VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) – Suositus ja kriteeristö

Lautakunnat

Valtiovarainministeriön julkaisuja – 2022:43

Valtiovarainministeriön julkaisuja 2022:43

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)

Suositus ja kriteeristö

Valtiovarainministeriö Helsinki 2022

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Valtiovarainministeriö

ISBN pdf: 978-952-367-275-8
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2022

Kuvailulehti
2.6.2022

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)
Suositus ja kriteeristö

Valtiovarainministeriön julkaisuja 2022:43		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	suomi	**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.

Julkaisu on päivitetty 15.2.2023, s. 57.

Tämän version korvaa uusi, muutettu aineisto osoitteessa
https://urn.fi/URN:ISBN:978-952-367-458-5

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

ISBN PDF	978-952-367-275-8	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-275-8		

Presentationsblad
2.6.2022

Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen Rekommendation och kriterier

Finansministeriets publikationer 2022:43		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	finska	**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.

Publikation uppdaterades den 15 februari 2023, s. 57.

Denna version ersätts av nytt, modifierat material på https://urn.fi/URN:ISBN:978-952-367-458-5

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	978-952-367-275-8	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-275-8		

Description sheet
2 June 2022

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

Publications of the Ministry of Finance 2022:43		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	Finnish	**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.

Publication was updated on 15th February 2023, p. 57.

This version is replaced by new, modified material at https://urn.fi/URN:ISBN:978-952-367-458-5

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	978-952-367-275-8	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-275-8		

Sisältö

1 Johdanto

Tämä on tiedonhallintalautakunnan suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä, jäljempänä *Julkri*, ja sen käytöstä. Julkri 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.

Suositus ja siihen liittävät liitteet on valmisteltu tiedonhallintalautakunnan kaudelle 1.5.2021–31.12.2021 asettamassa julkisen hallinnon tietoturvallisuuden arviointikriteeristön jaostossa sekä 1.1.-31.12.2022 asettamassa tietoturvallisuusjaostossa. Jaoston puheenjohtajana on toiminut erityisasiantuntija Eelis Laine valtiovarainministeriöstä ja sihteereinä tietoturva-asiantuntija Hanna Heikkinen ja johtava asiantuntija Tuula Seppo Digi- ja väestötietovirastosta. Tiedonhallintalautakunta on nimennyt jaoston jäseniksi asiantuntijoita eri tiedonhallintayksiköistä. Lisäksi jaosto on kokouksissa, työpajoissa ja seminaareissa kuullut laajalti myös jaoston ulkopuolisia asiantuntijoita. Suositusluonnos oli avoimesti kommentoivana julkisen lausuntopalvelun kautta 28.03.-19.04.2022 välisenä aikana.

Tietosuojan ja henkilötietojen turvaamisen osalta kriteeristöä on laadittu yhteistyössä Tietosuojavaltuutetun toimiston kanssa. Tietosuojavaltuutetun toimisto vastaa tietosuojakriteereistä (liite 1B) ja muista tietosuojaan liittyvistä osioista sekä antaa näistä lisätietoja. Muilta osin lisätietoja antaa Tiedonhallintalautakunta.

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019), jäljempänä *TihL* tai *tiedonhallintalaki*, 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. Jäljempänä näistä tietoturvallisuussääntelyn kohteista käytetään termiä *organisaatio*. 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.

Suosituksen laadinnassa on huomioitu Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä *TLA tai turvallisuusluokitteluasetus*, laki viranomaisen toiminnan julkisuudesta (621/1999), jäljempänä *julkisuuslaki* tai *JulkL*, EU:n yleinen tietosuoja-asetus ((EU) 2016/679), jäljempänä *tietosuoja-asetus* ja tietosuojalaki (1050/2018). Lisäksi on huomioitu Tietoturvallisuuden auditointityökalu viranomaisille (Katakri) ja Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) yhdenmukaisuuden varmistamiseksi.

Viranomaisen tietojärjestelmien turvallisuutta voidaan arvioida viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011), jäljempänä *arviointilaki*, mukaisilla arvioinneilla. Lisätietoja arviointi- ja hyväksymisprosessista löytyy ohjeesta ”Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit”.

Organisaatiot voivat käyttää tietosuoja-asetuksen mukaisia tietosuojaa koskevia sertifikaatteja yhtenä keinona sen osoittamiseksi, että rekisterinpitäjälle tai käsittelijälle säädettyjä velvollisuuksia noudatetaan. Yleisen tietosuoja-asetuksen 42 artiklan mukainen sertifiointi ei vähennä rekisterinpitäjän tai henkilötietojen käsittelijän vastuuta tietosuoja-asetuksen noudattamisesta eikä se rajoita tietosuojavaltuutetun toimiston tehtäviä ja valtuuksia. Henkilötietojen käsittelyä koskevasta osoitusvelvollisuudesta on saatavissa lisätietoja Tietosuojavaltuutetun ohjeesta ”Osoita noudattavasi tietosuojasäännöksiä”.

Viranomaiselle palveluja tarjoavan luotettavuuden arvioinnissa voidaan hyödyntää turvallisuusselvityslain (726/2014) mukaista yritysturvallisuusselvitystä, joka kohdistetaan Suomesta tuotettuun tai tulevaisuudessa tuotettavaan palveluun ja sen tarjoajaan. Lisätietoa on saatavissa Suojelupoliisin ohjeesta ”Yritysturvallisuusselvitys”. Kansainvälisten tietoturvallisuusvelvoitteiden alaisten tietojärjestelmien arvioinnit toteutetaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) mukaisilla menettelyillä. Ulkoasiainministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena. Lisätietoa on saatavissa Kansallisen turvallisuusviranomaisen ohjeistuksista.

2 Kriteeristö

Tässä suosituksessa ja sen liitteissä kuvataan julkisen hallinnon tietoturvallisuuden arviointikriteeristö ja suositus sen käyttöön. Suositus sisältää seuraavat liitteet:

- liite 1A Julkri-kriteerit,
- liite 1B Tietosuojakriteerit,
- liite 2 Julkri-työkalu (Excel),
- liite 3 Julkri-työkalun käyttöohje ja
- liite 4 Termistö.

Kriteeristö sisältää luottamuksellisuuden, saatavuuden ja eheyden perusteella eri tasoille luokiteltuja kriteereitä, joista työkalu poimii olennaiset ja valinnaiset kriteerit arvioitavan kohteen turvallisuusvaatimusten ja valitun käyttötapauksen perusteella. Lähtökohtaisesti olennaiset kriteerit tulisi sisällyttää arviointiin. Organisaatio voi riskiarvioinnin sekä tapauskohtaisen harkinnan perusteella sisällyttää arviointiin myös valinnaisia kriteerejä ja päättää, mitkä valinnaiset kriteerit sisällytetään arviointiin.

Kriteeristöä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Kriteeristö on suositus ja lainsäädännön vaatimukset voidaan täyttää myös muulla kuin kriteereissä kuvatulla tavalla. Julkri sisältää Katakri[1]- ja PiTuKri[2]-arviointikriteeristöjä laajemmin myös julkisen ja salassa pidettävän tiedon, varautumisen ja jatkuvuuden hallinnan sekä tietosuojan kriteereitä.

1 Katakri kts. Katakri – tietoturvallisuuden auditointityökalu viranomaisille - Ulkoministeriö (um.fi)

2 PiTuKri kts. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

2.1 Tarkoitus ja hyödyt

Kriteeristön käyttö tukee organisaatioita tietoturvallisuuden ja henkilötietojen suojaamisen suunnittelussa, toteuttamisessa ja arvioinnissa. Sitä voi hyödyntää lainmukaisuuden arvioinnissa ja osana tietosuoja-asetuksen mukaista osoitusvelvollisuutta. Organisaatio voi käyttää Julkria esimerkiksi seuraavissa tilanteissa:

- **Palvelun suunnittelussa ja vaatimusmäärittelyssä** ennen kehittämistä tai hankintaa tavoitteenaan tunnistaa palvelulle asetettavat vaatimukset.
- **Toimittajan arvioinnissa** tavoitteenaan tunnistaa vaatimukset toimittajalle kilpailutuksessa tai osana palvelusopimusta sekä varmistaa vaatimusten toteutuminen toimittajan toiminnassa.
- **Palvelun arvioinnissa** suhteessa hankinnan ja palvelusopimuksen vaatimuksiin.
- **Tietosuojaa koskevien vaatimusten toteutumisen arvioinnissa.**

Kriteeristö tukee organisaation riskilähtöistä turvallisuusjohtamista. Ennalta määritellyt käyttötapaukset helpottavat kriteeristön tilannekohtaista soveltamista. Lisäksi Julkrissa on mahdollista määritellä myös organisaatiokohtaisia käyttötapauksia usein toistuviin arviointitilanteisiin. Käyttötapauksia käsitellään Julkri-työkalun käyttöohjeessa (liite 3).

Kriteeristöä voidaan käyttää salassa pidettävän tiedon, henkilötiedon ja turvallisuusluokitellun tiedon käsittelyn arvioinnissa. Turvallisuusluokka I (TL I – ERITTÄIN SALAINEN) osalta organisaation tulee lisäksi huomioida tapauskohtaiset käsittelyn vaatimukset.

2.2 Rajaukset

Julkrissa on hallinnollisessa ja teknisessä osa-alueessa mainittu saavutettavuus yleisenä kriteerinä. Yksityiskohtaisempia saavutettavuuskriteerejä kriteeristö ei sisällä, joten organisaation tulee huomioida saavutettavuuteen liittyvät vaatimukset erikseen. (Laki digitaalisten palvelujen tarjoamisesta 306/2019).

Julkri ei sisällä kansainvälisen turvallisuusluokitellun tiedon tietoturvallisuuden arviointia (588/2004). Siihen liittyvästä ohjeistuksesta ja arviointikriteeristöstä vastaa ulkoministeriön alainen kansallinen turvallisuusviranomainen NSA.

Valmiuslain (1552/2011) piiriin kuuluvat toiminnan jatkuvuutta poikkeusoloissa koskevat toimenpiteet on rajattu kriteeristön ulkopuolelle. Kriteeristön varautumista koskeva tiedonhallintalakiin perustuva osio (VAR) kuitenkin osaltaan tukee organisaatiota myös poikkeusoloihin varautumista koskevien vaatimusten täyttämisessä.

Julkrissa ei ole huomioitu toimialakohtaisen lainsäädännön, kuten sosiaali- ja terveydenhuollon tai finanssialan vaatimuksia, eikä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018) mukaisia vaatimuksia.

Vaikka Julkri ei sisällä kansainvälisestä ja toimialakohtaisesta lainsäädännöstä johtuvia vaatimuksia, tulee organisaation kuitenkin tunnistaa ja ottaa huomioon toimialakohtaisesta lainsäädännöstä sekä kansainvälisestä lainsäädännöstä ja EU-sääntelystä johtuvat vaatimukset omassa toiminnassaan.

3 Kriteeristön rakenne ja osa-alueet

Kriteerit on ryhmitelty viiteen **osa-alueeseen**. Jokaisella osa-alueella on yksilöivä osa-alueen nimi, johon perustuu myös osa-alueeseen kuuluvien kriteerien tunnisteen alkuosa. Kriteeristön osa-alueet ja niiden lyhenteet ovat:

- hallinnollinen turvallisuus (HAL),
- fyysinen turvallisuus (FYY),
- tekninen turvallisuus (TEK),
- varautuminen ja jatkuvuudenhallinta (VAR),
- tietosuoja (TSU).

Osa-alue koostuu **pääkriteereistä** ja niitä täydentävistä **alikriteereistä**. Kriteerejä on yhteensä yli kaksi sataa. Pääkriteeri – alikriteeri rakennetta on hyödynnetty esimerkiksi sellaisissa tapauksissa, joissa samaan aihealueeseen liittyvät vaatimukset tiukentuvat siirryttäessä korkeammille turvallisuuden tasoille. Esimerkiksi salassa pidettäviä tietoja koskevaa pääkriteeriä voidaan täydentää TL IV luokkaan kuuluvia tietoja koskevan vaatimuksen toteutustapaa tarkentavalla alikriteerillä.

Kukin kriteeri on luokiteltu eri tasoille luottamuksellisuuden, eheyden, saatavuuden ja tietosuojan näkökulmista. Kriteeristä riippuen se voi liittyä yhteen tai useampaan näkökulmaan. Esimerkiksi sama käyttöoikeuksia koskeva kriteeri voi liittyä sekä luottamuksellisuuteen, eheyteen että tietosuojaan.

Kriteeristön eri osa-alueiden yleiskuvaukset on kuvattu seuraavissa luvuissa. Yksittäiset kriteerit ovat liitteissä 1A ja 1B.

3.1 Hallinnollinen turvallisuus

Hallinnollisen turvallisuuden osa-alueessa käsitellään niitä menetelmiä, joilla tietoturvallisuuden hallinta jalkautetaan osaksi koko organisaation toimintaa. Osa-alue kattaa yleisiä hallinnollisen turvallisuuden, henkilöstöturvallisuuden, tietojärjestelmien ja niiden hankinnan sekä käyttöturvallisuuden kriteereitä. Hallinnollisen turvallisuuden kriteereillä pyritään siihen, että organisaatiolla on riittävän hyvin toimiva tietoturvallisuuden hallintajärjestelmä sekä menettelyt sen varmistamiseksi, että tietoja käsittelevä henkilöstö toimii

asianmukaisesti. Organisaation tulee myös varmistaa, että tietojen käsittelyä koskevia velvoitteita noudatetaan tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta.

Monet hallinnollisen turvallisuuden osa-alueen kriteerit toimivat perustana muiden osa-alueiden kriteereille. Esimerkiksi suojattavien kohteiden tunnistamiseen, riskienhallintaan ja dokumentointiin liittyvät kriteerit ovat yleisiä, ja niitä tulee oletusarvoisesti hyödyntää muiden osa-alueiden kriteerien soveltamisen yhteydessä.

Hallinnolliseen turvallisuuteen liittyviä prosesseja tulee käsitellä kokonaisuuksina. Tietoturvallisuuden hallintamenettelyt tulee suhteuttaa riskienarvioinnin perusteella suojattavaan tietoon ja organisaation toimintaan.

Kriteeristön käyttö edellyttää tarkoituksenmukaista kohdentamista. Mikäli jotain toimintoja on arvioitu jo aiemmin, voidaan aiempia tuloksia hyödyntää soveltuvin osin. Esimerkiksi jos organisaation tietoliikenneympäristö on arvioitu viimeisen vuoden aikana, eikä siihen ole tehty merkittäviä muutoksia, voidaan tätä arviointia mahdollisesti hyödyntää tietoliikenneympäristöön asennettavan uuden tietojärjestelmän arvioinnissa.

Mikäli organisaatiossa käsitellään eri tasoille luokiteltuja tietoja erillisissä ympäristöissä ja prosesseissa, voi olla tarkoituksenmukaista jakaa arviointi erillisiin loogisiin kokonaisuuksiin. Esimerkiksi korkeammille tasoille turvallisuusluokiteltujen tietojen käsittely-ympäristön henkilöstön ohjeistuksen sisältö eroaa yleensä merkittävästi koko organisaatiota koskevista yleisistä ohjeistuksista.

Hyvään riskienhallintaan kuuluu menettelytapojen ja erityisesti riskien arvioinnin dokumentointi. Tietoturvallisuuden hallintaan liittyvät suunnitelmat ja ohjeet sekä arvioinnin tulokset ja johtopäätökset tulisi esittää kirjallisena. Dokumentteihin tulee täydentää tiedot toimenpiteiden toteutumisesta. Dokumentoinnilla tässä tarkoitetaan laajasti erilaisia kirjalliseen muotoon saatettavissa olevia tallenteita, kuten Intranet-sivuja ja toiminnanohjausjärjestelmän työmääräyksiä.

3.2 Fyysinen turvallisuus

Fyysinen turvallisuus (FYY) sisältää luvattoman tietoihin pääsyn estäviä ja rajoittavia toimitiloihin ja säilytysratkaisuihin liittyviä kriteereitä. Lisäksi osa-alueella on kuvattu tietojen käsittelyyn, säilyttämiseen, siirtämiseen, kuljettamiseen ja tuhoamiseen liittyviä kriteereitä. Fyysisen turvallisuuden osa-aluetta on mahdollista käyttää arvioitaessa tiedon suojaamiseksi toteutettuja fyysisen turvallisuuden toimenpiteitä.

Osa-alueen sisältö perustuu Katakri-kriteeristöön. Erityisesti turvallisuusluokitellun tiedon käsittelyä koskevien kriteerien sisältö on pyritty säilyttämään yhdenmukaisena Katakrin kanssa. Selkeimpiä eroja suhteessa Katakriin ovat kansainvälisiin tietoturvallisuusvelvoitteisiin perustuvien kriteerien jättäminen pois osa-alueelta sekä tiettyjen kriteerien luokittelu sovellettavaksi myös muille kuin turvallisuusluokitelluille tiedoille.

Osa-alueen rakenne on suunniteltu siten, että eri tasoisia turvallisuusalueita koskevat yhteiset kriteerit, vain hallinnollisia alueita koskevat kriteerit sekä vain turva-alueita koskevat kriteerit on koottu kukin omaan alalukuunsa. Tämä rakenne poikkeaa Katakrin rakenteesta, jossa osa kriteereistä on toistettu saman sisältöisinä eri tasoisilla turvallisuusalueilla.

Viranomaisten tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia (tiedonhallintalaki 15 § 2 mom). Turvallisuusluokiteltujen tietojen fyysiseksi suojaamiseksi, turvallisuusluokitteluasetuksessa on säädetty kahdentyyppisistä fyysisesti suojatuista turvallisuusalueista: hallinnollisista alueista ja turva-alueista. Julkrissa käytetään hallinnollisen alueen ja turva-alueen käsitteitä.

Salassa pidettäviä tietoja sisältävät tietovarannot sekä niiden käsittelyyn käytetyt tietojärjestelmät suositellaan sijoitettavaksi viranomaisen tähän tarkoitukseen määrittelemälle suojatulle-alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa ja tässä suosituksessa ja sen liitteenä olevassa kriteeristössä kuvattu hallinnollinen alue.

Hallinnollisella alueella tarkoitetaan käytännössä sellaista organisaation määrittelemää aluetta, johon sivulliset eivät pääse hallitsemattomasti ja johon on toteutettu riittävät toimenpiteet alueella käsiteltävien ja säilytettävien tietojen turvallisuuden varmistamiseksi. Alueen rakenteille ja muille toimenpiteille ei ole asetettu yksityiskohtaisia vaatimuksia vaan organisaatio voi suunnitella ne soveltaen riskilähtöisesti fyysisen (FYY) osa-alueen kriteereitä.

Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten turvatoimien toteuttamista siten, että estetään luvaton pääsy tietoihin:

a) varmistamalla, että tietoja käsitellään ja säilytetään asianmukaisesti,
b) mahdollistamalla pääsy tietoihin tiedonsaantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella,
c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet ja
d) estämällä oikeudetta tapahtuva tunkeutuminen tai viivyttämällä sitä.

Toimitiloissa, joissa toimii useampi organisaatio tulee kunkin tietoja käsittelevän organisaation varmistua siitä, että yhteisten toimitilojen tarjoama turvallisuus on riittävä suhteessa organisaatioon kohdistettuihin fyysisen turvallisuuden vaatimuksiin.

3.3 Tekninen turvallisuus

Tekninen osa-alue kattaa tietojärjestelmien ja tietoliikenneyhteyksien teknisiin ominaisuuksiin, turvalliseen käyttöön ja toimintamalleihin liittyvät kriteerit. Kriteerien tavoitteena on varmistaa, että tietojärjestelmät ja niiden käyttö toteuttavat yleiset teknisen tietoturvallisuuden, ja tarvittaessa myös tietosuojan, vaatimukset. Huomioitavaa kuitenkin on, että teknisen osa-alueen kriteerien toteuttaminen ei yksinään takaa yksittäisen tietojärjestelmän turvallisuutta, vaan myös muiden osa-alueiden kriteerit tulee huomioida.

Arvioinnin kohteena voi olla joko yksittäinen tietojärjestelmä tai tietojenkäsittely-ympäristö tai laajempi kokonaisuus tietojärjestelmiä. Arvioitaessa useista tietojärjestelmistä koostuvaa kokonaisuutta, tulee huomioida vaatimusten toteutuminen kaikissa yksittäisissä järjestelmissä.

Tekninen osa-alue ottaa huomioon myös järjestelmien sijoittumisen turvallisuusalueille ja niiden etäkäytön turvallisuusalueiden ulkopuolella. Tarkemmat vaatimukset hallinnolliselle alueelle ja turva-alueelle on määritelty fyysisen turvallisuuden osa-alueella.

Kriteeristössä viitataan usean kriteerin osalta, että salausratkaisun tulee olla riittävän turvallinen kyseiseen käyttötapaukseen. Salausratkaisun turvallisuuden arvioinnissa voi käyttää hyväksi esimerkiksi Kyberturvallisuuskeskuksen NCSA-toiminnon kansainvälisen turvallisuusluokitellun tiedon suojaamiseksi myöntämiä hyväksyntöjä. Lisätietoja on saatavilla Kyberturvallisuuskeskuksen verkkosivuilta.

3.4 Varautuminen ja jatkuvuudenhallinta

Osa-alueelle on koottu normaaliolojen varautumista ja jatkuvuudenhallintaa koskevia kriteereitä. Kriteerit perustuvat tiedonhallintalain (muun muassa 4 §:n 2 mom 2 k, 13 §:n 1, 2 ja 4 mom sekä 15 §) ja yleisiin vaatimuksiin laadittavista ohjeista ja tietoturvallisuustoimenpiteistä sekä standardissa ISO/IEC 27002 kuvattuihin tietoturvallisuuden jatkuvuutta kuvaaviin hallintakeinoihin. Valmiuslain piiriin kuuluvat toiminnan jatkuvuutta poikkeusoloissa koskevat toimenpiteet on rajattu kriteeristön ulkopuolelle. Kriteeristö kuitenkin osaltaan tukee organisaatiota myös poikkeusoloihin varautumista koskevien vaatimusten täyttämisessä.

Osa-alueen kriteerit koskevat pääasiassa saatavuudeltaan tärkeiksi tai kriittisiksi luokiteltuja kohteita. Saatavuuden tasot on kuvattu luvussa 4.2 Luokittelutasot. Riskiperusteisesti kriteereitä voidaan soveltaa myös matalampiin saatavuusluokkiin kuuluvissa kohteissa. Jatkuvuusvaatimusten sekä niiden taustalla olevan lainsäädännön selvittäminen koskee kuitenkin lähtökohtaisesti kaikkia organisaatioita.

Keskeisiä kriteereitä osa-alueella ovat varautumistoimenpiteet erilaisiin vakaviin häiriötilanteisiin, toiminnan jatkuvuussuunnitelmat sekä tietojärjestelmien toipumissuunnitelmat ja niiden harjoittelu. Jatkuvuudenhallinta liittyy läheisesti häiriöiden ja poikkeamatilanteiden hallintaprosesseihin, joihin liittyvät kriteerit on kuvattu HAL- ja TEK-osa-alueilla.

3.5 Tietosuoja

Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän taikka henkilön käyttämien päätelaitteiden yksilöivien teknisten tietojen perusteella.

Henkilötietojen käsittelyssä on noudatettava tietosuoja-asetuksen vaatimuksia, kun käsittely on kokonaan tai osittain automaattista tai tiedot muodostavat rekisterin osan. Tietosuoja-asetus suojaa henkilötietoja riippumatta siitä, mitä tekniikkaa tietojenkäsittelyssä käytetään. Tietojen säilytystavalla ei myöskään ole merkitystä. Tietoja voidaan säilyttää esimerkiksi tietojärjestelmässä, videovalvontajärjestelmässä tai paperiarkistossa.

Tietosuoja-osa-alueelle on koottu yksinomaan henkilötietojen käsittelyä koskevia kriteereitä, joita ovat esimerkiksi käsittelyn lainmukaisuutta, tietosuojaperiaatteita sekä rekisteröidyn oikeuksia koskevat kriteerit. Lisäksi henkilötietojen käsittelyyn sovelletaan Julkrissa muilla osa-alueilla olevia tietoturvakriteereistä. Henkilötietojen käsittelyssä sovellettavat tietoturvakriteerit ovat Julkrissa valtaosin yhteisiä muiden tietojen turvaamisessa käytettyjen kriteerien kanssa. Jokainen muilla osa-alueilla oleva kriteeri on luokiteltu sen mukaan, sovelletaanko sitä myös henkilötietojen käsittelyssä ja jos sovelletaan, koskeeko kriteeri kaikkia henkilötietoja vai ainoastaan erityisiä henkilötietoryhmiä. Muilla osa-alueilla olevia henkilötietojen käsittelyä koskevia kriteereitä on joissakin yksittäisissä tapauksissa tarkennettu tietosuoja-osa-alueella olevalla tarkentavalla kriteerillä.

4 Kriteerien tiedot

Arviointikriteeri koostuu tunnisteesta, luokitteluista, (luottamuksellisuus, eheys, saatavuus, henkilötieto), sisällöistä (nimi, vaatimus, yleiskuvaus ja toteutusesimerkki) sekä viittauksista eri lähteisiin.

Taulukko 1. Esimerkki Riskienhallinta kriteeristä.

Tunniste	HAL-06, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Riskienhallinta
Vaatimus	Organisaatio toteuttaa tietoturvallisuusriskien hallintaa ja on arvioinut olennaiset tietoihin kohdistuvat riskit sekä mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.
Yleiskuvaus	Tietoturvallisuusriskien hallintaprosessi koostuu toimintaympäristön määrittämisestä, riskien arvioinnista (tunnistaminen, analysointi, merkityksen arviointi), riskien käsittelystä, riskien hyväksynnästä, riskejä koskevasta viestinnästä ja tiedonvaihdosta sekä riskien seurannasta ja katselmoinnista. Tietoturvallisuusriskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa. Tietoturvallisuusriskien hallinnan avulla varmistetaan tietoturvallisuustoimenpiteiden riittävyys tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi. Riskienhallinta vaikuttaa muihin tietoturvallisuuden hallinnan eri osa-alueisiin. Riskienhallinta tulee suunnitella ja ohjeistaa siten, että siinä käsitellään systemaattisesti ja suunnitelmallisesti erilaisia tietoturvallisuuteen liittyviä riskejä kuten tietosisällön virheellisyyksistä johtuvia riskejä, organisaation toiminnan keskeytyksiin liittyviä riskejä sekä henkilötietojen tietoturvaloukkauksiin liittyviä riskejä.
Toteutusesimerkki	– Tietoturvallisuusriskien arvioinnissa ja analysoinnissa käytetään yleisesti hyväksyttyä menetelmää. – Tietoturvallisuusriskien arvioinneista laaditaan aikataulutettu ja vastuutettu vuosisuunnitelma. – Tietoturvallisuusriskien hallintaan osallistuu riittävästi asiantuntijoita. – Tietoturvallisuusriskien hallinnassa on otettu huomioon sidosryhmistä ja toimitusketjuista aiheutuvat riskit. – Tietoturvallisuusriskien arviointia hyödynnetään muissa tietoturvallisuuden hallinnan prosesseissa.
Lainsäädäntö	TihL 13 § 1 mom; TLA 6 §, 7 §
Viitteet	Julkri: FYY-01, TEK-01, TEK-14, TEK-16; Katakri: T-03
Muita lisätietoja	SFS-EN ISO/IEC 27001:2017 6.1 ja 8–10, SFS-EN ISO/IEC 27005:2018 luku 6, SFS ISO 31000:2018, PiTuKri TJ-03; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 5.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6

Yllä on kuvattu esimerkkinä hallinnollisen osa-alueen kriteeri Riskienhallinta. Kriteerin tunniste on HAL-06. Tässä tapauksessa luottamuksellisuuden (L) taso on julkinen, eheys (E) on vähäinen, saatavuus (S) on vähäinen ja kyseistä kriteeriä voi hyödyntää myös henkilötietojen käsittelyn arvioimisessa (TS). Luvuissa 4.1.-4.4 on kuvattu tarkemmin kriteerien tunnisteet ja niiden tasot.

4.1 Tunniste

Kriteerillä on yksilöivä tunniste, joka koostuu osa-alueen nimen lyhenteestä, pääkriteerin juoksevasta numerosta sekä alikriteerin juoksevasta numerosta. Yksilöivien tunnisteiden lyhenteet ovat hallinnollinen (HAL), tekninen (TEK), varautuminen (VAR) ja fyysinen (FYY) ja tietosuoja (TSU). Pääkriteerit on numeroitu osa-alueittain ja alikriteerit pääkriteereittäin. Esimerkiksi teknisen tietoturvallisuuden osa-alueella on pääkriteeri TEK-15 ja sillä alikriteerit TEK-15.1 ja TEK-15.2.

4.2 Luokittelutasot

Kriteerit on luokiteltu luottamuksellisuuden, eheyden ja saatavuuden näkökulmista. Jos kriteeri koskee myös henkilötietojen käsittelyä, on se luokiteltu lisäksi tietosuojan näkökulmasta. Täydentävät tietoturvallisuuden näkökulmat, kuten tiedon kiistämättömyys tai autenttisuus, on huomioitu kriteerien sisällöissä.

Kriteeri voi liittyä yhteen tai useampaan tietoturvallisuuden näkökulmaan ja se valikoituu mukaan arviointiin, jos se on olennainen yhdestäkin näkökulmasta. Esimerkiksi kriteeri voi olla merkitty eheyden näkökulmasta tasolle Normaali, mikä tarkoittaa, että kriteeri on olennainen kaikille niille tiedoille, jotka on luokiteltu eheyden näkökulmasta tasolle Normaali.

Monet kriteerit ovat luonteeltaan yleisiä ja liittyvät laajasti tietoturvallisuuden hallintaan. Tällaisia ovat esimerkiksi tehtävien ja vastuiden määrittelyyn, riskien hallintaan ja dokumentointiin liittyvät kriteerit.

4.2.1 Luottamuksellisuuden tasot

Luottamuksellisuus on tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä eikä se paljastu sivullisille. Tässä suosituksessa luottamuksellisuuden tasot on kuvattu asteikolla julkinen, salassa pidettävä, turvallisuusluokka IV, turvallisuusluokka III, turvallisuusluokka II ja turvallisuusluokka I. Taulukossa on kuvattu nämä tasot ja esimerkkejä. Tiedonhallintalautakunnan suositus (2021:5) sisältää suosituksia turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelyä koskevista tietoturvallisuustoimenpiteistä.

Taulukko 2. Luottamuksellisuuden tasot.

Taso	Kuvaus	Esimerkki
Julkinen	Viranomaisen asiakirjat ovat julkisia, jollei laissa erikseen toisin säädetä. (JulkL 1 §)	Kunnanvaltuuston pöytäkirjat julkisilta osiltaan, organisaation julkiset internet-sivut.
Salassa pidettävä	Viranomaisen asiakirja on pidettävä salassa, jos se laissa on säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. (julkisuuslaki 22 §)	Potilasasiakirjat, tiedot sosiaalihuollon asiakkaasta, psykologiset testit ja soveltuvuuskokeet.
Turvallisuusluokka IV (TL IV)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **lievää** vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.	TihL 18 §:ssä mainittujen suojattavien etujen kannalta olennaisen tietojärjestelmän turvajärjestelyiden dokumentaatio, jonka paljastuminen ei keskeytä toimintaa, mutta saattaa edellyttää muutoksia paljastuneissa suunnitelmissa.
Turvallisuusluokka III (TL III)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.	TihL 18 §:ssä mainittujen suojattavien etujen kannalta elintärkeiden toimintojen turvajärjestelyiden dokumentaatio, jonka paljastumisen vuoksi toiminta joudutaan keskeyttämään.
Turvallisuusluokka II (TL II)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **merkittävää vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.	TihL 18 §:ssä mainittujen suojattavien etujen kannalta elintärkeiden toimintojen turvajärjestelyiden dokumentaatio, jonka paljastumisen vuoksi laajan ihmisjoukon turvallisuutta ei voida taata ja jonka seurauksena toiminta joudutaan keskeyttämään pitkähköksi ajaksi.
Turvallisuusluokka I (TL I)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **erityisen suurta vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.	TihL 18 §:ssä mainittujen suojattavien etujen kannalta yhteiskunnan toimintakyvyn kannalta keskeisiin toimintoihin, kuten kriittiseen infrastruktuurin tai elintärkeän toiminnan turvajärjestelyjä koskevan tiedon paljastuminen, jonka seurauksena viranomaisen tai muun kriittisen infrastruktuurin toimijan toiminta todennäköisesti estyy ja vahinko on laajamittaista.

Kriteerejä ei ole luokiteltu luottamuksellisuuden näkökulmasta erikseen tasolle Harkinnanvaraisesti annettava. Organisaation on riskien perusteella harkittava, sisällytetäänkö harkinnanvaraisesti annettavien tietojen arviointiin salassa pidettävien tietojen kriteereitä. Tämä onnistuu määrittelemällä arvioinnin esiehdoissa luottamuksellisuus tasolle Julkinen, jolloin Julkri-työkalu tarjoaa salassa pidettäviä tietoja koskevat kriteerit valinnaisiksi.

4.2.2 Saatavuuden tasot

Saatavuus tarkoittaa sitä, miten tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla. Julkrissa saatavuuden tasot ovat vähäinen, normaali, tärkeä ja kriittinen. Taulukossa on kuvattu ja annettu esimerkkejä eri saatavuuden tasoista.

Taulukko 3. Saatavuuden tasot.

Taso	Kuvaus	Esimerkki
Vähäinen	Tiedon saatavuuden osalta pystytään hyväksymään useiden viikkojen mittaisia häiriöitä.	Henkilöstön pysäköintipaikkojen rekisteri, puiston penkkien vikarekisteri
Normaali	Tiedon saatavuuden osalta pystytään hyväksymään enintään päivien mittaisia häiriöitä.	Arkistojärjestelmä
Tärkeä	Tiedon saatavuuden osalta pystytään hyväksymään enintään tuntien mittaisia häiriöitä.	Potilastietojärjestelmä
Kriittinen	Tiedon saatavuuden osalta pystytään hyväksymään enintään minuuttien mittaisia häiriöitä.	Keskitetyt käyttäjän tunnistamispalvelut

4.2.3 Eheyden tasot

Eheys on tiedon ominaisuus, joka tarkoittaa sitä, että tietoa ei ole muutettu luvatta tai että se ei ole muuttunut vahingossa ja että mahdolliset muutokset voidaan todentaa. Taulukossa on kuvattu Julkrissa käytössä olevat eheydet tasot vähäinen, normaali ja tärkeä sekä annettu tasoihin joitakin esimerkkejä.

Taulukko 4. Eheyden tasot.

Taso	Kuvaus	Esimerkki
Vähäinen	Tiedon häviämisestä tai muuttumisesta ei aiheudu olennaista haittaa.	Toimisto-ohjelmistot, järjestelmien virhelokit.
Normaali	Tiedon häviäminen tai muuttuminen aiheuttaa kohtuullista haittaa, mutta se voidaan havaita ja siitä voidaan toipua.	Henkilöstöhallinnon järjestelmät.
Tärkeä	Tiedon häviäminen tai muuttuminen aiheuttaa merkittävää haittaa tai mainevahinkoa ja sen havaitseminen voi olla vaikeaa.	Laboratoriotuloksia välittävät integraatioalustat, joissa yksittäisten mittausten virheiden havainnointi voi olla vaikeaa. Henkilötietojen käsittelyyn liittyvät lokitiedot.
Kriittinen	Tiedon häviäminen tai muuttumista ei voida hyväksyä missään tilanteessa.	Yhteiskunnan toimivuuden kannalta keskeiset maksuliikennejärjestelmät tai raideliikenteen ohjausjärjestelmä

4.3 Sisällöt

Kriteerien sisältö koostuu nimestä, vaatimuksesta, yleiskuvauksesta ja toteutusesimerkistä.

- **Nimi** kuvaa otsikkotasolla mihin asiaan kriteeri kohdistuu. Nimi on yksi tai muutama kriteerin aihepiiriä kuvaileva sana. Alikriteerien nimi koostuu pääkriteerin nimestä sekä väliviivalla erotetusta tarkenteesta. Esimerkiksi Käyttöoikeudet – ajantasaisuus, joka on käyttöoikeudet -pääkriteeriä täsmentävä ajantasaisuutta koskeva alikriteeri.
- **Vaatimus** kuvaa tavoitteen, joka organisaation tulee täyttää. Vaatimus on lyhyehkö lause tai lyhyt kappale. Vaatimukset voidaan täyttää useilla eri toteutustavoilla. Vaatimukset ovat yksilöityjä, eli samaan vaatimukseen ei sisälly useita eri vaatimuksia. Mikäli alikriteeri ei sisällä erillistä vaatimusta, alikriteeri tarkentaa pääkriteeriä joko yleiskuvauksen tai toteutusesimerkin osalta.
- **Yleiskuvaus** sisältää kriteeriä taustoittavaa ja perustelevaa lisätietoa. Se ei ole vaatimus vaan peruste kriteerille. Yleiskuvauksessa voidaan esimerkiksi kuvata uhkia, joita kriteerin mukaisten hallintakeinojen avulla torjutaan. Mikäli samaan kokonaisuuteen liittyy useita alikriteereitä, laaditaan eri kriteereille yhteinen yleiskuvaus vain kertaalleen pääkriteerin yhteyteen.
- **Toteutusesimerkki** kuvaa miten organisaatio voi toteuttaa vaatimuksen. Toteutusesimerkki ei ole vaatimus, mutta se voi toimia suuntaa antavana ohjeena siitä tasosta, miten vaatimuksen voi täyttää.

4.4 Viittaukset

Kriteeri voi sisältää viittauksia lainsäädäntöön, ohjeisiin ja standardeihin sekä viittauksia Katakri- ja PiTuKri-arviointikriteereihin sekä muihin Julkri-kriteeristön kriteereihin. Viittaukset on pyritty yksilöimään siten, että vastaava kohta on löydettävissä nopeasti viiteaineistosta.

- **Lainsäädäntö** kuvaa mihin lainsäädäntöön kriteeri perustuu.
- **Muita lisätietoja** sisältävät viittauksia kriteeriin liittyviin tiedonhallintalautakunnan suosituksiin, PiTuKri-arviointikriteeristöön ja standardeihin.
- **Julkri-viite** sisältää viittauksen yhteen tai useampaan muuhun Julkri-kriteeristön kriteeriin, mikäli kriteeri muodostaa sovellettavan kokonaisuuden yhdessä jonkun toisen kriteerin kanssa.
- **Katakri-viite** sisältää viittauksen vastaavaan kriteeriin Katakri-arviointikriteeristössä, jos sellainen on olemassa.

5 Kriteeristön käyttö

Kriteeristöä voidaan soveltaa koko organisaation toimintaan, jonkun osa-alueen toimintaan tai hankittavan palvelun arviointiin. Tiedon eri tasoille tarkoitetut käsittely-ympäristöt suositellaan arvioitavaksi erikseen, jotta matalamman tason kohteisiin ei sovelleta liian korkeita kriteereitä eikä siten lisätä tarpeettomasti monimutkaisuutta ja kustannuksia.

Arvioinnin kohteen täsmällinen määrittely ja rajaus on yksi kriteeristön käytön tärkeimmistä vaiheista. Arviointi voi kohdistua yksittäiseen järjestelmään, mutta lisäksi tulee varmistaa, että eri arvioinnit yhdessä kattavat koko organisaation toiminnan.

Organisaatiossa käsitellään kriittisyydeltään ja luottamuksellisuudeltaan moniin eri luokkiin kuuluvia tietoja ja käsittelyssä käytetään monia eri tietojärjestelmiä sekä palveluita. Lisäksi eri tietojärjestelmien yhteydessä usein hyödynnetään yhteisiä alustapalveluita. Näistä seikoista johtuen organisaation kannattaa suunnitella arvioitavat kohteet loogisiksi kokonaisuuksiksi sekä hyödyntää jo aiemmin tehtyjä arviointeja.

Esimerkiksi jos hankitaan uusi tietojärjestelmä, jota tullaan operoimaan yhteisellä alustalla, jonka turvallisuus on jo aiemmin arvioitu, voidaan uuden tietojärjestelmän arvioinnista jättää pois aiemmin arvioidut yhteisen alustan vastuulla olevat kriteerit.

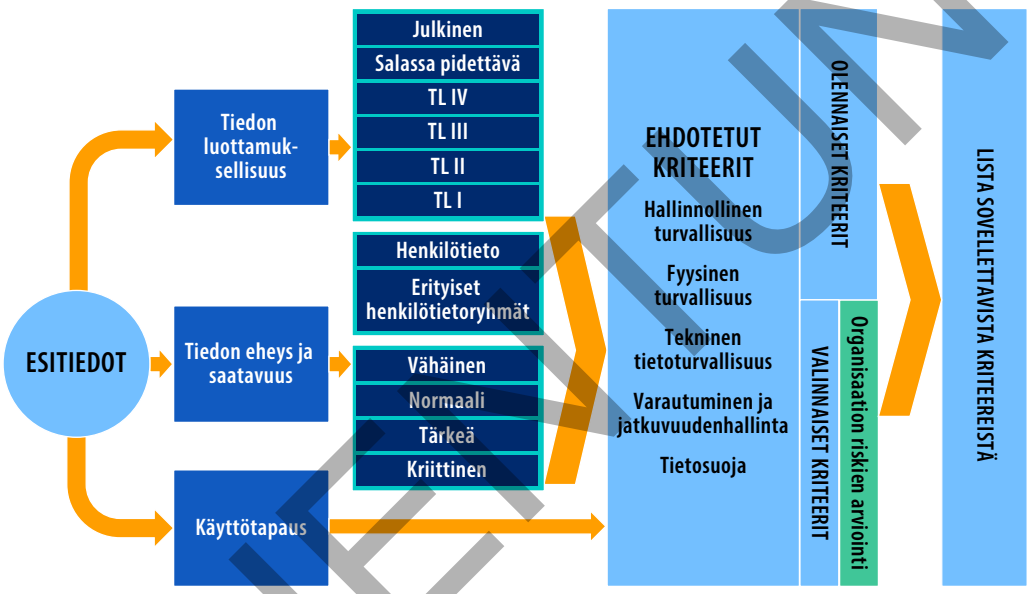
Käyttötapausten avulla organisaatio voi määritellä ennakolta eri tilanteisiin soveltuvia kriteereitä ja siten helpottaa kriteeristön käyttöä samankaltaisena toistuvissa tilanteissa. Käyttötapausten hyödyntämistä on kuvattu tarkemmin erillisessä liitteessä 3 Työkalun käyttöohje.

Ennen kriteeristön käyttöä organisaation tulee määritellä arvioinnin kohteesta seuraavat asiat:

- arvioitavalta kohteelta edellytettävä luottamuksellisuus, eheys ja saatavuus,
- sisältyykö arvioinnin kohteeseen henkilötietoja sekä kuuluvatko nämä tiedot erityisiin henkilötietoryhmiin,
- mahdollisesti arvioinnista poisjätettävät osa-alueet,
- käyttötapaus, jos arviointiin soveltuva käyttötapaus on olemassa.

Arvioinnin kohteen luokittelun perusteella kriteerit ovat olennaisia, valinnaisia tai jätetään arvioinnin ulkopuolelle. Organisaation on suositeltavaa sisällyttää olennaiset kriteerit arviointiin. Valinnaisten kriteerien osalta organisaatio päättää riskiarvion sekä tilannekohtaisen harkinnan perusteella kunkin kriteerin sisällyttämisestä arviointiin. Kuviossa 1. on esitetty prosessi kriteeristön käytöstä.

Kuvio 1. Havainnekuva kriteeristön käytöstä.



Hyödynnettäessä Julkri-kriteeristöä organisaation tietoturvallisuuden arvioinnissa, on lähtökohtaisesti täytettävä arviointiin sisältyvien kriteerien vaatimukset. Organisaatio voi kuitenkin jättää arviointiin sisältyvän kriteerin vaatimuksen täyttämättä, jos organisaatio voi osoittaa, että riskiä ei ole tai riski on hyväksyttävällä tasolla kriteerin vaatimuksen täyttämättä jättämisestä huolimatta. Esimerkiksi riskejä on pienennetty riittävästi muilla keinoilla hyödyntäen kompensoivia kontrolleja. Lainsäädännöstä suoraan johtuvat vaatimukset on kuitenkin täytettävä lainsäädännössä edellytetyllä tavalla.

Jos organisaatio tarvitsee todistuksen Julkri-kriteeristöön perustuvasta vaatimuksenmukaisuudesta, niin kaikkien arviointiin sisältyvien kriteerien tulee toteutua arvioinnin kohteessa. Jos kriteerin toteuttaminen ei kuitenkaan ole mahdollista, on yksilöitävä ja perusteltava kompensoivat menettelyt, joilla varmistetaan, että riski on hyväksyttävällä tasolla kriteerin toteuttamatta jättämisestä huolimatta.

Kriteeristöä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Kriteeristö on suositus ja lainsäädännön vaatimukset voidaan täyttää myös muulla kuin kriteereissä kuvatulla tavalla.

5.1 Arviointia edeltävät toimenpiteet

Ennen arvioinnin käynnistymistä suositellaan hankintojen turvallisuuden varmistamista, lainsäädäntöjohdannaisten riskien selvittämistä sekä sopimusehtojen soveltuvuus käyttötarkoitukseen. Tämä koskee ensisijaisesti tietojärjestelmille tai palveluille tehtäviä arviointeja. Tässä voidaan hyödyntää hallinnollisen turvallisuuden osa-alueen riskienhallintaan liittyviä kriteerejä HAL-06 ja HAL-06.1 sekä hankintojen turvallisuuteen liittyviä kriteerejä HAL-16 ja HAL-16.1. Mainittuja edeltäviä toimenpiteitä on kuvattu lyhyesti seuraavissa kappaleissa.

Tietoturvallisen tietojenkäsittelyn järjestäminen

Organisaation tulee varmistaa hankinnoissaan, että käytettävien tietojärjestelmien ja palveluiden osalta on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. Organisaation on ennakolta varmistuttava siitä, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti.

Lainsäädäntöjohdannaiset riskit

Organisaatio tulee tunnistaa lainsäädäntöjohdannaiset riskit, joilla viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa palveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy palvelun tai järjestelmän asiakkaiden salassa pidettäviin tietoihin.

Järjestelmä- ja palvelusopimukset

Palvelun tai järjestelmän palveluntarjoajan sopimusehdoista tulee varmistaa, että ne eivät rajoita kyseisen palvelun tai järjestelmän soveltuvuutta kyseiseen käyttötapaukseen koko niiden elinkaaren ajan.

LÄHTEET

Säädökset

Asevelvollisuuslaki (1438/2007). https://www.finlex.fi/fi/laki/ajantasa/2007/20071438. Viitattu 26.04.2022.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI. Viitattu 26.04.2022.

Laki digitaalisten palvelujen tarjoamisesta (306/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20190306. Viitattu 26.04.2022.

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181054. Viitattu 26.04.2022.

Laki julkisen hallinnon tiedonhallinnasta (906/2019). https://finlex.fi/fi/laki/ajantasa/2019/20190906. Viitattu 26.04.2022.

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). https://www.finlex.fi/fi/laki/ajantasa/2004/20040588. Viitattu 26.04.2022.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011). https://www.finlex.fi/fi/laki/ajantasa/2011/20111406. Viitattu 26.04.2022.

Laki viranomaisten toiminnan julkisuudesta (621/1999). https://www.finlex.fi/fi/laki/ajantasa/1999/19990621. Viitattu 26.04.2022.

Tietosuojalaki (1050/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181050. Viitattu 26.04.2022.

Turvallisuusselvityslaki (726/2014). https://www.finlex.fi/fi/laki/ajantasa/2014/20140726. Viitattu 26.04.2022.

Työaikalaki (872/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20190872. Viitattu 26.04.2022.

Valtion virkaehtosopimuslaki (664/1970). https://www.finlex.fi/fi/laki/ajantasa/1970/19700664. Viitattu 26.04.2022.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20191101. Viitattu 26.04.2022.

Valmiuslaki (1552/2011). https://www.finlex.fi/fi/laki/ajantasa/2011/20111552. Viitattu 26.04.2022.

Tiedonhallintalautakunnan suositukset

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö 2021:65. Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. http://urn.fi/URN:ISBN:978-952-367-897-2.

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö 2021:5. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. http://urn.fi/URN:ISBN:978-952-367-500-1.

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö 2022:4. Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. http://urn.fi/URN:ISBN:978-952-367-906-1

Ohjeet ja muut materiaalit

BSI IT-Grundschutz-Compendium 2021. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf. Viitattu 26.04.2022

CIS Critical Security Controls. https://www.cisecurity.org/controls. Viitattu 26.04.2022.

Hansel. 2017. Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja. Versio 1. tietosuoja-ohje.pdf (hansel.fi). Viitattu 28.4.2022.

Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246. Viitattu 26.04.2022.

NIST SP 800 -sarja. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information. Viitattu 26.04.2022.

NIST. Erityisesti 800–53 (tietoturvallisuuden ja tietosuojan hallintakeinot), 800–37 (riskienhallinta), 800-63B (käyttäjän tunnistaminen ja elinkaaren hallinta). https://csrc.nist.gov/publications/sp800. Viitattu 26.04.2022.

PiTuKri 2020 Pilvipalveluiden turvallisuuden arviointikriteeristö. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf. Viitattu 26.04.2022.

Suojelupoliisi. Suojelupoliisin ohje: Yritysturvallisuusselvitys". https://supo.fi/yritysturvallisuusselvitys. Viitattu 26.04.2022

Tietosuojavaltuutetun toimisto. Osoita noudattavasi tietosuojasäännöksiä. https://tietosuoja.fi/osoitusvelvollisuus. Viitattu 26.04.2022.
Turvallisuuskomitea (2017). Yhteiskunnan turvallisuusstrategia. https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/. Viitattu 26.04.2022.
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. Viitattu 26.04.2022.
Traficom 2021. Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut. Viitattu 26.04.2022.
Ulkoministeriö. Kansallinen turvallisuusviranomainen. https://um.fi/kansallinen-turvallisuusviranomainen. Viitattu 26.04.2022
Valtiovarainministeriö (2020:73). Pilvipalvelujen soveltamisohje - Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille. http://urn.fi/URN:ISBN:978-952-367-503-2

Yleisiä tarkastusluetteloita ja kovennusohjeita

CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/. Viitattu 26.04.2022.
DISA Security Technical Implementation Guides (STIGs). https://public.cyber.mil/stigs/. Viitattu 26.04.2022.
NIST - National Checklist Program Repository. https://ncp.nist.gov/repository. Viitattu 26.04.2022.

Liitteet

Liite 1A: Julkri-kriteerit

1 Kriteeristön rakenne ja osa-alueet

Kriteerit on ryhmitelty viiteen **osa-alueeseen**. Jokaisella osa-alueella on yksilöivä osa-alueen nimi, johon perustuu myös osa-alueeseen kuuluvien kriteerien tunnisteen alkuosa. Kriteeristön osa-alueet ja niiden lyhenteet ovat:

- hallinnollinen turvallisuus (HAL),
- fyysinen turvallisuus (FYY),
- tekninen turvallisuus (TEK),
- varautuminen ja jatkuvuudenhallinta (VAR) sekä
- tietosuoja (TSU).

Osa-alue koostuu **pääkriteereistä** ja niitä täydentävistä **alikriteereistä**. Kriteerejä on yhteensä yli kaksi sataa. Pääkriteeri – alikriteeri rakennetta on hyödynnetty esimerkiksi sellaisissa tapauksissa, joissa samaan aihealueeseen liittyvät vaatimukset tiukentuvat siirryttäessä korkeammille turvallisuuden tasoille. Esimerkiksi salassa pidettäviä tietoja koskevaa pääkriteeriä voidaan täydentää TL IV luokkaan kuuluvia tietoja koskevan vaatimuksen toteutustapaa tarkentavalla alikriteerillä.

Kukin kriteeri on luokiteltu eri tasoille luottamuksellisuuden, eheyden, saatavuuden ja tietosuojan näkökulmista. Kriteeristä riippuen se voi liittyä yhteen tai useampaan näkökulmaan. Esimerkiksi sama käyttöoikeuksia koskeva kriteeri voi liittyä sekä luottamuksellisuuteen, eheyteen että tietosuojaan.

Kriteeristön eri osa-alueiden yleiskuvaukset sekä osa-alueeseen sisältyvät kriteerit on kuvattu seuraavissa luvuissa. Tietosuoja-osa-alueen yleiskuvaus ja kriteerit on liitteessä 1B Tietosuojakriteerit.

2 Hallinnollinen turvallisuus

Hallinnollisen turvallisuuden osa-alueessa käsitellään niitä menetelmiä, joilla tietoturvallisuuden hallinta jalkautetaan osaksi koko organisaation toimintaa. Osa-alue kattaa yleisiä hallinnollisen turvallisuuden, henkilöstöturvallisuuden, tietojärjestelmien ja niiden hankinnan sekä käyttöturvallisuuden kriteereitä. Hallinnollisen turvallisuuden kriteereillä pyritään siihen, että organisaatiolla on riittävän hyvin toimiva tietoturvallisuuden hallintajärjestelmä sekä menettelyt sen varmistamiseksi, että tietoja käsittelevä henkilöstö toimii asianmukaisesti. Organisaation tulee myös varmistaa, että tietojen käsittelyä koskevia velvoitteita noudatetaan tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta.

Monet hallinnollisen turvallisuuden osa-alueen kriteerit toimivat perustana muiden osa-alueiden kriteereille. Esimerkiksi suojattavien kohteiden tunnistamiseen, riskienhallintaan ja dokumentointiin liittyvät kriteerit ovat yleisiä, ja niitä tulee oletusarvoisesti hyödyntää muiden osa-alueiden kriteerien soveltamisen yhteydessä.

Hallinnolliseen turvallisuuteen liittyviä prosesseja tulee käsitellä kokonaisuuksina. Tietoturvallisuuden hallintamenettelyt tulee suhteuttaa riskienarvioinnin perusteella suojattavaan tietoon ja organisaation toimintaan.

Kriteeristön käyttö edellyttää tarkoituksenmukaista kohdentamista. Mikäli jotain toimintoja on arvioitu jo aiemmin, voidaan aiempia tuloksia hyödyntää soveltuvin osin. Esimerkiksi jos organisaation tietoliikenneympäristö on arvioitu viimeisen vuoden aikana, eikä siihen ole tehty merkittäviä muutoksia, voidaan tätä arviointia mahdollisesti hyödyntää tietoliikenneympäristöön asennettavan uuden tietojärjestelmän arvioinnissa.

Mikäli organisaatiossa käsitellään eri tasoille luokiteltuja tietoja erillisissä ympäristöissä ja prosesseissa, voi olla tarkoituksenmukaista jakaa arviointi erillisiin loogisiin kokonaisuuksiin. Esimerkiksi korkeammille tasoille turvallisuusluokiteltujen tietojen käsittely-ympäristön henkilöstön ohjeistuksen sisältö eroaa yleensä merkittävästi koko organisaatiota koskevista yleisistä ohjeistuksista.

Hyvään riskienhallintaan kuuluu menettelytapojen ja erityisesti riskien arvioinnin dokumentointi. Tietoturvallisuuden hallintaan liittyvät suunnitelmat ja ohjeet sekä arvioinnin tulokset ja johtopäätökset tulisi esittää kirjallisena. Dokumentteihin tulee täydentää tiedot toimenpiteiden toteutumisesta. Dokumentoinnilla tässä tarkoitetaan laajasti erilaisia kirjalliseen muotoon saatettavissa olevia tallenteita, kuten Intranet-sivuja ja toiminnanohjausjärjestelmän työmääräyksiä.

Tunniste	HAL-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Periaatteet
Vaatimus	Organisaatiolla on ylimmän johdon hyväksymät tietoturvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan sekä ovat tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset.
Yleiskuvaus	Ylimmän johdon hyväksymillä tietoturvallisuusperiaatteilla osoitetaan, että johto on sitoutunut organisaation tietoturvallisuusperiaatteisiin ja periaatteet edustavat johdon tahtotilaa sekä tukevat organisaation toimintaa. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina tai osana yleisiä toimintaperiaatteita, politiikkaa tai strategiaa.
Toteutusesimerkki	
Lainsäädäntö	TihL 4 § 2 mom, 13 §
Viitteet	Katakri: T-01
Muita lisätietoja	ISO/IEC 27002:2022 5.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01
Tunniste	**HAL-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Tehtävät ja vastuut
Vaatimus	Organisaatio on määritellyt ja dokumentoinut tietoturvallisuuden hoitamisen tehtävät ja vastuut sisältäen myös palveluntuottajille kuuluvat vastuut.
Yleiskuvaus	Tietoturvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa. Organisaation johdon tehtävänä on määritellä tiedonhallintaan liittyvät vastuut. Kysymys ei ole tiedonhallintavastuiden delegoinnista, vaan niiden määrittelystä. Vastuut tulisi määritellä erityisesti turvallisuusohjeiden ylläpidosta, riskienhallinnasta, varautumisesta sekä turvallisuuden kokonaisvastuussa olevista henkilöistä. Tietoturvallisuuden vastuualueet määritellään yleensä osana turvallisuuden kokonaisvastuuta. Vastuiden määrittelyssä tulee ottaa huomioon myös toimittajan vastuulla olevat tehtävät. Pilvipalveluita käytettäessä on huomioitava erilaiset palvelumallit sekä niihin liittyvät vastuujakojen erot asiakkaan ja palvelun tuottajan välillä.
Toteutusesimerkki	Organisaatio on määritellyt turvallisuuden toteuttamisen tehtävät ja niihin liittyvät vastuut seuraavilta osin: a) turvallisuusjohtaminen b) fyysinen turvallisuus c) tekninen turvallisuus d) varautuminen ja jatkuvuudenhallinta e) tietosuoja f) riskienhallinta g) turvallisuuden kokonaisvastuu
Lainsäädäntö	TihL 4 § 2 mom
Viitteet	Katakri: T-02
Muita lisätietoja	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, luku 3

Tunniste	HAL-02.1, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä
Nimi	Tehtävät ja vastuut - tehtävien eriyttäminen
Vaatimus	Organisaation on varmistettava, että henkilöillä ei ole tietoturvallisuuden kannalta vaarallisia työyhdistelmiä
Yleiskuvaus	Organisaation tehtävien ja vastuualueiden on oltava eriytettyjä, jotta vähennetään organisaation suojattavan omaisuuden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Tällaisia vaarallisia yhdistelmiä ovat esimerkiksi yksi henkilö pääsee muuttamaan sekä tietojärjestelmän tietoja että tietojärjestelmän seurannassa käytettäviä lokitietoja. Vaaralliset työyhdistelmät on huomioitava myös ulkoistetuissa toiminnoissa.
Toteutusesimerkki	- Organisaatio on määritellyt vaaralliset työyhdistelmät - Vaaralliset työyhdistelmät tarkastetaan osana tehtävien määrittelyjä - Vaaralliset työyhdistelmät tarkastetaan osana käyttöoikeuksien hallintaa erityisesti pääkäyttäjä- ja valvontaroolien kohdalla
Lainsäädäntö	TihL 4 § 2 mom, 13 §
Viitteet	Katakri: I-06
Muita lisätietoja	ISO/IEC 27002:2022 5.3
Tunniste	**HAL-03, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Resurssit
Vaatimus	Organisaatiolla on käytössään riittävät resurssit ja asiantuntemus tietoturvallisuuden varmistamiseksi.
Yleiskuvaus	Resursoinnilla ja asiantuntemuksella varmistetaan, että tietoturvallisuustyö voidaan toteuttaa määriteltyjen periaatteiden mukaisesti. Tietoturvallisuustyön resursseilla tarkoitetaan sekä henkilöresursseja että taloudellisia panostuksia, kuten tietojärjestelmäinvestointeja. Yleisinä vaatimuksina voidaan pitää, että organisaatiolla tulee olla henkilöitä tietoturvallisuuden hallinnan edellyttämiin tehtäviin ja että henkilöillä osaamista ja aikaa vaadittujen tehtävien suorittamiseen. Lisäksi organisaatiolla tulee olla kykyä ja halua tehdä sellaiset tietoturvallisuuteen liittyvät investoinnit, jotka tietoturvallisuusvaatimusten ja riskien arvioinnin perusteella on tunnistettu tarpeellisiksi.
Toteutusesimerkki	- Tietoturvallisuustehtäviä hoitavilla on riittävä asiantuntemus sekä näistä on näyttöjä. - Tietoturvallisuustyön resurssit, tehtävät, vastuut ja valtuudet on määritelty organisaation toimintaan, kokoon ja riskeihin nähden riittävän kattavasti. - Resurssit riittävät tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen. - Resurssien riittävyyttä arvioidaan säännöllisesti. - Organisaatio tekee tarvittavat päätökset tietoturvallisuuden edellyttämistä laite- ja muista investoinneista
Lainsäädäntö	TihL 4 § 2 mom
Viitteet	Katakri: T-05
Muita lisätietoja	SFS-EN ISO/IEC 27001:2017 7.1, 7.2, 5.1

Tunniste	HAL-04, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Suojattavat kohteet
Vaatimus	Organisaatio tunnistaa suojattavat kohteet sekä pitää niistä ajantasaista dokumentaatiota.
Yleiskuvaus	Suojattavien kohteiden luettelointi on yksi tietoturvallisuuden hallinnan perusvaatimuksista. Suojattavia kohteita ovat tiedot, tietojärjestelmät, tietojenkäsittelyprosessit, tilat sekä muut mahdollisesti organisaation tietoturvallisuuteen vaikuttavat kohteet. Nykyisissä tietojenkäsittely-ympäristöissä suojattavia kohteita voivat olla myös muut kuin perinteiset tietotekniset kohteet, kuten erilaiset sensori- ja analyysilaitteet sekä IoT- ja automaatioympäristöt. Suojattavien kohteiden luettelointi on välttämätön edellytys suunnitelmallisen ja vaikuttavan tietoturvallisuuden hallinnan toteuttamiseksi. Ajantasaista luetteloa suojattavasta omaisuudesta hyödynnetään lähtötietona monilla tietoturvallisuuden hallinnan osa-alueilla.
Toteutusesimerkki	
Lainsäädäntö	TihL 5 § 2 mom, 13 §
Viitteet	
Muita lisätietoja	ISO/IEC 27002:2022 5.9; Suositus tiedonhallintamallista 2020:29
Tunniste	**HAL-04.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Suojattavat kohteet - vastuut
Vaatimus	Organisaatio määrittelee suojattavien kohteiden vastuut.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 4 § 2 mom
Viitteet	
Muita lisätietoja	ISO/IEC 27002:2022 5.9; Suositus tiedonhallintamallista VM 2020:29
Tunniste	**HAL-04.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Suojattavat kohteet - luokittelu
Vaatimus	Organisaation on luokiteltava tiedot sekä niihin liittyvät järjestelmät ja käsittelyprosessit niihin kohdistuvien vaatimusten perusteella.

Yleiskuvaus	Organisaation tulee tunnistaa lainsäädännöstä käsittelemänsä julkiset, salassa pidettävät, turvallisuusluokitellut ja henkilötiedot sekä niiden suojaamisen tarpeet. Luokittelulla tarkoitetaan erilaisista käsittelyvaatimuksista johtuvaa tarvetta suojata tietoa eri tasoilla. Luokittelemalla tietojenkäsittely-ympäristöt tietoaineiston mukaisesti, pystytään helpommin osoittamaan ja perustelemaan kuhunkin tietojenkäsittely-ympäristöön liittyvät tietoturvallisuustoimenpiteet. Luokittelu olisi sisällytettävä organisaation prosesseihin ja sen olisi oltava johdonmukainen ja yhdenmukainen koko organisaatiossa. Luokittelu toimii lähtötietona useille muille tietoturvallisuuden prosesseille. Esimerkiksi järjestelmien saatavuusvaatimukset liittyvät järjestelmien vikasietoisuuden ja varautumisen suunnitteluun ja luottamuksellisuusvaatimukset järjestelmien tietoturvallisuusvaatimusten määrittelyyn. Tietojärjestelmän tai muun useita tietoaineistoja sisältävän kohteen luokitus määräytyy ensi sijassa korkeimman luokituksen aineiston mukaan. Tietojärjestelmien luokitusta arvioitaessa tulee huomioida myös kasautumisvaikutus riskilähtöisesti. Suuresta määrästä tietyn luottamuksellisuuden tason tietoa koostuvissa tietojärjestelmissä asiakokonaisuus voi nousta luokitukseltaan yksittäistä tietoa korkeammalle tasolle. Määrä ei ole kuitenkaan ainoa tekijä, vaan joskus esimerkiksi kahden eri tietolähteen yhdistäminen voi johtaa tietovarannon luokituksen nousemiseen. Tyypillisesti kasautumisessa on kysymys IV-luokan tiedosta (esimerkiksi suuri määrä turvallisuusluokan IV tietoa voi muodostaa yhdistettynä turvallisuusluokan III tietovarannon).
Toteutusesimerkki	- Organisaatio määrittelee tietojen sekä niihin liittyvien tietojärjestelmien ja käsittelyprosessien luokittelussa käytettävät tasot luottamuksellisuuden, saatavuuden ja eheyden sekä näkökulmista. Tarvittaessa luokittelua voidaan laajentaa kattamaan myös muita näkökulmia kuten esimerkiksi sisältääkö tiedot henkilötietoja. - Organisaatio määrittelee kriteerit, joiden mukaan tiedot ja muut kohteet luokitellaan eri luokkiin. - Luokat ja niihin liittyvät kriteerit perustuvat lakisääteisiin vaatimuksiin, mutta organisaatioiden tulee täsmentää kriteerit siten, että ne ovat tarkoituksenmukaisia organisaatiossa työskenteleville henkilöille. - Luokittelu voidaan tehdä suojattavien kohteiden luetteloinnin yhteydessä ja sisällyttää luetteloon suojattavista tiedoista - esimerkiksi tiedonhallintamalliin.
Lainsäädäntö	TihL 4 § 2 mom, 5 §, 13 §, 18 §; TLA 3 §, 4 §; JulkL 24 §
Viitteet	Katakri: T-08
Muita lisätietoja	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65, luku 4.1; Suositus turvallisuusluokiteltavienasiakirjojen käsittelystä 2021:5 luku 2, luku 5.3; ISO/IEC 27002:2022 5.9
Tunniste	**HAL-04.3, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Suojattavat kohteet - kasautumisvaikutus
Vaatimus	Kasautumisvaikutus on huomioitu suojattavien kohteiden luokittelussa.
Yleiskuvaus	Tietojärjestelmän tai muun useita tietoaineistoja sisältävän kohteen luokitus määräytyy ensi sijassa korkeimman luokituksen aineiston mukaan. Tietojärjestelmien luokitusta arvioitaessa tulee huomioida myös kasautumisvaikutus riskilähtöisesti. Suuresta määrästä tietyn luottamuksellisuuden tason tietoa koostuvissa tietojärjestelmissä asiakokonaisuus voi nousta luokitukseltaan yksittäistä tietoa korkeammalle tasolle. Määrä ei ole kuitenkaan ainoa tekijä, vaan joskus esimerkiksi kahden eri tietolähteen yhdistäminen voi johtaa tietovarannon luokituksen nousemiseen. Tyypillisesti kasautumisessa on kysymys IV-luokan tiedosta (esimerkiksi suuri määrä turvallisuusluokan IV tietoa voi muodostaa yhdistettynä turvallisuusluokan III tietovarannon), mutta kasautumisvaikutus tulee huomioida myös turvallisuusluokittelemattoman salassa pidettävän tiedon suojaamisessa.
Toteutusesimerkki	
Lainsäädäntö	TihL 5 § 2 mom, 13 § 1 mom
Viitteet	Julkri: HAL-06, TEK-06; Katakri: T-08
Muita lisätietoja	

Tunniste	HAL-04.4, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Suojattavat kohteet - merkitseminen
Vaatimus	Organisaation on merkittävä tiedot lakisääteisten vaatimusten sekä organisaation määrittelemien luokitteluperiaatteiden mukaisesti.
Yleiskuvaus	Tiedon merkitsemistapojen pitää kattaa sekä fyysisessä että sähköisessä muodossa olevat tiedot ja niihin liittyvä suojattava omaisuus kuten tietovälineet. Merkintöjen olisi oltava organisaation määrittelemien luokitteluperiaatteiden mukaisia ja helposti tunnistettavia. Organisaation olisi ohjeistettava, mihin ja miten merkinnät kiinnitetään. Ohjeistuksessa tulee ottaa huomioon myös tulosteet. Lisäksi tarpeettoman työn säästämiseksi kannattaa ohjeistaa, milloin merkintöjä ei tarvita. Tietyissä tapauksissa, kuten esimerkiksi julkisuuslain mukaisista salassa pitoa koskevista merkinnöistä tulee myös käydä ilmi, miltä osin asiakirja on salassa pidettävä sekä mihin salassapito perustuu.
Toteutusesimerkki	
Lainsäädäntö	TihL 18 §; TLA 3 §, 4 §; JulkL 25 §
Viitteet	Katakri: T-08
Muita lisätietoja	Suositus turvallisuusluokiteltavienasiakirjojen käsittelystä 2021:5 luku 3; ISO/IEC 27002:2022 5.13
Tunniste	**HAL-04.5, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Suojattavat kohteet - riippuvuudet
Vaatimus	Organisaatio on tunnistanut ja dokumentoinut suojattavien kohteiden väliset riippuvuudet.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 5 §
Viitteet	
Muita lisätietoja	
Tunniste	**HAL-04.6, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Suojattavat kohteet - sidosryhmät
Vaatimus	Organisaatio on tunnistanut ja dokumentoinut suojattaviin kohteisiin liittyvät sidosryhmät.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 5 §
Viitteet	
Muita lisätietoja	

Tunniste	HAL-05, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Vaatimukset
Vaatimus	Organisaatio tunnistaa lainsäädännöstä, sidosryhmistä sekä organisaation toiminnasta johtuvat tietoturvavaatimukset.
Yleiskuvaus	Organisaation tulee tunnistaa ja yksilöidä lainsäädännöstä, eri sidosryhmien kanssa laadituista sopimuksista sekä organisaation toiminnasta johtuvat tietoturvallisuutta koskevat vaatimukset. Lisäksi organisaation tulee tunnistaa ja ottaa huomioon toimialakohtaisesta lainsäädännöstä sekä kansainvälisestä lainsäädännöstä ja EU-sääntelystä johtuvat vaatimukset. Julkisessa hallinnossa noudatettavat tiedonhallintalakiin perustuvat tietoturvallisuuden vähimmäisvaatimukset, ja niiden noudattamisesta annetut suositukset on määritelty tiedonhallintalautakunnan suosituksen 2021:65 luvussa 2. Organisaation tietoturvallisuusvaatimukset muodostuvat edellä mainituista vähimmäisvaatimuksista sekä muista tunnistetuista vaatimuksista. Kunkin vaatimuksen toteuttamisen menettely arvioidaan riskiarviointiprosessin avulla.
Toteutusesimerkki	
Lainsäädäntö	TihL 13 §
Viitteet	
Muita lisätietoja	SFS-EN ISO/IEC 27001:2017 4.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luvut 2 ja 4

Tunniste	HAL-05.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Vaatimukset - seuranta
Vaatimus	Organisaatio seuraa asetettujen tietoturvallisuusvaatimusten ja toimintaympäristön muutoksia ja tekee tarvittavat toimenpiteet niihin reagoimiseksi.
Yleiskuvaus	Lainsäädäntö, sopimusvaatimukset sekä muuttuvat tietoturvallisuusuhat edellyttävät säännöllistä vaatimusten ja uhkien seurantaa ja muutoksiin reagoimista.
Toteutusesimerkki	
Lainsäädäntö	TihL 4 § 2 mom, 13 § 1 mom
Viitteet	
Muita lisätietoja	SFS-EN ISO/IEC 27001:2017 9.1; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 4.1

Tunniste	HAL-05.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Vaatimukset - muutosvaikutukset
Vaatimus	Organisaatio arvioi olennaisten hallinnollisten uudistusten ja tietojärjestelmien käyttöönottojen muutosvaikutukset suhteessa tietoturvallisuusvaatimuksiin ja -toimenpiteisiin.
Yleiskuvaus	Olennaisten muutosten yhteydessä organisaatioilta edellytetään muutosvaikutusten arviointia. Osana muutosvaikutusten arviointia on arvioitava muutosten vaikutukset suhteessa tietoturvallisuusvaatimuksiin ja -toimenpiteisiin.
Toteutusesimerkki	
Lainsäädäntö	TihL 5 §
Viitteet	
Muita lisätietoja	Suositus tiedonhallinnan muutosvaikutusten arvioinnista 2020:53; ISO/IEC 27002:2022 5.31

Tunniste	HAL-06, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Riskienhallinta
Vaatimus	Organisaatio toteuttaa tietoturvallisuusriskien hallintaa ja on arvioinut olennaiset tietoihin kohdistuvat riskit sekä mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.
Yleiskuvaus	Tietoturvallisuusriskien hallintaprosessi koostuu toimintaympäristön määrittämisestä, riskien arvioinnista (tunnistaminen, analysointi, merkityksen arviointi), riskien käsittelystä, riskien hyväksynnästä, riskejä koskevasta viestinnästä ja tiedonvaihdosta sekä riskien seurannasta ja katselmoinnista. Tietoturvallisuusriskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa. Tietoturvallisuusriskien hallinnan avulla varmistetaan tietoturvallisuustoimenpiteiden riittävyys tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi. Riskienhallinta vaikuttaa muihin tietoturvallisuuden hallinnan eri osa-alueisiin. Riskienhallinta tulee suunnitella ja ohjeistaa siten, että siinä käsitellään systemaattisesti ja suunnitelmallisesti erilaisia tietoturvallisuuteen liittyviä riskejä kuten tietosisällön virheellisyyksistä johtuvia riskejä, organisaation toiminnan keskeytyksiin liittyviä riskejä sekä henkilötietojen tietoturvaloukkauksiin liittyviä riskejä.
Toteutusesimerkki	- Tietoturvallisuusriskien arvioinnissa ja analysoinnissa käytetään yleisesti hyväksyttyä menetelmää. - Tietoturvallisuusriskien arvioinneista laaditaan aikataulutettu ja vastuutettu vuosisuunnitelma - Tietoturvallisuusriskien hallintaan osallistuu riittävästi asiantuntijoita. - Tietoturvallisuusriskien hallinnassa on otettu huomioon sidosryhmistä ja toimitusketjuista aiheutuvat riskit. - Tietoturvallisuusriskien arviointia hyödynnetään muissa tietoturvallisuuden hallinnan prosesseissa.
Lainsäädäntö	TihL 13 § 1 mom; TLA 6 §, 7 §
Viitteet	Julkri: FYY-01, TEK-01, TEK-14, TEK-16; Katakri: T-03
Muita lisätietoja	SFS-EN ISO/IEC 27001:2017 6.1 ja 8–10; SFS-EN ISO/IEC 27005:2018 luku 6; SFS ISO 31000:2018; PiTuKri TJ-03; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 5.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6

Tunniste	HAL-06.1, L:Salassa pidettävä, E:, S:, TS:Henkilötieto
Nimi	Riskienhallinta - lainsäädäntöjohdannaiset riskit
Vaatimus	Palveluun liittyvät lainsäädäntöjohdannaiset riskit on tunnistettu, arvioitu ja niistä on huolehdittu.
Yleiskuvaus	Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa palveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy palvelun asiakkaiden salassa pidettäviin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin sekä muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimusoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia. Organisaation tulee varmistaa, että lainsäädäntöjohdannaiset riskit eivät rajoita palvelun soveltuvuutta sen käyttötarkoitukseen. Lainsäädäntöjohdannaisten riskien arvioinnissa on otettu huomioon koko palvelun tuottamisessa käytetty toimitusketju, ja niiden valtioiden säännökset, joiden mukaisesti palvelua tuotetaan sekä riski tietojen oikeudettomasta paljastumisesta näiden valtioiden viranomaisille. Suosituksen turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa (VM 2022:4) mukaisesti suositeltavaa on, että pilvipalveluihin liittyvien riskien hallitsemiseksi turvallisuusluokiteltujen tietoaineistojen käsittelyssä käytetään ainoastaan viranomaisten luotettaviksi arvioimia pilvipalveluita ja tarjoajia. Jos turvallisuusluokiteltuja tietoaineistoja käsitellään kansainvälisissä pilvipalveluissa, suosituksena on lisäksi, että käsiteltävät turvallisuusluokitellut tietoaineistot rajataan ja valitaan käyttötapausten ja niihin liittyvien viranomaisprosessien perusteella tarkasti ja siten, että ne ovat luovutettavissa valtioihin, joiden lainkäyttövaltaan pilvipalvelujen tarjoaja ja sen alihankkijat kuuluvat.

Toteutusesimerkki	Riskienarvioinnin tulisi kattaa lainsäädäntöjohdannaiset riskit vähintään seuraavien tekijöiden osalta: a) Palvelussa käsiteltävän tiedon fyysinen sijainti koko tiedon elinkaaren ajalta, kattaen myös mahdolliset alihankinta- ja ulkoistusketjut. b) Palvelun eri toimintojen (esimerkiksi ylläpito- ja hallintaratkaisut, varmistukset) ja komponenttien fyysinen sijainti koko tiedon elinkaaren ajalta. c) Mahdolliset muut palvelun tuottamiseen osallistuvat tahot, esimerkiksi mahdolliset alihankinta- ja ulkoistusketjut. d) Palvelun käyttöön ja palvelussa käsiteltäviin tietoihin sovellettava lainsäädäntö ja oikeuspaikka. e) Toimijat, joilla voi sovellettavasta lainsäädännöstä johtuen olla pääsy palvelussa käsiteltäviin tietoihin. Lainsäädäntöjohdannaisten riskien arvioimiseksi palvelun toimittajalta tulee edellyttää kuvauksia kyseisessä palvelussa käsiteltäviin tietoihin kohdistuvista lainsäädäntöjohdannaisista riskeistä. Kuvausten on oltava sellaisia, että niiden perusteella pystytään luotettavasti arvioimaan kyseisen palvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Kuvausten tulee kattaa palvelun käytön ja palvelussa käsiteltävien tietojen koko elinkaaren, huomioiden myös edellä mainittujen alakohtien a-e sisällön. Arvioinnissa suositellaan noudatettavan PiTuKrissa kuvattuja (EE-02 / Taulukko 2) jatkoarvioinnin yleisperiaatteita. Turvallisuusluokittelemattomien salassa pidettävien tietojen suojaamisessa on huomioitavaa, että tällaisten tietojen suojaamisessa voidaan hyväksyä turvallisuusluokiteltuun tietoon nähden laajemmin lainsäädäntöjohdannaisia riskejä.
Lainsäädäntö	TihL 13 § 1 mom; TLA 6 §, 7 §
Viitteet	Julkri: FYY-01, TEK-01, TEK-14, TEK-16, TSU-18; Katakri: T-03
Muita lisätietoja	SFS-EN ISO/IEC 27001:2017 6.1 ja 8–10; SFS-EN ISO/IEC 27005:2018 luku 6; SFS ISO 31000:2018; PiTuKri TJ-03 ja EE-02; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 5.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6
Tunniste	**HAL-07, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Seuranta ja valvonta
Vaatimus	Organisaatiossa on järjestetty seuranta ja valvonta tietoturvallisuuteen liittyvien prosessien toimivuudesta ja vaatimusten täyttymisestä.
Yleiskuvaus	Organisaation on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedon elinkaari alkaa tiedon tuottamis- tai vastaanottovaiheessa ja päättyy tiedon pysyvään säilyttämiseen arkistossa tai tiedon tuhoamiseen. Tiedon elinkaari kattaa kaikki tiedon käsittelyn vaiheet, jotka ovat tiedon tuottaminen tai vastaanotto, säilytys, käyttö, jakaminen, siirto ja arkistointi tai tuhoaminen. Tietoturvallisuuden seurannan mittareina voidaan käyttää sekä hallintakeinojen suorituskykyyn että vaikuttavuuteen perustuvia mittareita, jotka voivat olla numeerisia tai laadullisia. Seurannan perustana ovat havaitut poikkeamat, joiden pohjalta laaditaan ehdotuksia tietoturvallisuuden kehittämiseksi. Mittarit voivat olla esimerkiksi numeerisia raja-arvoja (esim. palveluiden saatavuus vähintään 99 %) tai vaatimustenmukaisuuden todentamista (esim. vuosikellon mukaiset arvioinnit ja katselmoinnit on hoidettu suunnitellusti).

Toteutusesimerkki	Paljon salassa pidettäviä tietoja käsittelevä organisaation on määritellyt esimerkiksi: a) mitä täytyy seurata ja mitata, b) millä seuranta-, mittaus-, analysointi- tai arviointimenetelmillä varmistetaan kelvolliset tulokset c) milloin seuranta ja mittaus on toteutettava d) ketkä toteuttavat seurannan ja mittaamisen e) milloin seurannan ja mittauksen tuloksia on analysoitava ja arvioitava f) ketkä analysoivat ja arvioivat saadut tulokset
Lainsäädäntö	TihL 4 § 2 mom, 13 § 1 mom
Viitteet	Katakri: T-01, I-19
Muita lisätietoja	SFS-EN ISO/IEC 27001:2017 9.1; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 7
Tunniste	**HAL-07.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Seuranta ja valvonta - tietojen käyttö ja luovutukset
Vaatimus	Organisaatio on tunnistanut lokitietojen keräämiseen liittyvät vaatimukset ja varmistanut niiden perusteella lokitietojen keräämisen ja seurannan riittävyyden.
Yleiskuvaus	Lokitiedot ovat yksi keskeisimmistä keinoista tietojen käytön ja luovutusten seurantaan. Tiedonhallintalain mukaan lokitiedot tulee kerätä, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lisäksi tietosuoja-asetuksen osoitusvelvollisuus henkilötietojen käsittelyn turvallisuudesta edellyttää usein käytännössä lokitietojen keruuta ja seurantaa. Lokitiedot tulee kerätä tietojärjestelmän käytöstä ja tietojen luovutuksista, mutta tietojen kerääminen on sidottu tarpeellisuuteen. Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, tulee luovuttavassa järjestelmässä kerätä luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen perusteensa. Lisäksi käyttölokitiedot tulee kerätä ainakin tietojärjestelmistä, joissa käsitellään henkilötietoja tai salassa pidettäviä tietoja.
Toteutusesimerkki	Paljon salassa pidettäviä tietoja käsittelevä organisaatio voi toteuttaa esimerkiksi seuraavat toimenpiteet: - Organisaatio määrittelee osana palvelujen ja tietojärjestelmien hankintaa niihin liittyvät lokitietojen keruun vaatimukset ja varmistaa niiden täyttymisen. - Organisaatio määrittelee tietojärjestelmittäin tietojen käytön ja luovutusten seurannan tarpeet ja menettelyt. - Seurannan menettelyitä arvioidaan määräajoin. - Organisaatio määrittelee lokitietojen säilyttämiseen, hävittämiseen ja suojaamiseen liittyvät vastuut ja varmistaa niiden täyttymisen. - Mikäli lokitietojen käyttö on laaja-alaista, organisaatio voi harkita keskitettyyn lokitietojen hallintaan (SIEM) siirtymistä.
Lainsäädäntö	TihL 17 §
Viitteet	Katakri: I-10
Muita lisätietoja	Kyberturvallisuuskeskus, Näin keräät ja käytät lokitietoja; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65, luku 14; ISO/IEC 27002:2022 5.31, 8.15

Tunniste	HAL-08, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Häiriöiden hallinta
Vaatimus	Organisaatiolla on tietoturvallisuushäiriöiden ja poikkeamatilanteiden käsittelyyn määritellyt prosessit ja ohjeet.
Yleiskuvaus	Tietoturvallisuushäiriöiden hallinnalla pyritään varmistamaan, että organisaatio kykenee toimimaan tehokkaasti ei-toivotuissa, odottamattomissa tilanteissa, minimoiden vahingot ja palauttaen tilanteen normaaliksi sekä varmistamaan, ettei samankaltainen häiriö ole mahdollinen muualla organisaatiossa. Organisaatiolla tulee olla häiriöiden käsittelyprosessi, joka ottaa kantaa vähintään tilanteen vakavuuden määrittelemiseen, lisävahinkojen estämiseen, todisteiden keräämiseen, tilanteen selvittämiseen, tilanteesta viestimiseen, korjaavien toimenpiteiden toteuttamiseen ja tilanteesta oppimiseen. Käsittelyprosessissa tulee ottaa huomioon palvelun aikakriittisyys ja sitä suunniteltaessa tulee arvioida tarpeet virka-ajan ulkopuolella tapahtuvien häiriöiden hallinnalle. Organisaatiossa on myös selvitetty, mitkä kansalliset ja kansainväliset säädökset tai organisaation tekemät sopimukset edellyttävät tietoturvapoikkeamista tai niiden epäilystä ilmoittamista viranomaisille. Ilmoittamisen kriteerit, vastuut, yhteystiedot sekä tiedottamisen määräajat on määritetty ja dokumentoitu.
Toteutusesimerkki	Tietoturvallisuushäiriöiden hallinta on - suunniteltu ottaen huomioon koko palveluketju sekä virka-ajan ulkopuolella tapahtuvat häiriöt, - ohjeistettu ja koulutettu, - dokumentoitu riittävällä tasolla, - harjoiteltu, sekä - viestintäkäytännöt ja vastuut on sovittu
Lainsäädäntö	TihL 4 § 2 mom ja 13 §; TLA 7 §
Viitteet	Katakri: T-07
Muita lisätietoja	ISO/IEC 27002:2022 5.24; PiTuKri TJ-04
Tunniste	**HAL-09, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Dokumentointi
Vaatimus	Tietoturvallisuuteen liittyvät politiikat, prosessit, ohjeet ja prosessien toteuttamisessa syntyvät tulokset on dokumentoitu.
Yleiskuvaus	
Toteutusesimerkki	- Organisaatio on määritellyt tietoturvallisuuden hallinnan edellyttämät sekä tietoturvallisuuden hallinnan eri prosesseissa syntyvät dokumentit. - Dokumentaatiolle on määritelty ylläpito- ja jakeluprosessit - Dokumentaation oikeudet ja suojaukset on määritelty
Lainsäädäntö	TihL 5 §, 6 §, 13 § 1 mom
Viitteet	Katakri: T-01
Muita lisätietoja	ISO/IEC 27002:2022 5.37

Tunniste	HAL-09.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Dokumentointi - ajantasaisuus
Vaatimus	Tietoturvallisuuteen liittyvä dokumentaatio on ajantasaista.
Yleiskuvaus	
Toteutusesimerkki	- Organisaatiolla on prosessi, jonka avulla seurataan dokumentaation kattavuutta ja ajantasaisuutta - Dokumentaation puutteisiin reagoidaan
Lainsäädäntö	TihL 5 §, 6 §, 13 § 1 mom
Viitteet	
Muita lisätietoja	ISO/IEC 27002:2022 5.37

Tunniste	HAL-10, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Henkilöstön luotettavuuden arviointi
Vaatimus	Organisaatio tunnistaa ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta.
Yleiskuvaus	Erityistä luotettavuutta edellyttäviä tehtäviä voidaan tunnistaa esimerkiksi määrittämällä tilanteet, joissa henkilö käsittelee turvallisuusluokiteltavia tai merkittävässä määrin ja säännöllisesti salassa pidettäviä tietoja tai työskentelee tiloissa, joissa henkilön tietoon voi tulla muutoin kuin satunnaisesti turvallisuusluokiteltavia tai salassa pidettäviä tietoja.
Toteutusesimerkki	- Organisaatio laatii kuvauksen sellaisista tietoaineistojen käsittelyyn liittyvistä tehtävistä, jotka edellyttävät erityistä luotettavuutta. - Näihin tehtäviin nimettävistä henkilöistä haetaan turvallisuusselvitys, mikäli tähän on turvallisuusselvityslain mukaan peruste. - Lisäksi tiedonhallintayksikkö ylläpitää luetteloa näistä tehtävistä.
Lainsäädäntö	TihL 12 §;
Viitteet	Katakri: T-10
Muita lisätietoja	Turvallisuusselvityslaki 726/2014; ISO/IEC 27002:2022 6.1

Tunniste	HAL-10.1, L:Salassa pidettävä, E:Kriittinen, S:Kriittinen, TS:Erityinen henkilötietoryhmä
Nimi	Henkilöstön luotettavuuden arviointi - turvallisuusselvitys
Vaatimus	Organisaatio arvioi turvallisuusselvityksen tarpeen ja mikäli sellaista edellytetään, myöntää henkilöille pääsyn suojattaviin kohteisiin vasta turvallisuusselvityksen jälkeen.
Yleiskuvaus	Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014). Henkilöturvallisuusselvitys voidaan tehdä ihmisestä, joka työssään pääsee esimerkiksi turvallisuuden kannalta tärkeään tilaan tai käsittelee salassa pidettävää tietoa. Turvallisuusselvityksen laajuus riippuu ihmisen työtehtävästä ja tarvittavista oikeuksista esimerkiksi salassa pidettävän tiedon käsittelyyn. Selvityksen laajuus ratkaisee, mitä tietolähteitä selvityksen tekemisessä käytetään. Henkilöä itseään voidaan tarvittaessa haastatella. Turvallisuusselvityksen hakee useimmiten työnantaja ja työntekijä täyttää aluksi turvallisuusselvitykseen liittyvät lomakkeet.
Toteutusesimerkki	- Rekrytointien, tehtävämuutosten sekä ulkoisten palveluhankintojen yhteydessä tarkastetaan, edellyttääkö tehtävä turvallisuusselvitystä, - tarvittaessa organisaatio on määritellyt turvallisuusselvitysten hakemiseen prosessin
Lainsäädäntö	TihL 12 §; TLA 9 §
Viitteet	Katakri: T-10
Muita lisätietoja	Valtion virkamieslaki 750/1994 8 c §
Tunniste	**HAL-11, L:Salassa pidettävä, E:, S:, TS:Henkilötieto**
Nimi	Salassapito- ja vaitiolovelvollisuus
Vaatimus	Tietoa käsitteleville henkilöille on selvitetty tietojen suojaamista ja asiakirjojen käsittelyä koskevat tietoturvallisuusperiaatteet ja -toimenpiteet.
Yleiskuvaus	
Toteutusesimerkki	- Henkilölle selvitetään tietojen suojaamista koskevat periaatteet ennen pääsyä tietoihin, - todisteeksi selvityksen saamisesta henkilö voi allekirjoittaa kirjallisen vaitiolositoumuksen ja allekirjoitus luetteloidaan ”vaitiolositoumusluetteloon” tai - sitoumuksen antamiseen on sähköinen menettely, joka hoidetaan automaattisesti ensimmäisen sisäänkirjautumisen yhteydessä
Lainsäädäntö	TihL 4 § 2 mom; TLA 6 §, 8 §; JulkL 25 §, 26 § 3 mom
Viitteet	Katakri: T-11
Muita lisätietoja	ISO/IEC 27002:2022 6.6; PiTuKri HT-03

Tunniste	HAL-12, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Ohjeet
Vaatimus	Organisaatiossa on ajantasaiset ja kattavat ohjeet tietoturvallisuuden varmistamiseksi.
Yleiskuvaus	Ohjeistamalla tietoturvallisuuden kannalta keskeiset asiat pyritään varmistumaan siitä, että toiminta ei ole henkilöriippuvaista. Organisaatiolla tulisi olla ajantasaiset ohjeet tietojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta sekä tietoturvallisuustoimenpiteistä. Ohjeet kattavat tietoihin liittyvät prosessit ja käsittely-ympäristöt tietojen koko elinkaaren ajalta.
Toteutusesimerkki	- Tietojen suojaamiseksi ja tietoturvallisuuden varmistamiseksi tarvittavat menettelyt ja ohjeet on dokumentoitu. - Turvallisuusohjeistus toteutetaan henkilöstön työtehtävien tarpeet huomioiden. - Turvallisuusohjeiden kattavuutta ja ajantasaisuutta seurataan säännöllisesti ja se on tarvittavien tahojen saatavilla.
Lainsäädäntö	TihL 4 § 2 mom, 13 § 1 mom; TLA 6 § ja 8 §
Viitteet	Julkri: TEK-17.2; Katakri: T-04
Muita lisätietoja	ISO/IEC 27002:2022 5.37; SFS-EN ISO/IEC 27001:2017 7.5; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 4

Tunniste	HAL-13, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Koulutukset
Vaatimus	Organisaatio varmistaa perehdytyksillä, koulutuksilla ja viestinnällä, että henkilöstöllä ja organisaation lukuun toimivilla on tuntemus voimassa olevista tietoturvallisuutta koskevista määräyksistä ja ohjeista.
Yleiskuvaus	Johdon on huolehdittava siitä, että organisaatiossa on tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja organisaation lukuun toimivilla on tuntemus voimassa olevista tietoturvallisuutta, tiedonhallintaa, tietojenkäsittelyä sekä tietojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja organisaation ohjeista sekä organisaation vastuulla oleviin tietoihin kohdistuvista riskeistä ja uhista. Erityisesti koulutuksissa on huomioitava etäkäyttöön, tietojärjestelmien hallinnointiin sekä muihin korkeamman riskin käsittelytilanteisiin liittyvät uhat ja ohjeet.
Toteutusesimerkki	- Tietoja käsittelevälle henkilölle on selvitetty tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt. - Koulutus toteutetaan henkilöstön työtehtävien tarpeet huomioiden. - Koulutuksen sisältö dokumentoidaan - Koulutuksiin osallistuneista pidetään kirjaa
Lainsäädäntö	TihL 4 § 2 mom; TLA 6 §, 8 §
Viitteet	Katakri: T-12
Muita lisätietoja	ISO/IEC 27002:2022 6.3; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 5

Tunniste	HAL-14, L:Julkinen, E:Vähäinen, S:, TS:Henkilötieto
Nimi	Käyttö- ja käsittelyoikeudet
Vaatimus	Organisaatio varmistaa, että tietojärjestelmien käyttöoikeudet ja tietojen käsittelyoikeudet määritellään tehtäviin liittyvien tarpeiden mukaan sekä pidetään ajantasaisina.
Yleiskuvaus	Käyttö- ja käsittelyoikeuksien hallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään niiden luvatonta käyttöä. Käyttäjälle annetaan tietojärjestelmiin vain sellaiset käyttöoikeudet ja -valtuudet, jotka ovat työtehtävien kannalta tarpeellisia. Käsittelyoikeus tietoihin voidaan antaa vain sille, jolla työtehtäviensä vuoksi on tarve saada tietoja tai muutoin käsitellä niitä, jolle on selvitetty tietojen suojaamista koskevat ohjeet ja joka tuntee tietojen käsittelyä koskevat velvoitteet.
Toteutusesimerkki	- Organisaatio on määritellyt periaatteet, joiden mukaan käyttö- ja käsittelyoikeudet myönnetään - Oikeuksien hyväksymiseen on määritelty vastuut ja menettelyt - Oikeuksien toteuttamiseen on määritelty vastuut ja menettelyt - Käyttöoikeuksien myöntäminen on dokumentoitu siten, että se on tarkastettavissa jälkikäteen
Lainsäädäntö	TihL 4 § 2 mom ja 16 §; TLA 8 §, 11 § 1 mom 3 k
Viitteet	Katakri: T-13, I-6
Muita lisätietoja	ISO/IEC 27002:2022 5.15, 5.18; PiTuKri HT-05; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65, luku 13; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5, luku 7.6
Tunniste	**HAL-14.1, L:TL III, E:, S:, TS:**
Nimi	Käyttö- ja käsittelyoikeudet - ajantasainen luettelo
Vaatimus	Organisaatio varmistaa, että sillä on ajantasaiset luettelot henkilöiden käyttö- ja käsittelyoikeuksista.
Yleiskuvaus	Valtionhallinnon viranomaisen on pidettävä luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan I, II tai III asiakirjoja. Luettelossa on mainittava henkilön tehtävä, johon turvallisuusluokitellun tiedon käsittelytarve perustuu.
Toteutusesimerkki	
Lainsäädäntö	TLA 8 §
Viitteet	Katakri: T-13
Muita lisätietoja	ISO/IEC 27002:2022 5.18; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 4.1
Tunniste	**HAL-14.2, L:Salassa pidettävä, E:Kriittinen, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Käyttö- ja käsittelyoikeudet - päättyminen
Vaatimus	Organisaatio varmistaa, että se, joka ei enää toimi tehtävissä, joihin oikeus tietojen käsittelyyn perustuu, palauttaa tiedot tai tuhoaa ne asianmukaisella tavalla.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom, 21 § 2 mom; TLA 8 §
Viitteet	Katakri: T-13
Muita lisätietoja	ISO/IEC 27002:2022 5.18; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 4.1

Tunniste	HAL-15, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Työskentelyn tietoturvallisuus koko palvelussuhteen ajan
Vaatimus	Organisaatio huolehtii työskentelyn tietoturvallisuudesta koko palvelussuhteen ajan.
Yleiskuvaus	Erityisesti tulee huomioida toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja palvelussuhteen päättyessä. Menettelyjä palvelussuhteen alussa ja aikana ovat esimerkiksi henkilöturvallisuusselvitykset, käsittely-, käyttö- ja pääsyoikeudet, ymmärrys salassapito- ja vaitiolovelvollisuudesta, turvallisuuskoulutus sekä muutoksissa näiden mahdollinen päivittäminen ja muutosten kouluttaminen. Palvelussuhteen päättymiseen liittyviä menettelyjä ovat esimerkiksi avainten, tunnusten sekä aineistojen ja materiaalien luovutus, sekä käsittely-, käyttö- ja pääsyoikeuksien poistaminen. Palvelussuhteen päättyessä on myös oleellista muistuttaa salassapito- ja vaitiolovelvollisuudesta.
Toteutusesimerkki	Toimenpiteet edellyttävät tyypillisesti menettelyohjeita, jotka on koulutettu ja saatavilla tarvittavilla henkilöstöryhmillä. Menettelyohjeet voidaan jakaa esimerkiksi palvelussuhteen elinkaaren mukaisiin kokonaisuuksiin. Ohjekokonaisuuksia voivat olla esimerkiksi rekrytointiohjeet, perehdyttämisohjeet, palvelussuhteen aikaisten muutosten ohjeet, palvelussuhteen päättymisen ohjeet ja ohjeet yksityiskohtaisempiin toimiin kuten esimerkiksi ohjeet käsittely-, käyttö- ja pääsyoikeuksien muutoksiin.
Lainsäädäntö	TihL 4 § 2 mom, 12 §, 16 §; TLA 6 §, 8 §
Viitteet	Katakri: T-09
Muita lisätietoja	ISO/IEC 27002:2022 6.1, 6.2, 6.3, 6.5; PiTuKri HT-01,Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 5; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5

Tunniste	HAL-16, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Hankintojen turvallisuus
Vaatimus	Organisaatio varmistaa jo ennakolta, että hankittavat tietojärjestelmät ja palvelut ovat tietoturvallisia sekä varmistaa niiden turvallisuuden muutostilanteissa koko järjestelmän elinkaaren ajan.
Yleiskuvaus	Hankinnoissa on varmistettava, että hankittavat tietojärjestelmät ja palvelut täyttävät käsiteltävien tietoaineistojen mukaiset tietoturvallisuusvaatimukset ja että tietojärjestelmät ovat soveltuvia viranomaisen tehtävien hoitamiseksi tuloksekkaasti ja tehokkaasti. Ennen hankintapäätöstä on suositeltavaa kartoittaa vaihtoehtoja ja karsia vaihtoehdoista jo varhaisessa vaiheessa sellaiset, jotka eivät pysty täyttämään lainsäädännön asettamia vähimmäisvaatimuksia. Eräs menetelmä tällaisen esikarsinnan tekemiseen on palveluntarjoajaehdokkaiden tuottamiin kuvauksiin tutustuminen ja niiden pohjalta hankittavan järjestelmän tai palvelun esiarviointi suhteessa vähimmäisvaatimuksiin. Eräs yleisesti käytetty menetelmä palveluiden turvallisuuden varmistamiseen on tietojärjestelmien ja niiden palveluntarjoajien arvioinnit, jota on kuvattu yksityiskohtaisemmin suosituksen ”Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa” luvussa 4. Osa palveluntarjoajista tarjoaa asiakkailleen mahdollisuuden ottaa käyttöönsä uusia toiminnallisuuksia, jotka ovat esikatselu- tai testausvaiheessa. Mikäli tällaisia toiminnallisuuksia halutaan ottaa käyttöön salassa pidettävän tiedon käsittelyyn, suositellaan riskienarvioinnissa huomioitavaksi muun muassa käyttöönottoon liittyvät vastuut. Uusien toiminnallisuuksien toteutuksessa voi vielä olla turvallisuuspuutteita, joista mahdollisesti aiheutuvien vahinkojen korvaaminen on sopimuksissa usein osoitettu asiakkaalle.
Toteutusesimerkki	Organisaatio määrittelee hankinta- ja kehitysprosesseissa tietoturvavaatimukset sekä varmistaa niiden täyttymisen. Vaatimusten riittävyyden takaamiseksi organisaatio edellyttää, että tietoturvavaatimukset määritellään, katselmoidaan ja hyväksytään ennen hankinnan etenemistä ja tietoturvatestaus on suoritettu hyväksytysti ennen tietojärjestelmien käyttöönottoja. Hankittavan palvelun tai järjestelmän tarjoajan/toimittajan tulee pystyä selvittämään vähintään seuraavat: 1) Palvelusta on järjestelmäkuvaus. Palveluntarjoajan kuvauksen perusteella on pystyttävä arvioimaan kyseisen palvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Järjestelmäkuvauksesta tulee käydä ilmi vähintään: a) Palvelun palvelu- ja toteutusmallit, sekä näihin liittyvät palvelutasosopimukset (Service Level Agreements, SLAs). b) Palvelun tarjoamisen elinkaaren (kehittäminen, käyttö, käytöstä poisto) periaatteet, menettelyt ja turvatoimet, valvontatoimet mukaan lukien. c) Palvelun kehittämisessä, ylläpidossa/hallinnassa ja käytössä käytettävän infrastruktuurin, verkon ja järjestelmäkomponenttien kuvaus. d) Muutostenhallinnan periaatteet ja käytännöt, erityisesti turvallisuuteen vaikuttavien muutosten käsittelyprosessit. e) Käsittelyprosessit merkittäville normaalikäytöstä poikkeaville tapahtumille, esimerkiksi toimintatavat merkittävissä järjestelmävikaantumisissa. f) Palvelun tarjoamiseen ja käyttöön liittyvät roolit ja vastuunjako asiakkaan ja palveluntarjoajan välillä. Kuvauksesta on käytävä selvästi esille ne toimet, jotka kuuluvat asiakkaan vastuulle palvelun turvallisuuden varmistamisessa. Palveluntarjoajan vastuisiin tulee sisältyä yhteistyövelvollisuus erityisesti poikkeamatilanteiden selvittelyssä. g) Alihankkijoille siirretyt tai ulkoistetut toiminnot. Infrastruktuurin, verkon ja järjestelmäkomponenttien kuvauksen tulee olla riittävän yksityiskohtainen, jotta kuvauksen pohjalta pystytään arvioimaan palvelun yleistä soveltuvuutta ja riskejä suhteessa asiakkaan käyttötapaukseen. Vrt. PiTuKri KT-01 (Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi). Infrastruktuurin kuvauksessa voidaan tietyin rajauksin hyödyntää myös ohjelmistokoodia, jonka pohjalta kyseinen infrastruktuuri rakennetaan.

Lainsäädäntö	TihL 13 § 4 mom; TLA:n 6 §; JulkL 26 §
Viitteet	Katakri: I-13
Muita lisätietoja	ISO/IEC 27002:2022 5.19, 5.20, 5.21, 8.29, 8.30; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 6; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 8; Suositus turvallisuusluokiteltujen asiakirjojen käsittelystä pilvipalveluissa 2022:4 luku 4; PiTuKri EE-01 ja KT-01
Tunniste	**HAL-16.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Hankintojen turvallisuus - sopimukset
Vaatimus	Organisaatio varmistaa, että tietoturvallisuuteen sisältyvät vaatimukset ja niiden säilyminen koko elinkaaren ajan on otettu huomioon sopimuksissa. Sopimusehdot eivät myöskään saa rajoittaa palvelun soveltuvuutta kyseiseen käyttötapaukseen.
Yleiskuvaus	Erityisesti pilvipalvelut ovat jatkuvan muutoksen alaisia. Pilvipalveluille ominaista on nopea ja voimakas kehittyminen, mikä edellyttää jatkuvaa sopimusten seurantaa ja valvontaa sekä muutoshallintaa. Muutokset kasvattavat riskiä siitä, että palvelu, sen tarjoaja tai jokin uusi ominaisuus muuttuu sopimuksen- tai vaatimustenvastaiseksi tai toteutuu määräysvaltamuutosriskejä. Myös palveluntuottajan omistajanvaihdokseen sisältyy riskejä, jotka tulee riittävässä laajuudessa ottaa huomioon sopimuksissa. Lisäksi on huomioitava, että tiedon elinkaaren ajan kestävästä tietoturvallisuudesta voi olla mahdotonta varmistua sellaisten palveluntarjoajien kanssa, jotka varaavat sopimuksiinsa yksipuolisen mahdollisuuden muuttaa sopimusehtojaan. Riskiperustaisesti on myös arvioitava sopimuksen luotettavuutta ja varmistuttava siitä, että tarjoajan sopimuksessa sopimat asiat on myös toteutettu sovitulla tavalla. Erityisesti pilvipalveluihin liittyvissä sopimuksissa tulee määritellä riittävän selkeästi mitkä tehtävät ovat palveluntuottajan vastuulla ja mitkä kuuluvat asiakkaan vastuulle. Henkilötietojen käsittely voi tietosuojasääntelyn näkökulmasta myös estyä, mikäli palveluntarjoaja ei pysty tarjoamaan tietosuojasääntelyn mukaista sopimusta, jonka muuttaminen ei ole mahdollista yksipuolisesti, toisin sanoen ilman palvelun asiakkaan suostumusta. Arvioinnissa tulee huomioida EU:n yleisen tietosuoja-asetuksen 28 artiklan 4. kohdan vaatimukset alikäsittelijöitä käytettäessä. Palveluntarjoajan (rekisterinpitäjän) tulee tehdä henkilötietojen käsittelijän kanssa kirjallinen sopimus. Palvelujen sopimuksiin ja käyttöehtoihin saattaa liittyä myös erilaisia toimittajakohtaisia tapoja määritellä palvelun tai sen osan fyysisiä sijaintimaita. Henkilötietojen siirtäminen EU-/ETA-alueen ulkopuolelle tulee aina tehdä EU:n yleisessä tietosuoja-asetuksessa (V luku) säädettyjen edellytysten mukaisesti. Muun muassa lainsäädäntöjohdannaisten riskien sekä jatkuvuuteen ja varautumiseen liittyen osalta tulee myös huomioida, että palvelun asiakkaan tietojen tulee sijaita koko elinkaarensa ajan vain sopimuksessa kuvatuissa fyysisissä sijainneissa. Poikkeuksena tilanne, jossa palvelun asiakas on kirjallisesti etukäteen hyväksynyt tietojen siirron tai käsittelyn muissa fyysisissä sijainneissa. Tällaisten tarpeiden täyttäminen ei yleensä ole uskottavasti mahdollista tilanteissa, joissa palveluntarjoaja varaa itselleen mahdollisuuden muuttaa sopimusehtojaan yksipuolisesti, toisin sanoen ilman asiakkaan suostumusta. On lisäksi huomioitava, että viranomaisen on ennakolta varmistuttava siitä, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti (621/1999, 26 §). Viranomaisen on myös ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle (TLA:n 6 §).
Toteutusesimerkki	
Lainsäädäntö	TihL 13 §; TLA:n 6 §; JulkL 26 §; Tietosuoja-asetus artikla 28.4
Viitteet	Katakri: I-13
Muita lisätietoja	ISO/IEC 27002:2022 5.20; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 6; PiTuKri TJ-07;

Tunniste	HAL-17, L:, E:Tärkeä, S:Tärkeä, TS:
Nimi	Tietojärjestelmien toiminnallinen käytettävyys ja vikasietoisuus
Vaatimus	Organisaatio varmistaa tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden riittävällä testauksella säännöllisesti.
Yleiskuvaus	Olennaisilla tietojärjestelmillä tarkoitetaan sellaisia tietojärjestelmiä, jotka ovat kriittisiä viranomaisen lakisääteisten tehtäviä toteuttamisen kannalta erityisesti hallinnon asiakkaille palveluja tuotettaessa. Toiminnallisella käytettävyydellä tarkoitetaan tietojärjestelmän käyttäjän kannalta sen varmistamista, että tietojärjestelmä on helposti opittava ja käytössä sen toimintalogiikka on helposti muistettava, sen toiminta tukee niitä työtehtäviä, joita käyttäjän pitää tehdä tietojärjestelmällä ja tietojärjestelmä edistää sen käytön virheettömyyttä.
Toteutusesimerkki	- Organisaatio tunnistaa ja luetteloi tehtävien hoitamisen kannalta olennaiset tietojärjestelmät esimerkiksi osana suojattavien kohteiden luettelointia ja tiedon luokittelua. - Organisaatio määrittelee olennaisten tietojärjestelmien saatavuuskriteerit, joita vasten vikasietoisuus voidaan testata. Järjestelmäkohtaisten saatavuuskriteerien määrittelyssä voidaan hyödyntää tietojärjestelmien saatavuusluokittelua. - Organisaatio määrittelee toiminnallisen käytettävyyden kriteerit. - Organisaation hankintaprosesseissa ja hankintaohjeissa on huomioitu toiminnalliseen käytettävyyteen ja vikasietoisuuteen liittyvät vaatimukset. - Organisaatio dokumentoi vikasietoisuuden testaukset.
Lainsäädäntö	TihL 13 § 2 mom
Viitteet	
Muita lisätietoja	ISO/IEC 27002:2022 8.29, Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 7
Tunniste	**HAL-17.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Tietojärjestelmien toiminnallinen käytettävyys ja vikasietoisuus - saavutettavuus
Vaatimus	Organisaation on varmistettava digitaalisten palveluiden saavutettavuus lainsäädännön edellyttämässä laajuudessa.
Yleiskuvaus	Saavutettavuus tarkoittaa sitä, että mahdollisimman moni erilainen ihminen voi käyttää verkkosivuja ja mobiilisovelluksia mahdollisimman helposti. Saavutettavuus on ihmisten erilaisuuden ja moninaisuuden huomiointia verkkosivujen ja mobiilisovelluksien suunnittelussa ja toteutuksessa. Saavutettavan digipalvelun suunnittelussa ja toteutuksessa pitää huomioida kolme osa-aluetta: tekninen toteutus, helppokäyttöisyys ja sisältöjen selkeys ja ymmärrettävyys. Koska saavutettavuus ei kuulu tiedonhallintalautakunnan toimivallan piiriin, on saavutettavuus mukana Julkri-kriteeristössä ainoastaan ylätason varmistuskriteerinä. Julkri-kriteeristöä ei siten käytetä saavutettavuuden arviointiin, mutta kriteeri on mukana muistuttamassa organisaatioita siitä, että myös saavutettavuuteen liittyvät asiat tulee varmistaa osana digitaalisten palveluiden suunnittelua ja toteutusta. Yksityiskohtaisemmat ohjeet ja vaatimukset löytyvät Etelä-Suomen Aluehallintoviraston ylläpitämältä www.saavutettavuusvaatimukset.fi -sivustolta.
Toteutusesimerkki	
Lainsäädäntö	Laki digitaalisten palvelujen tarjoamisesta (306/2019)
Viitteet	
Muita lisätietoja	www.saavutettavuusvaatimukset.fi

Tunniste	HAL-18, L:Julkinen, E:, S:, TS:
Nimi	Asiakirjajulkisuuden toteuttaminen
Vaatimus	Organisaatio varmistaa, että tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvän tietojenkäsittely suunnitellaan siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.
Yleiskuvaus	Vaatimus kohdistuu viranomaisiin, jotka käytännössä vastaavat tietoaineistoissa olevien tietojen saatavuudesta. Vaatimus korostaa sitä, että viranomaisen tietojärjestelmissä olevista tiedoista on pystyttävä muodostamaan tietojärjestelmässä olevilla hakutoiminnoilla viranomaisen asiakirjoja viranomaisen toiminnan julkisuuden toteuttamiseksi.
Toteutusesimerkki	- Organisaatiot määrittelevät vastuullaan oleviin tietoaineistoihin kohdistuvat tiedonsaantitarpeet ottaen huomioon erityisesti viranomaisten tietojen julkisuuteen kohdistuvat vaatimukset. - Organisaatiot huomioivat toteutus- ja hankintaprosesseissa vaatimukset asiakirjajulkisuuden vaivattomasta toteuttamisesta. - Organisaatio seuraa asiakirjajulkisuuden toteuttamiseen liittyviä tarpeita ja ylläpitää vanhoja tietojärjestelmiä tarpeen mukaan.
Lainsäädäntö	TihL 13 § 3 mom
Viitteet	
Muita lisätietoja	

Tunniste	HAL-19, L:Julkinen, E:, S:, TS:Henkilötieto
Nimi	Tietojen käsittely
Vaatimus	Organisaatio varmistaa, että tietoja käsitellään ja säilytetään siten, että pääsy tietoihin suojataan sivullisilta.
Yleiskuvaus	Tietojen käsittelyn ja säilytyksen tietoturvallisuuteen vaikuttavat muun muassa fyysisten tilojen turvallisuus, tietojen käsittelyssä käytettävien tietojärjestelmien ja päätelaitteiden turvallisuus sekä tietoja käsittelevien henkilöiden ohjeet ja koulutus. Organisaation turvallisuuden hallinnan prosessien avulla tulee varmistaa, että tarvittavat toimenpiteet kaikkien edellä lueteltujen osa-alueiden suhteen on tehty. Yksityiskohtaisempia kriteerit eri turvallisuustasoille luokiteltujen tietojen käsittelemisestä ja säilyttämisestä on esitetty fyysisen turvallisuuden ja teknisen turvallisuuden osa-alueilla.
Toteutusesimerkki	Organisaatio on varmistanut tietojen käsittelyn turvallisuuden esimerkiksi seuraavilla toimenpiteillä: - Organisaatio on varmistanut, että tietojen käsittelyyn ja säilytykseen tarkoitetut tilat täyttävät niissä käsiteltävien tai säilytettävien tietojen ja tietojärjestelmien asettamat vaatimukset sekä määritellyt tarvittavat hallinnolliset alueet ja turva-alueet. - Organisaatio on ohjeistanut missä tiloissa eri turvallisuustasoille luokiteltuja tietoja saa käsitellä ja säilyttää. - Organisaatio on ohjeistanut, miten tietoihin pääsy tulee suojata sivullisilta eri käsittely-ympäristöissä - Organisaatio on määritellyt miten eri tietojen käsittelyyn tarkoitetut tietojärjestelmät tulee säilyttää - Organisaatio on määritellyt tietojen käsittelyssä käytettävien päätelaitteiden vaatimukset.
Lainsäädäntö	TihL 13 §, 15 § 2 mom; TLA 10 § 1 mom
Viitteet	Julkri: FYY-03, FYY-04, TEK-09; Katakri: I-17
Muita lisätietoja	ISO/IEC 27002:2022 5.15; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 4;

3 Fyysinen turvallisuus

Fyysinen turvallisuus (FYY) sisältää luvattoman tietoihin pääsyn estäviä ja rajoittavia toimitiloihin ja säilytysratkaisuihin liittyviä kriteereitä. Lisäksi osa-alueella on kuvattu tietojen käsittelyyn, säilyttämiseen, siirtämiseen, kuljettamiseen ja tuhoamiseen liittyviä kriteereitä. Fyysisen turvallisuuden osa-aluetta on mahdollista käyttää arvioitaessa tiedon suojaamiseksi toteutettuja fyysisen turvallisuuden toimenpiteitä.

Osa-alueen sisältö perustuu Katakri-kriteeristöön. Erityisesti turvallisuusluokitellun tiedon käsittelyä koskevien kriteerien sisältö on pyritty säilyttämään yhdenmukaisena Katakrin kanssa. Selkeimpiä eroja suhteessa Katakriin ovat kansainvälisiin tietoturvallisuusvelvoitteisiin perustuvien kriteerien jättäminen pois osa-alueelta sekä tiettyjen kriteerien luokittelu sovellettavaksi myös muille kuin turvallisuusluokitelluille tiedoille.

Osa-alueen rakenne on suunniteltu siten, että eri tasoisia turvallisuusalueita koskevat yhteiset kriteerit, vain hallinnollisia alueita koskevat kriteerit sekä vain turva-alueita koskevat kriteerit on koottu kukin omaan alalukuunsa. Tämä rakenne poikkeaa Katakrin rakenteesta, jossa osa kriteereistä on toistettu saman sisältöisinä eri tasoisilla turvallisuusalueilla.

Viranomaisten tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia (tiedonhallintalaki 15 § 2 mom). Turvallisuusluokiteltujen tietojen fyysiseksi suojaamiseksi, turvallisuusluokitteluasetuksessa on säädetty kahdentyyppisistä fyysisesti suojatuista turvallisuusalueista: hallinnollisista alueista ja turva-alueista. Julkrissa käytetään hallinnollisen alueen ja turva-alueen käsitteitä.

Salassa pidettäviä tietoja sisältävät tietovarannot sekä niiden käsittelyyn käytetyt tietojärjestelmät suositellaan sijoitettavaksi viranomaisen tähän tarkoitukseen määrittelemälle suojatulle-alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa ja tässä suosituksessa ja sen liitteenä olevassa kriteeristössä kuvattu hallinnollinen alue.

Hallinnollisella alueella tarkoitetaan käytännössä sellaista organisaation määrittelemää aluetta, johon sivulliset eivät pääse hallitsemattomasti ja johon on toteutettu riittävät toimenpiteet alueella käsiteltävien ja säilytettävien tietojen turvallisuuden varmistamiseksi. Alueen rakenteille ja muille toimenpiteille ei ole asetettu yksityiskohtaisia vaatimuksia vaan organisaatio voi suunnitella ne soveltaen riskilähtöisesti fyysisen (FYY) osa-alueen kriteereitä.

Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten turvatoimien toteuttamista siten, että estetään luvaton pääsy tietoihin:

a) varmistamalla, että tietoja käsitellään ja säilytetään asianmukaisesti,
b) mahdollistamalla pääsy tietoihin tiedonsaantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella,
c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet ja
d) estämällä oikeudetta tapahtuva tunkeutuminen tai viivyttämällä sitä.

Toimitiloissa, joissa toimii useampi organisaatio tulee kunkin tietoja käsittelevän organisaation varmistua siitä, että yhteisten toimitilojen tarjoama turvallisuus on riittävä suhteessa organisaatioon kohdistettuihin fyysisen turvallisuuden vaatimuksiin.

Tunniste	FYY-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Fyysisen turvallisuuden riskien arviointi
Vaatimus	Fyysiset turvatoimet on mitoitettava riskien arvioinnin mukaisesti.
Yleiskuvaus	Riskien arvioinnissa tulee ottaa huomioon esimerkiksi pääsyoikeuksien hallintaan ja muihin turvallisuusjärjestelyihin liittyviin prosesseihin sisällytettävät tiedonsaantitarpeen, tehtävien eriyttämisen ja vähimpien oikeuksien periaatteet. Fyysisiä turvatoimia koskevan riskien arvioinnin tulee olla säännöllistä ja osa organisaation riskienhallinnan kokonaisuutta. Arvioiduilla riskeillä on nimetyt omistajat. Hyväksyttyjen fyysisten turvatoimien muutoksiin liittyvät riskit tulee arvioida muutosten yhteydessä. Erityisesti korvaavien fyysisten turvatoimien osalta tulee pystyä osoittamaan perustelut valituille turvatoimille.
Toteutusesimerkki	Riskien arvioinnissa on otettava huomioon kaikki asiaan kuuluvat tekijät, erityisesti seuraavat: a) Tietojen turvallisuusluokka ja salassapitoperuste; b) Tietojen käsittely- ja säilytystapa sekä määrä ottaen huomioon, että tietojen suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista; c) Tietojen käsittely- ja säilytysaika d) Tietojen käsittely- ja säilytyspaikan ympäristö: rakennuksen ympäristö, sijoittuminen rakennuksessa, tilassa tai sen osassa; e) Hälytystilanteisiin liittyvä vasteaika f) Ulkoistetut toiminnot, kuten huolto-, siivous-, kiinteistö- ja turvallisuuspalvelut g) Tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu uhka tiedoille
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom
Viitteet	Julkri: HAL-06; Katakri: F-02
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 36
Tunniste	**FYY-01.1, L:TL III, E:, S:, TS:**
Nimi	Fyysisen turvallisuuden riskien arviointi - TEMPEST
Vaatimus	Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös TEMPEST-riski.
Yleiskuvaus	Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös TEMPEST-riski, eli sähkömagneettisen hajasäteilyn aiheuttama riski. TEMPEST-riskiä voidaan yleensä pienentää muuttamalla tiedon käsittelypaikan sijaintia kiinteistössä.
Toteutusesimerkki	
Lainsäädäntö	TLA 11 § 2 mom
Viitteet	Julkri: TEK-15; Katakri: F-05.8, F-06.10
Muita lisätietoja	

Tunniste	FYY-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Fyysisten turvatoimien valinta (monitasoinen suojaus)
Vaatimus	Turvallisuusalueilla ja niitä ympäröivissä tiloissa on toteutettava turvallisuusalueen suojausta vaarantavia tekoja ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä, toimenpiteitä suojausta vaarantavien tekojen havaitsemiseksi ja jäljittämiseksi sekä toimenpiteitä vaarantanutta tekoa edeltäneen turvallisuustason palauttamiseksi viipymättä monitasoista suojausperiaatetta soveltaen. Laitteet on tarkastettava ja huollettava säännöllisin väliajoin.
Yleiskuvaus	Salassa pidettäviä tietoja ja asiakirjoja sisältävät tietovarannot sekä niiden käsittelyyn käytetyt tietojärjestelmät on sijoitettava viranomaisen tähän tarkoitukseen määrittelemälle suojatulle-alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa kuvattu hallinnollinen alue tai tieto pitää suojata riskiperusteisesti muilla turvakontrolleilla. Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Oikean standardiluokan valinta perustuu aina riskiarvioon. Yksittäisten vaatimusten yhteyteen lisätyssä Tavoitetaso-sarakkeessa on esitetty useimpiin monitasoisen suojauksen ratkaisuihin riittävä standardin mukainen luokka tai ohje. Yksittäisten turvatoimien hyväksymisen edellytyksenä ei kuitenkaan ole tavoitetason täyttyminen, koska fyysisten turvatoimien arviointi perustuu riskien arviointiin ja monitasoiseen suojauksen kokonaisuuteen. Joissakin tilanteissa voidaan riskien arviointiin perustuen edellyttää myös yksittäisiä tavoitetasoa korkeamman tason turvatoimia. Arvioitaessa laitteita ja järjestelmiä on varmistettava, että ne ovat toimintakuntoisia ja soveltuvia niiden käyttötarkoitukseen. Laitteiden ja järjestelmien vastaanottotarkastuksista, käytön aikaisista tarkastuksista ja tehdyistä huolloista tulisi olla nähtävissä dokumentaatio. Järjestelmäoikeuksia arvioitaessa tulisi kiinnittää huomiota erityisesti vähimpien oikeuksien periaatteen sekä tehtävien eriyttämisen toteutumiseen. Laitteiden ja järjestelmien sijoitustilan tulisi sijaita niiden suojaamalla turvallisuusalueella. Laitteiden ja järjestelmien ja niiden sijoitustilojen asennus-, tarkastus-, huolto- ja siivoustoimet toteutetaan vain alueelle itsenäisen pääsyoikeuden saaneen henkilön toimesta tai valvonnassa. Laitteiden ja järjestelmien etäyhteydet ja laiteasennukset tulee toteuttaa riskienarvioinnin perusteella riittävän tietoturvallisesti siten, että laitteisiin ja järjestelmiin pääsy on vain valtuutetuista päätelaitteista ja verkoista ja että tietoliikenneyhteyksien ja laitteiden ja järjestelmien rajapinnat on suojattu siten, että ulkopuolisilla ei ole pääsyä välitettyihin tietoihin. Salassa pidettävien tietojen käsittely on mahdollista myös yhteisissä työympäristöissä, joissa voi työskennellä useita eri organisaatioita. Tällöin fyysisen turvallisuuden tasosta sovitaan tarvittaessa etukäteen, jotta tilat mahdollistavat salassa pidettävän tiedon asianmukaisen käsittelyn ja säilyttämisen jokaisen organisaation tarpeet huomioiden. Olennaista näissä tapauksissa on tiedon käsittelijän vastuu käsitellä tietoja niin, ettei tietoon oikeudeton saa haltuunsa tietoja.

Toteutusesimerkki	Monitasoinen suojaus muodostuu hallinnollisista, toiminnallisista ja fyysisistä keinoista, kuten: a) rakenteelliset esteet: fyysinen este, jolla turvallisuusalueet ja sitä ympäröivät tilat rajataan ja luvatonta tunkeutumista vaikeutetaan ja hidastetaan; b) kulunvalvonta: kulunvalvonnalla rajataan pääsyä turvallisuusalueille ja sitä ympäröiviin tiloihin. Tavoitteena havaita luvattomat pääsy-yritykset, estää asiattomien henkilöiden pääsy ja valvoa alueella liikkuvia. Kulunvalvonta voi kohdistua alueeseen, alueen yhteen tai useampaan rakennukseen tai rakennuksen alueisiin tai huoneisiin. Valvonnassa voidaan hyödyntää mekaanisia, sähköisiä tai sähkömekaanisia teknisiä järjestelmiä tai muunlaisia fyysisiä keinoja. Myös vartiointihenkilöstö, vastaanottovirkailija tai oma henkilöstö voi osallistua valvontaan. c) tunkeutumisen ilmaisujärjestelmä: rakenteellisen esteen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisen ilmaisujärjestelmää (murtohälytysjärjestelmä). Järjestelmää voidaan käyttää myös vartiointihenkilöstön tekemän valvonnan asemasta tai tueksi. d) vartiointihenkilöstö: koulutettua, valvottua, varustettua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä vartiointihenkilöstöä voidaan käyttää muun muassa kulunvalvonnan tukena sekä turvallisuusalueelle tai sitä ympäröivien tilojen tunkeutumista suunnittelevien henkilöiden aikeiden havaitsemisessa ja toimien estämisessä. e) kameravalvonta: kameravalvontaa voidaan käyttää turvallisuusalueella tai sen ympärillä erityisesti laittoman tiedustelun ennalta ehkäisemisessä sekä ilmenevien poikkeamien ennalta ehkäisemisessä, hälytysten todentamisessa ja tapahtuneiden poikkeamien selvittämisessä. Vartiointihenkilöstö voi käyttää kameravalvontaa reaaliaikaisena, aktiivisena kuvan tarkkailuna tai jälkikäteen passiivisena kuvamateriaalin analysointina. f) turvallisuutta ylläpitävät menettelyt: vastuiden ja tehtävien määrittäminen, erilaiset prosessit ja toimintamallit, kuten pääsyoikeuksien ja avainten hallinta, henkilöstön ohjeistus ja perehdyttäminen sekä järjestelmien huolto- ja ylläpitotoimet. g) valaistus: mahdollinen tunkeutuja voidaan havaita valaistuksen avulla ja vartiointihenkilöstö voi valvoa aluetta tehokkaasti, joko suoraan tai kameravalvontajärjestelmää hyödyntämällä. h) muut asianmukaiset fyysiset toimenpiteet, joiden tarkoituksena on estää ja havaita luvaton pääsy tai ehkäistä turvallisuusluokiteltujen tietojen katoaminen tai vahingoittuminen.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 7 §
Viitteet	Katakri: F-03
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 33; ISO/IEC 27002:2022 7.1, 7.2, 7.3

Tunniste	FYY-03, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Tiedon käsittely
Vaatimus	Tietoja on käsiteltävä siten, että pääsy niihin suojataan sivullisilta.
Yleiskuvaus	Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen tietoon että laittomalta tiedustelulta. Suojaaminen tarkoittaa käytännössä esimerkiksi suoran näkö- tai kuuloyhteyden estämistä turvallisuusluokiteltuun tietoon. Turvallisuusluokiteltujen tietojen käsittely turvallisuusalueilla (hallinnollinen alue tai turva-alue) on pääsääntö, mutta on tilanteita – kuten etätyö tai työtehtävät turvallisuusalueiden ulkopuolella – jolloin tietoa joudutaan käsittelemään myös määritettyjen turvallisuusalueiden ulkopuolella. Tietoja voi käsitellä sekä paperimuodossa että vaatimukset täyttävässä päätelaitteessa turva-alueilla, hallinnollisilla alueilla tai niiden ulkopuolella edellyttäen, että pääsy tietoihin on suojattu sivullisilta. Käsittely on sallittua aina TL II -luokkaan asti kuitenkin siten, että turvallisuusluokan II tai III asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turva-alueelle.
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §
Viitteet	Julkri: HAL-19; Katakri: F-04
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 29

Tunniste	FYY-03.1, L:TL I, E:, S:, TS:
Nimi	Tiedon käsittely - TL I
Vaatimus	Turvallisuusluokan I asiakirjaa saa käsitellä ainoastaan turva-alueella.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 § 2 mom
Viitteet	Julkri: HAL-19; Katakri: F-04
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 29

Tunniste	FYY-04, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Tiedon säilytys
Vaatimus	Tietoja on säilytettävä siten, että pääsy niihin suojataan sivullisilta.
Yleiskuvaus	Suojaaminen tarkoittaa käytännössä esimerkiksi tiedon tai tietoa sisältävän päätelaitteen riittävän turvallista säilyttämistä. Tietojen käsittelyssä on huomioitava lisäksi toiminta työskentelytaukojen aikana, jolloin asiakirjat ja päätelaitteet on turvallisuusluokan perusteella sijoitettava soveltuvalle turvallisuusalueelle ja/tai säilytysyksikköön tauon ajaksi. Tiedon säilytyksellä viitataan tilanteeseen, jossa tieto ei ole sen käsittelijän välittömässä valvonnassa.
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §
Viitteet	Julkri: HAL-19; Katakri: F-04
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28–29
Tunniste	**FYY-04.1, L:TL IV, E:, S:, TS:**
Nimi	Tiedon säilytys - TL IV
Vaatimus	Organisaatio säilyttää paperiasiakirjat ja muut ei sähköisessä muodossa olevat tiedot - turva-alueella tai hallinnollisella alueella soveltuvaksi arvioidussa toimistokalusteessa tai - tilapäisesti turvallisuusalueiden ulkopuolella jos tiedon käsittelijä on sitoutunut noudattamaan annetuissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä. Organisaatio säilyttää sähköisessä muodossa olevat tiedot - turva-alueella tai hallinnollisella alueella vaatimukset täyttävässä laitteessa tai sähköisessä tietovälineessä tai - turvallisuusalueiden ulkopuolella vaatimukset täyttävässä päätelaitteessa tai sähköisessä tietovälineessä valvotussa tilassa tai soveltuvassa lukitussa toimistokalusteessa turvapussissa tai vastaavalla tavalla.
Yleiskuvaus	
Toteutusesimerkki	Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, tulisi alueen seinien, lattian, katon, ikkunoiden ja ovien täytettävä vähintään standardin SFS-EN-1627 luokkaa RC3 vastaava suoja. Mikäli turvallisuusluokitellun tiedon säilytysyksikkönä käytetään lukittua toimistokalustetta, on varmistuttava siitä, että tunkeutumisesta jää murtojälki.
Lainsäädäntö	TLA 10 §
Viitteet	Katakri: F-04
Muita lisätietoja	
Tunniste	**FYY-04.2, L:TL IV, E:, S:, TS:**
Nimi	Tiedon säilytys - Tietovarannot ja tietojärjestelmät - TL IV
Vaatimus	Turvallisuusluokan IV asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle (hallinnollinen alue tai turva-alue).
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 § 3 mom 3 kohta
Viitteet	Julkri: HAL-19; Katakri: F-04
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28–29

Tunniste	FYY-04.3, L:TL III, E:, S:, TS:
Nimi	Tiedon säilytys - Tietovarannot ja tietojärjestelmät - TL III
Vaatimus	Turvallisuusluokan II tai III asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turva-alueelle.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 § 3 mom 2 kohta
Viitteet	Julkri: HAL-19; Katakri: F-04
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28–29
Tunniste	**FYY-04.4, L:TL III, E:, S:, TS:**
Nimi	Tiedon säilytys - TL III
Vaatimus	Organisaatio säilyttää paperiasiakirjat ja muut ei sähköisessä muodossa olevat tiedot turva-alueella soveltuvaksi arvioidussa säilytysratkaisussa. Organisaatio säilyttää sähköisessä muodossa olevat tiedot - turva-alueella vaatimukset täyttävässä laitteessa tai sähköisessä tietovälineessä tai - turva-alueiden ulkopuolella vaatimukset täyttävässä päätelaitteessa valvotussa tilassa tai soveltuvassa lukitussa toimistokalusteessa turvapussissa tai vastaavalla tavalla.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 §
Viitteet	Katakri: F-04
Muita lisätietoja	
Tunniste	**FYY-04.5, L:TL II, E:, S:, TS:**
Nimi	Tiedon säilytys - TL II
Vaatimus	Organisaatio säilyttää paperiasiakirjat ja muut ei sähköisessä muodossa olevat tiedot turva-alueella soveltuvaksi arvioidussa säilytysratkaisussa. Organisaatio säilyttää sähköisessä muodossa olevat tiedot turva-alueella vaatimukset täyttävässä laitteessa tai sähköisessä tietovälineessä.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 §
Viitteet	Katakri: F-04
Muita lisätietoja	

Tunniste	FYY-04.6, L:TL I, E:, S:, TS:
Nimi	Tiedon säilytys - TL I
Vaatimus	Turvallisuusluokan I asiakirjaa saa säilyttää ainoastaan turva-alueella.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 § 2 mom
Viitteet	Julkri: HAL-19; Katakri: F-04
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 29
Tunniste	**FYY-05, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Turvallisuusalue
Vaatimus	Turvallisuusalueiden eli hallinnollisten alueiden sekä turva-alueiden on noudatettava tässä kriteerissä annettuja suosituksia.
Yleiskuvaus	Monet fyysisen turvallisuuden suositukset ovat yhteisiä sekä hallinnollisille alueille että turva-alueille. Tähän kriteeriin on koottu yhteiset suositukset, jotka tulee ottaa huomioon sekä hallinnollisten alueiden että turva-alueiden arvioinneissa.
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 9 §
Viitteet	Katakri: F-05.4, F-06.6
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39
Tunniste	**FYY-05.1, L:TL IV, E:, S:, TS:**
Nimi	Turvallisuusalue - Äänieristys
Vaatimus	Alueen äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena suojattavaan tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan suojattavista tiedoista, joihin kaikilla ei ole tiedonsaantitarvetta.
Yleiskuvaus	Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta kyseiseen keskusteltavaan tietoon, että laittomalta tiedustelulta. Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan suojattavista tiedoista. Äänieristystä voidaan arvioida esimerkiksi kuuntelemalla keskustelua tilan ulkopuolelta ovien, seinien sekä ilmastointiputkien ja muiden läpivientien kohdalta. Tilan äänieristystä voidaan myös tarvittaessa verrata rakenteille annettavaan ilmaääneneristävyysvaatimukseen.
Toteutusesimerkki	Vaatimus voidaan määrittää standardin SFS-EN-ISO 717-1 mukaisesti. Ilmaääneneristävyys voidaan todeta standardin SFS-EN-ISO 16283-1 mukaisesti tehdyllä mittauksella. Arvioinnissa tulee huomioida ilmanääneneristävyyden lisäksi myös runkoääneneristävyys. Äänieristysvaatimus voidaan tarvittaessa saavuttaa esimerkiksi tilan uudelleen sijoittelulla, rakenteiden ja läpivientien eristävyyden parantamisella tai arvioitavan tilan ulkopuolisten tilojen taustamelulla.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 § 1 mom
Viitteet	Katakri: F-05.4, F-06.6
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39

Tunniste	FYY-05.2, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Turvallisuusalue - Salaa katselun estäminen
Vaatimus	Jos tietoihin kohdistuu salaa tai vahingossa katselun riski, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet.
Yleiskuvaus	
Toteutusesimerkki	Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 § 1 mom
Viitteet	Julkri: HAL-19; Katakri: F-05.6, F-06.8
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 40 ja 45
Tunniste	**FYY-05.3, L:TL II, E:, S:, TS:**
Nimi	Turvallisuusalue - Tila- ja laitetarkastukset
Vaatimus	Organisaation on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella alueella, jossa käsitellään turvallisuusluokan II tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. Myös alue on tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin sekä mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta.
Yleiskuvaus	Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista luotettavasti (esim. matkapuhelimet, älykellot, jne.), laitteet tulee jättää tilan ulkopuolelle esimerkiksi tähän tarkoitukseen varattuun säilytysratkaisuun.
Toteutusesimerkki	
Lainsäädäntö	TLA 7 §, 10 § 1 mom, 11 § 2 mom
Viitteet	Katakri: F-05.7, F-06.9
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 40 ja 46
Tunniste	**FYY-05.4, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Turvallisuusalue - Pääsyoikeuksien ja avaintenhallinnan menettelyt
Vaatimus	Organisaation on määriteltävä alueen pääsyoikeuksien ja avainhallinnan menettelyt ja roolit.
Yleiskuvaus	Pääsyn rajaaminen alueelle voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien ja avainhallinnan menettelyistä. Alueen vara-avaimia säilytetään turvallisesti ja suljettuna sinetöityyn, sulkemispäiväyksellä ja kuittauksella varustettuun säilytyskuoreen tai vaihtoehtoisesti kulunvalvontaan liitetyssä avainkaapissa. Avaimet luovutetaan työtehtävään liittyen ja kuittausta vastaan. Menettely on kuvattu turvallisuuden hallintaohjeissa. Alueelle ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua: Lukot heloineen: SFS 7020+5970, luokat 1–4, tavoitetaso 3; Elektroniset kulunvalvontajärjestelmät: SFS-EN 60839-11-1 ja 2, Huomioitava esimerkiksi SFS-EN 50131-standardin vaatimukset, mikäli kulunvalvontajärjestelmä on osa tunkeutumisen ilmaisujärjestelmää.

Toteutusesimerkki	Alueelle on nimetty vastuuhenkilö, joka huolehtii seuraavista pääsyoikeuksien ja avainhallinnan menettelyistä. - pääsyoikeuksien ja avainten hallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu. - pääsyoikeuksien ja avainten haltijoista on lista. - pääsyoikeudet tarkastetaan säännöllisesti ja ne pidetään ajan tasalla. - avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet on vastuutettu. - avainkortteja, jakamattomia avaimia ja kulkutunnisteita säilytetään asianmukaisesti. - avaimen luovutusperuste kirjataan dokumenttiin. - avaimet luovutetaan vain itsenäisen pääsyoikeuden alueelle saaneelle henkilölle. - henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa avainten hallintaoikeuteen.
Lainsäädäntö	TihL 15 § 2 mom; TLA 9 §
Viitteet	Katakri: F-05.2, F-06.3
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 39 ja 44; ISO/IEC 27002:2022 7.2
Tunniste	**FYY-05.5, L:TL IV, E:, S:, TS:**
Nimi	Turvallisuusalue - Vierailijat
Vaatimus	Muilla kuin organisaation asianmukaisesti valtuuttamilla henkilöillä (vierailijoilla) on aina saattaja.
Yleiskuvaus	Vieraiden isännällä tulee olla itsenäinen pääsyoikeus turvallisuusalueelle, jolle hän vie vieraat sekä oikeus isännöidä vieraita. Vierailumenettelyillä on varmistuttava, ettei vierailulla vaaranneta alueella käsiteltävän tai säilytettävän tiedon luottamuksellisuutta. Alueella tehtävät huoltotoimenpiteet tapahtuvat vain alueelle itsenäisen pääsyoikeuden saaneen henkilön toimesta tai valvonnassa. Tiedon käsittely alueella on huolto-, asennus- ja siivoustoimien aikana kielletty, jos on vaara, että edellä mainittuja toimenpiteitä suorittava henkilöstö saa tiedon suojattavista tiedosta. Saattamaton vierailijamenettely (unescorted visitor) on mahdollista hyväksyä alueen niille vierailijoille, jotka täyttävät pääsyoikeuksien myöntämisen vaatimukset.
Toteutusesimerkki	Organisaation on hyväksynyt menettelyohjeen vierailijoita varten. Vierailijaohje voi käsitellä muun muassa seuraavia asioita: - Vieras tunnistetaan ja varustetaan vieraskortilla. - Vierailu kirjataan. - Vierailijoita ei päästetä tai jätetä alueille valvomatta ja isäntä vastaa ulkopuolisista henkilöistä koko vierailun ajan. - Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten. - Huolehtiminen siitä, ettei vieras pääse oikeudettomasti näkemään, kuulemaan tai muutoin saa haltuunsa suojattavaa tietoa. - Henkilökunta on ohjeistettu reagoimaan ilman tunnistetta liikkuviin henkilöihin.
Lainsäädäntö	TLA 9 §
Viitteet	Katakri: F-05.3, F-06.4
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 39 ja 44

Tunniste	FYY-06, L:Salassa pidettävä, E:, S:, TS:
Nimi	Hallinnollinen alue
Vaatimus	Hallinnollisen alueen tulee täyttää tässä osiossa esitetyt suositukset sekä riskilähtöisesti arvioidut tarkennukset siten, että turvatoimien tavoitteet saavutetaan.
Yleiskuvaus	Salassa pidettäviä tietoja ja asiakirjoja sisältävät tietovarannot sekä niiden käsittelyyn käytetyt tietojärjestelmät on sijoitettava viranomaisen tähän tarkoitukseen määrittelemälle suojatulle-alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa kuvattu hallinnollinen alue tai tieto pitää suojata riskiperusteisesti muilla turvakontrolleilla. Hallinnollisella alueella tarkoitetaan normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta. Hallinnollisen alueen tulee täyttää tässä osiossa esitetyt vähimmäisvaatimukset. Vähimmäisvaatimusten lisäksi tulee suunnitella, vastuuttaa, toteuttaa ja ylläpitää riskien arviointiin ja monitasoiseen suojausperiaatteeseen perustuvat muut riskienhallintatoimenpiteet siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit voidaan hyväksyä ja turvatoimien tavoitteet saavutetaan. Lisäksi hallinnollisen alueen tulee täyttää kaikki turvallisuusalueita koskevat yhteiset vaatimukset, jotka on kuvattu kriteerissä ”Turvallisuusalue”.
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 9 §
Viitteet	Julkri: FYY-05; Katakri: F-05
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 38
Tunniste	**FYY-06.1, L:TL IV, E:, S:, TS:**
Nimi	Hallinnollinen alue - alueen raja ja rakenteet
Vaatimus	Alueella on oltava selkeästi määritelty näkyvä raja, mutta aluetta rajaavalle rakenteelle (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet) ei aseteta erityisiä vaatimuksia.
Yleiskuvaus	Fyysisten turvatoimien tavoite tulee täyttyä ennen kuin turvallisuusalueet voidaan hyväksyä. Alueen rakenne voi olla normaalia toimistorakennetta. Aluetta rajaavia rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Näitä vahvennuksia tulee arvioida suhteessa alueen ympäröivien tilojen antamaan muuhun suojaan sekä vartiointihenkilöstön vasteaikaan. Alueen aukot, jotka eivät ole käytössä kulkemiseen, on voitava lukita tai sulkea, jotta alueelle kulkua voidaan hallinnoida asianmukaisesti. Mikäli hallinnollisen alueen rajoilla on käytetty mekaanista lukkoa, lukon avainten kopiointi tulisi olla estetty patenttisuojalla. Mikäli mahdollista, hätäpoistumistiet eivät saa kulkea turva-alueen kautta. Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät ratkaisut ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia.
Toteutusesimerkki	Standardeja, joita voidaan käyttää referenssinä arvioitaessa aluetta rajaavia rakenteita: Seinät ja ovet sekä lattia- ja kattorakenteet: SFS-EN 1627, RC1-RC6; Ikkunat (suojauslasi): SFS-EN 356, P4A-P5A ja P6B-P8B
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom;TLA 9 § 1 mom 1 k
Viitteet	Katakri: F-05.1
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 39

Tunniste	FYY-06.2, L:TL IV, E:, S:, TS:
Nimi	Hallinnollinen alue - kulunvalvonta
Vaatimus	Alueelle pääsyä tulee valvoa, mikäli se on riskien arvioinnin perusteella tarkoituksenmukaista.
Yleiskuvaus	Kulunvalvonta voi olla tarkoituksenmukaista esimerkiksi, jos alueella käsitellään turvallisuusluokan III tai korkeamman luokan tietoa.
Toteutusesimerkki	Suositus kulunvalvonnan toteuttamisesta: - Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita. - Henkilöllä on vain ne kulkuoikeudet, joita hän tarvitsee työtehtäviensä hoitamiseksi. - Kulkuoikeuden myöntämisperuste kirjataan dokumenttiin ja vain nimetyillä henkilöillä on kulkuoikeudet alueelle. - Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa kulkuoikeuksiin. - Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu, jos se on hyvin hallinnoitu.
Lainsäädäntö	TLA 7 §, 9 §
Viitteet	Katakri: F-05.2
Muita lisätietoja	

Tunniste	FYY-06.3, L:Salassa pidettävä, E:, S:, TS:
Nimi	Hallinnollinen alue - pääsyoikeuksien myöntäminen
Vaatimus	Ainoastaan asianmukaisesti valtuutetuilla henkilöillä on itsenäinen pääsy alueelle. Itsenäisen pääsyn alueelle voi myöntää tiedoista vastaava organisaatio tai sovituilla menettelyillä fyysisen tilan hallinnasta vastaava palvelun tuottaja, kuten esimerkiksi pilvipalvelun toimittaja.
Yleiskuvaus	Pääsyn rajaaminen alueelle voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen.
Toteutusesimerkki	
Lainsäädäntö	TLA 9 §
Viitteet	Julkri: FYY-05.4; Katakri: F-05.2
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39, PiTuKri FT-03

Tunniste	FYY-06.4, L:TL IV, E:, S:, TS:
Nimi	Hallinnollinen alue - tunkeutumisen ilmaisujärjestelmät
Vaatimus	Tarvittaessa tunkeutumisen ilmaisujärjestelmää voidaan käyttää täydentävänä monitasoisen suojauksen riskienhallintakeinona.
Yleiskuvaus	Alue ja sinne johtavat ovet voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa lukittavassa toimistokalusteessa ja murtoriski arvioidaan todennäköiseksi. Alue tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Alueen mahdollista tunkeutumisen ilmaisujärjestelmää tai korvaavaa järjestelyä arvioitaessa tulee ottaa huomioon alueen rakenteita koskevan vaatimuksen yhteydessä käsitelty vasteaika-arvio. Mikäli alue on valvottu tunkeutumisen ilmaisujärjestelmällä, alueen suositellaan olevan valvottu järjestelmän avulla, kun alueella ei työskennellä. Tunkeutumisen ilmaisujärjestelmän sijoitustilan tulisi sijaita sen suojaamalla turvallisuusalueella.
Toteutusesimerkki	Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua: Tunkeutumisen ilmaisujärjestelmät: SFS-EN 50131 luokat 1–4, tavoitetaso 2; Tunkeutumisen ilmaisujärjestelmän ilmoituksensiirto: SFS-EN 50136-1 luokat DP1 - DP4 ja SP5 - SP6; Vartioimisliikkeen hälytyskeskus: SFS-EN 50518
Lainsäädäntö	TLA 7 §
Viitteet	Katakri: F-05.5
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 40

Tunniste	FYY-07, L:TL III, E:, S:, TS:
Nimi	Turva-alue
Vaatimus	Turva-alueen tulee täyttää tässä osiossa esitetyt suositukset sekä riskilähtöisesti arvioidut lisätarkennukset siten, että monitasoisen suojauksen tavoitteet saavutetaan.
Yleiskuvaus	Turva-alueella tarkoitetaan organisaation työskentelyyn tarkoitettuja, hallinnollista aluetta paremmin suojattuja alueita ja tiloja, joissa turvallisuusluokiteltuja tietoja käsitellään ja säilytetään. Turva-alue voidaan tilapäisesti perustaa hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten. Turva-alueen tulee täyttää tässä osiossa esitetyt suositukset. Suositusten lisäksi tulee suunnitella, vastuuttaa, toteuttaa ja ylläpitää riskien arviointiin ja monitasoiseen suojausperiaatteeseen perustuvat muut riskienhallintatoimenpiteet siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit voidaan hyväksyä ja monitasoisen suojauksen tavoitteet saavutetaan. Lisäksi turva-alueen tulee huomioida kaikki turvallisuusalueita koskevat yhteiset suositukset, jotka on kuvattu kriteerissä ”Turvallisuusalue”.
Toteutusesimerkki	
Lainsäädäntö	TLA 7 §, 9 §
Viitteet	Julkri: FYY-05; Katakri: F-06
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43

Tunniste	FYY-07.1, L:TL III, E:, S:, TS:
Nimi	Turva-alue - alueen raja ja rakenteet
Vaatimus	Alueella on oltava selkeästi määritelty näkyvä raja. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen säilytyksen edellyttämä turvallisuustaso.
Yleiskuvaus	Alueen aukot, joita ei käytetä kulkemiseen, on voitava lukita tai sulkea kalteroinnilla tai vahvoilla terässäleikköillä, jotta alueelle kulkua on mahdollista hallinnoida luotettavasti. Aukot on valvottava tunkeutumisen ilmaisujärjestelmällä, mikäli alueella ei ole henkilöstöä palveluksessa vuorokauden ympäri tai tiloja ei tarkasteta normaalin työajan päätteeksi ja satunnaisiin aikoihin työajan ulkopuolella. Alueen rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Alueen rajan ja rakenteiden olisi tällöin oltava betonia, terästä, tiiltä tai vahvaa puuta. Puutteelliset rakenteet, kuten normaali toimistorakenne on vahvennettava. Seinäelementtejä ei saa voida irrottaa kokonaisina tilan ulkopuolelta. Näitä vahvennuksia tulee arvioida suhteessa alueen ympäröivien tilojen antamaan muuhun suojaan sekä vartiointihenkilöstön vasteaikaan. Ovien rakenteita tarkastettaessa on kiinnitettävä huomiota karmin rakenteeseen, oven ja karmin välykseen, sekä karmien kiinnitykseen seinärakenteeseen. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, tulisi alueen seinien, lattian, katon, ikkunoiden ja ovien täyttää vähintään standardin SFS-EN-1627 luokkaa RC3 vastaava suoja. Suojauslasitus tulisi ensisijaisesti toteuttaa osana normaalia ikkunarakennetta. Jälkiasennettavia ratkaisuja tulee välttää. Hätäpoistumistiet eivät saa kulkea turva-alueen kautta. Mikäli hätäpoistumistien on välttämätöntä kulkea turva-alueen kautta, tulee varmistua, että hätäpoistumistie on varustettu tunkeutumisen ilmaisujärjestelmällä. Turva-aluetta, jonka läpi kulkee hätäpoistumistie ei voida hyväksyä, mikäli turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin tai alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua.
Toteutusesimerkki	Seinät ja ovet sekä lattia- ja kattorakenteet: SFS-EN 1627, RC1-RC6, tavoitetaso RC3; Ikkunat (suojauslasi): SFS-EN 356, P4A-P5A ja P6B-P8B, tavoitetaso P5A
Lainsäädäntö	TLA 9 § 1 mom 2 k
Viitteet	Katakri: F-06.1
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43

Tunniste	FYY-07.2, L:TL III, E:, S:, TS:
Nimi	Turva-alue - kulunvalvonta
Vaatimus	Alueen rajalla tulee valvoa kaikkea kulkua sisään ja ulos kulkulupien avulla tai tunnistamalla henkilöt henkilökohtaisesti.
Yleiskuvaus	Kulunvalvonta voidaan toteuttaa joko elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Alueen rajalla voidaan käyttää kaksipuoleista kulunvalvontaa. Suosituksena on käyttää kaksoistunnistusta sisään ja/tai ulos mentäessä. Kulunvalvontajärjestelmän etäyhteydet ja lukijalaitteiden asennus tulee toteuttaa riskienarvioinnin perusteella riittävän tietoturvallisesti siten, että järjestelmään pääsy on vain valtuutetuista päätelaitteista ja verkoista ja että tietoliikenneyhteys ja kulunvalvontajärjestelmän rajapinnat on suojattu siten, että ulkopuolisilla ei ole pääsyä välitettyihin tietoihin. Kulunvalvontajärjestelmän sijoitustilan tulisi sijaita sen suojaamalla turvallisuusalueella.

Toteutusesimerkki	Suositus kulunvalvonnan toteuttamisesta: - Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita. - Turva-alueen kulkuoikeudet myöntää nimetty vastuuhenkilö organisaatiossa - Kulunvalvonnan hallintajärjestelmän menettelytavat on ohjeistettu ja dokumentoitu: -- Myönnetyistä kulkuoikeuksista laaditaan dokumentti ja sitä ylläpitää nimetty vastuuhenkilö. -- Henkilöllä on vain ne kulkuoikeudet, joita hän tarvitsee työtehtäviensä hoitamiseksi. -- Kulkuoikeuden myöntämisperuste kirjataan dokumenttiin ja vain nimetyillä henkilöillä on kulkuoikeudet alueelle. -- Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa kulkuoikeuksiin. -- Organisaatioon kuuluvan henkilöstön ja ulkopuolisten henkilöiden luettelot pidetään erillään. -- Kulkuoikeudet katselmoidaan säännöllisin väliajoin esimerkiksi 6kk:n välein organisaatiosta nimetyn vastuuhenkilön toimesta. -- Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu, jos se on hyvin hallinnoitu -- Peruskäyttäjän työasemalta tapahtuva oven avaus turva-alueelle pitää olla estetty - Turva-alueelle kulkuoikeus on vain alueelle oikeutetulla henkilöllä. Kulku alueelle pitää olla myöhemmin todennettavissa. - Kulku tilaan pitää olla myöhemmin todennettavissa. - Tunnisteiden tulee käyttää nykyaikaista ja salattua lukutekniikkaa tai edellyttää kaksoistunnistusta Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia: Elektroniset kulunvalvontajärjestelmät: SFS-EN 60839-11-1 ja 2, luokat 1-4. Kameravalvontajärjestelmät: SFS-EN 62676, Suunnittelu Finanssialan K-menetelmän mukaisesti. Kameravalvontajärjestelmän tallenteiden säilymisaika määritellään riskiperusteisesti organisaation poikkeamien havainnointikyvyn mukaisesti huomioiden ennakoivat ja reagoivat menettelyt. Suositeltava vähimmäisaika tallenteille on 1 kk. Lisäksi kameravalvontajärjestelmä voidaan liittää tunkeutumisen ilmaisujärjestelmään.
Lainsäädäntö	TLA 9 § 1 mom 2 k
Viitteet	Katakri: F-06.2
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43
Tunniste	**FYY-07.3, L:TL III, E:, S:, TS:**
Nimi	Turva-alue - pääsyoikeuksien myöntäminen
Vaatimus	Itsenäinen pääsyoikeus alueelle voidaan myöntää vain organisaation asianmukaisesti valtuuttamalle henkilölle, jonka luotettavuus on varmistettu ja jolla on erityinen lupa tulla alueelle.
Yleiskuvaus	Luotettavuus tulisi ensisijaisesti varmistaa henkilöturvallisuusselvitysmenettelyn avulla. Alueelle pääsemisen perusteena tulisi olla tiedonsaantitarve. Tapauskohtaisesti erityinen lupa voi tarkoittaa myös työskentelytarvetta alueella. Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta.
Toteutusesimerkki	
Lainsäädäntö	TLA 9 § 1 mom 2 k
Viitteet	Julkri: FYY-05.4; Katakri: F-06.3
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 44

Tunniste	FYY-07.4, L:TL III, E:, S:, TS:
Nimi	Turva-alue - vierailijat
Vaatimus	Jos turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin: - alueella tavanomaisesti säilytettyjen tietojen korkein turvallisuusluokka on ilmoitettava selkeästi sekä - kaikilla vierailijoilla on oltava erityinen lupa tulla alueelle, heillä on aina oltava saattaja ja heidän luotettavuutensa on oltava varmistettu asianmukaisesti, paitsi jos on varmistettu, ettei vierailijoilla ole pääsyä turvallisuusluokiteltuihin tietoihin.
Yleiskuvaus	Kriteeri täydentää kaikkia turvallisuusalueita koskevaa kriteeriä ”Turvallisuusalue - Vierailijat”.
Toteutusesimerkki	
Lainsäädäntö	TLA 9 § 1 mom 2 k, 10 § 1 mom
Viitteet	Julkri: FYY-05.5; Katakri: F-06.4
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 44

Tunniste	FYY-07.5, L:TL III, E:, S:, TS:
Nimi	Turva-alue - turvallisuusohjeet
Vaatimus	Kullekin turva-alueelle on laadittava ohjeet noudatettavista turvallisuusmenettelyistä.
Yleiskuvaus	Turvallisuusohjeet kattavat turvallisuusluokiteltuun tietoon liittyvät prosessit ja turvallisuusalueet koko tiedon elinkaaren ajalta. Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti. Turvallisuusohjeiden ajantasaisuus sekä jalkautuminen varmistetaan säännöllisesti, vähintään vuosittain.
Toteutusesimerkki	Kullekin turva-alueelle on laadittava turvallisuusmenettelyt, joissa on ohjeet seuraavista asioista: a) Tiedon säilyttäminen ja käsitteleminen alueella: turvallisuusluokka tiedoille, joita alueella voidaan käsitellä ja säilyttää. b) Sovellettavat valvonta- ja suojatoimenpiteet. c) Pääsyoikeuksien myöntäminen alueelle: henkilöt, joilla on pääsy alueelle ilman saattajaa erityisen luvan ja luotettavuuden varmistamisen perusteella. d) Vierailijat: tarvittaessa menettelyt saattajien käyttämiseksi tai turvallisuusluokiteltujen tietojen suojaamiseksi silloin, kun muille henkilöille myönnetään pääsy alueelle. e) Muut asiaan kuuluvat toimenpiteet ja menettelyt.
Lainsäädäntö	TihL 4 § 2 mom; TLA 10 § 1 mom
Viitteet	Julkri: HAL-12; Katakri: F-06.5
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 45

Tunniste	FYY-07.6, L:TL III, E:, S:, TS:
Nimi	Turva-alue - tunkeutumisen ilmaisujärjestelmät
Vaatimus	Alue, jolla ei ole henkilöstöä palveluksessa vuorokauden ympäri, on tarvittaessa tarkastettava normaalin työajan päätteeksi ja satunnaisiin aikoihin työajan ulkopuolella, paitsi jos alueelle on asennettu tunkeutumisen ilmaisujärjestelmä (murtohälytysjärjestelmä).
Yleiskuvaus	Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet) ja/tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Alueen mahdollista tunkeutumisen ilmaisujärjestelmää tai korvaavaa järjestelyä arvioitaessa tulee ottaa huomioon alueen rakenteita koskevan vaatimuksen yhteydessä käsitelty vasteaika-arvio. Mikäli alue on valvottu tunkeutumisen ilmaisujärjestelmällä, alueen suositellaan olevan valvottu järjestelmän avulla, kun alueella ei työskennellä. Ilmoituksensiirto tulisi toteuttaa valvottuna tai kahdennettuna yhteytenä. Ilmoituksensiirtolaitteen avulla tulee siirtää vartioimisliikkeelle tai muuhun turvallisuusvalvomoon vähintään seuraavat tiedot: murto, päälle/pois, sabotaasi, vika. Järjestelmää tulee operoida henkilökohtaisen koodin avulla. Järjestelmän etäyhteydet ja hallintalaitteiden asennus tulee toteuttaa riskienarvioinnin perusteella riittävän tietoturvallisesti siten, että järjestelmään pääsy on vain valtuutetuista päätelaitteista ja verkoista ja että tietoliikenneyhteys ja tunkeutumisen ilmaisujärjestelmän rajapinnat on suojattu siten, että ulkopuolisilla ei ole pääsyä välitettyihin tietoihin. Tunkeutumisen ilmaisujärjestelmän sijoitustilan tulisi sijaita sen suojaamalla turvallisuusalueella. Alueen tunkeutumisen ilmaisujärjestelmän hallinta tulee olla organisaation omassa hallinnassa. Hallinta voi olla ulkoistettu riskien arvioinnin ja tehtävien eriyttämisen perusteella. Järjestelmän hallintaan, sen antamiin hälytyksiin ja vastetoimintaan liittyvät menettelyt tulee arvioida. Ilmoituksensiirron (1krt/kk) ja vasteajan (1krt/v) testaus tulee olla säännöllistä ja dokumentoitua. Vartiointihenkilöstön tulee olla kohdekoulutettu alueella toimimiseen. Vartiointihenkilöstön osaamisen ja työvälineiden tulee olla riittävät suhteessa toimintaympäristön riskeihin. Hälytystilanteessa alueelle voidaan edellyttää saapuvan kaksi henkilöä samanaikaisesti, mikäli turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin tai alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua.
Toteutusesimerkki	Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia: Tunkeutumisen ilmaisujärjestelmät: SFS-EN 50131, luokat 1 – 4, tavoitetaso 3; Tunkeutumisen ilmaisujärjestelmän ilmoituksensiirto: SFS-EN 50136-1, luokat DP1 - DP4 ja SP5 - SP6, tavoitetaso DP3-DP4 (dual path) tai SP5-SP6 (single path); Vartioimisliikkeen hälytyskeskus: SFS-EN 50518, Liikkeen on oltava standardin mukaisesti pätevä ja lisäksi ylläpidettävä SFS-EN ISO 9001:n mukaista sertifioitua laadunhallintajärjestelmää tai liikkeen tulee olla arvioitu soveltuvin osin tätä standardia vastaavaksi.
Lainsäädäntö	TLA 7 §, 9 § 1 mom 2 k
Viitteet	Katakri: F-06.7
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 45

Tunniste	FYY-07.7, L:TL III, E:, S:, TS:
Nimi	Turva-alue - säilytysyksiköiden avaimet ja pääsykoodit
Vaatimus	Säilytysyksiköiden avaimet tai pääsykoodit ovat sellaisten henkilöiden hallussa, joilla on tiedonsaantitarve säilytysyksikössä säilytettävään tietoon. Kyseisten henkilöiden on osattava numeroyhdistelmät ulkoa. Turvallisuusluokiteltuja tietoja sisältävien säilytysyksiköiden numeroyhdistelmät on vaihdettava: - tehdaskoodit on vaihdettava uuden turvallisen säilytyspaikan vastaanoton yhteydessä - aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos. - aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen. - kun jokin lukoista on huollettu tai korjattu.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 8 §, 9 § 1 mom 2, 10 § 1 mom
Viitteet	Katakri: F-06.10
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 46
Tunniste	**FYY-08, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Tietojen kuljettaminen
Vaatimus	1. Tiedot tulee kuljettaa tietojen riittävän suojaamisen huomioivia, organisaation ohjeita noudattaen. 2. Tiedot on pakattava niin, että ne on suojattu luvattomalta ilmitulolta. 3. Tietoja saa kuljettaa turvallisuusalueiden ulkopuolelle suojaamalla sähköiset tietovälineet riittävän turvallisella salauksella. 4. Salaamattomia tietoja voidaan kuljettaa postipalvelujen välityksellä.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; TLA 13 §
Viitteet	Julkri: TEK-16, FYY-02; Katakri: F-08.1
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 26–28

Tunniste	FYY-08.1, L:TL IV, E:, S:, TS:
Nimi	Tietojen kuljettaminen - TL IV
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokan IV tiedoille vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Tieto pakataan suljettavaan kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää turvallisuusluokasta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän turvallisuusluokiteltua tietoa (kirjekuoren tai vastaavan on oltava läpinäkymätön). 2) Tieto toimitetaan kotimaassa tavallisena postina, kirjattuna kirjeenä tai ko. turvallisuusluokalle hyväksytyn menettelyn mukaisesti. Ulkomaille toimitus postin välityksellä vain viranomaisen erillishyväksyntään pohjautuen. 3) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä. 4) Organisaatiossa on tunnistettu vaatimukset ja toteutettu menettelyt erityissuojattavien tietojen (esimerkiksi salausavaimet) välittämiseksi.
Lainsäädäntö	TLA 13 §
Viitteet	Katakri: F-08.1
Muita lisätietoja	

Tunniste	FYY-08.2, L:TL III, E:, S:, TS:
Nimi	Tietojen kuljettaminen - TL III
Vaatimus	Turvallisuusluokan II-III salaamaton tieto on kuljettamista varten pakattava asianmukaisesti sekä kuljetettava se jatkuvan valvonnan alaisuudessa vastaanottajalle. Mainitun tiedon saa kuljettaa vastaanottajalle myös muulla turvallisella tavalla, jolla tiedon luottamuksellisuus ja eheys varmistetaan kyseiselle turvallisuusluokalle riittävällä tavalla.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokkien III tiedoille vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraavat toimenpiteet: 5) Tieto pakataan suljettavaan kaksinkertaiseen kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää turvallisuusluokasta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän turvallisuusluokiteltua tietoa (kirjekuorien tai vastaavien on oltava läpinäkymättömiä). 6) Tieto toimitetaan ko. turvallisuusluokiteltuun tietoon oikeutetun organisaation henkilön toimesta jatkuvan valvonnan alaisuudessa vastaanottajalle. Vaihtoehtoisesti toimitus ko. turvallisuusluokalle hyväksytyn menettelyn mukaisesti. 7) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä turvallisuusselvitettyä henkilöstöä.
Lainsäädäntö	TLA 13 §
Viitteet	Katakri: F-08.1
Muita lisätietoja	

Tunniste	FYY-08.3, L:TL II, E:, S:, TS:
Nimi	Tietojen kuljettaminen - TL II
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokan II tiedoille vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraavat toimenpiteet: 8) Tieto pakataan suljettavaan kaksinkertaiseen kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää turvallisuusluokasta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän turvallisuusluokiteltua tietoa (kirjekuorien tai vastaavien on oltava läpinäkymättömiä). Sisäkuoren on oltava sinetöity. Vastaanottaja on ohjeistettava tarkistamaan sinetöinnin eheys ja ilmoitettava välittömästi, mikäli eheyden vaarantumista epäillään.
Lainsäädäntö	TLA 13 §
Viitteet	Katakri: F-08.1
Muita lisätietoja	
Tunniste	**FYY-09, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Tietojen kopioiminen
Vaatimus	Kopioihin ja käännöksiin sovelletaan alkuperäistä tietoa koskevia turvatoimia.
Yleiskuvaus	Tulostimet ja kopiokoneet tulkitaan tietojärjestelmiksi ja niiden tulee siten täyttää vaatimukset sekä teknisen, fyysisen että hallinnollisen tietoturvallisuuden osalta. Tekniset vaatimukset voi täyttää muun muassa erillislaiteratkaisulla.
Toteutusesimerkki	Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Kopioita käsitellään kuten alkuperäistä tietoa. 2) Kopion voi luovuttaa edelleen vain henkilölle, jolla on käsittelyoikeus tietoon ja tarve tietosisältöön. 3) Kopion/tulosteen saa ottaa vain ko. turvallisuustason vaatimukset täyttävällä laitteella.
Lainsäädäntö	TihL 13 § 1 mom; TLA 2 § 2 mom
Viitteet	Katakri: F-08.2
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28
Tunniste	**FYY-09.1, L:TL II, E:, S:, TS:**
Nimi	Tietojen kopioiminen - TL II
Vaatimus	Tietojen kopiot ja niiden käsittelijät on luetteloitava. Tietojen kopiointia varten on hankittava tiedon laatineen viranomaisen lupa.
Yleiskuvaus	
Toteutusesimerkki	Vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraava toimenpide: 4) Kopiointi ja käsittelijät merkitään diaariin/rekisteriin tai luetteloidaan jollakin muulla vastaavalla menettelyllä.
Lainsäädäntö	TLA 14 § 1 mom 3 ja 4 k
Viitteet	Katakri: F-08.2
Muita lisätietoja	

Tunniste	FYY-10, L:TL III, E:, S:, TS:
Nimi	Tietojen kirjaaminen
Vaatimus	Turvallisuusluokan III tai sitä korkeamman luokan tiedon vastaanottaminen ja lähettäminen tulee kirjata. Turvallisuusluokan III tietojen ja niitä korkeamman tason tietojen käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi).
Yleiskuvaus	Kirjaamisella tarkoitetaan sellaisten menettelyjen soveltamista, joilla rekisteröidään tiedon elinkaari, mukaan lukien sen jakelu ja hävittäminen. Jos kyseessä on tietojärjestelmä, kirjaamismenettelyt voidaan suorittaa järjestelmän omien prosessien avulla. Tiedon elinkaaren rekisteröinnin käytännön toteutukset edellyttävät tyypillisesti muun muassa tapahtumien jäljitettävyydestä varmistumista.
Toteutusesimerkki	
Lainsäädäntö	TLA 14 § 1 mom 1 ja 2 k
Viitteet	Katakri: F-08.3
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 19–23
Tunniste	**FYY-11, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Tietojen fyysinen tuhoaminen
Vaatimus	Ei-sähköisten tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.
Yleiskuvaus	Tiedon suojaamisesta tulee huolehtia tiedon elinkaaren päättymiseen asti. Tämä tulee huomioida erityisesti tilanteissa, joissa käytetään kolmannen osapuolen palvelua tiedon tuhoamiseen. Käytännön toteutusmallina yleensä menettely, jossa tiedosta vastuussa oleva organisaatio valvoo tiedon tuhoamisprosessin aina elinkaaren päättymiseen saakka. Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Käytettäessä hyväksyttyjä silppukokoja, voidaan silppuamisesta syntyvä jäte hävittää normaalin toimistojätteen mukaisesti. Tuhoamiseen voidaan käyttää silppuamisen korvaavana tai sitä tukevana suojauksena myös muita menetelmiä, joilla tietojen kokoaminen estetään luotettavasti (esimerkiksi paperisilpun polttaminen). Sähköisten aineistojen tuhoaminen on kuvattu erikseen kriteerissä TEK-21.
Toteutusesimerkki	
Lainsäädäntö	TihL 21 §; TLA 15 §
Viitteet	Julkri: TEK-21; Katakri: F-08.4
Muita lisätietoja	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 29–31

Tunniste	FYY-11.1, L:TL IV, E:, S:, TS:
Nimi	Tietojen fyysinen tuhoaminen - TL IV
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	- Paperiaineistojen silppukoko on enintään 30 mm2 (DIN 66399 / P5 tai DIN 32757 / DIN 4). - Magneettisten kiintolevyjen silppukoko on enintään 320 mm2 (DIN 66399 / H-5. - SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm2 (DIN 66399 / E-5). - Optisten medioiden silppukoko on enintään 10 mm2 (DIN 66399 / O-5).
Lainsäädäntö	TLA 15 §
Viitteet	Katakri: F-08.4
Muita lisätietoja	

Tunniste	FYY-11.2, L:TL III, E:, S:, TS:
Nimi	Tietojen fyysinen tuhoaminen - TL III
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	- Paperiaineistojen silppukoko on enintään 30 mm2 (DIN 66399 / P5 tai DIN 32757 / DIN 4). - Magneettisten kiintolevyjen silppukoko on enintään 10 mm2 (DIN 66399 / H-6). - SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm2 (DIN 66399 / E-5). - Optisten medioiden silppukoko on enintään 5 mm2 (DIN 66399 / O-6).
Lainsäädäntö	TLA 15 §
Viitteet	Katakri: F-08.4
Muita lisätietoja	

Tunniste	FYY-11.3, L:TL II, E:, S:, TS:
Nimi	Tietojen fyysinen tuhoaminen - TL II
Vaatimus	Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle. Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö.
Yleiskuvaus	
Toteutusesimerkki	- Paperiaineistojen silppukoko on enintään 10 mm2 (DIN 66399 / P6). - Magneettisten kiintolevyjen silppukoko on enintään 10 mm2 (DIN 66399 / H-6). - SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 1 mm2 (DIN 66399 / E-6). - Optisten medioiden silppukoko on enintään 5 mm2 (DIN 66399 / O-6).
Lainsäädäntö	TLA 15 §
Viitteet	Katakri: F-08.4
Muita lisätietoja	

4 Tekninen turvallisuus

Tekninen osa-alue kattaa tietojärjestelmien ja tietoliikenneyhteyksien teknisiin ominaisuuksiin, turvalliseen käyttöön ja toimintamalleihin liittyvät kriteerit. Kriteerien tavoitteena on varmistaa, että tietojärjestelmät ja niiden käyttö toteuttavat yleiset teknisen tietoturvallisuuden, ja tarvittaessa myös tietosuojan, vaatimukset. Huomioitavaa kuitenkin on, että teknisen osa-alueen kriteerien toteuttaminen ei yksinään takaa yksittäisen tietojärjestelmän turvallisuutta, vaan myös muiden osa-alueiden kriteerit tulee huomioida.

Arvioinnin kohteena voi olla joko yksittäinen tietojärjestelmä tai tietojenkäsittely-ympäristö tai laajempi kokonaisuus tietojärjestelmiä. Arvioitaessa useista tietojärjestelmistä koostuvaa kokonaisuutta, tulee huomioida vaatimusten toteutuminen kaikissa yksittäisissä järjestelmissä.

Tekninen osa-alue ottaa huomioon myös järjestelmien sijoittumisen turvallisuusalueille ja niiden etäkäytön turvallisuusalueiden ulkopuolella. Tarkemmat vaatimukset hallinnolliselle alueelle ja turva-alueelle on määritelty fyysisen turvallisuuden osa-alueella.

Kriteeristössä viitataan usean kriteerin osalta, että salausratkaisun tulee olla riittävän turvallinen kyseiseen käyttötapaukseen. Salausratkaisun turvallisuuden arvioinnissa voi käyttää hyväksi esimerkiksi Kyberturvallisuuskeskuksen NCSA-toiminnon kansainvälisen turvallisuusluokitellun tiedon suojaamiseksi myöntämiä hyväksyntöjä. Lisätietoja on saatavilla Kyberturvallisuuskeskuksen verkkosivuilta.

Tunniste	TEK-01, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Verkon rakenteellinen turvallisuus
Vaatimus	Tietojenkäsittely-ympäristö on erotettu julkisista tietoverkoista ja muista heikomman turvallisuustason ympäristöistä riittävän turvallisella tavalla.
Yleiskuvaus	Tietojärjestelmien erottelu on eräs vaikuttavimmista tekijöistä salassa pidettävän tiedon suojaamisessa. Erottelun tavoitteena on rajata salassa pidettävän tiedon käsittely-ympäristö hallittavaksi kokonaisuudeksi, ja erityisesti pystyä rajaamaan salassa pidettävän tiedon käsittely vain riittävän turvallisiin ympäristöihin. Ylemmän turvallisuusluokan käsittely-ympäristössä on mahdollista käsitellä myös matalamman luokan tietoja, edellyttäen, että käsittely toteutetaan kokonaisuudessaan ylemmän turvallisuusluokan suojausten mukaisesti. Erottelu voidaan toteuttaa esimerkiksi palomuuriratkaisun avulla. Internet, sekä operaattorin tarjoamat MPLS-verkot ja esimerkiksi niin sanotut mustat kuidut (dark fiber) tulkitaan julkisiksi verkoiksi.
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 1 k
Viitteet	Katakri: I-01
Muita lisätietoja	Traficom: Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista (2.12.2021); ISO/IEC 27002:2022 8.20, 8.22; Tiedonhallintalautakunta: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2020:19, luku 6); PiTuKri TT-01
Tunniste	**TEK-01.1, L:Salassa pidettävä, E:Kriittinen, S:, TS:Henkilötieto**
Nimi	Verkon rakenteellinen turvallisuus - salaus yleisissä tietoverkoissa
Vaatimus	Yleisessä tietoverkossa salassa pidettävää tietoa sisältävä tietoliikenne salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia tai vaihtoisesti siirto toteutetaan muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä.
Yleiskuvaus	Käytettävien salausvahvuuksien ja -asetusten valinnassa voidaan hyödyntää lähtökohtaisesti turvallisuusluokan IV mukaisia vahvuuksia ja asetuksia.
Toteutusesimerkki	
Lainsäädäntö	TihL 14 §; TLA 12 § ja 11 §:n 1 mom 7 k
Viitteet	Julkri: FYY-7.1; Katakri: I-01, I-12, I-15
Muita lisätietoja	ISO/IEC 27002:2022 8.24
Tunniste	**TEK-01.2, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Verkon rakenteellinen turvallisuus - palomuuri
Vaatimus	Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuustasojen ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 §:n 1 mom 1 ja 2 k
Viitteet	Katakri: I-01
Muita lisätietoja	PiTuKri TT-01

Tunniste	TEK-01.3, L:TL IV, E:, S:, TS:
Nimi	Verkon rakenteellinen turvallisuus - käsittely-ympäristöjen erottaminen
Vaatimus	Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokittelemattoman salassa pidettävän tiedon sekä myös turvallisuusluokan IV tietojenkäsittely-ympäristön yhdistäminen eri turvallisuusluokan ympäristöihin voidaan toteuttaa palomuuriratkaisuilla ja rajaamalla riskialttiiden alemman turvallisuusluokan ympäristöä käyttävien palvelujen (web-selailu, Internetin kautta reitittyvä sähköposti, ja vastaavat) liikenne kulkemaan erillisten sisältöä suodattavien välityspalvelinten kautta. Turvallisuusluokittelemattoman salassa pidettävän sekä myös turvallisuusluokan IV käsittely-ympäristöjä on mahdollista kytkeä Internetiin ja muihin ei-luotettuihin verkkoihin, edellyttäen että kytkennän tuomia riskejä pystytään muilla suojauksilla pienentämään riittävästi. Internet-kytkentäisyyden tuomien riskien pienentäminen turvallisuusluokittelemattomalle salassa pidettävälle tiedolle sekä turvallisuusluokalle IV edellyttää erityisesti ohjelmistopäivityksistä huolehtimista, vähimpien oikeuksien periaatteen mukaisia käyttöoikeuksia, järjestelmäkovennuksia sekä kykyä poikkeamien havainnointiin ja korjaaviin toimiin. Tyypillinen käyttötapa turvallisuusluokittelemattoman salassa pidettävän tai/ja turvallisuusluokan IV käsittely-ympäristölle on organisaation rajattu tietojenkäsittely-ympäristön osa, joka voi muodostua esimerkiksi päätelaitepalveluista, sovelluspalveluista, tietoliikennepalveluista sekä niiden suojaamiseen liittyvistä järjestelyistä.
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 1 ja 2 k
Viitteet	Katakri: I-01, I-06, I-08, I-11, I-19
Muita lisätietoja	

Tunniste	TEK-01.4, L:TL IV, E:, S:, TS:
Nimi	Verkon rakenteellinen turvallisuus - salaaminen turva-alueiden ulkopuolella
Vaatimus	Hallitun fyysisen turvallisuusalueen ulkopuolelle menevä liikenne salataan riittävän turvallisella salausratkaisulla.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Katakri: I-01
Muita lisätietoja	

Tunniste	TEK-01.5, L:TL III, E:, S:, TS:
Nimi	Verkon rakenteellinen turvallisuus - yhdyskäytäväratkaisun käyttö
Vaatimus	Turvallisuusluokat III-II: Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää riittävän turvallisen yhdyskäytäväratkaisun käyttöä.
Yleiskuvaus	Tietojenkäsittely-ympäristöjen oletetaan lähtökohtaisesti olevan toisilleen ei-luotettuja myös tilanteissa, joissa yhdistetään eri organisaatioiden hallinnoimia tietojenkäsittely-ympäristöjä toisiinsa. Saman turvallisuusluokan käsittely-ympäristöjä voidaan liittää toisiinsa ko. turvallisuusluokalle riittävän turvallisen salausratkaisun avulla (esimerkiksi organisaation eri toimipisteiden ko. turvallisuusluokan käsittely-ympäristöjen yhteenliittäminen julkisen verkon ylitse). Huom. Turvallisuusluokan ylitys hallintaliikenteen osalta edellyttää ko. turvallisuusluokalle riittävän turvallisen yhdyskäytäväratkaisun käyttöä. Käytännössä hallintaliikenne rajataankin lähes poikkeuksetta turvallisuusluokittain. Hallintaliikenteen suojausperiaatteet on käsitelty yksityiskohtaisemmin TEK-04.

Toteutusesimerkki	Turvallisuusluokasta III lähtien yhdistäminen eri turvallisuusluokkien ympäristöihin voidaan toteuttaa riittävän turvallisilla yhdyskäytäväratkaisuilla. Yhdyskäytäväratkaisun tulee luotettavasti estää ylemmän turvallisuusluokan tiedon kulkeutuminen matalamman turvallisuusluokan ympäristöön. Turvallisten, hyväksyttävissä olevien yhdyskäytäväratkaisujen suunnitteluperiaatteita ja yleisiä ratkaisumalleja on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa (www.ncsa.fi > ”Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista”). Turvallisuusluokan III käsittely-ympäristöt ovat moniportaisesti loogisesti tai fyysisesti ei-luotetuista verkoista/järjestelmistä eristettyjä kokonaisuuksia. Fyysisellä eristämisellä tarkoitetaan OSI-mallin fyysisen kerroksen tasolla tapahtuvaa erottelua. Turvallisuusluokan III käsittely-ympäristöihin ei pääsääntöisesti kytketä mitään muita verkkoja tai järjestelmiä. Mikäli loppukäyttäjän työtehtävät edellyttävät pääsyä Internetiin tai muihin eri turvallisuusluokan järjestelmiin tai verkkoihin, se on yleensä perustelluinta järjestää erillisellä tietokoneella, jota ei kytketä turvallisuusluokan III verkkoon. Tapauskohtaisesti on mahdollista hyväksyä myös turvallisuusluokan III käsittely-ympäristön fyysisen kytkeminen erikseen tarkastettuun ja hyväksyttyyn verkkoon tai järjestelmään. Tällaiset erikseen hyväksytyt verkot tai järjestelmät jakautuvat yleisimmin neljään käyttötilanteeseen: A. Tiedonsiirtojärjestelmät Turvallisuusluokan III järjestelmä/verkko voi olla tiedonsiirtojärjestelmä kahden tai useamman fyysisen pisteen välillä. Tällöin jokaisen kytketyn pisteen tulisi olla turvallisuustasoltaan vastaavalla tasolla. Verkkotason rajapinta on useimmiten muotoa [fyysisesti eristetty verkko/työasema] - [palomuurilaitteisto/-ohjelmisto] – [turvallisuusluokalle hyväksytty salauslaite] - [palomuurilaitteisto/-ohjelmisto] - [Internet] – [palomuurilaitteisto/-ohjelmisto] - [turvallisuusluokalle hyväksytty salauslaite] - [palomuurilaitteisto/-ohjelmisto] - [fyysisesti eristetty verkko/työasema]. Vastaavilla järjestelyillä voidaan toteuttaa myös turvallisuusluokan II mukainen ratkaisu. B. Palvelujärjestelmät Turvallisuusluokan III järjestelmä/verkko voi olla esimerkiksi tietokantapalvelu, jota käytetään useasta fyysisestä pisteestä. Verkkotason rajapinta on tällöin vastaava kuin käyttötilanne A:ssa. C. Yhdyskäytäväratkaisut C1. Turvallisuusluokan III tiedon käsittely-ympäristöön voidaan siirtää tietoa alemman turvallisuusluokan ympäristöstä yksisuuntaisen liikenteen sallivan yhdyskäytäväratkaisun (esim. datadiodi) kautta. Vastaavilla järjestelyillä voidaan toteuttaa myös turvallisuusluokan II mukainen ratkaisu. Turvallisuusluokkien IV ja III väliseen liikennöintiin voidaan hyödyntää myös alkiotunnistukseen perustuvaa sisältösuodatusratkaisua (Vrt. kohta C2 alla). C2. Turvallisuusluokan III tiedon käsittely-ympäristöstä voidaan siirtää matalamman turvallisuusluokan tietoa matalamman turvallisuusluokan ympäristöön alkiotunnistukseen perustuvan sisältösuodatusratkaisun kautta. Sisältösuodatusratkaisun käyttö edellyttää tiedon tunnistamista ylemmän tason ympäristössä, ja vain matalamman tason tiedon siirtymisen sallimista ylemmän turvallisuusluokan ympäristöstä matalamman tason ympäristöön. D. Muut käsittely-ympäristöt Muut turvallisuusluokan III käsittely-ympäristöt ovat yleisimmin organisaation tuotekehitysverkkoja tai muita turvallisuusluokan III tiedon käsittely-ympäristöjä. Tällaisiin järjestelmiin voidaan kytkeä esimerkiksi vain tätä ympäristöä palveleva päivityspalvelin. Päivityspalvelimelta voidaan sallia keskitetty turvapäivitysten ja haittaohjelmatunnisteiden jakelu tietyin rajauksin. Jaeltavat päivitykset ja tunnistekannat voidaan tuoda päivityspalvelimelle ilmaraon yli, tai vaihtoehtoisesti esimerkiksi datadiodin läpi.
Lainsäädäntö	TLA 11 § 1 mom 1 ja 2 k
Viitteet	Julkri: TEK-04; Katakri: I-01
Muita lisätietoja	

Tunniste	TEK-01.6, L:TL II, E:, S:, TS:
Nimi	Verkon rakenteellinen turvallisuus - TL II käsittely
Vaatimus	Turvallisuusluokan II käsittely-ympäristöt ovat lähtökohtaisesti fyysisesti eristettyjä kokonaisuuksia.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokan ylittävä liikennöinti voidaan sallia vain datadiodien tai vastaavien OSI-mallin fyysisellä kerroksella toimivien yksisuuntaisten yhdyskäytäväratkaisujen kautta.
Lainsäädäntö	TLA 11 § 1 mom 1 ja 2 k
Viitteet	Katakri: I-01
Muita lisätietoja	

Tunniste	TEK-01.7, L:TL I, E:, S:, TS:
Nimi	Verkon rakenteellinen turvallisuus - TL I käsittely
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Lähtökohtaisesti turvallisuusluokan I tietojenkäsittely-ympäristöt suositellaan pidettäväksi fyysisesti eriytettyinä kaikista muista ympäristöistä. Tyypillisenä toteutustapana on fyysisellä turva-alueella, hajasäteilysuojatussa tilassa tapahtuva kaikista muista ympäristöistä fyysisesti eriytetty tietojenkäsittely tähän tarkoitukseen varatulla päätelaitteella. Toteutustapana voi olla myös vastaavasti turva-alueella hajasäteilysuojattuun tilaan fyysisesti sijoitettu ja muista ympäristöistä fyysisesti eriytetty päätelaitteista, niitä yhdistävästä paikallisesta verkosta ja tähän tarkoitukseen varatusta erillistulostimesta koostuva tietojenkäsittely-ympäristö. Tiedonsiirto fyysisesti eriytettyihin ympäristöihin tulee toteuttaa siten, että riski turvallisuusluokan I tiedon kulkeutumiseen matalamman turvallisuusluokan ympäristöön saatetaan mahdollisimman pieneksi. Tyypillisenä toteutustapana on kertakäyttöisten optisten medioiden hyödyntäminen tiedonsiirroissa matalamman turvallisuusluokan ympäristöstä ylemmän turvallisuusluokan ympäristöön. Mikäli turvallisuusluokan I tietojenkäsittely-ympäristö on toiminnallisten tarpeiden näkökulmasta ehdottoman välttämätöntä yhdistää matalamman turvallisuusluokan ympäristöön, tulisi yhdistäminen tapahtua turvallisuusluokalle I hyväksytyn yhdyskäytäväratkaisun kautta. Turvallisuusluokan I tietojenkäsittely-ympäristöjen erotteluun hyväksyttyjä yhdyskäytäväratkaisuja on saatavilla rajoitetusti, keskittyen tyypillisesti vain yksisuuntaisen liikennöinnin (TL II --> TL I) mahdollistavien datadiodiratkaisujen moniportaisiin ratkaisumalleihin. Yhdyskäytäväratkaisuja on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa.
Lainsäädäntö	TLA 11 § 1 mom 1 ja 2 k
Viitteet	Katakri: I-01
Muita lisätietoja	

Tunniste	TEK-02, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä
Nimi	Tietoliikenne-verkon vyöhykkeistäminen
Vaatimus	Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava monitasoisen suojaamisen periaatteen mukaisesti.
Yleiskuvaus	Tietoliikenneverkon jakaminen ko. turvallisuusluokan sisällä erillisille verkkoalueille (vyöhykkeet ja segmentit) voi tarkoittaa esimerkiksi tietojen suojaamisen näkökulmasta tarkoituksenmukaista työasema- ja palvelinerottelua, kattaen myös mahdolliset hankekohtaiset erottelutarpeet. Kaikkia liitettyjä tietotekniikkajärjestelmiä tulisi lähtökohtaisesti käsitellä epäluotettavina ja varautua yleisiin verkkohyökkäyksiin. Yleisiin verkkohyökkäyksiin varautumiseen sisältyy esimerkiksi vain tarpeellisten toiminnallisuuksien pitäminen päällä. Toisin sanoen jokaiselle päällä olevalle toiminnallisuudelle tulisi olla perusteltu toiminnallinen tarve. Toiminnallisuus tulisi rajata suppeimpaan toiminnalliset vaatimukset täyttävään osajoukkoon (esimerkiksi toiminnallisuuksien näkyvyyden rajaus). Lisäksi tulisi ottaa huomioon esimerkiksi osoitteiden väärentämisen (spoofing) estäminen ja verkkojen näkyvyyden rajaaminen.
Toteutusesimerkki	Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Tietoliikenneverkko on jaettu ko. turvallisuusluokan sisällä erillisiin verkkoalueisiin (vyöhykkeet, segmentit). 2) Verkko-alueiden välistä liikennettä rajoitetaan ja ympäristöön sisäänpäin tulevaan liikenteeseen noudatetaan default-deny sääntöä. 3) Tietojenkäsittely-ympäristössä on varauduttu yleisiin verkkohyökkäyksiin.
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 1 ja 2 k
Viitteet	Katakri: I-02
Muita lisätietoja	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02

Tunniste	TEK-02.1, L:TL IV, E:, S:, TS:
Nimi	Tietoliikenne-verkon vyöhykkeistäminen - vähimpien oikeuksien periaate
Vaatimus	Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien periaatteen mukaisesti ko. turvaluokan sisällä.
Yleiskuvaus	Verkkoalueiden välisen liikenteen valvonnan ja rajoittamisen voi toteuttaa turvallisuusluokan IV verkon ulkorajalla esimerkiksi siten, että kaikki sisäänpäin tulevat yhteydenavausyritykset estetään ja ulospäin lähtevät yhteydet rajataan vain välityspalvelimen kautta tulevaan web-selailuun sekä sähköpostiliikenteeseen. Kaikkien turvallisuusluokkien verkoissa riittävä vähimpien oikeuksien periaatteen huomiointi edellyttää tyypillisesti myös sitä, että turvallisuusluokan sisällä eri verkkoalueiden välillä sallitaan vain tarpeelliset yhteydet (lähde-kohde-protokolla) ja että muut yhteysyritykset havaitaan. Kyseisen luokan ympäristön sisällä suojauksia voidaan täydentää ja tukea myös niin sanotulla Zero Trust -lähestymistavalla, jossa eri toimijoiden toimintamahdollisuuksia voidaan rajoittaa ja valvoa erityisesti toimijoiden ja toiminteiden tunnistamiseen ja todentamiseen pohjautuen. Tulee kuitenkin huomioida, että Zero Trust -lähestymistapa ei korvaa eri suojaustarpeen/luokan tietojenkäsittely-ympäristöjen riittävän luotettavan erottelun vaatimusta (vrt. TEK-01.3 ja TEK-01.5). Zero Trust -lähestymistavan toteuttamisessa keskeisessä roolissa on tietojenkäsittely-ympäristön toimijoiden (käyttäjien ja laitteiden) tunnistaminen ja todentaminen, sekä riittävä salaaminen toimijoiden välisessä tietoliikenteessä. Kytkentöjen ja konfiguraatioiden turvallisesta toiminnasta tulee varmistua säännöllisesti, vrt. TEK-03. Turvallisuusluokalla IV tulisi myös ottaa huomioon palvelunestohyökkäyksen uhka, mikäli järjestelmä liitetään ei-luotettuun verkkoon. Suodatusten tulisi perustua vähimpien oikeuksien periaatteeseen ja suodatuksen tulisi sallia vain erikseen hyväksytty liikennöinti (default-deny). Suodatuksissa tulisi huomioida myös eri protokollien (esim. IPv4, IPv6, GRE, IPSec-tunnelit, reititysprotokollat, sekä myös ylempien kerrosten protokollat, esim. HTTP, SSH, FTP ja SMTP) toiminnallisuudet. Tarpeettomat protokollat tulisi poistaa käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa niille ei ole todellista käyttöperustetta, ja varmistettava liikennöinnin estyminen (verkko-, työasema- ja palvelintason) palomuurien suodatussäännöillä. Mikäli työasemissa, palvelimissa, verkkolaitteissa tai muissa vastaavissa järjestelmissä käytetään esimerkiksi IPv6-toiminnallisuutta, tulisi ottaa huomioon sen vaikutukset erityisesti liikenteen suodatukseen (palomuurauksen tulisi kattaa myös IPv6-liikenne) sekä reititykseen. Myös eri protokollien yhdistämis- ja yhteiskäyttöratkaisujen (esim. IPv4-IPv6-toteutukset, NAT-64, Teredo) vaikutukset tulisi ottaa huomioon verkon/järjestelmien turvallisuuden kokonaissuunnittelussa.
Toteutusesimerkki	Turvallisuusluokkien IV-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan aiemmin mainittujen toimenpiteiden lisäksi: 4) Verkko-alueiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti sallitaan (default-deny).
Lainsäädäntö	TLA 11 § 1 mom 1 ja 2 k
Viitteet	Julkri: TEK-03; Katakri: I-02
Muita lisätietoja	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02

Tunniste	TEK-03, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä
Nimi	Suodatus- ja valvontajärjestelmien hallinnointi
Vaatimus	Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan.
Yleiskuvaus	Liikennettä suodattavia ja/tai valvovia järjestelmiä ovat tyypillisesti palomuurit, reitittimet, IDS- ja IPS-järjestelmät sekä vastaavia toiminnallisuuksia sisältävät verkkolaitteet, palvelimet ja sovellukset. Riittävän dokumentaation toteutus edellyttää yleensä esimerkiksi verkkorakenteen kuvaamista verkkoalueineen (vyöhykkeet ja segmentit) sillä tarkkuudella, että dokumentaation pohjalta voidaan tarkastaa verkon vastaavan dokumentoitua, riittävän turvallista rakennetta. Käytettävyyden ja riittävän dokumentoinnin varmistamisen kannalta tarkoituksenmukainen ratkaisu on usein suodatus- ja valvontajärjestelmien asetusten (konfiguraatioiden, ml. esimerkiksi palomuurisäännöstöt) varmuuskopiointi, ja varmuuskopioiden turvallisuusluokan mukainen säilytys. Asetusten ja halutun toiminnan tarkasteluun hyväksyttävissä oleva tarkastustiheys riippuu erityisesti kohteessa tapahtuvien muutosten tiheydestä ja kohteen laajuudesta. Esimerkiksi organisaation turvallisuusluokan IV tietojenkäsittely-ympäristön palomuurisäännöstöt voivat olla laajoja ja muutoksia voi olla tarve tehdä usein. Tällaisissa ympäristöissä riittävä tarkastustiheys voi olla esimerkiksi vuosineljänneksittäin tai puolivuosittain. Toisaalta sellaisissa suppeissa ympäristöissä, missä suodatussäännöstöihin ei ole tarve tehdä muutoksia kuin hyvin harvoin, voi riittää vuosittaiset tarkastukset. Suodatus- tai valvontaohjelmiston toiminnallisuuksiin voi tulla muutoksia tai uusia ominaisuuksia myös säännöllisesti tehtävissä ohjelmistopäivityksissä. Suodatussäännöstön ja muun toiminnallisuuden oikeellisuus onkin perusteltua varmistaa myös säännöllisesti asennettavien ohjelmistopäivitysten yhteydessä. Uusien ominaisuuksien (esimerkiksi hienojakoisemman suodatuksen) hyödyntämismahdollisuudet ja käyttöönotto tulee arvioida osana muutostenhallintaa (vrt. I-16).
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 2 k
Viitteet	Katakri: I-03
Muita lisätietoja	ISO/IEC 27002:2022 8.21, 8.23

Tunniste	TEK-03.1, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä
Nimi	Suodatus- ja valvontajärjestelmien hallinnointi - vastuutus ja organisointi
Vaatimus	Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen, poistaminen ja valvonta on vastuutettu ja organisoitu.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 4 § 2 mom 1 k; TLA 11 § 1 mom 2 k
Viitteet	Katakri: I-03, I-16
Muita lisätietoja	ISO/IEC 27002:2022 5.35, PiTuKri MH-01

Tunniste	TEK-03.2, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä
Nimi	Suodatus- ja valvontajärjestelmien hallinnointi - dokumentointi
Vaatimus	Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 5 § 2 mom; TLA 11 § 1 mom 2 k
Viitteet	Julkri: HAL-09; Katakri: I-03
Muita lisätietoja	

Tunniste	TEK-03.3, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä
Nimi	Suodatus- ja valvontajärjestelmien hallinnointi - tarkastukset
Vaatimus	Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 2 k
Viitteet	Katakri: I-03
Muita lisätietoja	ISO/IEC 27002:2022 8.32

Tunniste	TEK-04, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Hallintayhteydet
Vaatimus	Hallintapääsy tapahtuu rajattujen, hallittujen ja valvottujen pisteiden kautta.
Yleiskuvaus	Laitteilla/liittymillä tarkoitetaan alla kuvatuissa toteutusesimerkeissä järjestelmiä, joihin pitäisi olla hallintaoikeudet vain ylläpitäjillä tai vastaavilla. Tällaisia ovat tyypillisesti esimerkiksi palomuurit, reitittimet, kytkimet, langattomat tukiasemat, palvelimet, työasemat, erilliset konsoliliittymät (esim. iLO, iDrac) ja Blade-runkojen hallintaliittymät. Hallintayhteyksien suojausten arvioinnissa tulisi huomioida erityisesti se, miltä osin ko. hallintayhteyden kautta pystytään vaarantamaan salassa pidettävät tiedot. Useimmat hallintayhteystavat mahdollistavat pääsyn salassa pidettävään tietoon joko suoraan (esimerkiksi tietokantaylläpito pääsee yleensä tarvittaessa tietokannan sisältöön) tai epäsuoraan (esimerkiksi verkkolaiteylläpito pystyy yleensä muuttamaan tietojärjestelmää suojaavia palomuurisääntöjä), mikä tekee näistä erityisen houkuttelevan kohteen myös pahantahtoisille toimijoille. Erityisesti tilanteissa, joissa hallintayhteys mahdollistaa suoran tai epäsuoran pääsyn turvallisuusluokiteltuun tietoon, tulisi hallintayhteys ja siihen käytettävät päätelaitteet rajata lähtökohtaisesti samalle turvallisuusluokalle, kuin mitä ko. tietojenkäsittely-ympäristökin. Matalamman tason ympäristön hallinta voi tietyissä erityistapauksissa olla mahdollista ylemmän turvallisuusluokan hallintaympäristöstä käsin, edellyttäen, että turvallisuusluokkien rajoilla on riittävän turvallinen yhdyskäytäväratkaisu, joka estää ylemmän turvallisuusluokan tietojen kulkeutumisen matalamman turvallisuusluokan ympäristöön. Erityisesti yhteysprotokollien ohjelmistohaavoittuvuuksista johtuen matalamman tason ympäristöjen hallintamahdollisuudet rajautuvat riskiperusteisesti tyypillisesti vain turvallisuusluokan IV ympäristöistä tapahtuvaan matalamman tason ympäristöjen hallintaan. Ylemmän turvallisuusluokan ympäristön hallinta ei lähtökohtaisesti ole hallintaliikenteen turvallisuuskriittisestä luonteesta johtuen mahdollista matalamman turvallisuusluokan ympäristöistä. Ylemmän turvallisuusluokan ympäristöstä voidaan riittävän turvallisen yhdyskäytäväratkaisun kautta tarjota joissain tapauksessa (read-only) valvontapääsy luokkaa matalamman turvallisuusluokan ympäristöön. Riittävän jäljitettävyyden toteuttamisessa voidaan hyödyntää ko. turvallisuusluokan sisällä esimerkiksi niin sanottua hyppykonekäytäntöä, jossa kaikki hallintatoimet toteutetaan äärimmilleen kovennettujen, järjestelmä- ja roolikohtaisten hyppykoneiden kautta mahdollistaen samalla kattavan jäljitettävyyden (lokituksen, vrt. TEK-12). Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa: - Pilvipalveluympäristöissä etähallinta on yleensä tyypillisin hallintamenettely sekä itse pilvipalvelualustan, että asiakkaan järjestelmien osalta. Etähallinnaksi tulkitaan esimerkiksi pilvipalveluntarjoajan ylläpitotoimet, jotka tapahtuvat fyysisesti suojatun konesaliympäristön ulkopuolelta käsin. Etähallinnaksi tulkitaan myös pilvipalvelun asiakkaan, omalle vastuulleen kuuluvaan järjestelmäosaan kohdistuvat ylläpitotoimet. - Hallintayhteyksien suojausten arvioinnissa tulisi huomioida erityisesti se, miltä osin ko. hallintayhteyden kautta pystytään vaarantamaan pilvipalvelussa käsiteltävät tiedot. Useimmat hallintayhteystavat mahdollistavat pääsyn tietoon joko suoraan (esimerkiksi tietokantaylläpito pääsee yleensä tarvittaessa tietokannan sisältöön) tai epäsuoraan (esimerkiksi verkkolaiteylläpito pystyy yleensä muuttamaan tietojärjestelmää suojaavia palomuurisääntöjä). Hallintayhteyksiin tulkitaan kuuluvaksi lähtökohtaisesti kaikki yhteystavat, joilla on mahdollista vaikuttaa salassa pidettävien tietojen suojauksiin. Hallintayhteyksiin kuuluvat tyypillisesti myös pilvipalvelun asiakkaalle tarjottavat web-konsolit/-portaalit ja vastaavat etähallintayhteydet. - Erityisesti tilanteissa, joissa hallintayhteys mahdollistaa suoran tai epäsuoran pääsyn salassa pidettävään tietoon, tulee hallintayhteys ja siihen käytettävät päätelaitteet rajata lähtökohtaisesti samalle suojaus-/turvatasolle, kuin mitä ko. tietojenkäsittely-ympäristökin. Turvallisuusluokitellun tiedon käsittelyyn käytetyn ympäristön hallinta ei lähtökohtaisesti ole hallintaliikenteen turvallisuuskriittisestä luonteesta johtuen mahdollista heikommin suojatuista ympäristöistä tai päätelaitteistä käsin. Turvallisuusluokiteltua tietoa sisältävän pilvipalvelualustan hallinnointi tuleekin rajata kyseisen turvallisuusluokan vaatimukset täyttäviin päätelaitteisiin. Huomioitava, että myös päätelaitteiden hallinnointiratkaisujen ja muiden niihin kytkeytyvien taustajärjestelmien tulee täyttää kyseisen turvallisuusluokan vaatimukset, kuten myös fyysiset tilat/alueet, joista hallintaa suoritaan. - Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.
Toteutusesimerkki	Rajattu pääsy tulee toteuttaa esimerkiksi hyppykoneiden, hallintaportaalien ja vastaavien menettelyiden kautta.

Lainsäädäntö	TihL 13 § 1 mom, 14 § 1 mom; TLA 11 § 1 mom
Viitteet	Julkri: TEK-12; Katakri: I-04
Muita lisätietoja	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
Tunniste	**TEK-04.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Hallintayhteydet - vahva tunnistaminen julkisessa verkossa
Vaatimus	Hallintapääsyn julkisesta verkosta tai muun käytettävän etähallintaratkaisun tulee edellyttää vahvaa, vähintään kahteen todennustekijään pohjautuvaa käyttäjätunnistusta.
Yleiskuvaus	Hallintayhteyksien suojaus on eräs kriittisimmistä tietojärjestelmien turvallisuuteen vaikuttavista tekijöistä. Erityisesti turvallisuusluokittelemattomia salassa pidettäviä sekä turvallisuusluokan IV järjestelmiä voi kuitenkin olla perusteltua pystyä hallinnoimaan myös fyysisesti suojattujen turvallisuusalueiden ulkopuolelta. Tilanteissa, joissa etähallinta nähdään perustelluksi, suositellaan se suojattavan etäkäyttöä kattavammilla turvatoimilla. Esimerkiksi turvallisuusluokan IV järjestelmän etähallintayhteydet voidaan rajata yksittäisiin fyysisiin ja loogisiin pisteisiin.
Toteutusesimerkki	Hallintayhteydet julkisesta verkosta edellyttävät esimerkiksi VPN-yhteyden muodostamista, jossa vähintään joko käyttäjä tai laite tunnistetaan vahvasti.
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 5 k
Viitteet	Katakri: I-04
Muita lisätietoja	ISO/IEC 27002:2022 8.2; PiTuKri IP-03
Tunniste	**TEK-04.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Hallintayhteydet - hallintayhteyksen salaaminen
Vaatimus	Hallintaliikenne julkisessa verkossa on salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 4 ja 7 k
Viitteet	Katakri: I-04
Muita lisätietoja	ISO/IEC 27002:2022 8.24
Tunniste	**TEK-04.3, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Hallintayhteydet - vähimmät oikeudet
Vaatimus	Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 16 §; TLA 11 § 1 mom 3 k
Viitteet	Julkri: HAL-2.1; Katakri: I-04
Muita lisätietoja	ISO/IEC 27002:2022 8.20

Tunniste	TEK-04.4, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Hallintayhteydet - henkilökohtaiset tunnukset
Vaatimus	Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia.
Yleiskuvaus	
Toteutusesimerkki	Mikäli henkilökohtaisten tunnusten käyttäminen ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille.
Lainsäädäntö	TihL 13 § 1 mom, 16 §; TLA 11 § 1 mom 3 ja 5 k
Viitteet	Katakri: I-04
Muita lisätietoja	PiTuKri IP-02
Tunniste	**TEK-04.5, L:TL IV, E:, S:, TS:**
Nimi	Hallintayhteydet - yhteyksien rajaaminen turvallisuusluokittain
Vaatimus	Hallintayhteydet on rajattu turvallisuusluokittain, ellei käytössä ole turvallisuusluokka huomioon ottaen riittävän turvallista yhdyskäytäväratkaisua.
Yleiskuvaus	
Toteutusesimerkki	Tietojenkäsittely-ympäristöön ei ole yhteenliitäntää hallintayhteyksille muiden turvallisuusluokkien ympäristöistä ilman turvallisuusluokan huomioon ottaen riittävän turvallista yhdyskäytäväratkaisua.
Lainsäädäntö	TLA 11 § 1 mom 1 k
Viitteet	Julkri: TEK-01; Katakri: I-04
Muita lisätietoja	
Tunniste	**TEK-04.6, L:TL IV, E:, S:, TS:**
Nimi	Hallintayhteydet - turvallisuusluokiteltua tietoa sisältävät hallintayhteydet
Vaatimus	Hallintaliikenteen sisältäessä turvallisuusluokiteltua tietoa ja kulkiessa matalamman turvallisuusluokan ympäristön kautta, turvallisuusluokitellut tiedot on salattu riittävän turvallisella salaustuotteella.
Yleiskuvaus	
Toteutusesimerkki	Ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään vain riittävän turvallisen salausratkaisun kautta tilanteissa, joissa hallintaliikenne kulkee matalamman turvallisuusluokan ympäristön kautta.
Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Katakri: I-04, I-12
Muita lisätietoja	

Tunniste	TEK-04.7, L:TL IV, E:, S:, TS:
Nimi	Hallintayhteydet - salaaminen turvallisuusluokan sisällä
Vaatimus	Hallintaliikenteen kulkiessa ko. turvallisuusluokan sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella.
Yleiskuvaus	
Toteutusesimerkki	Tilanteissa, joissa hallintaliikenne kulkee ko. turvallisuusluokan sisällä (ko. turvallisuusluokalle riittävän salauksen sisällä tai/ja ko. turvallisuusluokan tiedon säilyttämiseen hyväksytyn turvallisuusalueen sisällä muista ympäristöistä fyysisesti eriytetyn verkon sisällä), a) ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään fyysisesti (esim. konsolikaapeli), tai b) ko. turvallisuusluokan hallintayhteyden liikennekanava on muuten luotettavasti fyysisesti suojattu (esim. turva-alueen sisäiset kaapeloinnit), tai c) ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään matalamman tason salauksella (esim. SSH, HTTPS, SCP) suojatulla yhteydellä. 4) Laitteisiin/liittymiin sallitaan hallintayhteydenotot vähimpien oikeuksien periaatteen mukaisesti vain hyväksytyistä lähteistä ja määritellyin käyttäjäoikeuksin.
Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Katakri: I-04
Muita lisätietoja	

Tunniste	TEK-04.8, L:TL III, E:, S:, TS:
Nimi	Hallintayhteydet - TL III
Vaatimus	Turvallisuusluokan III käsittely-ympäristöjen etähallinta tulee suorittaa turva-alueelta.
Yleiskuvaus	Turvallisuusluokan III sekä muissa kriittisissä käsittely-ympäristöissä edellytetään etähallinnan teknistä sitomista hyväksyttyyn etähallintalaitteistoon (esim. laitetunnistus).
Toteutusesimerkki	Etähallinta on estetty teknisesti muita kuin hyväksyttyjä laitteita käyttäen.
Lainsäädäntö	TLA 10 § 3 mom 1 k
Viitteet	Katakri: I-18
Muita lisätietoja	

Tunniste	TEK-05, L:Salassa pidettävä, E:, S:, TS:Henkilötieto
Nimi	Langaton tiedonsiirto
Vaatimus	Langattomassa tiedonsiirrossa tietoliikenne salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia.
Yleiskuvaus	Radiorajapinnan käyttö langattomassa tiedonsiirrossa (esim. WLAN, Bluetooth) tulkitaan poistumiseksi fyysisesti suojatun alueen ulkopuolelle. Toisin sanoen radiorajapinnan käyttö rinnastetaan yleisen verkon kautta liikennöinniksi, mikä tulisi ottaa huomioon erityisesti liikenteen salauksessa ja fyysisen turvallisuuden toteuttamisessa. Useisiin langattomiin rajapintoihin liittyy myös protokolla- ja ohjelmistototeutusten puutteita, jotka voivat olla ulkopuolisten hyödynnettävissä. Vastaavaa suojausperiaatetta sovelletaan myös langattomiin oheislaitteisiin (esimerkiksi hiiret, näppäimistöt, kuulokkeet ja kuvansiirtojärjestelmät). Poikkeuksena tilanteet, joilla langattoman rajapinnan käyttöön liittyviä riskejä pystytään luotettavasti pienentämään fyysisen turvallisuuden menettelyillä (esimerkiksi langattoman hiiren käyttö turva-alueen sisällä huoneessa, jonka läheisyyteen pääsy on rajattu vain ko. käsiteltävään tietoon valtuutetuilla henkilöillä). Langattomista laitteista on huomioitava myös älypuhelimet ja vastaavat matalamman turvallisuustason laitteistot, joita ei tule kytkeä tietojenkäsittely-ympäristöön esimerkiksi akun lataamista varten. Käytettävissä tuotteissa ja algoritmeissä ei saa olla tunnettuja korjaamattomia haavoittuvuuksia ja heikkouksia, jotka vaarantavat tietoturvallisuuden. Lisäksi käytettävien tuotteiden valmistajan tulee tarjota tuotteille tietoturvapäivityksiä.
Toteutusesimerkki	1) Fyysisesti suojatun alueen ulkopuolelle kantautuva langaton tiedonsiirto salataan vaatimuksen mukaisesti. 2) Fyysisesti suojatun sisällä tapahtuvan vaatimuksia heikommin suojattu langaton tiedonsiirto (esim. langattomat oheislaitteet) voidaan hyväksyä, mikäli voidaan varmistua, että tiedon luottamuksellisuus ei vaarannu näiden yhteyksien kautta. 3) Langattomia yhteyksiä sisältäviä matalamman turvallisuustason laitteita ei liitetä ympäristöön.
Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Katakri: I-05, I-08, I-09, I-12, I-15, I-16
Muita lisätietoja	PiTuKri SA-01; ISO/IEC 27002:2022 8.22
Tunniste	**TEK-05.1, L:TL IV, E:, S:, TS:**
Nimi	Langaton tiedonsiirto - salaaminen
Vaatimus	Langattomassa tiedonsiirrossa tietoliikenne salataan kyseiselle turvaluokalle riittävän turvallisella salausratkaisulla.
Yleiskuvaus	
Toteutusesimerkki	TL IV -tasolla vaatimus voidaan toteuttaa esimerkiksi tunneloimalla liikenne riittävän turvallisella VPN-ratkaisulla tai käyttämällä hyväksyttyä sovellustason salausratkaisua.
Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Katakri: I-05
Muita lisätietoja	ISO/IEC 27002:2022 8.24; PiTuKri SA-01

Tunniste	TEK-06, L:Salassa pidettävä, E:, S:, TS:Henkilötieto
Nimi	Kasautumisvaikutus
Vaatimus	Kasautumisvaikutus on huomioitu tietojenkäsittely-ympäristön suojaamisessa.
Yleiskuvaus	Kun kohteen keskeisen tietovarannon turvallisuusluokka tulkitaan kasautumisvaikutuksesta johtuen yksittäisten tietoalkioiden tasoa korkeammaksi, tulee tietovarannon määritellyt suojausmenetelmät toteuttaa korkeamman tason vaatimusten mukaisesti. Määritellyillä suojausmenetelmillä tarkoitetaan menetelmiä, joilla rajataan pääsy vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, ja joilla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä havaitaan. Kun arviointityökaluna käytetään Julkria, tulisi kasautumisvaikutus tulkita siten, että tietovarannon suojauksilta edellytetään korkeamman tason mukaisena tietovarannon fyysisen turvallisuuden lisäksi kohtia TEK-14 (sovelluskerroksen turvallisuus), TEK-12 ja TEK-13 (jäljitettävyys ja havainnointikyky), HAL-02.1 (Tehtävät ja vastuut - tehtävien eriyttäminen) sekä TEK-07 (Pääsyoikeuksien hallinnointi). Onkin huomioitava, että kasautumisvaikutuksen seurauksena yhdellä luokalla noussut tietovarannon turvallisuusluokka ei edellytä hyväksyttävää yhdyskäytäväratkaisua tietovarannon (esim. TL III) ja päätelaitteiden (esim. TL IV) välille. Kasautumisvaikutuksen seurauksena turvallisuusluokan III tietovarantojen hallintaratkaisuissa tulee lisäksi erityisesti huomioida, että hallintaan käytettävät päätelaitteet ovat luotettavasti eroteltuja Internet-kytkentäisistä verkoista.
Toteutusesimerkki	
Lainsäädäntö	TihL 15 § 2 mom, 13 § 1 mom
Viitteet	Julkri: HAL-04.3
Muita lisätietoja	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01

Tunniste	TEK-07, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Pääsyoikeuksien hallinnointi
Vaatimus	Tietojärjestelmien käyttöoikeudet on määritelty.
Yleiskuvaus	Käyttöoikeuksien hallinnan keskeinen tavoite on pystyä varmistumaan siitä, että vain oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään suojattavaan tietoon.
Toteutusesimerkki	1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t). 2) Järjestelmän käyttäjistä on olemassa lista.
Lainsäädäntö	TihL 16 §; TLA 8 §, 11 § 1 mom 3 k
Viitteet	Julkri: HAL-14, HAL-14.1, HAL-19; Katakri: I-06
Muita lisätietoja	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01

Tunniste	TEK-07.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Pääsyoikeuksien hallinnointi - pääsyoikeuksien myöntäminen
Vaatimus	Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käyttötarpeesta on varmistuttu.
Yleiskuvaus	Käyttöoikeuksien taustalla on suositeltavaa olla jokin sopimus tai muu dokumentoitu peruste, joka voidaan todentaa (esim. työsuhde, sopimus toteutettavasta työstä ympäristössä).
Toteutusesimerkki	3) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. 4) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. 5) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen).
Lainsäädäntö	TihL 16 §; TLA 8 §, 11 § 1 mom 3 k
Viitteet	Julkri: HAL-14, HAL-10.1; Katakri: I-06
Muita lisätietoja	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01

Tunniste	TEK-07.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Pääsyoikeuksien hallinnointi - pääsyoikeuksien rajaaminen
Vaatimus	Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.
Yleiskuvaus	Käyttöoikeudet tulee rajata vain toiminnallisen tarpeen edellyttämään osajoukkoon. Tarpeettoman laajat oikeudet mahdollistavat ko. käyttäjälle, prosessille tai edellä mainitut haltuun saavalle hyökkääjälle tarpeettoman laajat toimintamahdolliset. Käyttöoikeuksien rajaamisella vähimpien oikeuksien periaatteen mukaiseksi voidaan pienentää sekä tahallisten että tahattomien tekojen, kuin myös esimerkiksi haittaohjelmista aiheutuvia riskejä. Erityisesti tulee huomioida, että ylläpito-oikeuksia käytetään vain ylläpitotoimiin. Ylläpitotunnuksella varustettua käyttäjätiliä ei tule käyttää esimerkiksi web-selailuun tai sähköpostin käyttöön. Turvallisuusluokitellun tiedon omistajat varaavat usein itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti monihankeverkoissa ja muissa vastaavissa ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulisi varmistua siitä, että verkon/järjestelmän rakenne mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä. Huom.: Tietojen erotteluvaatimusta ei turvallisuusluokan IV tiedoille sovelleta työasemiin tai muihin vastaaviin suppeisiin tietovarantoihin, edellyttäen, että käytössä on luotettavaksi arvioidut menetelmät kasautumisvaikutuksen ehkäisemiseksi. Tarkastusoikeuden varaavien tiedon omistajien tietoja ei edellytetä eroteltavan myöskään tilanteissa, joissa kaikilta tiedon omistajilta on saatu kirjallinen erillishyväksyntä tarkastusoikeuden mahdollistamien riskien hyväksymisestä tai jos tietojen omistajat sitoutuvat olemaan käyttämättä teknistä tarkastusoikeutta kyseiseen tietojenkäsittely-ympäristöön. Eri omistajien tietojen erottelumenetelmät jakautuvat kolmeen pääluokkaan. a) Loogisen tason erotteluun (esim. palvelinten virtualisointi ja käyttöoikeuksin rajoitetut verkkolevykansiot) perustuvat menetelmät soveltuvat turvallisuusluokan IV tiedoille. b) Luotettavaan loogiseen erotteluun (esim. hyväksytysti salatut virtuaalikoneet levyjärjestelmän asiakaskohtaisesti varatuilla fyysisillä levyillä, ja tiedon/tietoliikenteen hyväksytty salaus yhteiskäyttöisillä verkkolaitteilla) perustuvat menetelmät soveltuvat turvallisuusluokille IV ja III saman turvallisuusluokan sisäiseen erotteluun. c) Fyysisen tason erotteluun (tiedonomistajakohtaisesti varatut fyysiset laitteet) perustuvat menetelmät soveltuvat turvallisuusluokille IV, III, II ja I. Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa: - Vaatimuksen soveltamisessa tulee huomioida vastuujako pilvipalveluntarjoajan ja asiakkaan välillä. Tyypillisesti pilvipalveluntarjoaja on vastuussa pilvipalvelun tuottamiseen liittyvän järjestelmäkokonaisuuden käyttöoikeushallinnasta, asiakkaan vastuun koskiessa palveluntarjoajan palvelukokonaisuuden (IaaS, PaaS tai SaaS) päälle rakentuvan osuuden käyttöoikeushallintaa. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaankin huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia. - Erottelun toteuttaminen pilviteknologiaa hyödyntäen, huomioitavaa: -- Salassa pidettävän tiedon erottelu on toteutettava riittävän luotettavasti, joko loogisen tai/ja fyysisen erottelun menetelmillä. Eräs yleinen käytössä oleva erottelumenetelmä esimerkiksi yhteiskäyttöisten verkkolaitteiden ja tallennusjärjestelmien osalta on salaus. Asiakaskohtaisilla avaimistoilla toteutettavaa tietoliikenteen salausta (data-in-transit) ja salausta tallennettaessa (data-at-rest) voidaan hyödyntää myös muiden turvatavoitteiden, esimerkiksi laitteistojen turvallisen hävittämisen, tukevana suojauksena. -- Jos samaa laitteistoa käytetään useiden asiakkaiden tiedon käsittelyyn samanaikaisesti, tulee varmistua siitä, että tietojen fyysinen ja looginen erottelu on riittävän turvallinen. Mikäli asiasta ei saada riittävää varmuutta, tulee tietojen käsittelyyn käyttää erillisiä fyysisiä laitteita. Esimerkiksi turvallisuusluokitellut tiedot voidaan säilyttää fyysisesti erillisellä virtualisointialustalla, jossa esimerkiksi mahdollisiin prosessorihaavoittuvuuksiin liittyvät rajapinnat on rajattu vain turvallisuusluokiteltujen tietojen valtuutettujen käyttäjien saavutettaviksi. -- Jos samaa laitteistoa käytetään useiden eri asiakkaiden tietojen käsittelyyn, mutta ei samanaikaisesti, tulee varmistua myös siitä, että edellisen asiakkaan tiedot on poistettu riittävän turvallisesti laitteistosta (ml. kaikki osat, BIOS, erilaisten muiden laitteiden välimuistit). Mikäli asiasta ei saada riittävää varmuutta, tulee tietojen käsittelyyn käyttää erillisiä fyysisiä laitteita. Vrt. PiTuKri / SI-02 (Tietoaineistojen tuhoaminen). -- Turvallisuusluokitellun salassa pidettävän tiedon omistajat voivat varata itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulee varmistua siitä, että verkon/järjestelmän toteutustapa mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä. Erityisesti palvelumalleilla IaaS ja PaaS, turvallisuusluokitellun tiedon erottaminen tulee varmistaa fyysisesti erillisillä verkoilla tai salatuilla virtuaalisilla tai ohjelmistopohjaisilla paikallisverkoilla. Vrt. PiTuKri / SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella).

Toteutusesimerkki	6) Tietojärjestelmissä turvallisuusluokitellut tiedot on eritelty vähimpien oikeuksien periaatteen mukaisesti käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä. 7) Tietojärjestelmissä tarkastusoikeuden varaavien tiedon omistajien tiedot säilytetään toisistaan ko. turvallisuusluokalle riittävän turvallisella menetelmällä eroteltuna.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom 1 k, 16 §; TLA 8 §, 11 §:n 1 mom 3 ja 4 k
Viitteet	Katakri: I-06
Muita lisätietoja	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01, SA-03, KT-03
Tunniste	**TEK-07.3, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Pääsyoikeuksien hallinnointi - pääsyoikeuksien ajantasaisuus
Vaatimus	Käyttöoikeudet on pidettävä ajantasaisina.
Yleiskuvaus	
Toteutusesimerkki	8) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. 9) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti.
Lainsäädäntö	TihL 16 §
Viitteet	Julkri: HAL-14.1; Katakri: I-06
Muita lisätietoja	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01
Tunniste	**TEK-07.4, L:TL IV, E:, S:, TS:**
Nimi	Pääsyoikeuksien hallinnointi - turvallisuusluokiteltujen tietojen erottelu
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	1) Kunkin turvallisuusluokan tiedot pidetään erillään julkisista ja muiden turvallisuusluokkien tiedoista, tai eri tason tietoja käsitellään korkeimman turvallisuusluokan mukaisesti. 2) Palvelimissa, työasemissa ja muissa tallennusvälineissä turvallisuusluokitellut tiedot säilytetään riittävän turvallisella menetelmällä salattuna, mikäli salausta käytetään tarkastusoikeuden varaavien eri tiedon omistajien tietojen erotteluun, tai/ja mikäli tallennusvälineitä viedään niiden elinkaaren aikana kyseisen turvallisuusluokan säilyttämiseen hyväksytyn turvallisuusalueen ulkopuolelle.
Lainsäädäntö	TLA 11 § 1 mom 1 k
Viitteet	Katakri: I-06
Muita lisätietoja	

Tunniste	TEK-07.5, L:TL III, E:, S:, TS:
Nimi	Pääsyoikeuksien hallinnointi - TL III
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	Tehtävien erottelun riittävä toteutus riippuu merkittävästi kyseessä olevan järjestelmän käyttötapauksista. Useimmissa järjestelmissä riittävä tehtävien erottelu on toteutettavissa järjestelmän ylläpitoroolien (ja henkilöiden) ja lokien valvontaan osallistuvien roolien (ja henkilöiden) erottelulla toisistaan. Usein käytettynä valvontamekanismina on myös se, että kriittiset ylläpito- ja vastaavat toimet vaativat kahden tai useamman henkilön hyväksynnän.
Toteutusesimerkki	Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvatonman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi.
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 3 k
Viitteet	Julkri: HAL-2.1; Katakri: I-06, I-12
Muita lisätietoja	

Tunniste	TEK-08, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto
Nimi	Tietojenkäsittely-ympäristön toimijoiden tunnistaminen
Vaatimus	Tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti.
Yleiskuvaus	

Toteutusesimerkki	Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: Henkilöiden tunnistaminen: 1) Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet. 2) Kaikki käyttäjät tunnistetaan ja todennetaan. 3) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti. 4) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen. 5) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille. 6) Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. Salasanan vaihdon sopiva määräaika tulee suhteuttaa organisaation toimintaympäristön ja laitteessa käsiteltävän ja säilytettävän turvallisuusluokitellun tiedon luokituksen mukaan, muut turvallisuusratkaisut huomioiden. Tietojärjestelmien tunnistaminen: 7) Tietoa keskenään vaihtavat tietojärjestelmät tunnistetaan käyttötapaukseen soveltuvalla tekniikalla, kuten salasanoilla, avaimilla (esim. API-avain), tunnistevälineillä (tokeneilla, esim. oAuth) tai vastaavilla menetelmillä. Tunnistautuminen tehdään salattuja yhteyksiä pitkin. Huomioitavaa Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen ainakin siitä, että i) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle), ii) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, iii) todennuksessa käytettävät tunnistamistiedot (todennuskredentiaalit) ovat aina salatussa muodossa jos ne lähetetään verkon yli, iv) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, v) todennusmenetelmä on suojattu brute force -hyökkäyksiä vastaan. Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa: - Julkisen verkon yli saavutettavissa pilvipalveluissa käyttötapa tulkittavissa etäkäytöksi ja siten huomioitava esimerkiksi vaatimukset vahvasta, useaan todennustekijään pohjautuvasta tunnistaumisesta. - Tilanteissa, joissa pilvipalveluun tunnistautumisessa hyödynnetään federoitua identiteetinhallintaa, tai/ja identiteetin- ja pääsynhallintajärjestelmiä (organisaation omia tai esimerkiksi pilvipalveluntarjoajan tuottamia), tulee arvioinnissa kiinnittää erityistä huomiota tunnistuspalvelun sekä attribuuttien välitysketjun luotettavuuteen. Salassa pidettävän tiedon käsittelyyn soveltuvat vain sellaiset tunnistuspalvelut, jotka tarjoavat vahvaan ensitunnistamiseen perustuvaa identiteettiä ja joiden attribuuttien välitysketju pystytään toteuttamaan riittävän turvallisesti tunnistukseen nojaavaan palveluun asti. - Koska salassa pidettävän tiedon suojaus on yleensä suoraan riippuvainen tunnistuspalvelun luotettavuudesta, tunnistuspalvelun turvallisuudesta varmistuminen kuuluu lähes poikkeuksetta osaksi pilvipalvelun turvallisuuden arviointia. Esimerkiksi attribuuttien välityksen salausteknistä suojausta on tyypillisesti perusteltua arvioida samansuuntaisesti kuin kyseessä olevan tietotyypin suojaamiseen sovellettavan salausratkaisun avainten välitystä. - Identiteetinhallintamalleista organisaatiokeskeinen (organization-centric identity management) soveltuu yleensä esimerkiksi käyttäjäkeskeistä (user-centric) paremmin salassa pidettävän tiedon suojaamistarpeisiin, joissa on huomioitava myös käyttäjän sidonta tiettyyn organisaatioon sekä turvallisuustoteutuksen luotettavuudesta varmistuminen. - Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.
Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 5 k
Viitteet	Julkri: HAL-19; Katakri: I-07
Muita lisätietoja	ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02, SA-01, SA-02 ja SA-03.

Tunniste	TEK-08.1, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto
Nimi	Tietojenkäsittely-ympäristön toimijoiden tunnistaminen
Vaatimus	Kaikki käyttäjät tunnistetaan ja todennetaan yksilöllisillä henkilökohtaisilla käyttäjätunnisteilla.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom, 16 §; TLA 11 § 1 mom 3 ja 5 k
Viitteet	Katakri: I-07
Muita lisätietoja	PiTuKri IP-02
Tunniste	**TEK-08.2, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto**
Nimi	Tietojenkäsittely-ympäristön toimijoiden tunnistaminen
Vaatimus	Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom, 14 §, 16 §; TLA 11 § 1 mom 3 ja 5 k
Viitteet	Katakri: I-07
Muita lisätietoja	ISO/IEC 27002:2022 8.5; PiTuKri IP-02
Tunniste	**TEK-08.3, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto**
Nimi	Tietojenkäsittely-ympäristön toimijoiden tunnistaminen
Vaatimus	Käyttäjätunnukset lukittuvat tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; TLA 7 §
Viitteet	Katakri: I-07
Muita lisätietoja	ISO/IEC 27002:2022 8.5; PiTuKri IP-02

Tunniste	TEK-08.4, L:TL IV, E:Kriittinen, S:, TS:
Nimi	Tietojenkäsittely-ympäristön toimijoiden tunnistaminen - TL IV
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Laitteiden tunnistaminen: Turvallisuusluokitellun tiedon käsittelyyn käytetään vain organisaation tarjoamia ja hallinnoimia, kyseiselle turvallisuusluokalle hyväksyttyjä päätelaitteita. Kaikkien muiden laitteiden kytkeminen turvallisuusluokitellun tiedon käsittely-ympäristöön on yksiselitteisesti kielletty. Henkilöstö on ohjeistettu ja velvoitettu toimimaan ohjeistuksen mukaisesti. Tietojärjestelmien tunnistaminen: Tietoa keskenään vaihtavat tietojärjestelmät tunnistetaan käyttötapaukseen soveltuvalla tekniikalla, kuten salasanoilla, avaimilla (esim. API-avain), tunnistevälineillä (tokeneilla, esim. oAuth) tai vastaavilla menetelmillä. Tunnistautuminen tehdään salattuja yhteyksiä pitkin. Huomioitavaa: Turvallisuusluokan IV käsittely-ympäristöissä, joissa uhka palvelunestohyökkäyksen aiheuttamiseen (tunnusten lukitseminen esim. Internet-kytkentäisissä tunnistuspalveluissa) arvioidaan merkittäväksi, tunnuksen lukittuminen voidaan korvata jollain riskiä pienentävällä menettelyllä (esim. vastaamisen hidastamiseen, suodattamiseen tai väliaikaiseen lukitsemiseen perustuvat menettelyt). Turvallisuusluokan IV käsittely-ympäristöissä ei yleensä edellytetä päätelaitteen teknistä tunnistamista, mikäli käyttäjät tunnistetaan.
Lainsäädäntö	TLA 11 § 1 mom 5 k
Viitteet	Katakri: I-07
Muita lisätietoja	ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02

Tunniste	TEK-08.5, L:TL III, E:Kriittinen, S:, TS:
Nimi	Tietojenkäsittely-ympäristön toimijoiden tunnistaminen - TL III
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokkien III-II toteutetaan myös seuraavat toimenpiteet: 1) Edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta. 2) Päätelaitteet tunnistetaan teknisesti (laitetunnistus, 802.1X, tai vastaava menettely) ennen pääsyn sallimista verkkoon tai palveluun, ellei verkkoon kytkeytymistä ole fyysisen turvallisuuden menetelmin rajattu suppeaksi (esim. palvelimen sijoittaminen lukittuun laitekaappiin turva-alueen sisällä). Huomioitavaa Turvallisuusluokkien III ja II käsittely-ympäristöjen menetelmät vahvasta käyttäjätunnistuksesta ja päätelaitteen tunnistamisesta voidaan joissain tapauksissa toteuttaa siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisesti suojatulta alueelta (yleensä turva-alue, lukittu laitekaappi, tai vastaava), jonka pääsynvalvonnassa käytetään vahvaa, vähintään kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana-parilla. Tilanteissa, joissa käyttäjätunnistus nojaa fyysisen turvallisuuden menettelyihin, tulee myös fyysisen turvallisuuden menettelyjen täyttää jäljitettävyydelle asetetut vaatimukset erityisesti lokitietojen ja vastaavien tallenteiden säilytysaikojen suhteen.
Lainsäädäntö	TLA 11 § 1 mom 5 k
Viitteet	Katakri: I-07
Muita lisätietoja	

Tunniste	TEK-09, L:Salassa pidettävä, E:Kriittinen, S:, TS:Erityinen henkilötietoryhmä
Nimi	Tietojärjestelmien fyysinen turvallisuus
Vaatimus	Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.
Yleiskuvaus	Hallinnolliselle alueelle, turva-alueille sekä esimerkiksi säilytysyksiköille asetetut vaatimukset on kuvattu fyysisen turvallisuuden osiossa. Turvallisuusalueen ulkopuolella tapahtuva käyttö on etäkäyttöä, johon sovelletaan kyseisen kohdan vaatimuksia. Tilanteissa, joissa tietoa käsitellään tilapäisesti luokkaa matalamman tason tilassa, on huomioitava myös esimerkiksi toiminta työskentelytaukojen aikana (esim. tieto vietävä esimerkiksi turva-alueen kassakaappiin tauon ajaksi), näkyvyyden rajaus tilaan (esim. mahdollisten ikkunoiden peittäminen) ja käsittelytilaan pääsyn rajaaminen vain hyväksyttyihin henkilöihin. Päätelaitteen eheys tulee pystyä varmistamaan riittävällä tasolla, jotta tiedon luottamuksellisuus ei vaarannu päätelaitteen eheyden menetyksen seurauksena. Tyypillisin tapa tietojärjestelmän eheydestä varmistumiseen on sen suojaaminen turvallisuusalueiden fyysisen pääsynhallinnan menettelyin, mukaan lukien esimerkiksi kaikki tietojärjestelmään liittyvät fyysiset palvelimet, verkkolaitteet, päätelaitteet sekä esimerkiksi kaapeloinnit.
Toteutusesimerkki	
Lainsäädäntö	TihL 15 § 2 mom; TLA 10 §
Viitteet	Julkri: FYY-7.1, HAL-19; Katakri: I-17
Muita lisätietoja	ISO/IEC 27002:2022 7.1, 7.3, 7.6, 7.8; Tiedonhallintalautakunta: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2020:19, luku 5); PiTuKri FT-02; CPNI: Physical Security Advice

Tunniste	TEK-10, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä
Nimi	Järjestelmäkovennus
Vaatimus	Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.

Yleiskuvaus

Järjestelmissä on usein paljon ominaisuuksia, jotka ovat yleensä oletusarvoisesti päällä ja helppo ottaa käyttöön. Ominaisuuksien oletusasetukset eivät usein ole riittävän turvallisia. Jos tarpeettomia ominaisuuksia ei poisteta käytöstä, nämä ovat myös pahantahtoisen toimijan käytettävissä. Jos välttämättömien palvelujen riskialttiita oletusasetuksia ei muuteta, ovat nämä myös pahantahtoisen toimijan käytettävissä. Järjestelmissä on oletusarvoisesti usein käytössä esimerkiksi ennalta määriteltyjä ylläpitosalasanoja, valmiiksi asennettuja tarpeettomia ohjelmistoja ja tarpeettomia käyttäjätilejä.

Koventamisella tarkoitetaan yleisesti järjestelmän asetusten muuttamista siten, että järjestelmän haavoittuvuuspinta-alaa saadaan pienennettyä. Riskien pienentämiseksi järjestelmissä on yleisesti otettava käyttöön vain käyttövaatimusten kannalta olennaiset toiminnot, laitteet ja palvelut, ja esimerkiksi palvelujen näkyvyys tulee rajata mahdollisimman pieneksi. Vastaavasti esimerkiksi automaattisille prosesseille on annettava vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä, jotta rajoitetaan onnettomuuksista, virheistä tai järjestelmän resurssien luvattomasta käytöstä mahdollisesti aiheutuvia vahinkoja. Järjestelmän mahdollisesti turvattomat oletusasetukset ja esimerkiksi tarpeettomat oletuskäyttäjätilit tulee muuttaa tai poistaa.

Järjestelmillä tarkoitetaan verkon aktiivilaitteita, palvelimia, työasemia, mobiililaitteita, tulostimia, oheislaitteita ja muita tietojärjestelmäksi käsitettäviä laitteita. Palvelinten, työasemien ja vastaavien riittävän kovennuksen voi toteuttaa esimerkiksi DISA STIG:iä, CIS:iä tai vastaavaa tasoa mukaillen. Mikäli turvallisuusluokitellun tiedon käsittelyyn käytetään verkkotulostimia, puhelinjärjestelmiä tai vastaavia, edellä mainittuja periaatteita tulisi soveltaa myös näihin järjestelmiin. Koventamiseen ja kovennetun asennuksen ylläpitämiseen voidaan usein hyödyntää myös konfiguraationhallintatyökaluja.

Oleellista kovennuksista
1) Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin. Salasanoja säilytetään siten, että salasanat ovat suojattuna sekä saatavilla.
2) Ylimääräiset palvelut, sovellukset, yhteydet (myös BIOS-tasolla) ja laitteet on poistettu.
3) Käyttäjät, rajapinnat ja laitteet tunnistetaan (vrt. I-07).
4) Päällä olevat välttämättömät palvelut ovat saavutettavissa vain tarpeellisten verkkojen, laitteiden ja käyttäjätunnusten osalta.
5) Ohjelmistot (esim. laiteohjelmistot, sovellukset) pidetään ajantasaisina (vrt. I-19).
6) Kohteen yhteydet, mukaan lukien hallintayhteydet, ovat rajattuja, kovennettuja, käyttäjätunnistettuja sekä aikarajoitettuja (istunnon aikakatkaisu).
7) Käytössä olevat sovellukset, rajapinnat ja vastaavat on kovennettu, rajoitettu ja ominaisuudet on asetettu vähimpien oikeuksien periaatteen mukaiseksi.
8) Ohjelmistot, kuten käyttöjärjestelmät, sovellukset ja laiteohjelmistot, asetetaan keräämään tarvittavaa lokitietoa väärinkäytösten havaitsemiseksi (vrt. I-10).
9) Tietojärjestelmän käynnistäminen tuntemattomalta (muulta kuin ensisijaiseksi määritellyltä) laitteelta on estetty.

Korvaavia menetelmiä
Mikäli esimerkiksi verkkolaitteen hallinta ei ole teknisesti mahdollista käyttäjän yksilöivällä käyttäjätunnuksella, käyttäjän yksilöivä tunnistaminen voidaan järjestää käyttösäännöillä esimerkiksi siten, että salasanaan pääsy edellyttää kahden henkilön osallistumista. Mikäli ympäristön koko on suurehko, todennuksen järjestämiseen suositellaan kahdennettujen AAA-palvelimien (erityisesti TACACS+, RADIUS tai Kerberos) hyödyntämistä.

Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa:
Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Toteutusesimerkki	1) Kovennettavat kohteet on tunnistettu. 2) Kovennusten toteutus on määritelty. 3) Kohteet on kovennettu määritysten mukaisesti. 4) Kovennusten pysyminen päällä varmistetaan säännöllisesti, erityisesti päivitysten jälkeen koko tietojärjestelmän elinkaaren ajan. Erityisesti huomioitavaa: a) Kovennukset kohdistetaan kaikkiin tietojenkäsittely-ympäristön laitteisiin, joita ovat muun muassa verkon aktiivilaitteet, palvelimet, työasemat, mobiililaitteet, tulostimet, oheislaitteet ja muut tietojärjestelmäksi käsitettävät laitteet. b) Hyökkäyspinta-alan rajaamiseksi laitteissa on päällä vain tarvittavat palvelut, rajapinnat, yhteydet ja väylät, ja nämä toimivat vähimpien oikeuksien periaatteella. c) Laitteen laiteohjelmisto (firmware, BIOS ja vastaavat), käyttöjärjestelmä, sovellukset sekä muut vastaavat komponentit kovennetaan vähintään valmistajan kovennussuosituksen mukaisesti ja/tai käyttäen yleisesti tunnettua kovennusohjetta. Tämän lisäksi kovennukset räätälöidään järjestelmäkohtaisesti käyttötarkoituksen ja riskien perusteella. Jollei kovennusohjetta käytetylle komponentille ole olemassa, sovelletaan vastaavalle tuotteelle tarkoitettua ohjetta.
Lainsäädäntö	TihL 13 § 1 ja 4 mom; TLA 11 § 1 mom 6 k
Viitteet	Katakri: I-08
Muita lisätietoja	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
Tunniste	**TEK-10.1, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Järjestelmäkovennus - käytössä olevien palveluiden minimointi
Vaatimus	Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut.
Yleiskuvaus	Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; TLA 11 § 1 mom 6 k
Viitteet	Katakri: I-08
Muita lisätietoja	
Tunniste	**TEK-10.2, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä**
Nimi	Järjestelmäkovennus - kovennusten varmistaminen koko elinkaaren ajan
Vaatimus	Kovennusten voimassaolosta ja vaikuttavuudesta huolehditaan koko tietojärjestelmän elinkaaren ajan.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 ja 4 mom; TLA 11 § 1 mom 6 k
Viitteet	Katakri: I-08
Muita lisätietoja	

Tunniste	TEK-10.3, L:TL III, E:Kriittinen, S:, TS:
Nimi	Järjestelmäkovennus - turvallisuusluokitellut ympäristöt
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	Erityisesti korkeimpien turvallisuusluokkien ympäristöissä tarpeettomien komponenttien käytönesto on usein perusteltua toteuttaa fyysisesti kyseiset komponentit (esimerkiksi langattomat verkkokortit, kamerat, mikrofonit) laitteesta irrottaen. Tilanteissa, joissa kyseistä komponenttia ei voida fyysisesti irrottaa, korvaavana suojauksena voi joissain tapauksissa hyödyntää esimerkiksi kameroiden teippaamista sekä laitteiston ohjelmallista käytöstäpoistoa sekä käyttäjäasetus-, käyttöjärjestelmä- ja laiteohjelmistotasoilla. Joissain käyttöjärjestelmissä suojausta voidaan täydentää myös poistamalla kyseisen laitteen käyttöön liittyvät ohjelmisto-osiot (kernel module). Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus tulee huomioida kovennusohjeiden mahdollisesti sisältämät tasot sekä useiden eri kovennusohjeiden, kuten esimerkiksi valmistajakohtaiset ohjeet, CIS Benchmark ja DISA STIG, hyödyntäminen kovennusten kattavuuden varmistamisessa.
Toteutusesimerkki	Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan toteuttaa siten, että kohtien 1–4 lisäksi kovennuksiin käytetään useita kovennusohjeita ja kovennusohjeiden toteutuksen tiukkuutta kiristetään.
Lainsäädäntö	TihL 13 § 1 ja 4 mom; TLA 11 § 1 mom 6 k
Viitteet	Katakri: I-08
Muita lisätietoja	

Tunniste	TEK-11, L:Salassa pidettävä, E:Normaali, S:Normaali, TS:Erityinen henkilötietoryhmä
Nimi	Haittaohjelmilta suojautuminen
Vaatimus	Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.
Yleiskuvaus	Haittaohjelmariskejä vastaan voidaan suojautua esimerkiksi järjestelmien kovennusmenettelyillä , käyttöoikeuksien rajauksilla, järjestelmien pitämisellä turvallisuuspäivitysten tasolla, poikkeamien havainnointikyvyllä, henkilöstön turvatietoisuudesta varmistumalla ja myös haittaohjelman torjuntaohjelmistojen käytöllä. Riskejä voidaan pienentää myös riskialttiiden ympäristöjen eriyttämisellä tuotantoympäristöistä sekä muun muassa siirreltävien medioiden (esimerkiksi USB-muistien) käytön rajauksilla. Torjuntaohjelmistot voidaan jättää asentamatta ympäristöissä, joihin haittaohjelmien pääsy on muuten estetty (esim. järjestelmät, joissa ei ole mitään tiedon tuonti-/vientiliittymiä, tai joissa tarkasti rajatuissa liittymissä toteutetaan siirrettävän tiedon luotettava validointi/sanitointi).
Toteutusesimerkki	Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Järjestelmien käyttöoikeudet on rajattu vähimpien oikeuksien periaatteen mukaisesti. 2) Järjestelmät pidetään turvallisuuspäivitysten tasolla. 3) Järjestelmät on kovennettuja siten, että vain välttämättömät toiminnallisuudet ja ohjelmistokomponentit käytössä. 4) Henkilöstön turvatietoisuudesta on varmistuttu. Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta. 5) Haittaohjelman torjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille. Tällaisia ovat tyypillisesti muun muassa julkisen verkon yhdyskäytävät (esim. sähköposti- ja WWW-liikennöinti), sekä ulkoisiin rajapintoihin (muut verkot, USB-mediat ja vastaavat) yhteydessä olevat päätelaitteet. 6) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä. 7) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja ja hälytyksiä. 8) Haittaohjelmatunnisteet (ja vast.) päivittyvät säännöllisesti. 9) Haittaohjelmahavaintoja sekä hälytyksiä seurataan säännöllisesti ja niihin reagoidaan.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom; TLA 11 § 1 mom 2 ja 3 k
Viitteet	Katakri: I-09
Muita lisätietoja	ISO/IEC 27002:2022 8.7; PiTuKri JT-04
Tunniste	**TEK-11.1, L:TL IV, E:, S:, TS:**
Nimi	Haittaohjelmilta suojautuminen - TL IV
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan lisäksi: 1) On tunnistettu järjestelmät, joissa haittaohjelman torjuntaohjelmistoilla pystytään saamaan lisäsuojausta.
Lainsäädäntö	TLA 11 § 1 mom 2 k
Viitteet	Katakri: I-09
Muita lisätietoja	ISO/IEC 27002:2022 8.7; PiTuKri JT-04
Tunniste	**TEK-11.2, L:TL III, E:, S:, TS:**
Nimi	Haittaohjelmilta suojautuminen - TL III
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.

Yleiskuvaus	Julkisista verkoista eristetyt ympäristöt Järjestelmissä, joita ei kytketä julkiseen verkkoon, haittaohjelmatunnisteiden päivitys voidaan järjestää esimerkiksi käyttämällä hallittua suojattua päivitystenhakupalvelinta, jonka tunnistekanta pidetään ajan tasalla esimerkiksi erillisestä Internetiin kytketystä järjestelmästä tunnisteet käsin siirtämällä (esim. 1–3 kertaa viikossa), tai tuomalla tunnisteet hyväksytyn yhdyskäytäväratkaisun kautta. Tunnisteiden päivitystiheyden riittävyyden arviointi tulee suhteuttaa riskienarvioinnissa kyseisen ympäristön ominaispiirteisiin, erityisesti huomioiden ympäristön muun tiedonsiirron tiheyden. Huom.: Päivitysten eheydestä varmistumiseen tulisi olla menettelytapa (lähde, tarkistussummat, allekirjoitukset, jne.). USB-porttien ja vastaavien liityntöjen käytön tapauskohtaisiin ehtoihin voi sisältyä esimerkiksi, että järjestelmään voi kytkeä vain erikseen määritettyjä luotettavaksi todennettuja muistitikkuja (ja vastaavia), joita ei kytketä mihinkään muuhun järjestelmään. Tapauskohtaisiin ehtoihin voi sisältyä esimerkiksi järjestely, jossa vain organisaation tietohallinnon (tai vast.) jakamia muistivälineitä voidaan kytkeä organisaation järjestelmiin, ja että kaikkien muiden muistivälineiden kytkeminen on kielletty ja/tai teknisesti estetty. Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, tapauskohtaisiin ehtoihin sisältyy usein myös määrittelyt siitä, millä menetelmillä pienennetään tämän aiheuttamaa riskiä. Menetelmänä voi esimerkiksi olla ei-luotetusta lähteestä tulevan muistivälineen kytkeminen eristettyyn tarkastusjärjestelmään, jonne siirrettävä tieto siirretään, ja josta siirrettävä tieto viedään edelleen luotettuun järjestelmään erillistä muistivälinettä käyttäen.
Toteutusesimerkki	Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraavat toimenpiteet: Kaikki tiedon sisääntuonnin ja ulosviennin käyttötapaukset on tunnistettu. Turvalliset toimintatavat on määritetty, ohjeistettu ja valvonnan piirissä. Turvallisten toimintatapojen piiriin sisältyy tarvearviointi järjestelmien USB-porttien ja vastaavien liityntöjen käytölle. a) Tilanteissa, joissa liityntöjen käytölle ei ole kriittistä tarkastelua kestävää perustetta, liitynnät poistetaan käytöstä. b) Tilanteissa, joissa liityntöjen käytölle on kriittistä tarkastelua kestävät perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä. Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, huomioidaan lisäksi yleensä turvallisuusluokalla III vähintään muistialueen tarkastaminen.
Lainsäädäntö	TLA 11 § 1 mom 2 k
Viitteet	Katakri: I-09
Muita lisätietoja	
Tunniste	**TEK-11.3, L:TL II, E:, S:, TS:**
Nimi	Haittaohjelmilta suojautuminen - TL II
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, huomioidaan lisäksi yleensä turvallisuusluokasta II lähtien myös muistivälineen kontrolleritason räätälöinnin uhat.
Lainsäädäntö	TLA 11 § 1 mom 2 ja 5 k
Viitteet	Katakri: I-09
Muita lisätietoja	

Tunniste	TEK-12, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Turvallisuuteen liittyvien tapahtumien jäljitettävyys
Vaatimus	Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyden varmistamiseksi.
Yleiskuvaus	Jäljitettävyydellä tarkoitetaan järjestelmäympäristön tapahtumien kirjaamista siten, että poikkeamatilanteessa voidaan selvittää mitä toimia ympäristössä on tehty, kenen toimesta ja mitä vaikutuksia toimilla on ollut. Keskeisiä tallenteita ovat tyypillisesti kirjautumistietojen lisäksi keskeisten verkkolaitteiden ja palvelinten lokitiedot. Myös esimerkiksi työasemien ja vastaavien lokitiedot kuuluvat tähän erittäin usein. Kattavuusvaatimuksen toteuttamisessa voi usein hyödyntää sitä, että varmistaa, että ainakin työasemien, palvelinten, verkkolaitteiden (erityisesti palomuurien, myös työasemien sovellusmuurien) ja vastaavien lokitus on päällä. Verkkolaitteiden lokeista tulisi myös pystyä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. Tapahtumalokeja olisi syytä kerätä järjestelmän toiminnasta, käyttäjäaktiviteeteista, tietoturvallisuuteen liittyvistä tapahtumista ja poikkeuksista. Eräs suositeltu tapa lokien turvaamiseksi on ohjata keskeiset lokitiedot keskitetylle ja vahvasti suojatulle lokipalvelimelle, jonka tiedot varmuuskopioidaan päivittäin erilliseen, vähintään vastaavan turvallisuusluokan ympäristöön. Lokitietojen kerääminen ja tallennus tulee pyrkiä toteuttamaan siten, että lokitietojen poistaminen tai muuttaminen voidaan havaita myös tilanteissa, joissa esimerkiksi lokilähteen ja lokikeräimen välinen verkkoyhteys ei ole käytettävissä. Vastaavasti esimerkiksi verkosta pysyvästi irtikytkettyjen työasemien lokienkeräys sekä kerättyjen lokitietojen varmistukset edellyttävät säännöllistä prosessia. Sekä ylläpitäjien oikeusturvan, kuin myös tietomurtoepäilyjen tutkinnan tukemiseksi, suositellaan tehtävien erottelua toteutettavaksi siten, että lokitietojen ylläpito on eriytetty muusta ylläpitohenkilöstöstä. Jäljitettävyyden toteuttamisessa tulee huomioida myös tilanteet, joissa järjestelmään kirjautuneella on mahdollisuus suorittaa toimintoja toista tiliä käyttäen (user impersonation). Lokitietojen tallennus- ja seurantaohjelmiston toimivuutta tulee myös seurata, ja mahdolliset häiriöt tulee pystyä havaitsemaan lyhyelle aikaviiveellä (esim. yhden vuorokauden sisällä lokilähteen lopetettua lokien toimittamisen). Lokitietojen säilytysajoissa tulee huomioida kyseessä olevan käyttötapauksen tarpeet. Esimerkiksi joidenkin tietojen käsittely- ja luovutuslokeille voi olla perusteltua edellyttää eroavia säilytysaikoja, kuin poikkeamatilanteiden selvittämiseksi kerättäville lokitiedoille. Esimerkiksi viranomaistoiminnassa rikosoikeudelliset vanhentumisajat voivat johtaa tyypillisesti vähintään viiden vuoden säilytysaikatarpeisiin. Usein käytettynä käytäntönä on, että 6 kuukauden lokitiedot ovat saatavilla reaaliaikaisesti, ja pidemmän aikavälin lokitiedot ovat tarvittaessa saatavissa muutamien työpäivien viiveellä. Lokitietojen erilaisia käyttötapauksia on käsitelty myös Tiedonhallintalautakunnan suosituksessa (2020:21, luku 7). Toteutus edellyttää usein myös sen huomioon ottamista, että lokien säilytystilaa ja -aikaa kasvatetaan riittäviksi. Suositus: lokeille varataan tilaa ympäristössä riittäväksi arvioitava määrä. Riittävän ajan määritys voidaan tehdä esimerkiksi siten, että arvioidaan yhden kuukauden lokikertymän perusteella riittävä tila vaadittavalle säilytysaikajaksolle. Huom.: tilalle on syytä varata reilusti ”puskuria”, sillä poikkeavat tilanteet ja myös tietyt hyökkäystyypit kasvattavat lokimäärää merkittävästi.

Toteutusesimerkki	Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Toimintaan on jalkautettu kirjallinen lokien keräys-, luovutus-, hälytys- ja seurantapolitiikka/-ohje, joka on muodostettu ottaen huomioon toiminnan vaatimukset. 2) Tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. 3) Keskeiset tallenteet säilytetään vähintään 6 kuukautta, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. Käsittelylokit ja tallenteet, joita koskee esimerkiksi viranomaistoiminnan rikosoikeudelliset vanhentumisajat, säilytään vähintään 5 vuotta. 4) Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta).
Lainsäädäntö	TihL 17 §, 15 §; TLA 7 §,14 §
Viitteet	Julkri: HAL-7.1; Katakri: I-10
Muita lisätietoja	The United States Government Configuration Baseline (USGCB); ISO/IEC 27002:2022 5.33, 8.15, 8.17; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 7); PiTuKri JT-01
Tunniste	**TEK-12.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Turvallisuuteen liittyvien tapahtumien jäljitettävyys - tietojen luovutukset
Vaatimus	Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.
Yleiskuvaus	Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.
Toteutusesimerkki	
Lainsäädäntö	TihL 17 §, 15 §; TLA 7 §, 14 §
Viitteet	Julkri: HAL-07.1, TSU-18; Katakri: I-10
Muita lisätietoja	

Tunniste	TEK-12.2, L:TL III, E:, S:, TS:
Nimi	Turvallisuuteen liittyvien tapahtumien jäljitettävyys - TL III
Vaatimus	Turvallisuusluokan II–III tiedon käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi).
Yleiskuvaus	Turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvien lokitietojen säilytyksestä on annettu suositus VM 2021:5: ”Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä”.
Toteutusesimerkki	Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että kohtien 1–4 lisäksi toteutetaan seuraavat toimenpiteet: 5) Keskeiset tallenteet säilytetään vähintään 5 vuotta, ellei lainsäädäntö, suositukset tai sopimukset edellytä pitempää säilytysaikaa. Tallenteita, joilla on esimerkiksi poikkeamatilanteiden selvittelyn tai viranomaistoiminnan rikosoikeudelliselta kannalta hyvin vähäistä merkitystä, voidaan säilyttää lyhyemmän ajan, esimerkiksi 2-5 vuotta. 6) Lokitiedot varmuuskopioidaan säännöllisesti. 7) Samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on synkronoitu sovitun ajanlähteen kanssa. 8) On olemassa menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen. 9) Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkinnät.
Lainsäädäntö	TihL 17 §, 15 §; TLA 7 §, 14 §
Viitteet	Katakri: I-10
Muita lisätietoja	Valtiovarainministeriö: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5) 7.9.

Tunniste	TEK-12.3, L:TL I, E:, S:, TS:
Nimi	Turvallisuuteen liittyvien tapahtumien jäljitettävyys - TL I
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokan I tietojen käsittelyssä suositellaan riskiperustaisesti turvallisuusluokkaa II pidempiä säilytysaikoja lokitiedoille (esimerkiksi vähintään 10 vuotta). Turvallisuusluokan I tietojenkäsittely-ympäristöt ovat tyypillisesti suppeita, koostuen esimerkiksi kaikista verkoista pysyvästi irtikytketyistä päätelaitteista. Toisaalta esimerkiksi 10 vuoden lokikertymän säilyvyys on haastava toteuttaa uskottavasti vain päätelaitteilla, joten tällaisten päätelaitteiden lokienkeräys sekä kerättyjen lokitietojen varmistukset edellyttävätkin yleensä suunniteltua säännöllistä prosessia. Käytännön toteutustapana voi olla esimerkiksi lokitietojen säännöllinen kerääminen irtomedialle, jota käsitellään ja säilytetään sen elinkaaren ajan kuin turvallisuusluokan I tietoa. Lisäksi huomioitava, että mikäli tietojärjestelmän pääsynhallinta tai esimerkiksi toimien jäljitettävyys nojautuu fyysisen turvallisuuden menettelyihin, myös näistä syntyviä tallenteita saattaa olla perusteltua säilyttää ja hallinnoida turvallisuusluokan I mukaisilla menettelyillä.
Lainsäädäntö	TihL 17 §, 15 §; TLA 7 §, 14 §
Viitteet	Katakri: I-10
Muita lisätietoja	

Tunniste	TEK-13, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä
Nimi	Poikkeamien havainnointikyky ja toipuminen
Vaatimus	Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely-ympäristön suojattu tilanne viipymättä.
Yleiskuvaus	Tekninen poikkeamien havainnointikyky pohjautuu yleensä kolmeen lähteeseen: 1) Verkkoliikenteessä näkyviin tapahtumiin, 2) kerättyihin tallenteisiin (lokeihin) ja 3) kohteilla (hosts) näkyviin tapahtuviin. Riittävä tekninen havainnointikyky pystytään yleensä toteuttamaan edellä mainittuja havainnointilähteitä yhdistelemällä. Mitä tarkemmin kyseinen tietojenkäsittely-ympäristö ja sen normaali toiminta tunnetaan, sitä paremmin pystytään myös havainnoimaan normaalista toiminnasta eroavia tapahtumia. Normaalista toiminnasta eroavien tapahtumien havainnointi tukee myös sellaisten hyökkäysten havainnointia, joista ei ole saatavilla hyökkäysten tunnistetietoja (IoC, Indicator of Compromise). Tietojenkäsittely-ympäristön normaali toiminta tulisi tuntea koko elinkaaren ajalta, aina alkuhetkistä käytöstä poistoon asti. Myös muutostenhallinta (TEK-17) tukee poikkeamien havainnointikykyä, muun muassa laitteisto- ja ohjelmistokonfiguraatiomuutosten säännöllisen tarkastelun avulla. Tarkkailuun ja havaitun hyökkäyksen vaikutusten rajoittamiseen on useita soveltuvia toteutusmahdollisuuksia keskeisten verkkosolmujen tasolla tapahtuvasta tarkastelusta aina työasema-/palvelinkohtaisiin sensoreihin sekä näiden yhdistelmiin. Riippumatta käytetyistä verkkolaitteista ja toimittajista, verkkotason havainnointikyvyn käytännön toteutus edellyttää tyypillisesti verkkoliikenteen normaalin tilan tuntemista. Turvallisuusluokan IV käsittely-ympäristöissä verkkoliikennetason havainnointikyvyn tulisi kattaa erityisesti verkon/kohteen ulkorajan, ja III-luokasta lähtien ulkorajan yhdyskäytäväratkaisun sekä verkon/kohteen sisäpuolen liikennöinnin. Hyökkäyksen/väärinkäyttöyrityksen havaitseminen edellyttää useimmissa ympäristöissä käytännössä automatisoitujen havainnointi- ja hälytystyökalujen käyttöä. Joissain tilanteissa lokitietojen manuaalinen käsittely on myös mahdollista ja jopa välttämätöntä, mikäli automaattisin keinoin ei esimerkiksi ole havaittu poikkeamaa ja poikkeamatilanne vaatii tarkempaa selvitystä. Tulee myös muistaa, että lokeihin saa kerätä vain tietoturvaan liittyvien toimenpiteiden kannalta välttämättömiä tietoja, eikä toimenpiteitä toteutettaessa saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa. Yleisesti tulee huomioida, että havainnointikyky edellyttää kunkin tietojenkäsittely-ympäristön ominaispiirteiden tuntemista, ja muun muassa kriittisten kohteiden ja seurattavien tapahtumien määrittelyä ja räätälöintiä kyseessä olevan tietojenkäsittely-ympäristön mukaisesti, sekä havainnointikyvyn jatkuvaa ylläpitoa. Tietojenkäsittely-ympäristön palauttaminen takaisin suojattuun tilaan kohtuullisessa ajassa edellyttää yleensä suunniteltuja, kuvattuja, koulutettuja sekä harjoiteltuja prosesseja sekä teknisiä menetelmiä. Poikkeamien havainnointikyvyn kehittämisessä ja ylläpitämisessä tulee huomioida myös koko henkilöstön rooli. Esimerkiksi loppukäyttäjien ilmoittamat havainnot voivat tuottaa arvokasta tietoa hyökkäysten tai niiden yritysten havainnointiin.
Toteutusesimerkki	Verkkoliikenteen normaali tila (liikennemäärät, protokollat ja yhteydet) on tiedossa. On olemassa menettely, jolla verkkoliikenteen normaaliin tilaan nähden eroavat tapahtumat (esimerkiksi poikkeavat yhteydet tai niiden yritykset) pyritään havaitsemaan.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom, 17 §; TLA 7 §, 11 § 1 mom 2 k
Viitteet	Julkri: TEK-17; Katakri: I-11, T-07, T-12
Muita lisätietoja	ISO/IEC 27002:2022 5.25, 5.26, 8.15, 8.16; PiTuKri TT-02, JT-01, TJ-05

Tunniste	TEK-13.1, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä
Nimi	Poikkeamien havainnointikyky ja toipuminen - poikkeamien havainnointi lokitiedoista
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Suositellaan toteuttamaan menettely, jolla kerätyistä tallenteista ja tilannetiedosta (esimerkiksi muutokset lokikertymissä) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan).
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom, 17 §; TLA 7 §, 11 § 1 mom 2 k
Viitteet	Katakri: I-11
Muita lisätietoja	ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05
Tunniste	**TEK-13.2, L:TL IV, E:Tärkeä, S:, TS:**
Nimi	Poikkeamien havainnointikyky ja toipuminen - TL IV
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	1) On olemassa menettely, jolla kerätyistä tallenteista ja tilannetiedosta (esimerkiksi muutokset lokikertymissä) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan). 2) On olemassa menettely, jolla tietojenkäsittely-ympäristön kohteista (hosts, esimerkiksi työasemat ja palvelimet) voidaan havainnoida poikkeamia. 3) On olemassa menettely havaituista poikkeamista toipumiseen.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom, 17 §; TLA 7 §, 11 § 1 mom 2 k
Viitteet	Katakri: I-11
Muita lisätietoja	ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05
Tunniste	**TEK-13.3, L:TL I, E:, S:, TS:**
Nimi	Poikkeamien havainnointikyky ja toipuminen - TL I
Vaatimus	Käyttäjien ja ylläpitäjien toimintaa seurataan poikkeuksellisen toiminnan havaitsemiseksi.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokan I tietojen käsittelyssä suositellaan tehostettua poikkeamien havainnointikykyä, painottaen muun muassa tietojenkäsittely-ympäristön käyttäjien ja ylläpitäjien toiminnan seurantaa.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom, 17 §; TLA 7 §, 11 § 1 mom 2 k
Viitteet	Katakri: I-11
Muita lisätietoja	ISO/IEC 27002:2022 8.16; PiTuKri JT-01, TJ-05
Tunniste	**TEK-14, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Ohjelmistojen turvallisuuden varmistaminen
Vaatimus	Sovellukset ja ohjelmointirajapinnat (API:t) suunnitellaan, kehitetään, testataan ja otetaan käyttöön alan hyvien turvallisuuskäytäntöjen mukaisesti. Sovellusten ja rajapintojen on kestettävä niitä vastaan käytettävissä olevat yleiset hyökkäysmenetelmät ilman, että käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus vaarantuu.

Yleiskuvaus

Ohjelmistot ja niiden käyttötarkoitukset eri tietojenkäsittely-ympäristöissä eroavat toisistaan merkittävästi. Vastaavasti myös tarpeet ohjelmistojen turvalliseen toteutukseen ja käyttöönottoon eroavat merkittävästi eri tietojenkäsittely-ympäristöissä ja käyttötarkoituksissa. Esimerkiksi kaikista verkoista fyysisesti eriytetyssä työasemassa käytettävän toimisto-ohjelmiston turvallisuudelle asetettavat tarpeet eroavat tarpeista, jotka kohdistuvat useiden käyttäjien saavutettavissa olevaan asianhallintajärjestelmään.

Ohjelmistoihin liittyviä riskejä ja turvallisuustarpeita voidaan arvioida esimerkiksi ohjelmiston käyttötarkoituksen ja sen turvallisuutta mahdollisesti toteuttavan roolin, hyökkäyspinta-alan, sekä käsiteltävien tietojen luonteen ja turvallisuusluokan avulla. Mikäli ohjelmiston käyttötarkoituksena ja roolina on toimia esimerkiksi pääsyä rajaavana mekanismina turvallisuusluokiteltujen tietojen käsittelyssä, ohjelmiston luotettavasta toiminnasta tulisi pystyä varmistumaan. Ohjelmistoon kohdistuva hyökkäyspinta-ala voi vaikuttaa oleellisesti ohjelmistoon kohdistuviin turvallisuustarpeisiin. Tyypillisesti esimerkiksi turvallisuusluokan IV palvelut voivat olla saavutettavissa laajemmin ja heterogeenisemmän joukon toimesta, kuin esimerkiksi turvallisuusluokkien III-II palvelut. Ohjelmistoille asetettavat turvallisuusvaatimukset voivatkin olla turvallisuusluokan IV järjestelmissä joiltain osin tiukempia kuin esimerkiksi sellaisissa tiukasti eristetyissä ja suppeissa korkeamman turvallisuusluokan järjestelmissä, joissa jokaisella käyttäjällä on tiedonsaantitarve (need-to-know) kaikkeen järjestelmässä käsiteltävään tietoon. Käsiteltävien tietojen turvallisuusluokka ja oletettu kiinnostavuus ulkopuolisille toimijoille voi vaikuttaa ohjelmistoon kohdistuvaan riskiin ja suojaustarpeisiin. Esimerkiksi poliittisesti suuren ulkopuolisen kiinnostuksen kohteena olevat tiedot, tai korkealle turvallisuusluokitellut tiedot, voivat vaikuttaa merkittävästi ohjelmistoon kohdistuviin riskeihin ja turvallisuustarpeisiin myös kaikkein edistyneimpiin hyökkäyksiin varautumisessa.

Otettaessa käyttöön valmisohjelmistoa sekä tilattaessa räätälöityä tai itse tuotettua ohjelmistoa on tilaajan jo suunnitteluvaiheessa kiinnitettävä huomiota ohjelmiston ja sen käyttämien oheiskomponenttien tietoturvalliseen kehitykseen. Huomiota on kiinnitettävä myös muihin koko ohjelmiston elinkaaren kattaviin tekijöihin. Tekijöitä ovat esimerkiksi käyttöönotonaikaiset vaatimukset, sopimustekniikka, päivityskäytännöt ja muutostenhallinta. Turvallisuusluokitellun tiedon suojaukseen oleellisesti vaikuttavat ohjelmistot on toteutettava turvallisen ohjelmistokehityksen käytäntöihin nojautuen, kattaen sekä ohjelmistokoodin laadun että ohjelmistokehityksen prosessit.

Ohjelmiston vaatimusmäärittelyssä tulee jo hankintavaiheessa huomioida lainsäädännöstä johdetut vaatimukset. Erityisesti salauksiin (I-12), hallintaliittymiin (I-04), käyttäjähallintaan ja -tunnistukseen (I-06, I-07), kovennuksiin (I-08) ja jäljitettävyyteen (lokitukseen, I-10) liittyvät kokonaisuudet tulee huomioida myös ohjelmistojen toteutuksissa. Ohjelmistojen toteutukset eivät saa vaarantaa tiedonsaantitarpeen (need-to-know) toteutumista, tai tarjota ulkopuolisille toimijoille pääsyä suojattavaan tietojenkäsittely-ympäristöön tai sen osakokonaisuuksiin. Elinkaaren vaiheissa tulee varmistua erityisesti ohjelmistokorjausten tekemisen vastuutuksista, sekä mahdollistettava ohjelmiston turvallisuuden ylläpito myös uusia hyökkäystekniikoita vasten. Myös valmisohjelmistojen riittävästä laadusta voidaan pyrkiä varmistumaan vastaavia periaatteita noudattaen.

Joskus voi tulla tarve käyttää palveluita, joiden ohjelmakoodin ja sen kehityskäytäntöjen näkyvyys on heikkoa tai jopa olematonta. Tällaisten ohjelmistojen luotettavuudesta voidaan pyrkiä saamaan näyttöä esimerkiksi tutkimalla päivitystiheyksiä, dokumentaatiota ja mahdollista muuta näkyvyyttä, kuten olemassa olevia testiraportteja. Tällaisissa tilanteissa voi turvallisen konfiguroinnin lisäksi hyödyntää myös korvaavia suojauksia. Turvallisessa konfiguroinnissa ja korvaavina suojauksina voi tietyin rajoituksin hyödyntää esimerkiksi tehostettua havainnointikykyä, kovennuksia, koodin suorituksenaikaista rajoittamista (esim. AppLocker, SELinux, AppArmor), sovelluspalomuureja (WAF), sekä koko ohjelmiston loogista eriyttämistä esimerkiksi virtualisointia hyödyntäen.

Ohjelmistojen turvallisuudesta varmistumiseen tulee hyödyntää aihepiirin tarkentavia ohjeita ja standardeja. Näitä ovat esimerkiksi VAHTI Sovelluskehityksen tietoturvaohje (VAHTI 1/2013), OWASP Application Security Verification Standard (ASVS) ja Kyberturvallisuuskeskuksen ohje ”Turvallinen tuotekehitys: kohti hyväksyntää”.

Toteutusesimerkki	1) Ohjelmistojen (sovellukset, palvelut, järjestelmät) käyttötarkoitukset ja ohjelmistojen turvallisuutta mahdollisesti toteuttavat roolit on tunnistettu. 2) Ohjelmistojen (sovellukset, palvelut, järjestelmät) turvallisuustarpeet on arvioitu, huomioiden erityisesti ohjelmiston käyttötarkoituksen ja sen turvallisuutta mahdollisesti toteuttavan roolin, hyökkäyspinta-alan, sekä käsiteltävien tietojen luonteen ja turvallisuusluokan. 3) Ohjelmistojen (sovellukset, palvelut, järjestelmät) riippuvuudet ja rajapinnat on tunnistettu. Riippuvuuksiin ja rajapintoihin on kohdistettu ohjelmistoa vastaavat vaatimukset, huomioiden esimerkiksi käytetyt kirjastot, rajapinnat (API:t) ja laitteistosidonnaisuudet. Vaatimuksissa on huomioitu sekä palvelin- että asiakaspuolen osuudet. 4) Kriittiset ohjelmistot (sovellukset, palvelut, järjestelmät) toteutetaan tai toteutus tarkastetaan mahdollisuuksien mukaan luotettavaa standardia vasten tai/ja turvallisen ohjelmoinnin ohjetta hyödyntäen. 5) On varmistettu, että ohjelmistojen (sovellukset, palvelut, järjestelmät) ohjelmakoodin laadun ylläpito, kehitys ja muutoshallinta vastaavat tarpeita koko elinkaaren ajan. 6) On varmistettu, että ohjelmistot (sovellukset, palvelut, järjestelmät) täyttävät lainsäädännöstä johdetut vaatimukset. Erityisesti huomioitava salauksiin, hallintaliittymiin, käyttäjähallintaan ja -tunnistukseen, kovennuksiin ja jäljitettävyyteen liittyvät kokonaisuudet.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom; TLA 11 § 1 mom 2, 3, 4, 5 ja 6 k
Viitteet	Julkri: HAL-16; Katakri: I-13
Muita lisätietoja	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: Turvallinen tuotekehitys: kohti hyväksyntää; PiTuKri MH-02
Tunniste	**TEK-15, L:TL III, E:, S:, TS:**
Nimi	Hajasäteily (TEMPEST) ja elektroninen tiedustelu
Vaatimus	Turvatoimia toteutetaan turvallisuusluokiteltuihin tietoihin liittyvässä tietojenkäsittely-ympäristössä riittävän turvallisilla menetelmillä niin, että tahattomat sähkömagneettiset vuodot eivät vaaranna tietoja (TEMPEST-turvatoimet). Nämä turvatoimet on suhteutettava tiedon hyväksikäytön riskiin ja turvallisuusluokkaan. Käsiteltäessä turvallisuusluokan III tai II tietoja sähköisesti, on pidettävä huolta, että elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi.
Yleiskuvaus	Turvallisuusluokkien III-II käsittely-ympäristöissä raja-arvot ylittävän hajasäteilyn osalta suojautuminen toteutetaan ko. turvallisuusluokalle riittävän turvallisilla menettelyillä. Turvallisuusluokan III tietojen osalta on laajemmat mahdollisuudet hyväksyä korvaavia menettelyjä riittävän suojauksen saavuttamiseksi.
Toteutusesimerkki	1) Hajasäteilyyn liittyvät riskit on tunnistettu ja arvioitu. 2) Turvatoimet tai korvaavat menettelyt on mitoitettu riskeihin, tiedon turvallisuusluokkaan ja hyväksyttävään jäännösriskitasoon.
Lainsäädäntö	TLA 11 § 2 mom
Viitteet	Julkri: FYY-5.6; Katakri: I-14
Muita lisätietoja	Traficom: Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet; ISO/IEC 27002:2022 7.12

Tunniste	TEK-15.1, L:TL II, E:, S:, TS:
Nimi	Hajasäteily (TEMPEST) ja elektroninen tiedustelu - TL II
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	On toteutettu turvatoimet, jotka on mitoitettu riskeihin ja tiedon turvallisuusluokkaan. Kohteen hajasäteilyn vastatoimien riittävyys voidaan todentaa vyöhykemittauksella tai suojatun tilan mittauksella.
Lainsäädäntö	TLA 11 § 2 mom
Viitteet	Katakri: I-14
Muita lisätietoja	

Tunniste	TEK-15.2, L:TL I, E:, S:, TS:
Nimi	Hajasäteily (TEMPEST) ja elektroninen tiedustelu - TL I
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokan I tietojen suojaamisessa tulee huomioida turvallisuusluokan II tiedoista eroavat riskit ja suhteutettava nämä toteutettaviin turvatoimiin. Hajasäteilyä ja siltä suojautumisen periaatteita on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen hajasäteilyltä suojautumisen ohjeessa.
Lainsäädäntö	TLA 11 § 2 mom
Viitteet	Katakri: I-14
Muita lisätietoja	

Tunniste	TEK-16, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä
Nimi	Tiedon salaaminen
Vaatimus	Kun salassa pidettävää tietoa siirretään yleisissä tietoverkoissa, tieto salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä turvallisuusluokittelemattomia salassa pidettäviä tietoja.

Yleiskuvaus	Salassa pidettävän tiedon sähköiseen välitykseen liittyy useita riskejä. Riskien pienentäminen hyväksyttävälle tasolle edellyttää sekä henkilöstöön että tekniseen toteutukseen liittyvien tekijöiden huomiointia. Tilanteissa, joissa salassa pidettävää tietoa on tarve välittää esimerkiksi kahden organisaation välillä julkisen verkon kautta, turvallinen välitys edellyttää turvallisia salausratkaisuja ja avainhallintakäytäntöjä, sekä niiden käyttöön harjaantunutta henkilöstöä. Tilanteissa, joissa salausratkaisun käyttö edellyttää henkilöstön toimia (esimerkiksi salassa pidettävän dokumentin välitys toiseen organisaatioon sähköpostin salattuna liitteenä), tulee kiinnittää erityistä huomiota salausratkaisun turvallisen käytön jalkautukseen henkilöstölle. Teknisesti turvallinen salausratkaisu ei tuota salassa pidettävälle tiedolle riittävää suojausta esimerkiksi tilanteissa, joissa avainhallintakäytännöt ovat puutteellisia, tai joissa henkilöstö ei käytä salausratkaisua siihen liittyvien turvallisen käytön periaatteiden mukaisesti. Vastaanottajan riittävän luotettava varmistaminen riippuu merkittävästi käytetystä salausratkaisusta. Esimerkiksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen turvallisuusluokitellun tiedon suojaamiseen hyväksymien salausratkaisujen käyttöpolitiikoissa otetaan usein kantaa myös käyttäjien tunnistamiseen silloin, kun kyseistä salausratkaisua käytetään esimerkiksi toisessa organisaatiossa olevalle henkilölle viestintään. Toisaalta useissa salausratkaisuissa vastapuolen tunnistaminen nojaa avaimistonhallinnan luotettavuuteen (esimerkiksi jaettuun salaisuuteen perustuva organisaation toimipisteiden tai kahden eri organisaation verkkojen välinen (LAN-2-LAN) salaus, tai jaettuun salaisuuteen perustuva tiedostosalaus). Käytettävien salausvahvuuksien ja -asetusten valinnassa voidaan hyödyntää lähtökohtaisesti turvallisuusluokan IV mukaisia vahvuuksia ja asetuksia. Internet, sekä operaattorin tarjoamat MPLS-verkot ja esimerkiksi niin sanotut mustat kuidut tulkitaan julkisiksi verkoiksi. Tämä kattaa puhelimen, telekopion (faksi), sähköpostin, pikaviestimet ja muut vastaavat tietoverkon kautta toimivat tiedonsiirtomenetelmät.
Toteutusesimerkki	1) Siirrettäessä salassa pidettävää tietoa ko. tiedolle hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolella verkon kautta tulee ottaa huomioon erityisesti salauksen rooli keskeisenä suojauksena. a) Henkilöstöllä on käytössä työvälineet ja menetelmät turvallisuusluokittelemattoman salassa pidettävän tiedon suojaamiseksi salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia. b) Henkilöstön osaamisesta salausratkaisun turvalliseen käyttöön on varmistuttu (esimerkiksi ohjeistus, koulutus ja valvonta). 2) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät vähintään a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen. 3) Salausratkaisun toimitusketjun turvallisuudesta on varmistuttu riittävällä tasolla. Erityisesti salausratkaisun toimitusketju luotettavalta valmistajalta kohteen tietojenkäsittely-ympäristöön on varmistettu.
Lainsäädäntö	TihL 13 § 1 mom, 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Julkri: TEK-01; Katakri: I-01, I-12, I-15, I-18
Muita lisätietoja	Traficom: Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut; Traficom: Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat; Traficom: Turvallinen tuotekehitys: kohti hyväksyntää; Tiedonhallintalautakunta: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2020:19, luku 7); ISO/IEC 27002:2022 5.14, 5.31, 8.24; PiTuKri JT-05, SA-01, SA-02, SA-03

Tunniste	TEK-16.1, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä
Nimi	Tiedon salaaminen - salaaminen turvallisuusalueen sisällä
Vaatimus	Kun salassa pidettävää tietoa siirretään viranomaisen sisäisessä verkossa, voidaan käyttää alemman tason salausta tai salaamatonta tiedonsiirtoa riskinhallintaprosessin tulosten perusteella.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom; 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Julkri: FYY-7.1; Katakri: I-15
Muita lisätietoja	ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03
Tunniste	**TEK-16.2, L:TL IV, E:, S:, TS:**
Nimi	Tiedon salaaminen - turvallisuusluokitellun tiedon siirto turvallisuusalueiden ulkopuolella
Vaatimus	Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella, tieto/tietoliikenne salataan riittävän turvallisella menetelmällä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä turvallisuusluokiteltuja tietoja.
Yleiskuvaus	Erityisesti turvallisuusluokitellun tiedon suojaamisessa korostuu tarve käyttää salausratkaisuja, joiden riittävästä turvallisuudesta on luotettavaa näyttöä. Salausratkaisujen arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salausratkaisun oikeellisesta toiminnasta varmistumisen lisäksi huomioidaan muun muassa salausratkaisun käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa merkittävästi tilanteeseen, jossa salausta käytetään liikennöintiin hallitun fyysisesti suojatun alueen sisällä (esimerkiksi kahden turva-alueen välinen liikennöinti hallinnollisen alueen kautta). Muihin salausratkaisujen arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi ko. käyttötapauksen vaatimukset tiedon salassapitoajalle ja kryptografiselle eheydelle. Puhtaasti ohjelmistopohjaiset salausratkaisut ovat tyypillisesti hyväksyttävissä IV- ja joissain tilanteissa erityisehdoilla myös III-luokille. II-luokalle ja useimmin myös III-luokalle edellytetään tyypillisesti enemmän alustan luotettavuudelta. Salausratkaisujen hyväksyntäprosessia on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen ohjeessa salaustuotearvioinneista ja -hyväksynnistä. Salausratkaisun vähimmäisvaatimuksia on käsitelty myös Kyberturvallisuuskeskuksen ylläpitämässä salausvahvuuskuvauksessa, sekä turvallisen tuotekehityksen ohjeessa.
Toteutusesimerkki	1) Organisaatiossa on tunnistettu käyttötapaukset, joissa turvallisuusluokitellun tiedon suojaamiseen on tarve käyttää salausratkaisuja. Tunnistetut käyttötapaukset kattavat kaikki tilanteet, joissa turvallisuusluokitellun tiedon suojaaminen nojaa täysin tai osittain salausratkaisuun. Erityisesti on huomioitu liikennöinti julkisen tai matalamman turvallisuusluokan verkon kautta, tiedon välitys toiseen organisaatioon, ja turvallisuusalueiden ulkopuolelle vietävät päätelaitteet. 2) On hankittu ko. turvallisuusluokalle a) toimivaltaisen viranomaisen hyväksymät salausratkaisut ja käytetään niitä hyväksynnän yhteydessä määritellyn käyttöpolitiikan ja -asetusten mukaisesti, tai b) toimivaltaisen viranomaisen myöntämät tapauskohtaiset hyväksynnät ja käyttöpolitiikat-/asetukset sellaisille salausratkaisuille, joilla ei ollut entuudestaan voimassaolevaa hyväksyntää. 3) Siirrettäessä turvallisuusluokiteltua tietoa ko. turvallisuusluokalle hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella verkon kautta tulee ottaa huomioon erityisesti salauksen rooli keskeisenä suojauksena. a) Henkilöstöllä on käytössä työvälineet ja menetelmät turvallisuusluokitellun tiedon suojaamiseksi toimivaltaisen viranomaisen hyväksymällä salausratkaisulla. b) Henkilöstön osaamisesta riittävän turvallisen salausratkaisun turvalliseen käyttöön on varmistuttu (esimerkiksi ohjeistus, koulutus ja valvonta).

Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Julkri: FYY-7.1; Katakri: I-01, I-12, I-15, I-18, F-08.1
Muita lisätietoja	ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03
Tunniste	**TEK-16.3, L:TL IV, E:, S:, TS:**
Nimi	Tiedon salaaminen - turvallisuusluokitellun tiedon siirto turvallisuusalueiden sisällä
Vaatimus	Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen.
Yleiskuvaus	
Toteutusesimerkki	2) Tilanteissa, joissa turvallisuusluokiteltua tietoa siirretään fyysisesti suojattujen turvallisuusalueiden sisäpuolella, a) ko. turvallisuusluokan liikennekanava on fyysisesti suojattu (esimerkiksi kaapelointi, joka kulkee kokonaisuudessaan suppean, esimerkiksi vain yhden huoneen kattavan ko. turvallisuusluokan tiedon säilytykseen hyväksytyn fyysisesti suojatun turvallisuusalueen sisällä), tai b) tieto suojataan riittävän turvallisella matalamman tason salauksella (esim. HTTPS ko. turvallisuusluokan verkon sisäisessä liikenteessä).
Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Julkri: FYY-7.1; Katakri: I-15
Muita lisätietoja	
Tunniste	**TEK-16.4, L:TL III, E:, S:, TS:**
Nimi	Tiedon salaaminen - TL III
Vaatimus	Vain turvallisuusluokan III sähköisten tietojen säilytys on mahdollista kyseisen turvallisuusluokan mukaisessa päätelaitteessa turva-alueen ulkopuolella edellyttäen, että a) tiedot on suojattu ko. turvallisuusluokalle riittävän turvallisella salausratkaisulla , ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle edellytettävästä luottamuksellisuudesta ja eheydestä on huolehdittu riittävin menettelyin.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 §
Viitteet	Julkri: FYY-7.1; Katakri: F-04, I-12, I-17, I-18
Muita lisätietoja	

Tunniste	TEK-16.5, L:TL I, E:, S:, TS:
Nimi	Tiedon salaaminen - TL I
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	Muissa tilanteissa, joissa turvallisuusluokan I tietojen suojaamiseen käytetään salausratkaisuja, esimerkiksi päätelaitteiden kiintolevyjen salaukseen tai eri tiedon omistajien tietojen erotteluun, suositellaan huomioitavaksi, että turvallisuusluokan I tietojen suojaamiseen riittävän luotettavia, hyväksyttyjä salausratkaisuja on saatavilla äärimmäisen rajoitetusti. Tällaisissa tilanteissa salausratkaisut ovatkin lähtökohtaisesti vain tukevassa roolissa muille suojauksille, erityisesti fyysiselle pääsynhallinnalle.
Toteutusesimerkki	Erityisesti huomioitava, että turvallisuusluokan I tietojen suojaamiseen riittävän luotettavia, hyväksyttyjä salausratkaisuja on saatavilla erittäin rajoitetusti. Tämä edellyttääkin tyypillisesti turvallisuusluokan I tietojen siirtämistä turvallisuusluokalle I hyväksytyllä kuriirimenettelyllä tilanteissa, joissa turvallisuusluokan I tietoa on tarve siirtää fyysisten turva-alueiden välillä.
Lainsäädäntö	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §
Viitteet	Katakri: I-15
Muita lisätietoja	
Tunniste	**TEK-17, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Muutoshallintamenettelyt
Vaatimus	Tietojenkäsittely-ympäristöön tehtäviin muutoksiin on käytössä turvallisuuden huomioiva muutostenhallintamenettely.

Yleiskuvaus	Tietojenkäsittely-ympäristön tietoturvallisuuden ja muutosten luotettava hallinta edellyttää, että ympäristön teknin-en rakenne ja esimerkiksi kaikki siihen kuuluvat laitteistot ja ohjelmistot ovat tiedossa. Tietojärjestelmien asetuk-sien ja toiminnan muuttumista tulee valvoa ja havaittujen muutosten tulee johtaa niiden oikeellisuuden tarkistami-seen. Ajantasaista kirjanpitoa vasten tarvittavat muutokset kyetään koko elinkaaren ajan kohdistamaan täsmällises-ti, muutosten vaikutukset ovat helpommin ennustettavissa ja ympäristön turvallisuuden tarkastelu on mahdollista suorittaa. Kirjanpidon toteuttamisessa voi hyödyntää esimerkiksi verkkokuvia, laite- ja ohjelmistokomponenttiluet-teloita sekä konfiguraatiotietokantoja. Tietojenkäsittely-ympäristön tietoturvallisuudesta tulee pystyä varmistumaan koko elinkaaren ajan. Tämä edellyttää muutostarpeiden jatkuvaa seurantaa sekä säännöllisiä muutoksia. Muutostarpeita voi seurata esimerkiksi tietojen-käsittely-ympäristön järjestelmien elinkaaren päättymisestä tai nykyisten suojausten kyvyttömyydestä vastata uu-siin hyökkäysmenetelmiin. Esimerkiksi ohjelmistojen päivitykset voivat aiheuttaa odottamattomia seurauksia, kuten turvallisuusasetusten ja käyttöoikeuksien muuttumista tai uusien turvattomien palvelujen mukaantuloa tietojenkä-sittely-ympäristöön. Haitallisia seurauksia voidaan pyrkiä ennaltaehkäisemään esimerkiksi kattavalla testauksella ja muutoslokien (tyypillisesti esim. changelog, readme) tarkastelulla. Haitallisia seurauksia voidaan pyrkiä havainnoi-maan esimerkiksi (testiympäristöön asennettujen) päivitysten jälkeisten konfiguraatioiden tarkastelulla, sekä muun muassa automatisoiduilla skannauksilla ja konfiguraatiovertailuilla. Laitteiston suojauksessa luvattomien laitteiden kytkemistä vastaan voidaan hyödyntää esimerkiksi a) laitteiden sijoittamista sinetöityyn ja/tai hälytyslaitteella varustettuun turvakehikkoon tai vastaavaan, b) peukalointia vastaan suojattujen laitteiden käyttämistä, tai c) jotain vastaavaa menettelyä (esim. käytettävien laitteiden sinetöintiä). Käytettäessä sinetöintiin perustuvaa me-netelmää, tulisi sinettien eheyden tarkastamiseen olla säännöllinen prosessi. Luvattomien muutosten tai laitteistojen tarkasteluun hyväksyttävissä oleva tarkastustiheys riippuu kyseessä olevas-sa kohteessa toteutetuista menetelmistä, joilla rajoitetaan ja valvotaan kohteeseen (tietojärjestelmä, fyysinen tila) pääsyä. Useimmissa ympäristöissä voi riittää tarkastukset esimerkiksi puolivuosittain tai vuosittain. Luvattomien laitteistojen kytkemistä vastaan suojautumisessa tulee huomioida myös henkilöstön ohjeistus. On otet-tava huomioon, että päätelaitteisiin ei saa kytkeä muita kuin kyseisen turvallisuusluokan tietojenkäsittely-ympäris-töön hyväksyttyjä oheislaitteita (esim. näyttö, näppäimistö, hiiri) ja medioita (esimerkiksi vain kyseiseen ympäris-töön hyväksytty USB-muisti). Erityisesti tilanteissa, joissa päätelaitetta käytetään matalamman turvallisuusluokan fyysisessä tilassa, ei yleensä ole mahdollista käyttää ko. tilassa säilytettäviä oheislaitteita tai medioita.
Toteutusesimerkki	1) Tietojenkäsittely-ympäristön kokoonpanosta on olemassa ajantasainen kirjanpito. Kirjanpidolla tarkoitetaan lait-teisto- ja ohjelmistokirjanpitoa, sekä tietoa turvallisuuteen vaikuttavista konfiguraatioista ja menettelyistä. 2) Tietojenkäsittelyyn ja tietojenkäsittely-ympäristöön liittyviin muutoksiin on käytössä muutostenhallintamenette-ly. Muutokset ovat jäljitettävissä. 3) On olemassa menetelmät, joilla varmistetaan tietojenkäsittely-ympäristön turvallisuustason säilyminen tehtyjen muutosten yhteydessä.
Lainsäädäntö	TihL 13 §, 15 §
Viitteet	Katakri: I-03, I-05, I-16, I-17, I-18, T-04, T-12
Muita lisätietoja	ISO/IEC 27002:2022 5.9, 5.36, 5.37, 8.19, 8.29, 8.32; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 5); PiTuKri MH-01

Tunniste	TEK-17.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Muutoshallintamenettelyt - uudelleenarviointi
Vaatimus	Tietoturvallisuutta koskevat tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 13 § 1 mom
Viitteet	Katakri: I-16
Muita lisätietoja	

Tunniste	TEK-17.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Muutoshallintamenettelyt - dokumentointi
Vaatimus	Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten- ja asetustenhallintaprosessia.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 5 § 2 mom
Viitteet	Katakri: I-16
Muita lisätietoja	ISO/IEC 27002:2022 8.9, 8.32

Tunniste	TEK-17.3, L:TL IV, E:Tärkeä, S:Tärkeä, TS:
Nimi	Muutoshallintamenettelyt - TL IV
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	1) Tietojenkäsittely-ympäristö on dokumentoitu sellaisella tasolla, että siitä pystytään selvittämään tietojenkäsittely-ympäristössä käytetyt laitteet ja ohjelmistot versiotietoineen (laite-, käyttöjärjestelmä- ja sovellusohjelmistot) ja se tukee myös haavoittuvuuksien hallintaa. 2) Tietojenkäsittely-ympäristöjä tarkkaillaan luvattomien muutosten tai laitteistojen havaitsemiseksi. Tietojenkäsittely-ympäristön kirjanpito pidetään ajan tasalla koko elinkaaren ajan. 3) Tietojenkäsittely-ympäristön turvallisuuden toteuttamiseen liittyvän aineiston (dokumentaatiot, sähköiset kirjanpidot ja vast.) luokittelu- ja suojaamistarpeet on määritetty.
Lainsäädäntö	TihL 5 § 2 mom, 13 § 1 mom
Viitteet	Katakri: I-16
Muita lisätietoja	ISO/IEC 27002:2022 5.9, 8.8

Tunniste	TEK-17.4, L:TL II, E:Kriittinen, S:Kriittinen, TS:
Nimi	Muutoshallintamenettelyt - TL II
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	1) Laitteistot suojataan luvattomien laitteiden (näppäilynauhoittimet, langattomat lähettimet ml. mobiililaitteet ja vastaavat) liittämistä vastaan.
Lainsäädäntö	TLA 11 § 1 mom 2 ja 5 k
Viitteet	Katakri: I-16
Muita lisätietoja	

Tunniste	TEK-18, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto
Nimi	Etäkäyttö
Vaatimus	Etäkäytössä käyttäjät ohjeistettu ja tunnistetaan riittävän luotettavasti.
Yleiskuvaus	Etäkäytöllä ja -hallinnalla tarkoitetaan perinteisessä merkityksessään organisaation toimitilojen ulkopuolelta tapahtuvaa tietojärjestelmien käyttöä/hallintaa tätä tarkoitusta varten hankitulla päätelaitteella. Normaalisti päätelaitteena toimii organisaation henkilön käyttöön antama kannettava tietokone. Turvallisuusluokitellun tiedon osalta etäkäyttö soveltuu perinteisessä merkityksessään vain turvallisuusluokan IV tiedoille. Henkilöstön koulutuksessa ja ohjeistuksessa on huomioitava erityisesti salassa pidettävien tietojen suojaaminen sivullisilta. Sivullisilta suojaamiseen sisältyy muun muassa mahdollisten käsittelypaikkojen valinta ja erilaisiin paikkoihin liittyvät rajoitteet käsittelylle (salakatselun ja salakuuntelun estäminen), päätelaitteiden ja muiden työvälineiden suojaaminen varkauksilta ja peukaloinneilta (säilytys vain lukitussa tilassa ja aina muistialueiden salaus aktivoituna, sekä esimerkiksi suojapakkausten ja -koteloiden käyttö), sekä muut kyseisten päätelaitteiden ja muiden työvälineiden turvallisen käytön menettelyt.
Toteutusesimerkki	1) Etäkäytössä käyttäjät tunnistetaan luotettavasti. 2) Etäkäyttö on ohjeistettu ja sitä valvotaan.
Lainsäädäntö	TihL 4 § 2 mom, 13 § 1 mom; TLA 10 § 1 mom
Viitteet	Julkri: HAL-12, HAL-13, HAL-19; Katakri: I-17, I-18
Muita lisätietoja	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

Tunniste	TEK-18.1, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä
Nimi	Etäkäyttö - tietojen ja tietoliikenteen salaaminen
Vaatimus	Turvallisuusalueen ulkopuolella etäkäytössä käytettävät päätelaitteet, muistivälineet ja tietoliikenneyhteydet ovat suojattu käyttäen sellaisia salausratkaisuja, joissa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat valmistajilta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia.
Yleiskuvaus	Siirrettävien tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) osalta voidaan sallia salaamattomien laitteiden käyttö siinä tapauksessa, että tietovälineitä ei koskaan jätetä valvomatta hyväksyttyjen turvallisuusalueen ulkopuolella.

Toteutusesimerkki	1) Päätelaitteessa olevat tiedot tulee olla suojattu salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia. 2) Järjestelmien etäkäyttö edellyttää tietoliikenteen salausratkaisua, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia. 3) Tietovälineitä ei saa jättää valvomatta, elleivät turvallisuusalueiden ulkopuolelle viedyt salassa pidettävää tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattuja ratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §, 11 §, 12 §, 13 §
Viitteet	Julkri: FYY-7.1; Katakri: I-18
Muita lisätietoja	ISO/IEC 27002:2022 7.9, 7.10, 8.1
Tunniste	**TEK-18.2, L:TL IV, E:, S:, TS:**
Nimi	Etäkäyttö - turvallisuusluokitettujen tietojen ja tietoliikenteen salaaminen
Vaatimus	Turvallisuusalueen ulkopuolella etäkäytössä käytettävät päätelaitteet, muistivälineet ja tietoliikenneyhteydet ovat suojattu käyttäen ko. turvallisuusluokan huomioiden riittävän turvallisia salausratkaisuja.
Yleiskuvaus	Siirrettävien tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) osalta voidaan sallia salaamattomien laitteiden käyttö siinä tapauksessa, että tietovälineitä ei koskaan jätetä valvomatta hyväksyttyjen turva-alueiden ulkopuolella.
Toteutusesimerkki	1) Päätelaitteessa olevat tiedot tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella salausratkaisulla, ja päätelaitteen ko. turvallisuusluokalle riittävästä eheydestä tulee huolehtia. 2) Järjestelmien etäkäyttö edellyttää ko. turvallisuusluokan tietojen suojaamiseen riittävän turvallista liikenteen salausta. 3) Elleivät turvallisuusalueiden ulkopuolelle viedyt turvallisuusluokiteltua tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu ko. turvallisuusluokalle riittävän turvallisella menetelmällä, tietovälineitä ei jätetä valvomatta.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §, 11 §, 12 §, 13 §
Viitteet	Julkri: FYY-7.1; Katakri: I-18
Muita lisätietoja	ISO/IEC 27002:2022 7.9, 7.10, 8.1
Tunniste	**TEK-18.3, L:TL IV, E:Tärkeä, S:, TS:**
Nimi	Etäkäyttö - käyttäjien vahva tunnistaminen
Vaatimus	Etäkäytössä järjestelmien käyttäjät tunnistetaan käyttäen vahvaa, vähintään kahteen todennustekijään perustuvaa käyttäjätunnistusta.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 §, 11 § 1 mom 5 k
Viitteet	Katakri: F-04, I-18
Muita lisätietoja	

Tunniste	TEK-18.4, L:TL IV, E:Kriittinen, S:, TS:
Nimi	Etäkäyttö - hyväksytyt laitteet
Vaatimus	Etäkäytössä käytetään vain käyttöympäristöön hyväksyttyjä ja tunnistettuja laitteita.
Yleiskuvaus	
Toteutusesimerkki	Vain käyttöympäristöön hyväksyttyjä laitteita ja etäyhteyksiä käytetään.
Lainsäädäntö	TLA 10 §, 11 § 1 mom 5 k
Viitteet	Katakri: F-04, I-18
Muita lisätietoja	

Tunniste	TEK-18.5, L:TL III, E:, S:, TS:
Nimi	Etäkäyttö - turvallisuusluokitellun tiedon käyttö julkisella paikalla
Vaatimus	Turvallisuusluokiteltuja tietoja ei lueta tai muuten käsitellä matkalla tai julkisilla paikoilla.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 § 1 mom, 13 §
Viitteet	Julkri: FYY-7.1; Katakri: I-18
Muita lisätietoja	

Tunniste	TEK-18.6, L:TL III, E:Kriittinen, S:, TS:
Nimi	Etäkäyttö - laitetunnistus
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	Turvallisuusluokkien III ja II käsittely-ympäristöissä sekä muissa kriittisissä käsittely-ympäristöissä edellytetään käytön teknistä sitomista hyväksyttyyn etäkäyttölaitteistoon (esim. laitetunnistus).
Toteutusesimerkki	Etäkäyttö on estetty teknisesti muita kuin hyväksyttyjä laitteita käyttäen.
Lainsäädäntö	TLA 10 §, 11 § 1 mom 5 k
Viitteet	Katakri: I-18
Muita lisätietoja	

Tunniste	TEK-18.7, L:TL III, E:Kriittinen, S:, TS:
Nimi	Etäkäyttö - TL III
Vaatimus	Turvallisuusluokan III sähköisten tietojen etäkäyttö (käsittely) ja säilytys on mahdollista kyseisen turvallisuusluokan mukaisessa päätelaitteessa turva-alueiden ulkopuolella edellyttäen, että a) tiedot on suojattu ko. turvallisuusluokalle riittävän turvallisella salausratkaisulla, ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle edellytettävästä luottamuksellisuudesta ja eheydestä on huolehdittu riittävin menettelyin.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 10 § (TL III)
Viitteet	Katakri: I-18
Muita lisätietoja	

Tunniste	TEK-18.8, L:TL II, E:, S:, TS:
Nimi	Etäkäyttö - etäkäyttö turvallisuusalueella
Vaatimus	Järjestelmien etäkäyttö rajataan toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle.
Yleiskuvaus	Tiedon käsittely edellyttää fyysisesti suojattua turvallisuusaluetta tai korvaavia menettelyjä, joilla saavutetaan vastaavat fyysisen turvallisuuden olosuhteet.
Toteutusesimerkki	
Lainsäädäntö	TLA 10 § (TL II)
Viitteet	Katakri: I-18
Muita lisätietoja	
Tunniste	**TEK-18.9, L:TL I, E:, S:, TS:**
Nimi	Etäkäyttö - TL I
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	Turvallisuusluokan I tietoa saa säilyttää tai muutoin käsitellä ainoastaan turva-alueilla (TLA, 10 §), mikä asettaa rajoitteet myös etäkäytön mahdollisuuksille.
Toteutusesimerkki	
Lainsäädäntö	TLA 10 § (TL I)
Viitteet	Katakri: I-18
Muita lisätietoja	
Tunniste	**TEK-19, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto**
Nimi	Ohjelmistohaavoittuvuuksien hallinta
Vaatimus	Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.

Yleiskuvaus	Ohjelmistohaavoittuvuuksien hyödyntäminen on useissa hyökkäystyypeissä jossain vaiheessa mukana. On huomioitava, että haavoittuvaa lähdekoodia on niin käyttöjärjestelmäohjelmistoissa, palvelinsovelluksissa, loppukäyttäjäsovelluksissa, kuin esimerkiksi laiteohjelmistotason (firmware) sovelluksissa ja ajureissa, BIOS:issa ja erillisissä hallintaliittymissä (esim. iLo, iDrac). Ohjelmistovirheiden lisäksi haavoittuvuuksia aiheutuu konfiguraatiovirheistä ja vanhoista käytänteistä, esimerkiksi vanhentuneiden salausalgoritmien käytöstä. Vastuulliset toimittajat korjaavat ohjelmistoistaan löytyneitä haavoittuvuuksia. Riskejä voidaan pienentää korjausten asennuksilla. Haavoittuvuuden hallintaa toteuttaessa tulee huolehtia haavoittuvuusskannerin, CMDB:n ja muiden järjestelmien ajantasaisuudesta ja tietoturvallisuudesta. Haavoittuvuuksien hallinnan tulisi tähdätä tarkan tilannekuvan muodostamiseen siten, että toimintaan liittyy ohjelmisto- ja järjestelmäympäristön jatkuva seuranta ja kehittäminen. Osana tilannekuvan ylläpitoa havaittujen puutteiden ja erilaisten haavoittuvuuksien aiheuttama riski tulisi arvioida suhteessa käyttöympäristöön ja asettaa korjaavat toimenpiteet perustuen tämän arvion kriittisyyteen. Korjaavia toimenpiteitä ovat mm. ohjelmistotoimittajien haavoittuvuuskorjaukset, päivitykset ja konfiguraatiomuutokset, jotka tähtäävät riskin poistamiseen tai rajaamiseen. Lisäksi on syytä seurata käytettävien ohjelmistoversioiden tukea niiden toimittajalta. Vanhentuneisiin ohjelmistoversioihin ei julkaista aktiivisesti päivityksiä, jolloin myös tietoturvahaavoittuvuuksien korjaaminen voi olla mahdotonta. Tehokas prosessimainen haavoittuvuuksien hallinta edellyttää organisoitua ja vastuutettua toimintamallia, sekä yleensä myös organisaation sisäisten ja ulkoisten sidosryhmien yhteistyötä. Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa: - Turvapäivitysten asennuksessa voidaan hyödyntää myös menettelyä, jossa esimerkiksi virtuaalikoneista ylläpidetään luotettua, turvapäivitysten tasolla olevaa levykuvaa (golden image), ja käytössä olevat virtuaalikoneet korvataan tällä ajantasaisella levykuvalla säännöllisesti. Tässä ratkaisumallissa erityisesti huolellisuutta tulee kohdistaa menettelyihin, joilla pyritään varmistamaan levykuvan eheys. - Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.
Toteutusesimerkki	Vaatimus voidaan toteuttaa siten, että haavoittuvuuksien hallintaan on olemassa prosessi, joka sisältää vähintään alla mainitut toimenpiteet: 1) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan aktiivisesti ja tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti. 2) Päivitysten asentumisen onnistumista tarkastellaan säännöllisesti, vähintään kuukausittain. 3) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti vähintään (haavoittuvuusskannaus) vuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. 4) Löytyneiden haavoittuvuuksien sekä päivitysmenettelyjen puutteiden käsittely on järjestetty siten, että tietojenkäsittely-ympäristön suojaamiseen oleellisesti vaikuttavat heikkoudet poistetaan, korjataan tai muuten rajoitetaan siten, että turvallisuusluokiteltujen tietojen käsittely ei tarpeettomasti vaarannu.
Lainsäädäntö	TihL 13 §; TLA 11 § 1 mom 2 k
Viitteet	Julkri: HAL-16, HAL-16.1; Katakri: I-19
Muita lisätietoja	ISO/IEC 27002:2022 8.8; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-04

Tunniste	TEK-19.1, L:TL IV, E:Tärkeä, S:Tärkeä, TS:
Nimi	Ohjelmistohaavoittuvuuksien hallinta - TL IV
Vaatimus	Tietojenkäsittely-ympäristön laitteet tarkastetaan kattavasti ohjelmistohaavoittuvuuksien varalta vähintään vuosittain ja merkittävien muutosten yhteydessä.
Yleiskuvaus	
Toteutusesimerkki	1) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti vähintään (haavoittuvuusskannaus, CMDB jne.) vuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. 2) Laitteisto- ja ohjelmistokirjanpidon (ml. CMDB) sekä skannausohjelmiston ajantasaisuudesta ja tietoturvallisuudesta on huolehdittu.
Lainsäädäntö	TihL 13 §; TLA 11 § 1 mom 2 k
Viitteet	Katakri: I-19
Muita lisätietoja	ISO/IEC 27002:2022 8.8; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-04
Tunniste	**TEK-19.2, L:TL III, E:Kriittinen, S:Kriittinen, TS:**
Nimi	Ohjelmistohaavoittuvuuksien hallinta - TL III
Vaatimus	Tietojenkäsittely-ympäristön laitteet tarkastetaan kattavasti ohjelmistohaavoittuvuuksien varalta vähintään puolivuosittain ja merkittävien muutosten yhteydessä.
Yleiskuvaus	
Toteutusesimerkki	Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti vähintään (haavoittuvuusskannaus, CMDB jne.) puolivuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. ”Merkittäviin muutoksiin” voidaan laskea esimerkiksi verkkotopologian muutokset, uusien järjestelmien käyttöönotot ja/tai vanhojen service pack -tason päivitykset, palomuurien ja vastaavien suodatussääntöjen merkittävät muutokset, jne.
Lainsäädäntö	TihL 13 §; TLA 11 § 1 mom 2 k
Viitteet	Katakri: I-19
Muita lisätietoja	

Tunniste	TEK-20, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Varmuuskopiointi
Vaatimus	Varmistus- ja palautusprosessit on suunniteltu, toteutettu, testattu ja kuvattu siten, että ne vastaavat lainsäädännön ja toiminnan vaatimuksia.
Yleiskuvaus	Varmuuskopiointi suositellaan aina mitoitettavan toimintavaatimuksiin. Toimintavaatimuksiin nähden riittävässä varmuuskopioinnissa tulisi huomioida ainakin seuraavat: 1) Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää (recovery point objective, RPO). 2) Varmuuskopiot kattavat kaiken järjestelmän toiminnan jatkuvuuden kannalta olennaisen tiedon. 3) Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palauttuminen voi kestää (recovery time objective, RTO). 4) Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti. 5) Palautusprosessin dokumentointi on riittävällä tasolla. 6) Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä, jne.). Huom. Varmuuskopiot tulisi suojata fyysisen ja loogisen pääsynhallinnan menetelmin vähintään tiedon (mahdollisesti kasautumisvaikutuksen nostaman) turvallisuusluokan mukaisesti.
Toteutusesimerkki	Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Varmuuskopiot käsitellään ja säilytetään niiden elinkaaren ajan vähintään vastaavan turvallisuustason järjestelmissä. 2) Mikäli varmuuskopioita siirretään ko. turvallisuusluokan fyysisesti suojatun turvallisuusalueen ulkopuolelle, on menettelyt toteutettava kohtien TEK-16:ssa (sähköinen välitys) ja/tai FYY-08 (posti/kuriiri) sekä TEK-18 (kuljetus fyysisesti suojatun alueen ulkopuolelle). 3) Varmistusmediat hävitetään luotettavasti. 4) Järjestelmän ja tiedon palauttamista testataan säännöllisesti esimerkiksi automatisoidusti, jotta tieto voidaan palauttaa oikeaan tilaansa eheyden varmistamiseksi.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom; TLA 2 § 2 mom, 7 §, 11 § 1 mom 4 k
Viitteet	Julkri: VAR-09; Katakri: I-20
Muita lisätietoja	ISO/IEC 27002:2022 8.13; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 5); PiTuKri KT-03

Tunniste	TEK-20.1, L:TL IV, E:, S:, TS:
Nimi	Varmuuskopiointi -TL IV
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	Käsiteltäessä samalla varmistusjärjestelmällä eri omistajien tietoja, tarkastusoikeuden mahdollistavat erottelumenettelyt on toteutettava varmistusjärjestelmän liittymien ja tallennemedioiden osalta (esim. omistaja-/hankekohtaiset eri avaimilla salatut nauhat, joita säilytetään asiakaskohtaisissa kassakaapeissa/kassakaappilokeroissa).
Toteutusesimerkki	Käsiteltäessä samalla varmistusjärjestelmällä tarkastusoikeuden varaavien eri omistajien tietoja, tarkastusoikeuden mahdollistavat erottelumenettelyt on toteutettava ko. turvallisuusluokan mukaisesti varmistusjärjestelmän liittymien ja tallennemedioiden osalta.
Lainsäädäntö	TihL 13 § 1 mom, 16 §; TLA 7 §, 10 § 1 mom, 11 § 1 mom 3 k
Viitteet	Katakri: I-06, I-20
Muita lisätietoja	ISO/IEC 27002:2022 8.13; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 5); PiTuKri KT-03

Tunniste	TEK-20.2, L:TL III, E:, S:, TS:
Nimi	Varmuuskopiointi - varmuuskopioiden rekisteröinti ja käsittelyn seuranta
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Varmuuskopioista on rekisterit ja varmuuskopioiden käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai tietoon (esimerkiksi dokumentin osaksi).
Lainsäädäntö	TLA 14 §
Viitteet	Katakri: F-08.3, I-20
Muita lisätietoja	

Tunniste	TEK-21, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Sähköisessä muodossa olevien tietojen tuhoaminen
Vaatimus	Sähköisessä muodossa olevien tietojen tuhoaminen on järjestetty luotettavasti. Salassa pidettävien tietojen tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.
Yleiskuvaus	Tiedon suojaamisesta tulee huolehtia tiedon elinkaaren päättymiseen asti. Tämä tulee huomioida erityisesti tilanteissa, joissa käytetään kolmannen osapuolen palvelua tiedon tuhoamiseen, esimerkiksi kiintolevyjen sulattamiseen. Käytännön toteutusmallina yleensä menettely, jossa tiedosta vastuussa oleva organisaatio valvoo tiedon tuhoamisprosessin aina elinkaaren päättymiseen saakka. Tiedon turvallinen tuhoaminen tulee huomioida myös laitteiden elinkaaren hallinnassa ja hävittämisessä mukaan lukien oheislaitteet ja erilaiset muistivälineet. Myös henkilöstön rooli on syytä huomioida tuhoamisprosesseissa. Organisaation tulee järjestää henkilöstölle yksikäsitteinen tapa tietojen tuhoamiseen. +N79
Toteutusesimerkki	Tuhoaminen eri menetelmiä yhdistäen Tuhoamiseen voidaan käyttää silppuamisen korvaavana tai sitä tukevana suojauksena myös muita menetelmiä, joilla tietojen kokoaminen estetään luotettavasti (esimerkiksi silputun kiintolevyn sulattaminen). Myös salauksella pystytään pienentämään huomattavasti tietoon kohdistuvia riskejä tiedon ja laitteistojen elinkaarten eri vaiheissa. Sähköisessä muodossa olevien tietojen tuhoamisessa huomioon otettavaa Sähköisessä muodossa olevien tietojen luotettavan tuhoamisen menettelyjen tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu turvallisuusluokiteltua tietoa. Laitteistojen osien (kiintolevyt, muistit, muistikortit, jne.) sisältämän turvallisuusluokitellun tiedon luotettavasta tuhoamisesta on huolehdittava erityisesti käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä. Mikäli luotettava tyhjennys (esimerkiksi riittävän turvallinen ylikirjoitusmenettely) ei ole mahdollista, turvallisuusluokiteltua tietoa sisältävää osaa ei tule luovuttaa kolmansille osapuolille. Tilanteissa, joissa laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä, tulisi kolmannen osapuolen suorittamia huoltotoimenpiteitä valvoa, ja pyrkiä varmistumaan siitä, että turvallisuusluokiteltua tietoa ei viedä huoltotoimenpiteen yhteydessä.
Lainsäädäntö	TihL 21 § 2 mom; TLA 15 §
Viitteet	Julkri: FYY-11, FYY-11.1, FYY-11.2, FYY-11.3; Katakri: T-12, F-08.3, F-08.4, I-21
Muita lisätietoja	Traficom: Kiintolevyjen elinkaaren hallinta (26.10.2016); CPNI: Secure destruction of sensitive items (2017); ISO/IEC 27002:2022 7.10, 7.14; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 4); PiTuKri SI-02

Tunniste	TEK-21.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Sähköisessä muodossa olevien tietojen tuhoaminen - arkistointi
Vaatimus	Tietojen arkistointivelvollisuus on huomioitu tiedon elinkaaren hallinnassa.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TihL 21 §
Viitteet	
Muita lisätietoja	

Tunniste	TEK-21.2, L:Salassa pidettävä, E:, S:, TS:Henkilötieto
Nimi	Sähköisessä muodossa olevien tietojen tuhoaminen - pilvipalveluissa olevan tiedon tuhoaminen
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa: - Mikäli turvallisuusluokittelemattomat salassa pidettävät tiedot on tallennettu pilvipalveluun vain riittävän luotettavaksi arvioidussa salatussa muodossa, jäännösriskit saattavat olla hyväksyttävissä, mikäli salaukseen käytetty avaimisto pystytään luotettavasti tuhoamaan. Menettely voi soveltua myös henkilötietojen tuhoamiseen niiden lakisääteisen säilytysajan jälkeen.
Toteutusesimerkki	
Lainsäädäntö	TihL 21 § 2 mom
Viitteet	
Muita lisätietoja	ISO/IEC 27002:2022 5.23; PiTuKri SA-03

Tunniste	TEK-21.3, L:TL IV, E:, S:, TS:
Nimi	Sähköisessä muodossa olevien tietojen tuhoaminen - TL IV
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Tuhoaminen ylikirjoittamalla Tuhottaessa turvallisuusluokiteltua materiaalia ylikirjoittamalla, suositellaan noudatettavaksi Kyberturvallisuuskeskuksen ohjeen ”Kiintolevyjen elinkaaren hallinta” mukaisia vaatimuksia ylikirjoitukselle sekä muistivälineiden uusiokäytölle. Tuhoaminen silppuamalla Tuhottaessa turvallisuusluokiteltua materiaalia silppuamalla, noudatetaan suosituksen ”VM 2021:5 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä” mukaisia vaatimuksia kyseisen turvallisuusluokan aineiston silppukoolle.
Lainsäädäntö	TihL 21 § 2 mom; TLA 15 §
Viitteet	Julkri: FYY-11.1, FYY-11.2, FYY-11.3; Katakri: I-21
Muita lisätietoja	Traficom: Kiintolevyjen elinkaaren hallinta (26.10.2016); Tiedonhallintalautakunta: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5)

Tunniste	TEK-21.4, L:TL II, E:, S:, TS:
Nimi	Sähköisessä muodossa olevien tietojen tuhoaminen - toisen viranomaisen laatimat tiedot
Vaatimus	Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 15 § 2 mom
Viitteet	Katakri: I-21
Muita lisätietoja	

Tunniste	TEK-21.5, L:TL II, E:, S:, TS:
Nimi	Sähköisessä muodossa olevien tietojen tuhoaminen - tuhoamisen suorittaja
Vaatimus	Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö.
Yleiskuvaus	
Toteutusesimerkki	
Lainsäädäntö	TLA 15 § 2 mom
Viitteet	Katakri: I-21
Muita lisätietoja	

Tunniste	TEK-21.6, L:TL I, E:, S:, TS:
Nimi	Sähköisessä muodossa olevien tietojen tuhoaminen - TL I
Vaatimus	Alikriteeri tarkentaa pääkriteerin vaatimusta.
Yleiskuvaus	
Toteutusesimerkki	Turvallisuusluokan I sähköisessä muodossa olevan tiedon tuhoamisessa voidaan hyödyntää ”VM 2021:5 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä” koottuja turvallisuusluokan II silppukokoja, mikäli suojausta täydennetään viranomaisen hyväksymillä menettelyillä. Tällaisia menettelyihin sisältyvät tyypillisesti muun muassa silpun jatkokäsittely valvotusti polttamalla tai sulattamalla.
Lainsäädäntö	TLA 15 §
Viitteet	Katakri: I-21
Muita lisätietoja	

Tunniste	TEK-22, L:, E:, S:Normaali, TS:
Nimi	Tietojärjestelmien saatavuus
Vaatimus	Viranomaisen on varmistettava tietojärjestelmien saatavuus koko niiden elinkaaren ajan.
Yleiskuvaus	Saatavuusvaatimusten toteutuksen tulee huomioida tietojärjestelmältä edellytettävä kuormituksen kesto, vikasietoisuus ja palautumisaika.
Toteutusesimerkki	Saatavuusvaatimukset on tunnistettu. On tunnistettu vähintään pisin aika, jonka järjestelmä voi olla pois käytöstä, palautusaikatavoite ja palautuspistetavoite.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom 4 k
Viitteet	Julkri: VAR-02
Muita lisätietoja	ISO/IEC 27002:2022 8.6, 8.14
Tunniste	**TEK-22.1, L:, E:, S:Normaali, TS:**
Nimi	Tietojärjestelmien saatavuus - saatavuutta suojaavat menettelyt
Vaatimus	Saattavuutta suojaavien menettelyiden toteutus on suhteutettu palautusaikatavoitteeseen.
Yleiskuvaus	
Toteutusesimerkki	Saatavuutta suojaavat menettelyt on toteutettu järjestelmäkohtaisesti räätälöidyillä suojauksilla. Suojauksiin voi sisältyä esimerkiksi keskeisten verkkoyhteyksien, laitteistojen ja sovellusten ajoympäristöjen kahdentamiset.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom 4 k
Viitteet	Julkri: VAR-02, VAR-06, VAR-07, VAR-08
Muita lisätietoja	ISO/IEC 27002:2022 5.30
Tunniste	**TEK-22.2, L:, E:, S:Normaali, TS:**
Nimi	Tietojärjestelmien saatavuus - palveluiden valvonta
Vaatimus	Palveluiden ja tietojärjestelmien saatavuutta seurataan ja valvotaan niiden kriittisyyden edellyttämällä tasolla.
Yleiskuvaus	
Toteutusesimerkki	1) Jos palvelulla on saatavuus vaatimuksia, seurataan sen saatavuutta valvontajärjestelmällä. 2) Valvontajärjestelmän tulee lähettää hälyttää havaitusta saatavuuspoikkeamista.
Lainsäädäntö	TihL 13 § 1 mom, 15 § 1 mom 4 k
Viitteet	Julkri: HAL-07
Muita lisätietoja	ISO/IEC 27002:2022 8.16

Tunniste	TEK-23, L:, E:Tärkeä, S:Tärkeä, TS:
Nimi	Tietojärjestelmien toiminnallinen käytettävyys
Vaatimus	Viranomainen on varmistanut tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden.
Yleiskuvaus	Toiminnallisen käytettävyyden varmistamisessa on suositeltavaa käyttää niin teknisiä käytettävyystestauksia kuin käyttäjillä suoritettavia käytettävyystestejä tai heuristisia asiantuntija-arviointeja. Räätälöidyissä järjestelmissä käytettävyys tulisi määritellä ja suunnitella organisaatiossa hyväksytyn menetelmän mukaan. Käytettävyyttä tulisi testata jatkuvasti kehittämisen aikana. Valmisohjelmistojen käytettävyys tulisi testata hyväksymistestauksen yhteydessä. Testaus tulisi toteuttaa erilaisten käyttäjäryhmien näkökulmasta. Käytettävyystestausta voidaan tehdä jo hankintavaiheessa, jolloin voidaan paremmin varmistaa hankittavan järjestelmän soveltuvuus käyttötarpeeseen. Tiedonhallintalain täyttämistä voi tukea myös digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) mukaisilla, yleisölle tarjottavien palvelujen saavutettavuutteen liittyvillä menettelyillä.
Toteutusesimerkki	1) Viranomaisen tehtävien hoitamisen kannalta olennaiset tietojärjestelmät on tunnistettu. Olennaisiksi tunnistetuista tietojärjestelmistä on olemassa lista. 2) Olennaisiksi tunnistettujen tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys varmistetaan testauksen avulla niin hankintavaiheessa kuin merkittävien ylläpitotoimien yhteydessä. Varmistamisessa huomioidaan erityisesti, että a) tietojärjestelmä on helposti opittava, b) tietojärjestelmän toimintalogiikka on helposti muistettava, c) tietojärjestelmän toiminta tukee niitä työtehtäviä, joissa käyttäjä järjestelmää hyödyntää ja d) tietojärjestelmä edistää sen käytön virheettömyyttä.
Lainsäädäntö	TihL 13 § 2 mom
Viitteet	Julkri: HAL-17, HAL-17.1
Muita lisätietoja	

5 Varautuminen ja jatkuvuudenhallinta

Osa-alueelle on koottu normaaliolojen varautumista ja jatkuvuudenhallintaa koskevia kriteereitä. Kriteerit perustuvat tiedonhallintalain (muun muassa 4 §:n 2 mom 2 k, 13 §:n 1, 2 ja 4 mom sekä 15 §) ja yleisiin vaatimuksiin laadittavista ohjeista ja tietoturvallisuustoimenpiteistä sekä standardissa ISO/IEC 27002 kuvattuihin tietoturvallisuuden jatkuvuutta kuvaaviin hallintakeinoihin. Valmiuslain piiriin kuuluvat toiminnan jatkuvuutta poikkeusoloissa koskevat toimenpiteet on rajattu kriteeristön ulkopuolelle. Kriteeristö kuitenkin osaltaan tukee organisaatiota myös poikkeusoloihin varautumista koskevien vaatimusten täyttämisessä.

Osa-alueen kriteerit koskevat pääasiassa saatavuudeltaan tärkeiksi tai kriittisiksi luokiteltuja kohteita. Saatavuuden tasot on kuvattu luvussa 4.2 Luokittelutasot. Riskiperusteisesti kriteereitä voidaan soveltaa myös matalampiin saatavuusluokkiin kuuluvissa kohteissa. Jatkuvuusvaatimusten sekä niiden taustalla olevan lainsäädännön selvittäminen koskee kuitenkin lähtökohtaisesti kaikkia organisaatioita.

Keskeisiä kriteereitä osa-alueella ovat varautumistoimenpiteet erilaisiin vakaviin häiriötilanteisiin, toiminnan jatkuvuussuunnitelmat sekä tietojärjestelmien toipumissuunnitelmat ja niiden harjoittelu. Jatkuvuudenhallinta liittyy läheisesti häiriöiden ja poikkeamatilanteiden hallintaprosesseihin, joihin liittyvät kriteerit on kuvattu HAL- ja TEK-osa-alueilla.

Tunniste	VAR-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Varautumista ohjaava lainsäädäntö
Vaatimus	Organisaatio on tunnistanut toimintaansa ja palveluihinsa liittyvät ICT-varautumista ohjaavan kansallisen ja EU-lainsäädännön sekä muut ICT-varautumiseen liittyvät normit.
Yleiskuvaus	Lainsäädäntö ja normit määrittävät minimitason ICT-varautumisen toteuttamiselle. Tämän lisäksi organisaation on huomioitava oman toimintansa erityispiirteistä nousevat tarpeet. Toimintojen sisäisten ja ulkoisten riippuvuussuhteiden ymmärtäminen on perusedellytys varautumisen kustannustehokkaalle johtamiselle.
Toteutusesimerkki	Organisaatiossa selvitetään ICT-varautumiseen ja jatkuvuudenhallintaan liittyvä lainsäädäntö, määräykset, ohjeet, standardit ja sopimukset sekä mahdolliset kansainväliset velvoitteet. Erityisen tärkeää on, että sekä palvelua hankkiva että palvelua tuottava organisaatio tuntee palveluun vaikuttavat määräykset ja pitävät toisensa näistä tietoisina. Organisaation toimintaa ohjaava lainsäädäntö ja muut ohjaavat asiakirjat on useimmiten tunnistettu ja listattu tietoturva- ja riskienhallintapolitiikan perusteissa. Strategioissa, periaatteissa ja toiminnan suunnittelussa on huomioitu valtioneuvostotason ohjausasiakirjoissa asetetut ICT-varautumista ohjaavat linjaukset.
Lainsäädäntö	TihL 4 § 2 mom 2 k; 13 § 1 mom
Viitteet	Julkri: HAL-05
Muita lisätietoja	PiTuKri TJ-07, PiTuKri EE-02

Tunniste	VAR-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Jatkuvuusvaatimusten määrittely
Vaatimus	Toiminnan ja siihen liittyvien olennaisten palvelujen ja tietojärjestelmien jatkuvuusvaatimukset on määritelty.
Yleiskuvaus	Palvelun tai järjestelmän palautumisajan tavoitteet tulee määrittää sen mukaisesti, miten pitkään organisaation toiminnan näkökulmasta järjestelmä voi pisimmillään olla poissa käytöstä. Toiminnan näkökulmasta tulee määrittää, miten paljon tai miten pitkältä ajalta tietoa voidaan menettää.
Toteutusesimerkki	Organisaation tulee määrittää jatkuvuusvaatimukset yhteistyössä riskienhallinnan, tietoturvan, tietosuojan, toiminnan sekä arkkitehtuurien kanssa. Ydintoimintojen ja -prosessien suojattavat palvelut ja järjestelmät on tunnistettu ja niille on asetettu saatavuustavoitteet ydintoimintojen tai ydinprosessien vaatimusten mukaisesti. Palautumistoimenpiteiden käynnistämiskyky on määritetty palveluittain.
Lainsäädäntö	TihL 4 § 2 mom 1 k, 13 § 1 ja 2 mom, 15 § 1 mom.
Viitteet	Julkri: HAL-05
Muita lisätietoja	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6 ja luku 11; ISO/IEC 27002:2022 5.30

Tunniste	VAR-02.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Jatkuvuusvaatimusten määrittely - palveluiden siirrot
Vaatimus	Jatkuvuusvaatimuksissa on huomioitu palveluiden kotiuttamiset ja siirrot toiselle palveluntarjoajalle.
Yleiskuvaus	Palvelua hankittaessa tulee huomioida, että palvelua voi olla hankala kotiuttaa ja toimittajalukkoon jäänyttä palvelua vaikea siirtää toiselle palveluntarjoajalle. Erityisesti vaatimus tulee huomioida hankittaessa pilvipalveluita.
Toteutusesimerkki	
Lainsäädäntö	TihL 4 § 2 mom 1 k, 13 § 1, 2 ja 4 mom, 15 § 1 mom.
Viitteet	Julkri: HAL-05
Muita lisätietoja	Pilvipalveluiden soveltamisohje 2020:73; ISO/IEC 27002:2022 5.23
Tunniste	**VAR-03, L:, E:, S:Tärkeä, TS:**
Nimi	Jatkuvuussuunnitelmat
Vaatimus	Jatkuvuussuunnitelmat on laadittu ja otettu käyttöön.
Yleiskuvaus	Organisaation jatkuvuussuunnitelma sisältää periaatteet siitä, miten toiminta järjestetään suunnitelmallisesti eri tilanteissa. Organisaation jatkuvuussuunnittelussa tunnistetaan ne palvelut, joista organisaation ydintoiminnot ovat riippuvaisia, arvioidaan mitä vaikutuksia eripituisilla ICT-palvelujen katkoilla on organisaation ydintoimintoihin. Jatkuvuussuunnitelmissa tulee huomioida myös tietoturvallisuuden vaaditun tason säilyminen poikkeustilanteiden aikana.
Toteutusesimerkki	Jatkuvuussuunnitelmaan on kirjattu käytettävissä oleva henkilöstö, avainhenkilöt ja varahenkilöt sekä arvio heidän saatavuudestaan. Jatkuvuussuunnitelmissa on kuvattu, miten toimitaan häiriötilanteiden aikana sekä kuinka niiden jälkeen siirrytään takaisin normaaliin toimintaan. Organisaatiolla on tarvittaessa suunnitelma ICT-palvelujen tuotannon siirtämisestä toisiin tiloihin, mikäli nykyiset tilat muuttuvat käyttökelvottomiksi. Jatkuvuussuunnitelmat yhteensovitetaan sidosryhmien kanssa riittävän laajasti koko toimintaketjussa. Häiriötilanteiden viestinnän suunnittelu on osa jatkuvuussuunnitelmaa.
Lainsäädäntö	TihL 4 § 2 mom 2 k,15 §
Viitteet	
Muita lisätietoja	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11; ISO/IEC 27002:2022 5.23
Tunniste	**VAR-03.1, L:, E:, S:Tärkeä, TS:**
Nimi	Jatkuvuussuunnitelmien testaus ja harjoittelu
Vaatimus	Jatkuvuussuunnitelmia testataan ja harjoitellaan säännöllisesti.
Yleiskuvaus	Harjoittelemalla testataan suunnitelmien toimivuus erilaisissa tilanteissa. Havaintoja käytetään suunnitelmien kehittämiseen.
Toteutusesimerkki	Organisaatiot vastaavat omasta harjoitustoiminnastaan ja määrittelevät jatkuvuussuunnitelmien testaamisen käytännöt. Organisaatio harjoittelee sisäisesti sekä valtakunnallisissa että alueellisissa ja paikallisissa harjoituksissa toiminnan edellyttämässä laajuudessa.
Lainsäädäntö	TihL 4 § 2 mom,13 § 2 mom; 15 §
Viitteet	Katakri: I-13
Muita lisätietoja	ISO/IEC 27002:2022 5.23

Tunniste	VAR-04, L:, E:, S:Tärkeä, TS:
Nimi	Resurssit ja osaaminen
Vaatimus	Henkilöt tuntevat omaan toimintaan liittyvät jatkuvuus- ja toipumissuunnitelmat sekä osaavat toimia niiden mukaisesti. Varahenkilöt on nimetty ja heidän kykynsä hoitaa tehtävät normaalitilanteissa on varmistettu.
Yleiskuvaus	
Toteutusesimerkki	Jokainen koulutettu henkilö tuntee periaatteet organisaation varautumisesta sekä tietää eri tilannemallien vaikutuksen omaan tehtäväänsä. Heitä kannustetaan osallistumaan erilaisiin varautumista tukeviin yhteistyöryhmiin.
Lainsäädäntö	TihL 4 § 2 mom
Viitteet	Julkri: HAL-03; Katakri: T-04
Muita lisätietoja	

Tunniste	VAR-05, L:, E:, S:Tärkeä, TS:
Nimi	Henkilöstön saatavuus ja varajärjestelyt
Vaatimus	Kriittisten tehtävien suorittamiseksi on suunniteltu ja valmisteltu erityistilanteiden vaihtoehtoiset toimintatavat ja henkilöstön saatavuus ja varajärjestelyt.
Yleiskuvaus	
Toteutusesimerkki	Lainsäädännön mahdollistamat toimenpiteet on tunnistettu ja toteutettu tarvittavassa laajuudessa esimerkiksi lakko-oikeuksien poistamisen, hätätöiden käytön ja henkilövarausten (VAP) osalta.
Lainsäädäntö	TihL 4 § 2 mom 2 k; 13 § 1 mom, 15 § 1 mom 4 k
Viitteet	
Muita lisätietoja	Työaikalaki 872/2019, 19 §; Valtion virkaehtosopimuslaki 664/1970 11 §; Asevelvollisuuslaki 1438/2007 89 §

Tunniste	VAR-06, L:, E:, S:Tärkeä, TS:
Nimi	Tietoliikenteen varmistaminen
Vaatimus	Tietoliikennepalveluissa ja -sopimuksissa on huomioitu toiminnan kannalta tärkeiden palveluiden saatavuus häiriötilanteissa.
Yleiskuvaus	
Toteutusesimerkki	Tärkeiden palvelujen verkkoympäristöt ja tietoliikennepalvelut varmennetaan esimerkiksi kahdentamalla. Tietoliikenne voidaan kahdentaa fyysisesti kahta eri reittiä pitkin kahden eri operaattorin toimesta. Tärkeissä ympäristöissä varmistetaan, että yksittäisen tietoliikennekomponentin vikaantuminen ei keskeytä palvelun toimintaa. Erikseen valittuihin työasemiin voidaan esimerkiksi asentaa erillinen tietoliikenneyhteys, jonka kautta voi päästä yleiseen tietoverkkoon. Sopimusvaiheessa tulisi huomioida myös Suomen ulkopuolisten yhteyksien vikasietoisuus.
Lainsäädäntö	TihL 13 § 1, 2 ja 4 mom, 15 §
Viitteet	Julkri: HAL-16.1
Muita lisätietoja	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11

Tunniste	VAR-07, L:, E:, S:Tärkeä, TS:
Nimi	Tietoteknisten ympäristöjen varmentaminen
Vaatimus	Tietoteknisissä ympäristöissä ja niihin liittyvissä sopimuksissa on huomioitu toiminnan kannalta tärkeiden palveluiden saatavuus häiriötilanteissa.
Yleiskuvaus	
Toteutusesimerkki	Tärkeiden palvelujen tietotekniset ympäristöt varmennetaan esimerkiksi kahdentamalla siten, että yksittäisten komponenttien vikaantumiset eivät aiheuta toiminnan edellyttämää palvelutasoa pidempiä käyttökatkoja. Tietotekniset ympäristöt voidaan varmentaa varavoimalla tai varavoimaliitännöillä siten, että sähkönjakelu voidaan käynnistää riittävän nopeasti ja ylläpitää sitä riittävän ajan suhteessa toiminnan vaatimuksiin.
Lainsäädäntö	TihL 13 § 1, 2 ja 4 mom, 15 §
Viitteet	Julkri: HAL-16.1
Muita lisätietoja	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11

Tunniste	VAR-08, L:, E:, S:Kriittinen, TS:
Nimi	Vikasietoisuus
Vaatimus	ICT-infrastruktuuri sekä olennaiset tietojärjestelmät on toteutettu riittävän vikasietoisiksi ja käyttövarmoiksi riskiarvioinnin perusteella.
Yleiskuvaus	Tietojärjestelmien häiriöihin on varauduttu nopean palautumisen varmistamiseksi. Palautumisessa hyödynnetään mekanismeja, joiden tavoitteena on reaaliaikainen tai lähes reaaliaikainen viansietokyky kriittisten järjestelmien saatavuuden ylläpitämiseksi.
Toteutusesimerkki	Kriittisten palvelujen verkko-, palvelin- ja laiteympäristöt varmennetaan esimerkiksi kahdentamalla. Organisaatiossa otetaan järjestelmistä varmistusten lisäksi suojakopioita, joita säilytetään vähintään eri palotilassa kun varsinaisia tietoja. Tietoaineistot on riskiarviointiin perustuen hajautettu maantieteellisesti vähintään kahteen eri paikkaan ja riittävän etäälle toisistaan Suomen rajojen sisäpuolella. Julkisen hallinnon kriittisimmät palvelut ja niiden tiedonsiirto toteutetaan mahdollisuuksien mukaan turvallisuusverkon vaatimusten mukaisesti.
Lainsäädäntö	TihL 13 § 1 ja 2 mom, 15 §
Viitteet	
Muita lisätietoja	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6

Tunniste	VAR-08.1, L:, E:, S:Kriittinen, TS:
Nimi	Vikasietoisuus - riippuvuudet
Vaatimus	Palvelujen riippuvuus muista palveluista ja toisista toimijoista on otettu huomioon koko tietojenkäsittely-ympäristön ja sen vikasietoisuuden suunnittelussa.
Yleiskuvaus	
Toteutusesimerkki	Organisaatio on tunnistanut kriittiset palvelut sekä niiden koko palveluketjun. Koko palveluketju on toteutettu hyödyntäen riittävän vikasietoisia palveluita. Vikasietoisuuden toteutuksessa hyödynnetään vikasietoisia alustaratkaisuja kuten esimerkiksi turvallisuusverkkoa.
Lainsäädäntö	TihL 13 § 1 ja 2 mom, 15 §
Viitteet	
Muita lisätietoja	Yhteiskunnan turvallisuusstrategia 2017

Tunniste	VAR-09, L:, E:, S:Tärkeä, TS:
Nimi	Tietojärjestelmien toipumissuunnitelmat
Vaatimus	Tietojärjestelmien toipumissuunnitelmien tulee olla laadittu, otettu käyttöön ja yhteensovitettu keskenään.
Yleiskuvaus	Toipumissuunnitelmat on määritetty organisaation toiminnan kannalta tärkeiden tietojärjestelmien häiriötilanteista palautumiseen.
Toteutusesimerkki	ICT-palveluiden tarvitsemat minimitasot voidaan määritellä palvelusta laaditussa SLA-sopimuksessa sekä toipumissuunnitelmassa. Minimitasot voidaan asettaa aikavaatimuksina, laitteistoalustana tai tietoliikennekapasiteettina, joka vähintään tarvitaan. Toipumissuunnitelmien olemassaolosta vastaa aina palvelun tilaaja. Ulkoistetussa palvelussa järjestelmäkohtaisten toipumissuunnitelmien valmistelusta vastaa palveluntarjoaja. Tilaaja varmistaa, että palveluntarjoaja on testaa toipumissuunnitelmia säännöllisesti.
Lainsäädäntö	TihL 4 § 2 mom 2 k, 13 § 1 ja 2 mom, 15 § 1 mom
Viitteet	Julkri: VAR-02
Muita lisätietoja	

Liite 1B: Tietosuojakriteerit

Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella taikka henkilön käyttämien päätelaitteiden yksilöivien teknisten tietojen perusteella.

Henkilötietojen käsittelyssä on noudatettava tietosuoja-asetuksen vaatimuksia, kun käsittely on kokonaan tai osittain automaattista tai tiedot muodostavat rekisterin osan. Tietosuoja-asetus suojaa henkilötietoja riippumatta siitä, mitä tekniikkaa tietojenkäsittelyssä käytetään. Tietojen säilytystavalla ei myöskään ole merkitystä. Tietoja voidaan säilyttää esimerkiksi tietojärjestelmässä, videovalvontajärjestelmässä tai paperiarkistossa.

Henkilötietojen suojaamisessa voidaan hyödyntää edellä kuvattujen osa-alueiden tietoturvakriteereitä. Jokainen osa-alueilla oleva kriteeri on luokiteltu sen mukaan, sovelletaanko sitä myös henkilötietojen käsittelyssä ja jos sovelletaan, koskeeko kriteeri kaikkia henkilötietoja vai ainoastaan erityisiä henkilötietoryhmiä.

Tunniste	TSU-01, L:, E:, S:, TS:Henkilötieto
Nimi	Käsiteltävien henkilötietojen tunnistaminen
Vaatimus	Organisaatio tunnistaa kaikki käsittelemänsä henkilötiedot.
Yleiskuvaus	Käsiteltävien henkilötietojen tunnistaminen on välttämätön edellytys henkilötietojen suojaamiselle ja liittyy läheisesti organisaation tiedonhallintamallin laatimiseen sekä sen yhteydessä tehtävään organisaation tietovarantojen tunnistamiseen.
Toteutusesimerkki	Käsiteltävien henkilötietojen tunnistaminen ja dokumentointi voidaan tehdä osana organisaation suojattavien kohteiden tunnistamista, tehtäessä selostetta käsittelytoimista tai muodostettaessa tiedonhallintamallia.
Lainsäädäntö	TihL 5 §; Tietosuoja-asetus Art 5 (1) (c)
Viitteet	Julkri: HAL-04
Muita lisätietoja	

Tunniste	TSU-01.1, L:, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Käsiteltävien henkilötietojen tunnistaminen - Erityiset henkilötietoryhmät tai rikostuomioihin ja rikoksiin liittyvät tiedot
Vaatimus	Organisaatio tunnistaa käsittelemiensä erityisiin henkilötietoryhmiin kuuluvat tai rikostuomioihin ja rikoksiin liittyvät tiedot.
Yleiskuvaus	Erityisiin henkilötietoryhmiin kuuluvat tiedot, joista ilmenee henkilön rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys, sekä geneettiset tai biometriset tiedot (henkilön yksiselitteistä tunnistamista varten), terveyttä koskevat tiedot tai henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot. Edellä mainitut erityiset henkilötietoryhmät ovat suurelta osin julkisuulain perusteella salassa pidettäviä tietoja, joihin kohdistuu tavanomaisia henkilötietoja korkeammat turvallisuusvaatimukset. Tämän vuoksi organisaation tulee tunnistaa, mikäli käsittely koskee erityisiä henkilötietoryhmiä sekä luokitella tiedot erityisiin henkilötietoryhmiin kuuluviksi. Rikostuomioihin ja rikoksiin liittyvät henkilötiedot ovat myös salassa pidettäviä ja niihin sovelletaan tavanomaisia henkilötietoja korkeampia turvallisuusvaatimuksia sekä erillisiä käsittelyn lainmukaisuuteen liittyviä vaatimuksia, minkä johdosta ne tulee tunnistaa ja luokitella erikseen.
Toteutusesimerkki	Näihin henkilötietoryhmiin kuuluvien henkilötietojen tunnistaminen ja dokumentointi voidaan tehdä osana organisaation suojattavien kohteiden tunnistamista, tehtäessä selostetta käsittelytoimista tai muodostettaessa tiedonhallintamallia.
Lainsäädäntö	Tietosuoja-asetus Art 9 ja 10
Viitteet	Julkri: HAL-04.2
Muita lisätietoja	

Tunniste	TSU-02, L:, E:, S:, TS:Henkilötieto
Nimi	Organisaation roolit
Vaatimus	Organisaatio määrittelee käsittelemiensä henkilötietojen osalta, toimiiko organisaatio rekisterinpitäjänä, yhteisrekisterinpitäjänä vai henkilötietojen käsittelijänä.
Yleiskuvaus	Rekisterinpitäjäksi kutsutaan luonnollista henkilöä tai oikeushenkilöä, yritystä, viranomaista tai yhteisöä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjänä toimii yleensä itse organisaatio, ei organisaatioon kuuluva henkilö Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Henkilötietojen käsittelijäksi kutsutaan rekisterinpitäjästä ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun rekisterinpitäjän ohjeiden mukaisesti. HUOM! Organisaation rooli voi olla eri kussakin henkilötietojen käsittelytapauksessa, sillä se on riippuvainen siitä, kuka määrittää käsittelyn tarkoitukset ja keinot. Organisaatio voi käsitellä henkilötietoja toisen lukuun käsittelijänä. Se on kuitenkin rekisterinpitäjä sellaisten henkilötietojen käsittelyssä, joita se käsittelee omasta puolestaan, eikä asiakkaina olevien rekisterinpitäjien puolesta. Organisaatio on rekisterinpitäjä esimerkiksi silloin, kun se käsittelee organisaation oman henkilökunnan henkilötietoja. Henkilötietojen käsittelijä voi käsitellä henkilötietoja vain rekisterinpitäjän määrittelemiin tarkoituksiin. Henkilötietojen käsittelijä ei voi ryhtyä käsittelemään rekisterinpitäjän lukuun käsiteltäviä tietoja omiin tarkoituksiinsa määrittelemällä henkilötietojen käsittelyn tarkoituksia ja keinoja.
Toteutusesimerkki	Organisaation rooli voidaan dokumentoida yhdeksi lähtötiedoksi henkilötietojen käsittelyä kuvaavaan dokumentaatioon, esimerkiksi selosteisiin käsittelytoimista ja tiedonhallintamalliin.
Lainsäädäntö	Tietosuoja-asetus Art 4 (7–8), 26 ja 28
Viitteet	
Muita lisätietoja	

Tunniste	TSU-03, L:, E:, S:, TS:Henkilötieto
Nimi	Yhteisrekisterinpitäjät
Vaatimus	Toimiessaan yhteisrekisterinpitäjänä organisaatio määrittelee läpinäkyvällä järjestelyllä muiden yhteisrekisterinpitäjien kanssa rekisterinpitäjien velvoitteiden noudattamisesta sekä rekisteröityjen informoinnista.
Yleiskuvaus	Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Ne määrittelevät keskinäisellä järjestelyllä läpinäkyvällä tavalla kunkin vastuualueen tietosuoja-asetuksessa vahvistettujen velvoitteiden noudattamiseksi, erityisesti rekisteröityjen oikeuksien käytön ja rekisteröityjen informoinnin osalta. Järjestelyn yhteydessä voidaan nimetä rekisteröidyille yhteyspiste. Järjestelystä on käytävä asianmukaisesti ilmi yhteisten rekisterinpitäjien todelliset roolit ja suhteet rekisteröityihin nähden. Järjestelyn keskeisten osien on oltava rekisteröidyn saatavilla. Riippumatta järjestelyn ehdoista rekisteröity voi käyttää tietosuoja-asetuksen mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään ja kutakin rekisterinpitäjää vastaan.
Toteutusesimerkki	Organisaatio voi esimerkiksi tehdä sopimuksen eri yhteisrekisteripitäjien kanssa tai dokumentoida kirjallisesti yhteisrekisterinpitäjyyteen liittyvät menettelyt sekä julkaista ne verkossa ja asettaa saataville toimipisteissä.
Lainsäädäntö	Tietosuoja-asetus Art 26
Viitteet	
Muita lisätietoja	

Tunniste	TSU-04, L:, E:, S:, TS:Henkilötieto
Nimi	Henkilötietojen käsittelijä
Vaatimus	Organisaatio käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet.
Yleiskuvaus	Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu. Henkilötietojen käsittelijöiden toimet voivat olla hyvin tarkkaan rajattuja, kuten postin toimituksen ulkoistaminen. Tehtävät voivat olla myös laajoja ja yleisiä, ja niihin voi liittyä tietyn palvelun hallinta toisen organisaation puolesta, esimerkiksi yrityksen työntekijöiden palkanmaksuun liittyvät tehtävät. Henkilötietojen käsittelijää koskeva sääntely koskee esimerkiksi seuraavia palveluntarjoajia: - IT-palveluntarjoajat, ohjelmistojen integroijat, kyberturvallisuusyritykset ja IT-konsulttiyritykset, joilla on pääsy rekisterinpitäjän henkilötietoihin. - Terveydenhuollon laboratorio, joka käsittelee näytteitä rekisterinpitäjän lukuun. - Markkinointi- ja viestintätoimistot, jotka käsittelevät henkilötietoja asiakkaidensa puolesta. - Yleisemmin kaikki organisaatiot, joiden tarjoamiin palveluihin sisältyy henkilötietojen käsittelyä toisen organisaation puolesta. - Myös julkista viranomaista tai järjestöä voidaan pitää henkilötietojen käsittelijänä. Ohjelmistojulkaisijoita ja laitevalmistajia, esimerkiksi työajan seurantalaitteiden, biometristen laitteiden tai lääkinnällisten laitteiden valmistajia, ei pidetä henkilötietojen käsittelijöinä, jos niillä ei ole pääsyä henkilötietoihin, eivätkä ne käsittele henkilötietoja.
Toteutusesimerkki	Organisaatio voi arvioida käsittelijän kyvykkyyttä esimerkiksi käsittelijän toimittaman dokumentaation, hyväksyttyjen käytännesääntöjen tai sertifiointien avulla.
Lainsäädäntö	Tietosuoja-asetus Art 28
Viitteet	Julkri: HAL-16
Muita lisätietoja	

Tunniste	TSU-04.1, L:, E:, S:, TS:Henkilötieto
Nimi	Henkilötietojen käsittelijä - Sopimukset
Vaatimus	Organisaatio laatii henkilötietojen käsittelijöiden kanssa tietosuoja-asetuksen vaatimukset täyttävät sopimukset.
Yleiskuvaus	Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella tai muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Sopimuksen yksityiskohtaisemmat sisältövaatimukset on määritelty tietosuoja-asetuksen 28 artiklassa.
Toteutusesimerkki	Organisaatio voi laatia henkilötietojen käsittelyä koskevan sopimuksen esimerkiksi hyödyntämällä dokumentteja: Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja (tekijät: Hansel, Kuntaliitto, Kuntahankinnat, hankinnat.fi) osana sopimusta. Sopimusehtojen lisäksi rekisterinpitäjän tulee toimittaa käsittelijälle tai muutoin sopia käsittelijän kanssa henkilötietojen käsittelyssä noudatettavat ohjeet. Henkilötietojen käsittelijä voi käyttää toisen henkilötietojen käsittelijän (alikäsittelijän) palveluita vain rekisterinpitäjän kirjallisella luvalla. Lupa voi olla joko tiettyä käsittelijää varten myönnetty tai yleinen, jolloin rekisterinpitäjälle on ilmoitettava muutoksista alikäsittelijöillä ja annettava mahdollisuus vastustaa niitä.
Lainsäädäntö	Tietosuoja-asetus Art 28
Viitteet	Julkri: HAL-16.1
Muita lisätietoja	

Tunniste	TSU-05, L:, E:, S:, TS:Henkilötieto
Nimi	Tehtävät ja vastuut
Vaatimus	Organisaatio määrittelee henkilötietojen käsittelyyn liittyvät tehtävät ja vastuut.
Yleiskuvaus	Organisaation johdon tehtävänä on määritellä henkilötietojen käsittelyyn liittyvät vastuut. Tietosuojavastuut liittyvät tietoturvavastuiden määrittelyyn mm. käsittelyn turvallisuuteen liittyvien toimenpiteiden osalta, jotka ovat monissa tilanteissa yhteisiä henkilötiedoille ja muille organisaation käsittelemille tiedoille.
Toteutusesimerkki	Tehtävät ja vastuut kirjata työjärjestyksiin, tehtävänkuvauksiin, toimintaohjeisiin tai vastuumatriiseihin. Tehtävät voi kirjata myös roolipohjaisesti, mutta tällöin on varmistettava, että rooleihin liittyvät henkilöt on löydettävissä helposti dokumentaation perusteella. Tietosuojaan liittyvien tehtävien laajuus vaihtelee organisaatiokohtaisesti. Henkilötietointensiivisissä organisaatioissa voidaan toimia esimerkiksi siten, että organisaatio nimeää yhden tai useamman henkilön vastuuseen koko organisaation laajuisen hallinnointi- ja tietosuojaohjelman kehittämisestä, toteuttamisesta, ylläpitämisestä ja seurannasta, jotta voidaan varmistaa vaatimustenmukaisuus suhteessa kaikkiin soveltuviin henkilötietojen käsittelyä koskeviin lakeihin ja viranomaisvaatimuksiin. Joissakin organisaatioissa voi olla myös tarve nimetä erikseen henkilöt toteuttamaan rekisteröidyn oikeuksia koskevia pyyntöjä. Vaikka tietosuojasääntöjen noudattamisen varmistamiseksi nimitettäisiin tietty luonnollinen henkilö, tämä henkilö ei ole rekisterinpitäjä vaan toimii sen oikeushenkilön puolesta, joka on viime kädessä rekisterinpitäjänä vastuussa sääntöjen rikkomisesta. Vastaavasti vaikka tietyllä osastolla tai yksiköllä olisi operatiivinen vastuu tiettyjen käsittelytoimien noudattamisen varmistamisesta, tämä ei tarkoita sitä, että kyseisestä osastosta tai yksiköstä tulisi rekisterinpitäjä (koko organisaation sijaan).
Lainsäädäntö	Tietosuoja-asetus Art 12, 24
Viitteet	Julkri: HAL-02
Muita lisätietoja	

Tunniste	TSU-05.1, L:, E:, S:, TS:Henkilötieto
Nimi	Tehtävät ja vastuut - Tietosuojavastaava
Vaatimus	Organisaatio nimeää tehtävään soveltuvan tietosuojavastaavan ja julkistaa hänen yhteystietonsa.
Yleiskuvaus	Viranomaisen on nimettävä tietosuojavastaava paitsi, jos kyseessä on lainkäyttötehtäviään hoitava tuomioistuin. Useammalla viranomaisella voi olla yhteinen tietosuojavastaava. Tietosuojavastaavaksi nimetyllä henkilöllä tulee olla asiantuntemusta tietosuojalainsäädännöstä sekä kyky hoitaa tietosuojavastaavalle asetuksessa määritellyt tehtävät. Tietosuojavastaava voi kuulua henkilöstöön tai hoitaa tehtäviä palvelusopimuksen perusteella. Organisaation tulee julkistaa tietosuojavastaavan yhteystiedot sekä ilmoittaa ne valvontaviranomaiselle.
Toteutusesimerkki	
Lainsäädäntö	Tietosuoja-asetus Art 37–39
Viitteet	
Muita lisätietoja	

Tunniste	TSU-05.2, L:, E:, S:, TS:Henkilötieto
Nimi	Tehtävät ja vastuut - Tietosuojavastaavan asema ja tehtävät
Vaatimus	Organisaatio määrittelee tietosuojavastaavan aseman, resurssit ja valtuudet siten, että hänellä on edellytykset hoitaa tietosuojavastaavalle kuuluvat tehtävät.
Yleiskuvaus	Tietosuojavastaavalle kuuluvat seuraavat tehtävät: - seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemiaan puutteita - antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille - antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta - on rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa - on tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa Tietosuojavastaavan aseman ja toimintaedellytysten varmistamiseksi organisaation tulee - varmistaa että tietosuojavastaava otetaan mukaan tietosuojaa koskevien asioiden käsittelyyn - varmistaa tietosuojavastaavan resurssit ja pääsy tarvittaviin tietoihin - varmistaa tietosuojavastaavan riippumattomuus tehtävien suorittamisessa Tietosuojavastaavaa koskee tehtäviin liittyen salassapitovelvollisuus (julkisuuslaki 621/1999 22-23 §)
Toteutusesimerkki	Tietosuojavastaavan tehtävien toteutus voi vaihdella paljonkin riippuen henkilötietojen käsittelyn laajuudesta ja luonteesta organisaatiossa. Tietosuojavastaava voi suorittaa muita tehtäviä edellyttäen, että ne eivät aiheuta eturistiriitoja tietosuojavastaavan tehtävien kanssa. Laajoissa organisaatioissa tietosuojavastaavan tehtäviä voidaan hajauttaa usealle henkilölle.
Lainsäädäntö	Tietosuoja-asetus Art 37–39; JulkL 22–23 §
Viitteet	
Muita lisätietoja	

Tunniste	TSU-06, L:, E:, S:, TS:Henkilötieto
Nimi	Henkilötietojen käsittelyn ohjeet
Vaatimus	Organisaatio laatii henkilötietojen käsittelyä koskevat ohjeet ja varmistaa, että henkilötietoja käsitellään näiden ohjeiden mukaisesti.
Yleiskuvaus	Henkilötietojen käsittelijä tai kukaan rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö, jolla on pääsy henkilötietoihin, ei saa käsitellä niitä muuten kuin rekisterinpitäjän ohjeiden mukaisesti. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.
Toteutusesimerkki	Organisaatio voi muodostaa yleiset henkilötietojen käsittelyä koskevat ohjeet sekä täydentää niitä tarpeen mukaan prosessikohtaisilla lisäohjeilla. Organisaation tulee myös varmistaa ohjeiden jakelun, perehdytysten, koulutusten ja viestinnän avulla, että ajantasaiset henkilötietojen käsittelyä koskevat ohjeet ovat kaikkien niitä tarvitsevien saatavilla ja tiedossa.
Lainsäädäntö	Tietosuoja-asetus Art 29, 32(4)
Viitteet	Julkri: HAL-12
Muita lisätietoja	

Tunniste	TSU-07, L:, E:, S:, TS:Henkilötieto
Nimi	Käsittelyn lainmukaisuus
Vaatimus	Organisaatio tunnistaa käsittelemiensä henkilötietojen lainmukaiset käsittelyperusteet ja dokumentoi ne.
Yleiskuvaus	Henkilötietojen käsittely edellyttää aina laista löytyvää käsittelyperustetta. Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy: a) rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten; b) käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä; c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi; d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi; e) käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi; f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi. (f alakohtaa ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä.) Mikäli käsittely koskee henkilötunnusta, erityisiä henkilötietoryhmiä, rikostuomioita ja rikoksia ja niihin liittyviä turvaamistoimia tai perustuu suostumukseen, organisaatio ottaa huomioon niihin liittyvät lisävaatimukset.
Toteutusesimerkki	Organisaatio määrittää kaikki henkilötietojen käsittelyiden perusteet on ennen käsittelyiden aloittamista. Kun henkilötietojen käsittely sidotaan johonkin käsittelyperusteeseen, perustetta ei voi enää vaihtaa toiseen. Organisaatio dokumentoi käsittelyperusteet.
Lainsäädäntö	Tietosuoja-asetus Art 5 (1)(a), 6, 7, 8, 10; Tietosuojalaki 4 §, 5 §, 7 §, 29 §
Viitteet	
Muita lisätietoja	

Tunniste	TSU-07.1, L:, E:, S:,TS:Henkilötieto
Nimi	Käsittelyn lainmukaisuus - Suostumus
Vaatimus	Jos henkilötietojen käsittely perustuu poikkeuksellisesti suostumukseen, organisaatio varmistaa, että suostumuksen tietosuoja-asetuksessa säädetyt edellytykset täyttyvät.
Yleiskuvaus	Jotta suostumus on pätevä, sen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Suostumuksen vapaaehtoisuuden arviointiin on kiinnitettävä erityistä huomiota. Viranomainen voi käyttää tietojenkäsittelyä koskevaa suostumusta käsittelyperusteena vain poikkeuksellisesti, sillä rekisteröidyn ja rekisterinpitäjän välillä on usein selkeä vallan epätasapaino. Useimmissa tapauksissa on myös selvää, ettei rekisteröidyllä ole muita realistisia vaihtoehtoja kuin hyväksyä viranomaisen tietojenkäsittely. Suostumuksen pyytämiselle on tietosuoja-asetuksessa säädetty seuraavat edellytykset: 1. Jos tietojenkäsittely perustuu suostumukseen, rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. 2. Jos rekisteröity antaa suostumuksensa kirjallisessa ilmoituksessa, joka koskee myös muita asioita, suostumuksen antamista koskeva pyyntö on esitettävä selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Mikään tietosuoja-asetusta rikkova osa sellaisesta ilmoituksesta ei ole sitova. 3. Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen. Ennen suostumuksen antamista rekisteröidylle on ilmoitettava tästä. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen. 4. Arvioitaessa suostumuksen vapaaehtoisuutta on otettava mahdollisimman kattavasti huomioon muun muassa se, onko palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi asetettu suostumus sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen sopimuksen täytäntöönpanoa varten.
Toteutusesimerkki	Organisaatio määrittää prosessit sekä suostumuksen pyytämiseen että peruuttamiseen, joissa varmistetaan, että kaikki pyytämisen edellytykset täyttyvät. Prosesseissa tulee huomioida dokumentointi, jotta suostumuksen edellytysten täyttyminen on osoitettavissa jälkikäteen. Suostumuksen edellytysten täyttymisen varmistamisessa organisaatio voi hyödyntää tietosuojavaltuutetun sivuilla olevia ohjeita.
Lainsäädäntö	Tietosuoja-asetus Art 4(1)(11), Art 7
Viitteet	
Muita lisätietoja	

Tunniste	TSU-07.2, L:, E:, S:, TS:Henkilötieto
Nimi	Käsittelyn lainmukaisuus - Henkilötunnus
Vaatimus	Organisaatio tunnistaa henkilötunnuksen käsittelyperusteet ja dokumentoi ne.
Yleiskuvaus	Henkilötunnusta saa käsitellä rekisteröidyn suostumuksella tai, jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää: 1) laissa säädetyn tehtävän suorittamiseksi; 2) rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi; tai 3) historiallista tai tieteellistä tutkimusta taikka tilastointia varten. Henkilötunnusta saa käsitellä luotonannossa tai saatavan perimisessä, vakuutus-, luottolaitos-, maksupalvelu-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa. Sen lisäksi, henkilötunnuksen saa luovuttaa osoitetietojen päivittämiseksi tai moninkertaisten postilähetysten välttämiseksi suoritettavaa tietojenkäsittelyä varten, jos henkilötunnus jo on luovutuksensaajan käytettävissä.
Toteutusesimerkki	Organisaatio voi esimerkiksi erikseen määritellä kaikki ne käsittelytoimet, joissa henkilötunnusta käytetään ja varmistaa kunkin toimenpiteen kohdalla, että henkilötunnuksen käytölle on laissa hyväksytty peruste.
Lainsäädäntö	Tietosuojalaki 29 §
Viitteet	
Muita lisätietoja	

Tunniste	TSU-07.3, L:, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Käsittelyn lainmukaisuus - Erityiset henkilötietoryhmät
Vaatimus	Organisaatio tunnistaa käsittelemiensä erityisten henkilötietoryhmien käsittelyperusteet ja dokumentoi ne.
Yleiskuvaus	Erityisten henkilötietoryhmien, kuten etnistä alkuperää tai terveyttä koskevien tietojen käsittely on lähtökohtaisesti kiellettyä. Käsittely on kuitenkin mahdollista silloin, kun käsittelykieltoon on säädetty poikkeus tietosuoja-asetuksessa tai kansallisessa lainsäädännössä.
Toteutusesimerkki	Ennen erityisiin henkilötietoryhmiin liittyvän henkilötietojen käsittelyn aloittamista organisaatio voi toimia esimerkiksi seuraavalla tavalla: - Organisaatio selvittää ja dokumentoi käsittelyn perusteet ja varmistaa, että ne perustuvat johonkin tietosuoja-asetuksessa tai kansallisessa lainsäädännössä määriteltyyn poikkeukseen.
Lainsäädäntö	Tietosuoja-asetus Art 9; Tietosuojalaki 6 § 1 mom
Viitteet	
Muita lisätietoja	

Tunniste	TSU-07.4, L:, E:, S:, TS:Henkilötieto
Nimi	Käsittelyn lainmukaisuus - Rikostuomioihin ja rikoksiin liittyvät henkilötiedot
Vaatimus	Organisaatio tunnistaa käsittelemiensä rikostuomioihin ja rikoksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittelyperusteet ja dokumentoi ne.
Yleiskuvaus	Rikostuomioihin ja rikoksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittely lainmukaisella käsittelyperusteella on mahdollista vain viranomaisen valvonnassa tai jos a. käsittely on tarpeen oikeusvaateen selvittämiseksi, laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi; b. tietojen käsittelystä säädetään laissa tai joka johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä; tai c. tietoja käsitellään tieteellistä tai historiallista tutkimusta taikka tilastointia varten. Kattavaa rikosrekisteriä pidetään vain julkisen viranomaisen valvonnassa.
Toteutusesimerkki	Ennen rikostuomioihin ja rikkomuksiin liittyvän henkilötietojen käsittelyn aloittamista organisaatio voi toimia esimerkiksi seuraavalla tavalla: - Organisaatio selvittää ja dokumentoi käsittelyn perusteet ja varmistaa niiden asianmukaisuuden.
Lainsäädäntö	Tietosuoja-asetus Art 10; Tietosuojalaki 7 §
Viitteet	
Muita lisätietoja	

Tunniste	TSU-08, L:, E:, S:, TS:Henkilötieto
Nimi	Tarpeellisuus ja oikeasuhtaisuus
Vaatimus	Organisaatio varmistaa, että henkilötietojen käsittely on tarpeellista ja oikeasuhtaista käsittelyn laillisten tarkoitusten saavuttamiseksi.
Yleiskuvaus	Henkilötietoja olisi käsiteltävä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoilla.
Toteutusesimerkki	Ennen henkilötietojen käsittelyn aloittamista organisaatio selvittää ja dokumentoi voidaanko käsittelyn tarkoitusta kohtuudella toteuttaa ilman henkilötietojen käsittelyä. Jos käsittelyn tarkoitus, esimerkiksi palvelun toteuttaminen, on mahdollista tehdä siten, että tiettyjä tietoja ei käsitellä, ei henkilötietojen käsittely niiltä osin ole tarpeellista eikä henkilötietoja tule silloin käsitellä.
Lainsäädäntö	Tietosuoja-asetus Art 5
Viitteet	
Muita lisätietoja	

Tunniste	TSU-09, L:, E:, S:, TS:Henkilötieto
Nimi	Käyttötarkoitussidonnaisuus
Vaatimus	Organisaatio kerää henkilötietoja vain tietyssä, nimenomaisessa ja laillisessa tarkoituksessa, eikä käsittele henkilötietoja alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin.
Yleiskuvaus	Henkilötietojen käsittelyn tarkoitus tai tarkoitukset on suunniteltava ja määritettävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Tietoja ei saa käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin. Henkilötietojen käsittely voi olla mahdollista määritetyn käyttötarkoituksen ohella myös sellaiseen käyttötarkoitukseen, joka katsotaan yhteensopivaksi alkuperäisen käyttötarkoituksen kanssa. Käsittelyn on oltava lainmukaista myös muiden tietosuojasäännösten näkökulmasta; yhteensopiva käyttötarkoitus ei oikeuta rekisterinpitäjää poikkeamaan muista tietosuojasäännöksistä. Henkilötietojen käsittely seuraaviin tarkoituksiin on yhteensopivaa, jos tietosuoja-asetuksen suojatoimia noudatetaan asianmukaisesti. - yleisen edun mukainen arkistointi - tieteellinen tai historiallinen tutkimus - tilastolliset tarkoitukset
Toteutusesimerkki	Organisaatio voi varmistaa käyttötarkoitussidonnaisuuden noudattamista esimerkiksi: - dokumentoimalla huolellisesti kaikki henkilötietojen käyttötarkoitukset ja käsittelyprosessit, - tarkastamalla säännöllisesti, että henkilötietoja ei käytetä muihin käyttötarkoituksiin sekä - tiedottamalla käyttötarkoitussidonnaisuuden periaatteesta ohjeissa ja koulutuksissa.
Lainsäädäntö	Tietosuoja-asetus Art 5(1)(b), 6(4)
Viitteet	
Muita lisätietoja	

Tunniste	TSU-10, L:, E:, S:, TS:Henkilötieto
Nimi	Tietojen minimointi
Vaatimus	Organisaatio käsittelee henkilötietoja vain siinä määrin, kun se on tarpeellista käsittelyn tarkoituksen kannalta.
Yleiskuvaus	Tiedon minimoinnilla tarkoitetaan rekisteröidyistä kerättävien ja käsiteltävien tietojen määrän minimointia. Käsiteltävien henkilötietojen on oltava - asianmukaisia eli kerättyjen tietojen on oltava sellaisia tietoja, joilla kyetään täyttämään määritelty käyttötarkoitus - olennaisia eli kerätyillä henkilötiedoilla on oltava selkeä yhteys määriteltyyn käyttötarkoitukseen ja - rajoitettuja eli tarpeellisia määritellyn henkilötietojen käyttötarkoituksen kannalta. Henkilötietojen oikean määrän arvioimiseksi on selkeästi tunnistettava se syy, miksi kyseisiä henkilötietoja tarvitaan. Käyttötarkoituksen kautta pystytään määrittelemään, mitkä henkilötiedot ovat välttämättömiä käsittelyn tarkoituksen toteuttamiseksi Organisaatio varmistaa, että henkilötunnusta ei merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

Toteutusesimerkki	Henkilötietojen tarpeellisuuden arviointi voidaan määritellä osaksi henkilötietojen käsittelyn aloittamiseen ja muutostilanteisiin liittyviä prosesseja. Arvioinnissa on tulee käydä läpi kaikki yksittäiset henkilötietoryhmät ja arvioida niiden tarpeellisuus suhteessa käsittelyn tarkoituksiin.. Organisaatio voi ennen henkilötietojen käsittelyn aloittamista toimia esimerkiksi seuraavalla tavalla: - Pseudonymisoida tai anonymisoida tiedot silloin kun se on mahdollista. - Varmistaa, että järjestelmien näytöissä, sekä tulostettavissa ja laadittavissa asiakirjoissa ei näy tarpeettomia henkilötietoja (erityisesti henkilötunnusta ja erityisiä henkilötietoryhmiä) esimerkiksi järjestelmien näkymien suunnittelulla, ohjeistamalla asian, nostamalla asian esiin perehdytyksissä ja koulutuksissa tai tekemällä tarkastuksia henkilötietoja sisältäviin asiakirjoihin. - Varmistaa, että henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.
Lainsäädäntö	Tietosuoja-asetus Art 51(c), 25(2); Tietosuojalaki 29.4 §
Viitteet	
Muita lisätietoja	
Tunniste	**TSU-11, L:, E:, S:, TS:Henkilötieto**
Nimi	Säilytyksen rajoittaminen
Vaatimus	Organisaatio säilyttää henkilötietoja muodossa, josta rekisteröity on tunnistettavissa, ainoastaan niin kauan, kun on tarpeen tietojen käsittelyn tarkoitusten toteuttamista varten.
Yleiskuvaus	Rekisterinpitäjän on suunniteltava ja pystyttävä perustelemaan henkilötietojen säilytysaika. Henkilötietojen säilytysajat on myös dokumentoitava. Rekisterinpitäjän on arvioitava henkilötietojen säilytysaikaa ja tarpeellisuutta kysymyksessä olevaa käyttötarkoitusta vasten. Henkilötietoja saa säilyttää vain niin kauan, kun ne ovat tarpeen henkilötietojen käyttötarkoituksen kannalta. Henkilötietojen säilytysaikaan voi vaikuttaa myös kansallinen lainsäädäntö, jossa säädetään säilytysajoista, esimerkiksi kirjanpitolaki. Rekisterinpitäjän on itse huomioitava laista tulevat säilytysajat. Kun henkilötietoja ei enää tarvita, ne tulee anonymisoida tai poistaa. Rekisterinpitäjän on varmistettava, että sen käytössä olevat tietojärjestelmä (ml. pilvipalvelut) ja muut käsittelyprosessit tukevat säilytysaikojen noudattamista ja säännöllistä arvioimista. Myös rekisteröity voi pyytää rekisterinpitäjää poistamaan henkilötiedot silloin, kun niitä ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä käsiteltiin. Henkilötietoja voi säilyttää alkuperäistä käyttötarkoitusta kauemmin ainoastaan silloin, kun henkilötietoja käsitellään ainoastaan yleisen edun mukaista arkistointia, tieteellistä tai historiallista tutkimusta tai tilastollisia tarkoituksia varten, jos tietosuoja-asetuksen suojatoimia noudatetaan asianmukaisesti. Suojatoimien on katettava niin tekniset kuin organisatoriset toimenpiteet, joilla taataan erityisesti tietojen minimoinnin periaatteen noudattaminen. Minimoinnin periaate edellyttää myös mahdollisimman lyhyttä säilytysaikaa. Henkilötietoja ei saa käsitellä, jos tarkoitukset on mahdollista toteuttaa anonyymeillä tiedoilla.
Toteutusesimerkki	Organisaatio voi määritellä osaksi henkilötietojen käsittelyn aloittamisen prosessia henkilötietojen säilytysajan tai sen määräytymisen perusteen määrittelyn sekä prosessin, jonka mukaan henkilötiedot poistetaan säilytysajan päättyessä Organisaatio varmistaa, että myös varmuuskopiot poistuvat henkilötietoja poistettaessa.
Lainsäädäntö	Tietosuoja-asetus Art 5(1) (e), 25(2)
Viitteet	
Muita lisätietoja	

Tunniste	TSU-12, L:, E:, S:, TS:Henkilötieto
Nimi	Täsmällisyys
Vaatimus	Organisaatio varmistaa, että henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä sekä toteuttaa kaikki mahdolliset kohtuulliset toimenpiteet käsittelyn tarkoituksiin nähden epätarkkojen ja virheellisten henkilötietojen poistamiseksi tai oikaisemiseksi viipymättä.
Yleiskuvaus	Organisaation tulee varmistua hallussaan olevien tietojen täsmällisyydestä ja tarvittavasta ajantasaisuudesta. Tietojen oikeellisuuden varmistaminen on erityisen tärkeää silloin, kun henkilötietojen perusteella tehdään yksilön kannalta olennaisia päätöksiä. Epätäsmälliset ja virheelliset tiedot voivat vakavalla tavalla vaarantaa rekisteröidyn oikeuksia. Esimerkiksi virheelliset terveydentilaa koskevat tiedot potilasrekisterissä voivat johtaa vääriin hoitotoimenpiteisiin. Organisaation tulee toteuttaa kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. Mitä tärkeämpää tiedon täsmällisyys on, sitä enemmän rekisterinpitäjän on tehtävä toimenpiteitä tietojen oikeellisuuden varmistamiseksi. Rekisterinpitäjällä on oltava käytössään menetelmiä tiedon täsmällisyyden ja oikeellisuuden säännölliseen arviointiin sekä tarpeellisten päivitysten tekemiseen. Myös rekisteröidyllä on yleensä oikeus arvioida rekisterinpitäjän käyttämiä henkilötietoja ja tarvittaessa esittää oikaisupyyntöjä epätarkkojen tai virheellisten tietojen osalta sekä poistopyyntöjä tarpeettomien tietojen osalta. Jos rekisterinpitäjä luovuttaa hallussaan olevia henkilötietoja eteenpäin, on vastaanottajista syytä pitää kirjaa. Rekisterinpitäjällä on velvollisuus ilmoittaa kaikenlaisista henkilötietojen oikaisuista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Ilmoitusvelvollisuudesta on mahdollista poiketa vain silloin, kun se osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Rekisteröidyllä on myös oikeus pyytää tietoa henkilötietojen vastaanottajista. Tieto henkilötiedon virheellisyydestä tulee tarvittaessa voida välittää myös alkuperäiselle tietolähteelle, minkä vuoksi henkilötiedon oheen tulee merkitä tietolähde, kun tietoja saadaan toiselta rekisterinpitäjältä.
Toteutusesimerkki	Rekisterinpitäjä voi esimerkiksi määritellä prosessit tiedon täsmällisyyden ja oikeellisuuden säännölliseen arviointiin, tarpeellisten päivitysten tekemiseen sekä henkilötietojen oikaisuista ilmoittamiseen jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu ja tietolähteelle, jolta alkuperäinen korjattu tieto on saatu.
Lainsäädäntö	Tietosuoja-asetus Art 5(1)(d)
Viitteet	
Muita lisätietoja	

Tunniste	TSU-13, L:, E:, S:, TS:Henkilötieto
Nimi	Käsittelyn turvallisuus
Vaatimus	Organisaatio varmistaa henkilötietojen turvallisuuden käyttäen asianmukaisia teknisiä tai organisatorisia toimia.
Yleiskuvaus	Ottaen huomioon toteuttamiskustannukset, käsittelyn luonne, laajuus, sekä todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten a) henkilötietojen pseudonymisointi ja salaus; b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus; c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa; d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi. Hyväksyttyjen käytännesääntöjen tai hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että asetettuja vaatimuksia noudatetaan.
Toteutusesimerkki	Henkilötietojen käsittelyn turvallisuuden varmistaminen voidaan toteuttaa osana organisaation muiden tietoturvakontrollien määrittelyä ja toteutusta ottamalla henkilötietoihin kohdistuvat riskit yhdeksi osaksi riskien arviointia päätettäessä minkä tasoisia teknisiä ja organisatorisia suojatoimia organisaation vastuulla oleviin tietoihin kohdistetaan. Organisaatio voi varmistaa käsittelyn turvallisuutta esimerkiksi toteuttamalla tämän kriteeristön mukaisia kriteereitä ja kiinnittämällä erityisesti huomiota vähimmäiskriteereitä täydentävien kriteerien valintaan riskiperusteisesti.
Lainsäädäntö	Tietosuoja-asetus Art 5, 32
Viitteet	
Muita lisätietoja	

Tunniste	TSU-13.1, L:, E:, S:, TS:Erityinen henkilötietoryhmä
Nimi	Käsittelyn turvallisuus - Erityiset henkilötietoryhmät tai rikostuomioihin ja rikoksiin liittyvät tiedot
Vaatimus	Käsiteltäessä erityisiin henkilötietoryhmiin kuuluvia tai rikostuomioihin ja rikoksiin liittyviä henkilötietoja organisaatio toteuttaa asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi.
Yleiskuvaus	Näitä erityisiä toimenpiteitä ovat: 1) toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty; 2) toimenpiteet, joilla parannetaan henkilötietoja käsittelevän henkilöstön osaamista; 3) tietosuojavastaavan nimittäminen; 4) rekisterinpitäjän ja käsittelijän sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin; 5) henkilötietojen pseudonymisointi; 6) henkilötietojen salaaminen; 7) toimenpiteet, joilla käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, mukaan lukien kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa; 8) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi; 9) erityiset menettelysäännöt, joilla varmistetaan tietosuoja-asetuksen ja tämän lain noudattaminen siirrettäessä henkilötietoja tai käsiteltäessä henkilötietoja muuhun tarkoitukseen; 10) tietosuoja-asetuksen 35 artiklan mukainen tietosuojaa koskevan vaikutustenarvioinnin laatiminen; 11) muut tekniset, menettelylliset ja organisatoriset toimenpiteet.
Toteutusesimerkki	Käsiteltäessä erityisiin henkilötietoryhmiin kuuluvia tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja organisaatio: - varmistaa henkilötietojen käsittelyn turvallisuuden ottaen huomioon, että kyseessä ovat mahdollisesti salassa pidettävät henkilötiedot, joiden luottamuksellisuuteen ja eheyteen kohdistuu korkeampia vaatimuksia ja suurempia riskejä - arvioi tarpeen erityisille toimenpiteille rekisteröidyn oikeuksien suojaamiseksi ja toteuttaa riskiarvion perusteella niistä tarpeelliset.
Lainsäädäntö	Tietosuoja-asetus Art 5, 32; Tietosuojalaki 6 § 2 mom ja 7 § 2 mom
Viitteet	
Muita lisätietoja	

Tunniste	TSU-14, L:, E:, S:, TS:Henkilötieto
Nimi	Tietoturvaloukkaukset
Vaatimus	Organisaatio dokumentoi kaikki henkilötietojen tietoturvaloukkaukset, sekä määrittelee toimintatavat niistä ilmoittamiseen valvontaviranomaiselle ja rekisteröidyille.
Yleiskuvaus	Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Henkilötietojen tietoturvaloukkauksen yhteydessä on dokumentoitava siihen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet. Tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun tietoturvaloukkaus on havaittu, jos tietoturvaloukkaus todennäköisesti aiheuttaa riskin henkilöiden oikeuksille ja vapauksille. Jos loukkaus voi aiheuttaa henkilöille korkean riskin, heille on ilmoitettava tapahtuneesta tietoturvaloukkauksesta henkilökohtaisesti ilman aiheetonta viivytystä. Mikäli organisaatio toimii henkilötietojen käsittelijänä, sen on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.
Toteutusesimerkki	Organisaatio voi esimerkiksi määritellä osaksi yleistä häiriönhallintaprosessia henkilötietoihin kohdistuvien tietoturvaloukkausten arvioinnin ja käsittelyn, johon sisältyvät ohjeet ja vastuut tietoturvaloukkausten arvioinnista, käsittelystä, tietoturvaloukkauksiin liittyvien tietojen keruusta sekä tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle ja rekisteröidyille. Organisaatio kerää ja tallentaa tapahtuneesta henkilötietojen tietoturvaloukkauksesta mm. tietoturvaloukkauksen kuvauksen (kuten sen luonne ja kohteena olevat tiedot), tapahtuma-ajan lokitiedot, ilmoitusvelvoitteiden täyttämiseksi tarvittavat tiedot, tiedot loukkauksen vaikutuksista ja seurauksista, riskiarvioinnin sekä tehdyt toimenpiteet ja tietoturvaloukkaukseen liittyvät päätökset.
Lainsäädäntö	Tietosuoja-asetus Art 33
Viitteet	Julkri: HAL-08, HAL-09
Muita lisätietoja	

Tunniste	TSU-15, L:, E:, S:, TS:Henkilötieto
Nimi	Osoitusvelvollisuus
Vaatimus	Organisaatio pystyy osoittamaan noudattavansa yleisen tietosuoja-asetuksen vaatimuksia.
Yleiskuvaus	Henkilötietojen käsittelyssä on noudatettava tietosuoja-asetuksen säännöksiä. Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on myös pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä. Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet täyttääkseen osoitusvelvollisuuden vaatimukset. Osoitusvelvollisuus tarkoittaa myös dokumentointivelvollisuutta, käytännössä tiettyjen toimenpiteiden tekemistä ja kirjaamista. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa. Tietosuoja-asetuksessa on osoitusvelvollisuutta koskevia vaatimuksia, joiden velvoittavuus on arvioitava tapauskohtaisesti. Osoitusvelvollisuuden laajuus riippuu muun muassa organisaation koosta, henkilötietojen määrästä ja siitä, millaisia henkilötietoja rekisterinpitäjä käsittelee. Rekisterinpitäjän on huomioitava osoitusvelvollisuus jo henkilötietojen käsittelyn suunnitteluvaiheessa.
Toteutusesimerkki	Osoitusvelvollisuuden toteuttamiseksi organisaatio voi esimerkiksi määritellä ja dokumentoida kirjallisesti kaikki tietosuojan toteuttamiseen liittyvät prosessit sekä varmistaa, että näiden prosessien lopputuloksena syntyy dokumentaatio, jolla voidaan osoittaa, että prosesseja on noudatettu.
Lainsäädäntö	Tietosuoja-asetus Art 5(2), 24
Viitteet	Julkri: HAL-09
Muita lisätietoja	

Tunniste	TSU-16, L:, E:, S:, TS:Henkilötieto
Nimi	Tietosuojariskien hallinta
Vaatimus	Organisaatio arvioi henkilötietojen käsittelyyn kohdistuvat olennaiset riskit sekä toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet riskiarvioinnin mukaisesti.
Yleiskuvaus	Tietosuojariskien hallinta tarkoittaa järjestelmällistä, koordinoitua ja jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään ja seurataan rekisteröidyn oikeuksiin ja vapauksiin kohdistuvia riskejä. Tietosuojariskien arvio on tehtävä rekisteröidyn näkökulmasta eli organisaation on arvioitava - mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi vaarantaa ja - mitä vahinkoja (fyysisiä, aineellisia tai aineettomia) rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Tietosuojariskien arvioinnissa on otettava huomioon seuraavat tekijät: a) käsittelyn luonne (esim. erityiset henkilötietoryhmät, rekisteröidyn vaikeus käyttää oikeuksiaan johtuen esim. käsittelyn ennakoimattomuudesta tai läpinäkymättömyydestä, uusi teknologia ja innovaatiot, rekisteröidyn heikko asema), b) käsittelyn laajuus (rekisteröityjen lukumäärä, tiedon määrä, säilytysaika, maantieteellinen kattavuus), c) käsittelyn asiayhteys (esim. luottamuksellisuus, kotirauha, eri yhteyksissä kerättyjen henkilötietojen yhdistely), d) käsittelyn tarkoitukset (esim. rekisteröityjen tarkkailu, seuranta ja valvonta, henkilöiden arviointi tai pisteytys, automaattinen päätöksenteko, jolla on vaikutuksia rekisteröityyn , sekä e) luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Riskin tunnistamisen merkitys korostuu erityisesti silloin, kun rekisterinpitäjä määrittää teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan tietosuojan toteutuminen henkilötietojen käsittelyssä. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstölle annettuja ohjeita tietosuojan toteuttamiseksi, omavalvonnan kautta tapahtuvaa käytönvalvontaa, tietojärjestelmien tietoturvaa, henkilötietojen tietoturvaloukkauksesta ilmoittamista, henkilötietojen salausta, henkilötietojen pseudonymisointia ja muita suojatoimenpiteitä. Riskien hallinta on jatkuvaa toimintaa: toimenpiteiden riittävyyttä suhteessa käsittelyyn liittyvään riskiin on arvioitava jatkuvasti ja päivitettävä tarvittaessa. Rekisterinpitäjällä on myös osoitusvelvollisuus riskiperusteisen lähestymistavan noudattamisesta.
Toteutusesimerkki	Tietosuojariskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa. Organisaatio toteuttaa tämän kriteeristön mukaisia hallintakeinoja ja kiinnittämää erityisesti huomiota vähimmäiskriteereitä täydentävien kriteerien valintaan riskiperusteisesti. Tietosuojariskien hallinnassa on otettu huomioon sidosryhmistä ja toimitusketjuista aiheutuvat riskit. Tietosuojan vaikutusten arviointi (TSU-17) sekä siihen sisältyvä erityinen tietosuojariskien arviointi on pakollinen silloin, kun suunniteltu käsittely voi aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.
Lainsäädäntö	Tietosuoja-asetus Art 24, 25, 32–34, 35
Viitteet	Julkri: HAL-06
Muita lisätietoja	

Tunniste	TSU-17, L:, E:, S:, TS:Henkilötieto
Nimi	Tietosuojan vaikutustenarviointi
Vaatimus	Organisaatio toteuttaa ennen henkilötietojen käsittelyä arvioinnin suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle silloin, kun henkilötietojen käsittelyyn liittyy korkeita riskejä rekisteröidylle.
Yleiskuvaus	Vaikutustenarvioinnin tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Vaikutustenarvioinnissa kuvataan henkilötietojen käsittelyä, arvioidaan käsittelyn tarpeellisuutta, oikeasuhteisuutta ja henkilötietojen käsittelystä aiheutuvia riskejä sekä tarvittavia toimenpiteitä, joilla riskeihin puututaan. Tavoitteena on sen arviointi, onko jäljelle jäänyt riski oikeutettu ja hyväksyttävissä käsillä olevissa olosuhteissa. Vaikutustenarviointi auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, sen dokumentoinnissa ja osoittamisessa. Organisaation on tehtävä vaikutustenarviointi silloin, kun suunnitellaan henkilötietojen käsittelyä, joka todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. Vaikutustenarviointi on tehtävä ennen käsittelyn aloittamista ja sitä on päivitettävä tarvittaessa. Vaikutustenarviointi on tehtävä erityisesti silloin, kun - henkilötietojen käsittelyssä käytetään uutta teknologiaa - käsitellään laajamittaisesti rikostuomioihin ja rikoksiin liittyviä henkilötietoja tai erityisiä henkilötietoryhmiä, kuten terveystietoja, etnistä alkuperää, poliittisia mielipiteitä, uskonnollista vakaumusta tai seksuaalista suuntautumista - henkilön henkilökohtaisia ominaisuuksia arvioidaan automaattisen käsittelyn avulla, järjestelmällisesti ja kattavasti, ja arvio johtaa päätöksiin, joilla on oikeusvaikutuksia tai jotka muuten vaikuttavat henkilöön merkittävästi - yleisölle avointa aluetta valvotaan järjestelmällisesti ja laajamittaisesti. Tietosuojavaltuutetun toimisto on julkaissut verkkosivuillaan luettelon käsittelytoimien tyypeistä, joiden yhteydessä rekisterinpitäjän tulee tehdä tietosuojaa koskeva vaikutustenarviointi. Lisäksi kansallinen erityislainsäädäntö voi edellyttää tietosuojan vaikutusten arvioinnin tekemistä. Vaikutustenarvioinnin tekemistä koskevia vaatimuksia sovelletaan myös ennen 25.5.2018 alkaneisiin, jo käynnissä oleviin käsittelytoimiin.
Toteutusesimerkki	Organisaatiolla voi määritellä prosessin, jonka mukaisesti arvioidaan vaikutustenarvioinnin tarpeellisuus organisaation suorittamille erilaisille henkilötietojen käsittelytoimille. Vaikutustenarviointien toteuttamista varten organisaatio voi laatia ohjeet ja dokumentointimenettelyt, joilla varmistetaan vaikutustenarviointien oikeanlainen ja yhdenmukainen toteutus. Organisaation on pyydettävä tietosuojavastaavan neuvoja vaikutustenarvioinnin tekemisessä, jos rekisterinpitäjä on nimennyt tietosuojavastaavan. Jos henkilötietoja käsittelee osittain tai kokonaan henkilötietojen käsittelijä, hänen on autettava vaikutustenarvioinnin tekemisessä. Vaikutustenarviointien ohjeiden ja pohjien laatimisessa organisaatio voi hyödyntää tietosuojavaltuutetun sivuilla olevia ohjeita. Huom! Pääosa vaikutustenarvioinnissa koottavista tiedoista ja suoritettavista toimenpiteistä on sellaisia, jotka tulee tehdä kaikille henkilötietojen käsittelytoimille riippumatta siitä, tarvitaanko vaikutustenarviointia vai ei. Organisaation kannattaa varmistaa, että tällaiset lähtötiedot ovat saatavilla ja hyödyntää niitä vaikutustenarvioinnissa.
Lainsäädäntö	Tietosuoja-asetus Art 35
Viitteet	
Muita lisätietoja	

Tunniste	TSU-17.1, L:, E:, S:, TS:Henkilötieto
Nimi	Tietosuojan vaikutustenarviointi - Ennakkokuuleminen
Vaatimus	Organisaatio kuulee tarvittaessa tietosuojavaltuutetun toimistoa ennen henkilötietojen käsittelyn aloittamista.
Yleiskuvaus	Organisaation on kuultava tietosuojavaltuutettua ennen henkilötietojen käsittelyn aloittamista, kun vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin rekisteröidylle, eikä rekisterinpitäjä ole omilla toimenpiteillään saanut riskiä alhaisemmaksi. Tietosuojaviranomaista on kuultava esimerkiksi silloin, kun rekisteröidyt voisivat joutua kärsimään huomattavista tai peruuttamattomista seurauksista, joita he eivät välttämättä pysty torjumaan. Ennakkokuulemisen johdosta tietosuojavaltuutettu antaa rekisterinpitäjälle tai käsittelijälle kirjalliset ohjeet niistä toimenpiteistä, joihin on ryhdyttävä riskin alentamiseksi. Tarvittaessa tietosuojavaltuutettu voi ennakkokuulemisen yhteydessä käyttää myös sille tietosuoja-asetuksessa annettuja toimivaltuuksia, kuten varoitusta. Rekisteripitäjän ja käsittelijän on toteuttava ohjeen mukaiset lisätoiminpiteet ennen henkilötietojen käsittelyn aloittamista, jotta käsittely voidaan katsoa lainmukaiseksi.
Toteutusesimerkki	Organisaatio voi määritellä ennakkokuulemisen tarpeen tarkastuksen ja ennakkokuulemisen suorittamisen esimerkiksi yhdeksi osaksi vaikutustenarvioinnin ja henkilötietojen käsittelyn aloittamisen prosesseja.
Lainsäädäntö	Tietosuoja-asetus Art 36
Viitteet	
Muita lisätietoja	

Tunniste	TSU-18, L:, E:, S:, TS:Henkilötieto
Nimi	Henkilötietojen siirto ETA:n ulkopuolelle
Vaatimus	Organisaatio on tunnistanut toimintaansa liittyvät kansainväliset henkilötietojen siirrot ETA-alueen ulkopuolelle ja niihin käytettävät siirtoperusteet, sekä varmistanut tapauskohtaisesti, että siirrettäville henkilötiedoille taataan kolmannen maan lainsäädännössä ja käytännöissä sellainen henkilötietojen suojan taso, joka vastaa olennaisilta osin ETA-alueen tasoa.
Yleiskuvaus	Organisaatio voi siirtää henkilötietoja kolmansien maiden julkisille elimille tai kansainvälisille järjestöille Euroopan komission hyväksymän tietosuojan riittävyyttä koskevan päätöksen perusteella (Art. 45). Jos siirtoon soveltuvaa päätöstä tietosuojan riittävyydestä ei ole tehty, tietoja voidaan siirtää joko - julkisten elinten välisten kansainvälisten sopimusten (Art. 46 (2)(a), - julkisten elinten välisten hallinnollisten järjestelyjen avulla (Art. 46 (3)(b), - muita asianmukaisia suojatoimia soveltaen (Art. 46), tai - viimesijaisesti erityistilanteita koskevia poikkeuksia soveltaen ja suppeasti tulkiten, jos asianmukaisten suojatoimien käyttö ei ole mahdollista (Art. 49); poikkeuksien käytön on liityttävä pääasiassa satunnaisiin käsittelytoimiin, jotka eivät ole toistuvia. Organisaatio on tapauskohtaisesti arvioinut riittääkö käytetty siirtomekanismi takaamaan olennaisilta osin saman tietosuojan tason kuin ETA-alueella ja ottanut tarvittaessa käyttöön täydentäviä suojatoimia. HUOM. Organisaatio on huomioinut myös henkilötietojen käsittelijöiden (esimerkiksi pilvipalveluiden tarjoajien) osalta, missä henkilötiedot fyysisesti sijaitsevat. Esimerkiksi palveluntarjoajana toimivan henkilötietojen käsittelijän pääsy etäyhteydellä henkilötietoihin ETA:n ulkopuolelta katsotaan henkilötietojen siirroksi ETA- alueen ulkopuolelle. HUOM. Lähtökohtaisesti pilvipalveluntarjoajalla on aina pääsy palvelussa käsiteltävään tietoon, mikäli tieto on elinkaarensa aikana palvelussa selväkielisessä muodossaan (esimerkiksi asiakkaalle näytettävä kuvana) tai palveluntarjoajalla on pääsy tiedon salaamiseen käytettyihin salausavaimiin. HUOM. Jos minkään siirtoperusteen edellytykset eivät täyty, henkilötietoja ei voida siirtää ETA:n ulkopuolelle.

Toteutusesimerkki	Kolmansiin maihin siirrettävien henkilötietojen, käytettyjen siirtoperusteiden, siirron vastaanottajien ja siirron suorittajien tunnistaminen ja dokumentointi voidaan tehdä osana organisaation suojattavien kohteiden tunnistamista, tehtäessä selostetta käsittelytoimista tai muodostettaessa tiedonhallintamallia. Organisaatio voi varmistaa, että siirrettävät henkilötiedot ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään, noudattaen esimerkiksi tiedon täsmällisyyden (TSU-13) arviointiin määriteltyjä prosesseja ja käytäntöjä. Organisaatio voi hyödyntää varhaisessa vaiheessa tietosuojavaltuutetun ja Euroopan tietosuojaneuvoston sivuilta löytyviä ohjeita (erityisesti tietosuojaneuvoston ohje 2/2020 henkilötietojen siirtämisessä ETA-alueen ja sen ulkopuolisten viranomaisten ja julkisten elinten välillä) varmistaessaan, että julkisten elinten välisissä oikeudellisesti sitovissa välineissä tai hallinnollisissa järjestelyissä (kansainväliset sopimukset), noudatetaan yleistä tietosuoja-asetusta. Organisaatio voi tapauskohtaisesti arvioidessaan taataanko siirrettäville henkilötiedoille kolmannen maan lainsäädännössä ja/tai käytännöissä sellainen henkilötietojen suojan taso, joka vastaa olennaisilta osin ETA-alueen tasoa, sekä valitessaan mahdollisesti tarvittavia täydentäviä suojatoimenpiteitä hyödyntää Euroopan tietosuojaneuvoston suosituksia 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi, sekä suosituksia 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista. Organisaatio selvittää soveltuvat menettelylliset vaatimukset, mikäli se siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle soveltaen jotain seuraavista suojatoimista: vakiosopimuslausekkeet (Art. 46 (2)(c) ja (d) GDPR), julkisten elinten väliset hallinnolliset järjestelyt (Art. 46(3)(b) GDPR), hyväksytyt käytännesäännöt (Art. 46 (2) (e), hyväksytty sertifiointimekanismi (Art. 46(2)(f) GDPR) tai ad hoc sopimuslausekkeet (Art. 46.3(a) GDPR). Voit hyödyntää soveltuvien menettelyllisten vaatimusten arvioinnissa Euroopan tietosuojaneuvoston suosituksia 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi Organisaatio arvioi säännöllisin väliajoin yhdessä siirron vastaanottajien kanssa tapahtuuko kolmannen maan henkilötietojen suojan tasossa tai eurooppalaisten tietosuojaviranomaisten ohjeistuksissa muutoksia ja päivitä käytäntöjä tarvittaessa.
Lainsäädäntö	Tietosuoja-asetus V luku
Viitteet	
Muita lisätietoja	

Tunniste	TSU-19, L:, E:, S:, TS:Henkilötieto
Nimi	Rekisteröidyn oikeudet
Vaatimus	Organisaatio toteuttaa rekisteröidyn oikeudet.
Yleiskuvaus	Kun rekisterinpitäjä käsittelee henkilötietoja, sen on toteutettava asianmukaiset toimenpiteet rekisteröityjen oikeuksien toteuttamiseksi sekä helpotettava näiden oikeuksien käyttämistä. Organisaation on varmistettava pyyntöjä esittävän rekisteröidyn henkilöllisyys ja noudatettava tietosuoja-asetuksessa asetettuja pyyntöön vastaamisen määräaikoja. Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus - saada tietoa henkilötietojensa käsittelystä - saada pääsy tietoihin - oikaista tietoja - poistaa tiedot ja tulla unohdetuksi - rajoittaa tietojen käsittelyä - siirtää tiedot järjestelmästä toiseen - vastustaa tietojen käsittelyä - olla joutumatta automaattisen päätöksenteon kohteeksi.
Toteutusesimerkki	Rekisteröityjen oikeuksien toteuttamista varten organisaatio voi toteuttaa ja dokumentoida prosessit, joiden avulla varmistetaan ja voidaan osoittaa rekisteröityjen oikeuksien toteutuminen. Rekisteröityjen oikeuksiin liittyvien prosessien suunnittelu on tärkeää erityisesti niissä tapauksissa, joissa rekisteröityjen tiedetään käyttävän oikeuksiaan paljon.
Lainsäädäntö	Tietosuoja-asetus Art 12–21
Viitteet	
Muita lisätietoja	

Tunniste	TSU-19.1, L:, E:, S:, TS:Henkilötieto
Nimi	Rekisteröidyn oikeudet - Rekisteröidyn käytettävissä olevien oikeuksien tunnistaminen
Vaatimus	Organisaatio on määritellyt tunnistamansa henkilötietojen lainmukaisen käsittelyperusteen mukaisesti, mitkä rekisteröidyn oikeudet liittyvät kyseessä olevaan käsittelyyn.
Yleiskuvaus	Rekisteröity ei voi käyttää kaikkia oikeuksiaan kaikissa tilanteissa. Se, mitä oikeuksia rekisteröity voi kulloinkin käyttää, riippuu siitä, millä perusteella kyseessä olevia henkilötietoja käsitellään. Organisaatio voi hyödyntää tietosuojavaltuutetun toimiston verkkosivuilla olevaa aineistoa siitä, millä tavalla käsittelyperuste vaikuttaa käytettävissä oleviin oikeuksiin. Kunkin oikeuden toteuttamisesta voi yksittäistapauksessa kieltäytyä. Kieltäytyminen on mahdollista, jos käsillä on jokin oikeuden kohdalla relevantti kieltäytymisperuste tai oikeuden toteuttamisen edellytykset eivät muutoin täyty. Oikeuksiin voi lisäksi olla säädetty poikkeuksia kysymyksessä olevaa organisaatiota koskevassa erityislainsäädännössä.
Toteutusesimerkki	Organisaatio määrittele käsittelyperusteen mukaisesti, mitkä tietosuojaoikeudet liittyvät kyseessä olevaan käsittelyyn. Organisaatio kuvaa, millä tavalla oikeudet otetaan huomioon henkilötietojen käsittelyssä sekä miten oikeuksia koskevat pyynnöt käsitellään ja toteutetaan.
Lainsäädäntö	Tietosuoja-asetus Art 14 (5)(b-d), 17 (3), 20 (1) ja (3), 21 (1) ja (6), 22 (2), 23, 85, 89; Tietosuojalaki 31–34 §
Viitteet	
Muita lisätietoja	

Tunniste	TSU-19.2, L:, E:, S:, TS:Henkilötieto
Nimi	Rekisteröidyn oikeudet - Läpinäkyvä informointi
Vaatimus	Organisaatio informoi rekisteröityjä henkilötietojen käsittelystä säädetyllä tavalla.
Yleiskuvaus	Henkilötietoja on käsiteltävä rekisteröidyn kannalta läpinäkyvästi. Tästä yleisestä informoinnista on joitakin poikkeuksia. Informoinnin tarkoituksena on, että rekisteröity saa kattavan ja selkeän kuvan henkilötietojen käsittelyn kokonaisuudesta. Rekisterinpitäjän tulee arvioida, onko annettu informaatio kielen ja johdonmukaisuuden kannalta ymmärrettävää kohderyhmän näkökulmasta. Informoinnin tarkemmat vaatimukset riippuvat osittain siitä, kerätäänkö tietoja henkilöltä itseltään vai muualta. Informoinnin tarkempia vaatimuksia ovat: - tietosisältö - esittämistapaa koskevat vaatimukset - jakelua ja toimittamistapaa koskevat vaatimukset - ajankohtaa koskevat vaatimukset Informointi on toteutettava tietojen keruun yhteydessä tai kohtuullisen ajan (viimeistään kuukauden) kuluessa henkilötietojen saamisesta, jos tietoja ei ole saatu rekisteröidyltä. Informointi on toteutettava viimeistään, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran tai kun tietoja luovutetaan ensimmäisen kerran tilanteissa, joissa tietoja saadaan muualta kuin rekisteröidyltä itseltään ja niitä käytetään viestintään rekisteröidyn kanssa tai niitä on tarkoitus luovuttaa toiselle vastaanottajalle.
Toteutusesimerkki	Sähköisesti tehtävän tiedonkeruun yhteydessä informointi voidaan hoitaa esimerkiksi tietosuojaselosteella, johon on suora linkki lomakkeelta, jolla tietoja kerätään. Tietosuojaselosteesta kerrotaan näkyvillä ilmoituksilla. Mikäli tietojen keruu tapahtuu rekisteröidyn ollessa fyysisesti läsnä, voidaan informointi tehdä kirjallisesti tai pyydettäessä myös suullisesti. Olennaista on, että rekisteröity saa helposti henkilötietojen käsittelyä koskevat tiedot tiiviissä, läpinäkyvässä, helposti ymmärrettävässä ja selkeässä muodossa.
Lainsäädäntö	Tietosuoja-asetus Art 5, 13–14
Viitteet	
Muita lisätietoja	

Tunniste	TSU-19.3, L:, E:, S:, TS:Henkilötieto
Nimi	Rekisteröidyn oikeudet - Oikeus saada pääsy tietoihin
Vaatimus	Organisaatio toimittaa pyynnöstä rekisteröidylle jäljennöksen käsiteltävistä henkilötiedoista sekä informaatiota henkilötietojen käsittelystä.
Yleiskuvaus	Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy henkilötietoihin sekä henkilötietojen käsittelyä koskevat tiedot kuten esimerkiksi käsittelyn tarkoitukset, henkilötietoryhmät, vastaanottajat ja säilytysajat. Jos henkilötietoja siirretään kolmanteen maahan tai kansainväliselle järjestölle, rekisteröidyllä on oikeus saada ilmoitus siirtoa koskevista asianmukaisista suojatoimista. Rekisterinpitäjän on toimitettava jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity pyytää useampia jäljennöksiä, rekisterinpitäjä voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää.
Toteutusesimerkki	Organisaatio voi määritellä prosessin rekisteröityjen pyyntöjen täyttämiseen sekä sisällyttää rekisteröityjen informointiin tiedot siitä, miten pyynnöt toimitetaan rekisterinpitäjälle. Mikäli pyyntöjä on paljon, organisaation kannattaa myös suunnitella ja ohjeistaa menettelyt, joilla pyynnöt voidaan täyttää tehokkaasti.
Lainsäädäntö	Tietosuoja-asetus Art 15
Viitteet	
Muita lisätietoja	

Tunniste	TSU-19.4, L:, E:, S:, TS:Henkilötieto
Nimi	Rekisteröidyn oikeudet - Tietojen oikaiseminen, poistaminen, siirtäminen, käsittelyn rajoittaminen ja vastustaminen
Vaatimus	Organisaatio toteuttaa tietojen oikaisemiseen, poistamiseen, siirtämiseen, käsittelyn rajoittamisen ja vastustamiseen liittyvät pyynnöt.
Yleiskuvaus	Rekisteröidyllä on joukko henkilötietoihin liittyviä oikeuksia, jotka organisaation tulee toteuttaa pyydettäessä kuten: Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Ottaen huomioon tarkoitukset, joihin tietoja käsiteltiin, rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitys. Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä, ja rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä, edellyttäen että jokin asetuksessa mainituista perusteista täyttyy. Näitä perusteita ovat esimerkiksi tietojen käyttötarpeen päättyminen tai suostumuksen peruuttaminen. Rekisteröidyllä on oikeus siihen, että rekisterinpitäjä rajoittaa käsittelyä tietyissä tilanteissa kuten esimerkiksi, jos rekisteröity kiistää henkilötietojen paikkansapitävyyden. Rekisterinpitäjä on myös velvollinen ilmoittamaan edellä mainituista toimenpiteistä jokaiselle henkilötietojen vastaanottajalle. Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle jos käsittely perustuu suostumukseen tai sopimukseen. Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu yleiseen etuun, julkisen vallan käyttämiseen tai oikeutettuun etuun. Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä tällaista markkinointia varten, mukaan lukien profilointia silloin kun se liittyy tällaiseen suoramarkkinointiin.
Toteutusesimerkki	Oikeuksien käyttämiseen liittyvät yksityiskohtaiset prosessit voi suunnitella ottaen huomioon pyyntöjen määrän sekä tietosuoja-asetuksessa määritellyt eri oikeuksiin liittyvät yksityiskohdat. Jos pyyntöjä on paljon, prosessit kannattaa suunnitella ja ohjeistaa huolella. Muussa tapauksessa riittää, että organisaatio varmistaa kyvykkyyden tarvittaessa toteuttaa rekisteröityjen pyynnöt ja että sillä on riittävä tuntemus tietosuoja-asetuksessa esitetyistä yksityiskohtaisista pyyntöjen toteuttamiseen liittyvistä vaatimuksista.
Lainsäädäntö	Tietosuoja-asetus Art 16–21
Viitteet	
Muita lisätietoja	

Tunniste	TSU-20, L:, E:, S:, TS:Henkilötieto
Nimi	Automatisoidut yksittäispäätökset
Vaatimus	Organisaatio tunnistaa tilanteet, joissa henkilötietojen käsittelyyn sisältyy automaattista päätöksentekoa sekä varmistaa että automaattista päätöksentekoa ei tehdä muutoin kuin tietosuoja-asetuksessa erikseen sallituissa tapauksissa.
Yleiskuvaus	Organisaatio ei saa tehdä rekisteröityjä koskevia päätöksiä, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Automaattinen päätöksenteko (ml. profilointi) on sallittua, jos päätös - on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten - on hyväksytty rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä - perustuu rekisteröidyn nimenomaiseen suostumukseen. Profilointi tarkoittaa henkilötietojen automaattista käsittelyä, jossa arvioidaan ihmisen henkilökohtaisia ominaisuuksia. Profiloinnilla tarkoitetaan erityisesti työsuoritukseen, taloudellisen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin liittyvien piirteiden analysointia tai ennakointia. Profilointi - on automaattista tai osittain automaattista - kohdistuu henkilötietoihin ja - arvioi henkilökohtaisia ominaisuuksia. Päätöksenteko on automaattista, kun - on kyse pelkästään automaattiseen henkilötietojen käsittelyyn perustuvasta päätöksenteosta ja - tehtävillä päätöksillä on oikeusvaikutuksia tai tällaiset päätökset muuten vaikuttavat rekisteröityyn merkittävästi.
Toteutusesimerkki	Mikäli organisaatio tekee automaattista päätöksentekoa tai profilointia, organisaatio voi käsittelyn aloittamisen yhteydessä sekä määräajoin varmistaa suhteessa tietosuoja-asetuksessa esitettyihin yksityiskohtaisiin vaatimuksiin, että automaattiseen päätöksentekoon ja profilointiin liittyvät vaatimukset täyttyvät. Organisaatio on huolehdittava automaattiseen päätöksenteon yhteydessä (ml. profilointi) vähintään seuraavista suojatoimenpiteistä: - rekisteröidyille kerrotaan tietojen käsittelystä - rekisteröidyille tarjotaan yksinkertaisia tapoja vaatia ihmisen osallistumista tietojen käsittelemiseen, esittää oma kantansa ja riitauttaa päätös - käsiteltävät tiedot ja algoritmit tarkistetaan säännöllisesti, jotta voidaan varmistaa, että päätöksentekoprosessi toimii kuten tarkoitettu, eikä johda esimerkiksi yksilöitä syrjivään tietojen käsittelyyn. - henkilötietojen käsittelystä on tehty vaikutusten arviointi
Lainsäädäntö	Tietosuoja-asetus Art 22
Viitteet	
Muita lisätietoja	

Tunniste	TSU-21, L:, E:, S:, TS:Henkilötieto
Nimi	Seloste käsittelytoimista
Vaatimus	Organisaatio laatii kirjallisen kuvauksen organisaation suorittamista henkilötietojen käsittelytoimista.
Yleiskuvaus	Seloste käsittelytoimista on tehtävä, jos organisaatiossa on yli 250 työntekijää ja sen on katettava kaikki käsittelytoimet. Seloste käsittelytoimista on tehtävä työntekijöiden määrästä riippumatta, kun - henkilötietojen käsittely aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille tai - henkilötietojen käsittely ei ole satunnaista tai - käsiteltävät henkilötiedot sisältävät erityisiä tietoryhmiä tai rikostuomioihin ja rikoksiin liittyviä henkilötietoja. Tällöin selosteeseen on sisällytettävä vain niihin liittyvät käsittelytoimet.
Toteutusesimerkki	Rekisterinpitäjä ja henkilötietojen käsittelijä voivat laatia selosteet käsittelytoimista esimerkiksi hyödyntämällä tietosuojavaltuutetun sivuilta löytyviä ohjeita ja mallipohjia.
Lainsäädäntö	Tietosuoja-asetus Art 30
Viitteet	
Muita lisätietoja	

Liite 2: Julkri-työkalu

Liite on tallennettu omana tiedostonaan osoitteeseen https://urn.fi/URN:ISBN:978-952-367-275-8

Bilagan finns som en separat fil på adressen https://urn.fi/URN:ISBN:978-952-367-275-8

The appendix is available as a separate file at https://urn.fi/URN:ISBN:978-952-367-275-8

Liite 3: Julkri työkalun käyttöohje

1 Työkalun käyttö

Tässä ohjeessa kuvataan, miten Julkri-kriteeristöä käytetään sitä varten kehitetyn Excel-työkalun (liite 2) avulla. Työkalun ideana on, että käyttäjä antaa ensin arviointitilannetta kuvaavat esiehdot, joiden perusteella työkalu valitsee olennaiset, valinnaiset sekä arvioinnin ulkopuolelle jätettävät kriteerit.

1.1 Esiehtojen määrittely

Työkalussa määritellään ensimmäisenä arvioinnin lähtötiedot välilehdellä Esiehdot olevien alasvetovalikoiden avulla. Esiehtoina tulee syöttää seuraavat tiedot:

- arvioitavalta kohteelta vaadittava luottamuksellisuus, eheys ja saatavuus, (käytetyt luokittelutasot on määritelty Julkri-suosituksen luvussa 4.2)
- sisältyykö arvioinnin kohteeseen henkilötietoja ja kuuluvatko nämä tiedot erityisiin henkilötietoryhmiin,
- arviointiin sisällytettävät ja arvioinnista poisjätettävät osa-alueet,
- käyttötapaus, jos arviointiin soveltuva käyttötapaus on olemassa.

1.2 Olennaiset kriteerit ja niiden täydentäminen

Työkalu näyttää annettujen esiehtojen perusteella välilehdellä Valitut kriteerit kunkin kriteerin osalta onko se olennainen, valinnainen vai jätetäänkö se arvioinnin ulkopuolelle (Ei sisälly arviointiin). Organisaatio tekee päätöksen kriteerikohtaisesti kunkin kriteerin soveltamisesta. Päätökset kirjataan kriteerikohtaisesti sarakkeeseen Päätös soveltamisesta.

Päätös soveltamisesta sarakkeeseen tulee kirjata perustelut erityisesti niistä valinnaisista kriteereistä, jotka organisaatio riskiarvioinnin perusteella päättää jättää toteuttamatta. Perustelut tulee kirjata siten, että niistä käy selkeästi ilmi, millä perusteella kriteerin soveltamatta jättämisestä huolimatta riskin on arvioitu olevan hyväksyttävällä tasolla. Perustelut voi kirjata esimerkiksi kuvaamalla kompensoivat kontrollit tai viittaamalla erilliseen riskiarvioon.

Olennaisia kriteerejä on lähtökohtaisesti sovellettava. Valinnaisten kriteereiden soveltamisesta organisaatio tekee päätöksen riskiarvioinnin ja tapauskohtaisen arvioinnin perusteella. Kriteerejä, jotka eivät sisälly arviointiin, ei lähtökohtaisesti tarvitse soveltaa. Organisaatio voi perustelluista syistä poiketa tästä periaatteesta.

1.3 Kriteerien käyttö arvioinnissa

Edellä kuvattujen vaiheiden perusteella muodostettua kriteeristöä käytetään arvioinnin kohteessa joko tietoturvallisuuden arviointiin tai arviointia edeltäviin tietoturvallisuustoimenpiteiden suunnitteluun.

Työkalun välilehdellä Valitut kriteerit oleva luettelo sovellettavista kriteereistä toimii pohjana, johon voi dokumentoida kriteerikohtaisesti arviointien tulokset sekä toimenpiteet, aikataulut ja vastuut puutteiden korjaamiseksi.

1.4 Työkalun toimintaperiaatteet

Kriteerien valinta perustuu esiehtojen avulla annettavien valintakriteerien yhteisvaikutukseen. Kriteerien valinnassa työkalu noudattaa seuraavaa valintalogiikkaa:

- Turvallisuustasot
  - Kriteeri on olennainen, jos kriteerille määritelty turvallisuustaso on sama tai alempi kuin käyttäjän esiehdoissa määrittelemä tarkastelun kohteen turvallisuustaso. Eli, jos käyttäjä on määritellyt, että arvioinnin kohde sisältää salassa pidettäviä tietoja, niin olennaisia ovat kaikki kriteerit, jotka on luokiteltu koskemaan salassa pidettäviä tai julkisia tietoja.
  - Kun käsitellään henkilötietoja olennaisia kriteereitä ovat ne, jotka on tietosuojan osalta luokiteltu tasolle henkilötieto.
  - Kun käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja, ovat kaikki tietosuojan osalta luokitellut kriteerit olennaisia.
  - Kriteeri on turvallisuustasojen perusteella olennainen, jos se on yhdenkin turvallisuusnäkökulman (luottamuksellisuus, eheys, saatavuus tai tietosuoja) perusteella olennainen.

  - Kriteeri on valinnainen, jos kriteeri ei ole olennainen ja sen turvallisuustaso on yhtä tasoa korkeampi kuin käyttäjän esiehdoissa antama turvallisuustaso. Esimerkiksi jos tarkastelun kohde sisältää salassa pidettäviä tietoja niin TL IV-tasolle luokitellut kriteerit ovat valinnaisia ja käyttäjä päättää riskiarvion perusteella sovelletaanko niitä vai ei. Lisäksi käsiteltäessä luokkaan henkilötieto kuuluvia tietoja, valinnaisia kriteereitä ovat tasolle erityinen henkilötietoryhmä luokitellut kriteerit.

- Osa-alueet
  - Kukin osa-alue voidaan valita mukaan arviointiin (Kyllä) tai jättää pois (Ei).
  - Jos jokin osa-alue on jätetty pois, mikään osa-alueen kriteeri ei sisälly arviointiin. Esimerkiksi jos käsittely ei sisällä henkilötietoja voidaan tietosuojan osa-alue jättää pois tai jos hallinnollisen osa-alueen arviointi jo aiemmin suoritettu, voidaan se jättää pois.
- Käyttötapaukset
  - Kriteeri on olennainen, jos se on määritelty käyttötapauksen perusteella olennaiseksi.
  - Kriteeri voi olla määritelty käyttötapauksessa valinnaiseksi, jolloin organisaatio tekee päätöksen kriteerin soveltamisesta sen perusteella, onko kriteeri tarpeellinen kyseisessä arviointitilanteessa.
- Yhteisvaikutus
  - Kriteeri ei sisälly arviointiin, jos se ei sisälly arviointiin turvallisuustason, osa-alueen tai käyttötapauksen perusteella.
  - Kriteeri on valinnainen, jos se on turvallisuustason tai käyttötapauksen perusteella valinnainen eikä sitä ole rajattu arvioinnin ulkopuolelle turvallisuustason, osa-alueen tai käyttötapauksen perusteella.
  - Muissa tapauksissa kriteeri on olennainen.

1.5 Pystynäkymä ja kriteerien suodatus

Pystynäkymä-välilehdellä näytetään kriteerit helposti luettavassa muodossa. Pystynäkymässä näytettäviä tietoja voi suodattaa kriteerien olennaisuuden ja soveltamispäätösten perusteella. Kriteerien olennaisuus määräytyy Esiehdot-välilehdellä tehtyjen valintojen perusteella. Soveltamispäätökset tehdään Valitut-kriteerit välilehdellä.

Suodatukset voi tehdä Pystynäkymä-välilehdellä soluissa D1 ja E1 olevien alasvetovalikoiden avulla. Suodatuksessa käytetään Excelin normaaleja suodatusominaisuuksia.

Pystynäkymässä ei voi hakea tietoja kriteerien sisällön perusteella, koska näkymässä vain näytetään tietoja muilta välilehdiltä. Tietojen haku on mahdollista Kriteeristö-välilehdellä.

2 Käyttötapaukset

Kriteeristöön on ennalta määritelty käyttötapauksia, joihin on poimittu kyseiseen tilanteeseen soveltuvat kriteerit. Organisaatiot voivat myös itse määritellä käyttötapauksia usein toistuviin arviointitilanteisiin. Organisaatiokohtaisten käyttötapausten määrittelyn avulla voidaan tehostaa kriteeristön hyödyntämistä eri tilanteissa, kun käyttötapaukseen voidaan valita ennalta tunnistettujen riskien perusteella sopiva taso ja lisäksi kriteereistä voidaan tiputtaa pois tilanteeseen soveltumattomat kriteerit.

2.1 Ennalta määritellyt käyttötapaukset

2.1.1 Tiedonhallintayksikön hallinnollinen turvallisuusarviointi

Käyttötapaus on tarkoitettu tiedonhallintayksikön tiedonhallintalain mukaisen tietoturvallisuuden vähimmäistason ja tietosuojan arviointiin. Se sisältää arvioinnin hallinnollisen turvallisuuden, tietosuojan sekä varautumisen ja jatkuvuuden hallinnan näkökulmista. Käyttötapausta voi täydentää fyysisen turvallisuuden ja tietojärjestelmäarvioinneilla.

2.1.2 SaaS-pilvipalvelun arviointi

Käyttötapaus on tarkoitettu SaaS-palveluina tuotettujen pilvipalveluiden turvallisuuden arviointiin. Sen avulla voidaan arvioida, täyttääkö arvioitava palvelu tiedonhallintalain mukaiset vaatimukset tietoturvallisuuden varmistamiseksi. Arvioinnissa voidaan käyttää hyväksi pilvipalveluiden tuottajan sertifikaatteja, dokumentaatiota ja muita mahdollisia todisteita turvallisuusvaatimusten toteutumisesta. Jos käytettävässä palvelussa on tarkoitus käsitellä henkilötietoja, tulee arvioinnissa huomioida myös tietosuojaa koskevat kriteerit. Käyttötapaus rajoittuu luottamuksellisuuden osalta enintään salassa pidettävän tiedon käsittelyyn pilvipalveluissa.

2.1.3 Asiantuntijatyön hankinta

Käyttötapaus on tarkoitettu asiantuntijatyön ja konsulttipalveluiden hankinnan turvallisuusvaatimusten toteutumisen arviointiin, kun halutaan varmistua asiantuntijapalveluita

tuottavan organisaation tietoturvallisuudesta. Arvioinnin laajuus riippuu toimeksiannon toteutustavasta. Esimerkiksi jos työtä tehdään tilaavan organisaation laitteilla, voidaan tekninen osio jättää soveltamatta, jos vastaava arviointi on tehty käytettävien laitteiden ja järjestelmien osalta. Jos työ tehdään toimittajan tiloissa, sovelletaan siihen fyysisten turvallisuuden vaatimuksia tai etätyön vaatimuksia.

2.1.4 Tietojärjestelmän palvelutuotannon arviointi

Käyttötapaus määrittää tietojärjestelmän palvelutuotantoympäristön tai palveluntuottajan arvioinnissa sovellettavan kriteeristön. Käyttötapausta voidaan käyttää, esimerkiksi tietojärjestelmien kehityksessä tai palvelutuotannossa käytettävien tietojenkäsittely-ympäristöjen tietoturvallisuuden arvioitiin tai vastaavia palveluita tarjoavien toimittajien tietoturvallisuuden arviointiin. Käyttötapaus huomioi erityisesti palvelutuotannon jatkuvuudenhallintaan ja fyysiseen turvallisuuteen liittyvät kriteerit.

2.2 Organisaatiokohtaiset käyttötapaukset

Käyttötapaukset helpottavat huomattavasti kriteerien valintaa usein toistuvissa tilanteissa. Esimääriteltyjen käyttötapausten lisäksi organisaatio voi määritellä uusia tai muokata valmiita käyttötapauksia. Käyttötapausten määrittelyssä ja käytössä tulee noudattaa erityistä huolellisuutta, jotta ei rajata ulos olennaisia kriteereitä eikä menetetä joustavuutta, joita muut kriteerien valintaan liittyvät ominaisuudet mahdollistavat.

Käyttötapausten määrittelyssä on suositeltavaa noudattaa seuraavia menettelyitä:

Rajaukset: Organisaation tulee määritellä käyttötapauksen rajaukset, joiden perusteella voidaan päättää, onko jokin kriteeri tarpeellinen juuri tässä käyttötapauksessa vai hoidetaanko asia jonkun arvioinnin ulkopuolelle kuuluvan vastuutahon toimesta. Esimerkiksi jos organisaatio lisää uuden palvelun organisaation yhteiseen infrastruktuuriin, voidaan yhteistä infrastruktuuria koskevat kriteerit arvioida kertaalleen ja jättää pois palvelukohtaisista arvioinneista.

Valinnaiset kriteerit: Mikäli on mahdollista, että joissakin tapauksissa kriteeriä sovelletaan ja joissakin ei, kannattaa se määritellä valinnaiseksi. Kriteerien rajaamista kokonaan pois käyttötapauksesta ei tule tehdä, jos on mahdollista, että se on tarpeellinen joissakin käyttötapaukseen sisältyvissä arviointitilanteissa.

Riskiarviot: Samantyyppisissä samalle turvallisuustasolle sisältyvissä käyttötapauksissa voidaan hyödyntää samaa riskiarviota, jolloin samaa riskiperusteista kriteerien arviointia ei tarvitse tarpeettomasti toistaa.

- Tämä voidaan toteuttaa siten, että käyttötapauksesta rajataan kokonaan pois sellaiset kriteerit, joita ei riskiarvion perusteella sovelleta.
- Vastaavasti käyttötapaukseen voidaan etukäteen tehdyn riskiarvion perusteella sisällyttää olennaisena kriteerit, jotka turvallisuustason perusteella luokitellaan valinnaisiksi. Tällöin kaikki valinnaiset kriteerit voidaan arviointitilanteessa merkitä sovellettaviksi ilman uutta riskiarviota.

Dokumentointi: Käyttötapaukset tulee dokumentoida riittävän tarkasti. Erityisesti tulee kuvata rajaukset ja riskiperusteet, joihin kriteerien sisällyttäminen käyttötapaukseen tai poisjättäminen käyttötapauksesta perustuu. Nämä perusteet tulee kuvata niin tarkasti, että myös riippumaton taho voi tarvittaessa arvioida, onko kriteerin poisjättäminen ollut perusteltua

2.3 Käyttötapauksen kuvaaminen työkaluun

Käyttötapauksen nimi sekä lyhyt yleiskuvaus käyttötapauksen sisällöstä kirjataan välilehdelle Käyttötapauskuvaukset. Käyttötapauksen yleiskuvauksessa kuvataan, millaisiin arviointitilanteisiin käyttötapaus soveltuu.

Koska käyttötapauksen soveltamiseen liittyy useita eri näkökohtia, on suositeltavaa laatia käyttötapauksesta myös erillinen yksityiskohtaisempi kuvaus, jonka perusteella käyttötapauksen hyödyntäjä voi arvioida, soveltuuko käyttötapaus arviointitilanteeseen.

Käyttötapauksessa sovellettavat kriteerit määritellään välilehdellä Käyttötapauskriteerit. Välilehden ylimmälle riville on linkitetty Käyttötapauskuvaukset välilehdellä määriteltyjen käyttötapausten nimet. Käyttötapauksen kriteerien määrittely tehdään kunkin käyttötapauksen sarakkeeseen seuraavasti:

- Käyttötapaukseen sisältyvät olennaiset kriteerit: 1
- Käyttötapaukseen sisältyvät valinnaiset kriteerit: 2
- Käyttötapauksesta poisjätetyt kriteerit: 0

Liite 4: Termistö

Termi	Määritelmä	Lähde
Arviointi	Tarkastelun kohdetta koskevan tiedon analysointi ja tulkitseminen ja niiden pohjalta tehtävä kohteen arvottaminen. (vrt. auditointi). Itsearviointi ja ulkoinen arviointi.	Tepa-termipankki
Asiakirja	Asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.	Julkisuuslaki 5 § 1 mom
Autenttisuus/autenttinen	Aito, väärentämätön, luotettava	Kielitoimiston sanakirja
Eheys	Tiedon ominaisuus, joka ilmentää sitä, että tietoa ei ole muutettu luvatta tai että se ei ole muuttunut vahingossa ja että mahdolliset muutokset voidaan todentaa. Tiedon tai tietojärjestelmän eheys voi tarkoittaa myös sitä, että tieto on sisäisesti ristiriidatonta.	Tepa-termipankki
Erityiset henkilötietoryhmät	Erityisiin henkilötietoryhmiin kuuluvia henkilötietoja ovat sellaiset tiedot, joista ilmenee henkilön rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveyttä koskevia tietoja, seksuaalinen suuntautuminen tai käyttäytyminen, geneettisiä ja biometrisiä tietoja henkilön tunnistautumista varten. Erityisiin henkilötietoryhmiin kuuluvia tietojen käsittely on lähtökohtaisesti kielletty. Tietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille.	Tietosuoja.fi

Termi	Määritelmä	Lähde
Henkilötieto	Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella.	Tietosuoja.fi
Julkinen	Viranomaisen asiakirja, jota ei ole säädetty tai määrätty salassa pidettäväksi. Poikkeuksena tähän ovat ns. harkinnanvaraisesti annettavat asiakirjat eli esimerkiksi valmisteluvaiheen asiakirjat, jotka eivät ole vielä tulleet julkisiksi.	Julkisuuslaki 1, 16 a ja 22 §
Kiistämättömyys, kiistaton	Kieltämätön, eittämätön, kiistämätön, vastaansanomaton, itsestään selvä, varma, ehdoton. Kiistämättömyys on ominaisuus, joka ilmentää sitä, että tiedon lähettäjä tai vastaanottaja tai tietoon liittyvä tapahtuma voidaan varmistaa luotettavasti myös jälkikäteen.	Kielitoimiston sanakirja Tepa-termipankki
Käyttötapaus	Käyttötapauksella tarkoitetaan Julkrissa sellaista toistuvaa arviointitilannetta, jossa voidaan soveltaa samaa valittua kriteerijoukkoa. Esimerkkinä käyttötapauksesta voi olla palveluntuottajan tietoturvallisuuden arviointi, josta on jätetty pois vain viranomaista koskevat kriteerit.	
Luottamuksellisuus	Tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä eikä se paljastu muille.	Tepa-termipankki
Saatavuus	Tiedon ominaisuus, joka ilmentää sitä, miten tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.	Tepa-termipankki

Termi	Määritelmä	Lähde
Salassa pidettävä	Viranomaisen asiakirja, joka on julkisuuslaissa tai muussa laissa säädetty salassa pidettäväksi tai jonka viranomainen on lain nojalla määrännyt salassa pidettäväksi tai asiakirja, joka sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus.	Julkisuuslaki 22 ja 24 §
Tieto	Tiedolla tarkoitetaan tässä suosituksessa samaa kuin asiakirjalla.	
Tietoaineisto	Asiakirjoista ja muista vastaavista tiedoista muodostuva, tiettyyn viranomaisen tehtävään tai palveluun liittyvä tietokokonaisuus.	Tiedonhallintalaki 2 §
Tiedonhallinta-yksikkö	Viranomainen, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti.	Tiedonhallintalaki 2 ja 4 § 1 mom
Tietojärjestelmä	Tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestely. Tietojärjestelmiä ovat esimerkiksi erilaiset pilvipalvelut ja ohjelmistojen käsittelyyn käytettävät päätelaitteet.	Tiedonhallintalaki 2 §
Turvallisuusluokiteltu asiakirja	Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.	Tiedonhallintalaki 18 § Julkisuuslaki 24 §

Termi	Määritelmä	Lähde
Vaatimus	Vaatimus on kohteelle asetettu yksittäinen tavoite, joka kohteen tulee pystyä toteuttamaan. Vaatimus on osa kriteeriä. Vaatimus voidaan toteuttaa useilla eri tavoilla. Vaatimus on mahdollisimman yksilöity, eli samaan vaatimukseen ei sisälly useita eri vaatimuksia.	
Vaatimuksenmukaisuus	Julkrissa suositeltujen vaatimusten täyttymistä arvioinnin kohteessa.	

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-275-8 (pdf)

Kesäkuu 2022