organisationen kan fastställa för uppfyllandet av begäranden som har registrerats i processen samt inkludera i den information som ges till de registrerade uppgifter om hur begäranden ska sändas till den personuppgiftsansvarige. Om det kommer många begäranden, lönar det sig för organisationen att också planera och ge anvisningar för förfaranden som effektivt uppfyller begäranden.
Lagstiftning	Dataskyddsförordningen art 15
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-19.4, L:, E:, S:, TS:Personuppgift
Namn	Den registrerades rättigheter – Rättelse, radering, överföring, begränsning av behandlingen av uppgifter och rätten att göra invändningar.
Krav	Organisationen uppfyller begäranden som gäller rättelse, radering, överföring, begränsning av behandlingen av uppgifter och rätten att göra invändningar.
Allmän beskrivning	Den registrerade har ett antal rättigheter som gäller personuppgifter och organisationen ska uppfylla dem på begäran, såsom: En registrerad har rätt att begära att den personuppgiftsansvarige utan onödigt dröjsmål rättar inexakta och felaktiga personuppgifter som gäller honom eller henne. Med beaktande av de syften för vilka uppgifterna behandlades, har den registrerade rätt att få bristfälliga personuppgifter kompletterade genom att bland annat lämna in tilläggsutredning. Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om någon av de grunder som anges i förordningen gäller. Sådana grunder är till exempel att behovet av att använda uppgifter upphör eller samtycke återkallas. Den registrerade har rätt till att den personuppgiftsansvarige begränsar behandlingen i vissa situationer, till exempel om den registrerade bestrider personuppgifternas korrekthet. Den personuppgiftsansvarige är även skyldig att meddela varje mottagare av personuppgifter om ovan nämnda åtgärder. Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig, om behandlingen grundar sig på samtycke. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på allmänt intresse, myndighetsutövning eller berättigat intresse. Om personuppgifterna behandlas för direkt marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.
Exempel på genomförande	Detaljerade processer som gäller utövandet av rättigheter kan planeras med beaktande av antalet begäranden samt de detaljer som i dataskyddsförordningen fastställs för olika rättigheter. Om antalet begäranden är stort, lönar det sig att noggrant planera och ge anvisningar för processerna. Annars räcker det mer att organisationen säkerställer förmågan att vid behov uppfylla de registrerades begäranden och att den har tillräckliga kunskaper om de detaljerade krav som gäller uppfyllandet av begäranden enligt dataskyddsförordningen.
Lagstiftning	Dataskyddsförordningen art 16–21
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-20, L:, E:, S:, TS:Personuppgift
Namn	Automatiserat individuellt beslutsfattande
Krav	Organisationen identifierar de situationer där automatiserat beslutsfattande ingår i behandlingen av personuppgifter samt säkerställer att automatiserat beslutsfattande inte utförs utom i fall som separat tillåts i dataskyddsförordningen.
Allmän beskrivning	Organisationen får inte fatta sådana beslut som gäller den registrerade som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Automatiserat beslutsfattande (inkl. profilering) är tillåtet om beslutet – är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige – tillåts enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av – grundar sig på den registrerades uttryckliga samtycke. Med profilering avses automatiskt behandling av personuppgifter där människans personliga egenskaper bedöms. Med profilering avses analys eller förutsägelser av särdrag som gäller i synnerhet arbetsprestationer, den ekonomiska situationen, personliga preferenser, intressen, pålitlighet, beteende, position eller rörelser. Profilering – är automatiskt eller delvis automatiskt – hänför sig till personuppgifter och – bedömer personliga egenskaper. Beslutsfattande är automatiskt då – det handlar om enbart beslutsfattande som grundar sig på automatisk behandling av personuppgifter och – de beslut som fattas har rättsverkningar eller då besluten i väsentlig grad i övrigt påverkar den registrerade.
Exempel på genomförande	Om organisationen utför automatiserat beslutsfattande eller profilering, kan organisationen i samband med att behandlingen inleds samt regelbundet säkerställa i förhållande till de detaljerade krav som läggs fram i dataskyddsförordningen att de krav som gäller automatiserat beslutsfattande och profilering uppfylls. Organisationen ska i samband med automatiskt beslutsfattande (inkl. profilering) se till att åtminstone följande skyddsåtgärder genomförs: – de registrerade underrättas om behandlingen av uppgifter – de registrerade erbjuds enkla sätt att kräva att människor deltar i behandlingen av uppgifter, framföra sin ståndpunkt och väcka talan – de uppgifter och algoritmer som ska behandlas granskas regelbundet, för att säkerställa att beslutsprocessen fungerar på det avsedda sättet, och inte leder till exempel till individdiskriminerande behandling av uppgifter. – man har gjort en konsekvensbedömning avseende behandlingen av personuppgifter.
Lagstiftning	Dataskyddsförordningen art 22
Referenser	
Övrig tilläggsinformation	

Identifierare	TSU-21, L:, E:, S:, TS:Personuppgift
Namn	Register över behandling
Krav	Organisationen tar fram en skriftlig beskrivning av den behandling av personuppgifter som organisationens utför.
Allmän beskrivning	Register över behandling ska genomföras om organisationen sysselsätter över 250 personer och den ska omfatta alla behandlingsåtgärder. Register över behandling ska genomföras oberoende av antalet anställda om – den behandling som utförs sannolikt kommer att medföra en risk för registrerades rättigheter och friheter eller – behandlingen av personuppgifter inte är tillfällig eller – behandlingen omfattar särskilda kategorier av uppgifter eller personuppgifter om fällande domar i brottmål och överträdelser. Då ska endast behandlingsåtgärder inkluderas i registret.
Exempel på genomförande	Den personuppgiftsansvarig och personuppgiftsbiträdet kan utarbeta register över behandling till exempel genom att använda de anvisningar och standardmallar som finns på dataombudsmannens webbplats.
Lagstiftning	Dataskyddsförordningen art 30
Referenser	
Övrig tilläggsinformation	

Bilaga 2: Julkri-vertyget

Bilagan finns som en separat fil på adressen https://urn.fi/URN:ISBN:978-952-367-462-2

Bilaga 3: Anvisningar för användning av Julkri-verktyget

1 Användning av verktyget

Dessa anvisningar beskriver hur Julkri-kriterierna används med hjälp av det Excel-verktyg (bilaga 2) som har utvecklats för det. Idéen med verktyget är att användaren först anger förhandsvillkor som beskriver bedömningssituationen, utifrån vilka verktyget väljer väsentliga och valfria kriterier samt kriterier som lämnas utanför bedömningen.

1.1 Definiering av förhandsvillkor

I verktyget definieras först utgångsinformation för bedömningen med hjälp av rullgardinsmenyerna på Esiehdot-fliken. Som förhandsvillkor matas in följande uppgifter:

- den konfidentialitet, integritet och tillgänglighet som förutsätts av objektet (de klassificeringsnivåer som används fastställs i kapitel 4.2 i Julkri-rekommendationen)
- huruvida objektet innefattar personuppgifter och huruvida dessa uppgifter hör till särskilda kategorier av personuppgifter,
- delområden som inkluderas eller inte ska beaktas i bedömningen,
- användningsfallet, om ett användningsfall som lämpar sig för bedömningen existerar.

1.2 Väsentliga kriterier och komplettering av dem

Verktyget visar utgående från de givna förhandsvillkoren på fliken Valitut kriteerit för varje kriterium om det är väsentligt, valfritt eller om det lämnas utanför bedömningen (Ei sisälly arviointiin). Organisationen fattar kriteriespecifikt beslut om tillämpning av varje kriterium. Besluten antecknas kriteriespecifikt i kolumnen Päätös soveltamisesta.

I kolumnen Päätös soveltamisesta antecknas motivering särskilt till de valfria kriterier som organisationen utgående från riskbedömningen låter bli att genomföra. Motiveringen ska skrivas in så att det tydligt framgår på vilka grunder man trots att kriteriet inte tillämpas bedömer att risken ligger på en godtagbar nivå. Motiveringen kan skrivas till exempel genom att beskriva kompenserade kontroller eller genom att hänvisa till en separat riskbedömning.

Utgångspunkten är att väsentliga kriterier ska tillämpas. Organisationen fattar beslut om tillämpning av valfria kriterier utifrån riskbedömningen och fallspecifik bedömning. Utgångspunkten är att kriterier, som inte ingår i bedömningen, inte behöver tillämpas. Organisationen kan av motiverade skäl avvika från denna princip.

1.3 Användning av kriterier i bedömningen

Den uppsättning kriterier som tas fram enligt ovan nämnda faser används för föremålet för bedömning antingen för bedömning av informationssäkerheten eller för planering av informationssäkerhetsåtgärder som föregår bedömningen.

Listan över tillämpliga kriterier på verktygets flik Valitut kriterit utgör ett underlag, där man kriteriespecifikt kan dokumentera bedömningsresultaten samt åtgärder, tidsscheman och ansvar för att åtgärda brister.

1.4 Verktygets verksamhetsprinciper

Valet av kriterier utgår från den sammantagna effekten av de urvalskriterier som ges med hjälp av förhandsvillkoren. Vid val av kriterier följer verktyget följande urvalslogik:

- Säkerhetsnivåer
  - Kriteriet är väsentligt om den säkerhetsnivå som har fastställts för kriteriet är densamma eller lägre än säkerhetsnivån för det föremål för granskning som användaren har fastställt i förhandsvillkoren. Detta betyder att om användaren har fastställt att föremålet för granskning innehåller sekretessbelagda uppgifter, är ändå alla kriterier, som har klassificerats till att gälla sekretessbelagda eller offentliga uppgifter, väsentliga.
  - Vid behandling av personuppgifter är väsentliga kriterier sådana som i fråga om dataskydd har klassificerats på nivån personuppgift.
  - Vid behandling av särskilda kategorier av personuppgifter är alla kriterier som har klassificerats i fråga om dataskydd väsentliga.
  - Kriteriet är utgående från säkerhetsnivåer väsentligt, om det med tanke på en enda säkerhetsaspekt (konfidentialitet, integritet, tillgänglighet eller dataskydd) är väsentligt.

  - Kriteriet är valfritt om kriteriet inte är väsentligt och om dess säkerhetsnivå är en nivå högre än den säkerhetsnivå som användaren har angett i förhandsvillkoren. Om till exempel föremålet för granskning innehåller sekretessbelagda uppgifter, är kriterier som har klassificerats på TL IV-nivån valfria och användaren beslutar utgående från riskbedömningen om dessa tillämpas eller inte. Dessutom är vid behandling av uppgifter som hör till kategorin personuppgift valfria kriterier sådana kriterier som har klassificerats på nivån särskilda kategorier av personuppgifter.

- Delområden

  - Varje delområde kan tas med i bedömningen (Kyllä) eller utelämnas (Ei).

  - Om ett delområde har utelämnats, ingår inga kriterier i delområden i bedömningen. Om till exempel behandlingen inte innehåller personuppgifter kan delområdet för dataskydd utelämnas eller om bedömning av det administrativa delområdet redan har genomförts tidigare, kan det utelämnas.

- Användningsfall

  - Kriteriet är väsentligt om det har fastställts som väsentligt utgående från ett användningsfall.

  - Ett kriterium kan ha fastställts i ett användningsfall som valfritt, varvid organisationen fattar beslut om tillämpning av kriteriet utgående från om kriteriet är nödvändigt i bedömningssituationen i fråga.

- Samverkan

  - Ett kriterium ingår inte i bedömningen, om den inte omfattas av bedömning utgående från säkerhetsnivå, delområde eller användningsfall.

  - Ett kriterium är valfritt om det utgående från säkerhetsnivå eller användningsfall är valfritt och om det inte har avgränsats utanför bedömningen utgående från säkerhetsnivå, delområde eller användningsfall.

  - I andra fall är kriteriet väsentligt.

1.5 Vertikal vy och filtrering av kriterier

På fliken Pystynäkymä visas kriterierna i en lätt läsbar form. De uppgifter som visas i den vertikala vyn kan filtreras utgående från kriteriernas väsentlighet och tillämpningsbesluten. Kriteriernas väsentlighet fastställs utifrån de val som har gjorts på Esiehdot-fliken. Tillämpningsbesluten görs på fliken Valitut kriteerit.

Filtreringar kan göras på fliken Pystynäkymä med hjälp av rullgardinsmenyerna i cellerna D1 och E1. Vid filtrering används Excels normala filtreringsegenskaper.

I den vertikala vyn kan man inte söka uppgifter utifrån kriteriernas innehåll, eftersom vyn endast visar uppgifter från andra flikar. Uppgifter kan sökas på fliken Kriteeristö.

2 Användningsfall

I uppsättningen kriterier har man på förhand fastställt användningsfall, för vilka man har plockat kriterier som är lämpliga för situationen. Organisationerna kan även själva fastställa användningsfall för bedömningssituationer som upprepas ofta. Med hjälp av fastställande av organisationsspecifika användningsfall kan man effektivisera utnyttjandet av kriterier i olika situationer, då man utgående från på förhand identifierade risker kan välja en lämplig nivå för användningsfallet och då man dessutom kan utelämna kriterier som inte är lämpliga för situationen.

2.1 På förhand definierade användningsfall

2.1.1 Administrativ säkerhetsbedömning av informationshanteringsenheten

Ett användningsfall är avsett för informationshanteringsenhetens bedömning av miniminivån för informationssäkerhet och dataskydd enligt lagen om informationshantering. I den ingår en bedömning med tanke på administrativ säkerhet, dataskydd samt beredskap och kontinuitetshantering. Användningsfall kan kompletteras med bedömningar av fysisk säkerhet och informationssystemen.

2.1.2 Bedömning av SaaS-molntjänsten

Användningsfallet är avsett för bedömning av säkerheten hos molntjänster som produceras som SaaS-tjänster. Med hjälp av det kan man bedöma om den tjänst som bedöms uppfyller kraven på att säkerställa informationssäkerhet enligt lagen om informationshantering. I bedömningen kan man använda molntjänstleverantörens certifikat, dokumentation och andra eventuella bevis på att säkerhetskraven uppfylls. Om man ämnar behandla personuppgifter i den tjänst som används ska bedömningen även beakta kriterier som gäller dataskydd. Användningsfallet begränsas i fråga om konfidentialitet högst till behandling av sekretessbelagda uppgifter i molntjänster.

2.1.3 Upphandling av expertarbete

Användningsfallet är avsett för att bedöma hur säkerhetskraven uppfylls vid upphandling av expertarbete och konsulttjänster, då man vill försäkra sig om informationssäkerheten i den organisation som tillhandahåller experttjänster. Bedömningens omfattning beror på sättet att genomföra uppdraget. Om till exempel arbetet utförs med utrustning som tillhör den beställande organisationen, kan man låta bli att tillämpa den tekniska delen, om motsvarande bedömning har utförts för den utrustning och de system som används. Om arbetet utförs i leverantörens lokaler tillämpas kraven på fysisk säkerhet eller kraven på distansarbete.

2.1.4 Bedömning av informationssystemets serviceproduktion

Användningsfallet fastställer de kriterier som tillämpas vid bedömning av informationssystemets serviceproduktionsmiljö eller serviceproducenten. Användningsfallet kan användas till exempel vid utveckling av informationssystem eller för bedömning av informationssäkerheten i databehandlingsmiljöer som används i serviceproduktionen eller för bedömning av informationssäkerheten hos leverantörer som erbjuder motsvarande tjänster. Användningsfallet beaktar särskilt kriterier som gäller serviceproduktionens kontinuitetshantering och fysiska säkerhet.

2.2 Organisationsspecifika användningsfall

Användningsfallen underlättar betydligt valet av kriterier i situationer som upprepas ofta. Förutom de på förhand fastställda användningsfallen kan organisationen fastställa nya eller ändra färdiga användningsfall. Vid fastställande och användning av användningsfall ska man iaktta särskild försiktighet, så att man inte utelämnar väsentliga kriterier eller förlorar den flexibilitet som andra egenskaper som gäller val av kriterier möjliggör.

Det rekommenderas att följande förfaranden följs vid fastställande av användningsfall:

Avgränsningar: Organisationen ska fastställa de avgränsningar av användningsfall, utifrån vilka man kan besluta om ett visst kriterium är nödvändigt uttryckligen för detta användningsfall eller om ärendet sköts av en ansvarig instans som lämnas utanför bedömningen. Till exempel om organisationen lägger till en ny tjänst till organisationens gemensamma infrastruktur, kan de kriterier som gäller den gemensamma infrastrukturen bedömas en gång och sedan utelämnas ur de tjänstespecifika bedömningarna.

Valfria kriterier: Om det är möjligt att tillämpa ett kriterium i vissa fall och inte i andra, lönar det sig att fastställa det som valfritt. Kriterier ska inte helt avgränsas från ett

användningsfall om det är möjligt att de kan vara nödvändiga i någon bedömningssituation som hör till användningsfallet.

Riskbedömningar: För liknande användningsfall som hör till samma säkerhetsnivå kan man använda samma riskbedömning, varvid man inte behöver upprepa riskbaserad bedömning av kriterier i onödan.

- Detta kan genomföras så att man helt lämnar utanför användningsfallet sådana kriterier som utgående från riskbedömningen inte tillämpas.
- På motsvarande sätt kan man baserat på en riskbedömning som har gjorts på förhand för användningsfallet i ett användningsfall inkludera som väsentliga kriterier sådana kriterier som utifrån säkerhetsnivån klassificeras som valfria. Då kan man ange i bedömningssituationen att alla valfria kriterier ska tillämpas utan en ny riskbedömning.

Dokumentation: Användningsfallen ska alltid dokumenteras tillräckligt exakt. I synnerhet ska man beskriva de avgränsningar och riskgrunder på vilka inkludering eller utelämnande av kriterier i ett användningsfall baserar sig. Dessa grunder ska beskrivas så exakt att även ett oberoende organ vid behov kan bedöma om det har varit motiverat att utelämna kriteriet.

2.3 Beskrivning av användningsfallet i verktyget

Namnet på användningsfallet samt en kort allmän beskrivning av användningsfallets innehåll skrivs på fliken Käyttötapauskuvaukset. I den allmänna beskrivningen av användningsfallet beskrivs för vilka bedömningssituationer användningsfallet lämpar sig.

Eftersom tillämpningen av användningsfall inbegriper flera olika aspekter, rekommenderas att det tas fram en separat, mer detaljerad beskrivning av användningsfallet som hjälper den som använder användningsfallet att bedöma om användningsfallet är lämpligt för bedömningssituationen.

De kriterier som tillämpas på användningsfallet fastställs på fliken Käyttötapauskriteerit. På flikens översta rad finns namnen på de användningsfall som fastställs på fliken Käyttötapauskuvaukset. Fastställandet av kriterierna för användningsfallen görs i kolumnen för varje användningsfall enligt följande:

- Väsentliga kriterier som hör till användningsfallet: 1
- Valfria kriterier som hör till användningsfallet: 2
- Kriterier som har lämnats utanför användningsfallet: 0

Bilaga 4: Terminologi

Term	Definition	Källa
Utvärdering	Analys och tolkning av uppgifter som granskas och värdering av objektet. (jfr revision) Självvärdering och extern utvärdering.	Termbanken Tepa
Handling	Med handling avses utom en framställning i skrift eller bild även ett meddelande som avser ett visst objekt eller ärende och uttrycks i form av tecken som på grund av användningen är avsedda att höra samman och vilket endast kan uppfattas med hjälp av automatisk databehandling eller en ljud- eller bildåtergivningsanordning eller något annat hjälpmedel.	Lagen om offentlighet 5 § 1 mom.
Autenticitet/autentisk	Genuin, oförfalskad, tillförlitlig	Ordboken Kielitoimiston sanakirja
Integritet	En egenskap hos information som innebär att informationen inte har ändrats utan lov eller att det inte ändrats av misstag och att eventuella ändringar kan verifieras. Integritet hos information eller ett informationssystem kan också betyda att informationen är internt konsekvent.	Termbanken Tepa
Särskilda kategorier av personuppgifter	Personuppgifter som hör till särskilda kategorier av personuppgifter är sådana uppgifter som redogör för personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförbund, hälsorelaterade uppgifter, sexuella läggning eller beteende, genetiska och biometriska uppgifter för identifiering av personen. Behandling av personuppgifter som hör till särskilda kategorier av personuppgifter är i princip förbjuden. Dessa uppgifter ska skyddas särskilt noggrant, eftersom behandling av dessa kan orsaka avsevärda risker vad gäller personens grundläggande fri- och rättigheter.	Tietosuoja.fi
Personuppgift	Med personuppgifter avses alla uppgifter som anknyter till en identifierad eller identifierbar person. En person kan identifieras till exempel utifrån namn, personbeteckning eller någon faktor som är kännetecknande för personen i fråga.	Tietosuoja.fi

Term	Definition	Källa
Offentlig	En myndighetshandling som inte har föreskrivits i eller med stöd av lag som sekretessbelagd. Ett undantag är så kallade handlingar som uppges enligt prövning, dvs. till exempel handlingar som förbereds och som inte ännu är offentliga.	Lagen om offentlighet 1, 16 a och 22 §
Oavvislighet, oavvislig	Obestridlig, oförneklig, obestridd, oemotsäglig, självklar, säker, ovillkorlig. Oavvislighet är en egenskap som uttrycker att den som sänder eller tar emot uppgifter eller en händelse i anknytning till en uppgift kan tillförlitligt verifieras också i efterhand.	Ordboken Kielitoimiston sanakirja Termbanken Tepa
Användningsfall	Med användningsfall avses i Julkri en sådan utvärderingssituation som upprepas och där man kan tillämpa samma valda uppsättning kriterier. Ett exempel på användningsfall kan vara bedömning av en serviceproducents informationssäkerhet, där endast kriterier som gäller myndigheter har utelämnats.	
Konfidentialitet	En egenskap som ger uttryck åt att informationen endast kan användas om man har rätt att använda den och att informationen inte avslöjas för utomstående.	Termbanken Tepa
Tillgänglighet	Med tillgänglighet avses hur information, ett informationssystem eller en tjänst kan utnyttjas vid önskad tidpunkt och på det sätt som krävs.	Termbanken Tepa
Sekretessbelagd	En myndighetshandling ska sekretessbeläggas, om det i lagen om offentlighet eller någon annan lag föreskrivs eller en myndighet med stöd av lag har föreskrivit att den ska vara sekretessbelagd eller om handlingen innehåller uppgifter för vilka tystnadsplikt föreskrivs genom lag.	Lagen om offentlighet 22 § och 24 §
Uppgift	Uppgift har i denna rekommendation samma betydelse som handling.	
Informationsmaterial	En datauppsättning som består av handlingar och annan motsvarande information och har samband med en viss myndighetsuppgift eller myndighetstjänst.	Lagen om informationshantering 2 §
Informationshanteringsenheten	En myndighet med uppgift att ordna informationshantering i enlighet med kraven i lagen om informationshantering.	Lagen om informationshanteringslagen 2 och 4 § 1 mom.

Term	Definition	Källa
Informations-system	Ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling. Till exempel är olika molntjänster och terminaler som används till behandling av programvara informationssystem.	Lagen om informations-hantering 2 §
Säkerhets-klassificerad handling	En anteckning om sekretessklassen ska göras i en handling om den eller information som den innehåller är sekretessbelagd på grundval av 24 § 1 mom. 2, 5 eller 7–11 punkten i lagen om offentlighet i myndigheternas verksamhet och avslöjande eller obehörig användning av informationen som ingår i handlingen kan orsaka skada för landets försvar, beredskapen inför undantagsförhållanden, internationella relationer, brottsbekämpningen, den allmänna säkerheten eller stats- och nationalekonomins funktion eller på ett jämförbart sätt orsaka skada för Finlands säkerhet.	Lagen om informations-hantering 18 § Lagen om offentlighet 24 §
Krav	Krav är ett enskilt mål som har fastställts för ett objekt och som objektet ska kunna uppfylla. Ett krav är en del av ett kriterium. Ett krav kan genomföras på många olika sätt. Kravet är så specificerat som möjligt, vilket innebär att ett krav inte består av flera olika krav.	
Överens-stämmelse med kraven	Uppfyllandet av de krav som rekommenderas i Julkri hos föremålet för utvärdering.	

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN 978-952-367-462-2 (pdf)

Juni 2023