Rami Laitila

JULKISEN HALLINNON TIETOTURVALLISUUDEN ARVIOINTIKRITEERISTÖ TIETOTURVA-ARVIOINTIEN VÄLINEENÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Laitila, Rami
Julkisen hallinnon tietoturvallisuuden arviointikriteeristö tietoturva-arviointien välineenä
Jyväskylä: Jyväskylän yliopisto, 2023, 63 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tutkimuksessa pyrittiin selvittämään, miten Julkri eli Julkisen hallinnon tietoturvallisuuden arviointikriteeristö toimii tietoturva-arviointien välineenä ja miten se suhteutuu aiemmin julkaistuihin tietoturvallisuuden hallintajärjestelmästandardeihin ja tietoturvallisuuden arviointikriteeristöihin.

Tutkimus toteutettiin kirjallisuuskatsauksena aiempaan tietoturvallisuuden hallintajärjestelmiin sekä tietoturvallisuuden sääntelyyn liittyvään tutkimukseen, Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön sekä sen taustalla vaikuttavaan lainsäädäntöön. Julkria vertailtiin muihin kansallisiin ja kansainvälisiin tietoturvallisuuden arviointikriteeristöihin ja niissä esitettyihin vaatimuksiin.

Tutkimuksen tuloksena syntyi työkalu, jossa kullekin kriteeristön vaatimukselle on määritetty sen arviointiin soveltuvat hallinnolliset ja tekniset todennusmenetelmät, joilla vaatimustenmukaisuus voidaan luotettavasti todentaa osana ulkopuolisen tahon suorittamaa riippumatonta arviointia.

Tutkimuksen havaintojen perusteella Julkri on kattava kriteeristö, joka yhdistää useampien olemassa olevien tietoturvallisuuden arviointikriteeristöjen vaatimukset muihin lainsäädännössä esitettyihin vaatimuksiin. Tutkimuksessaa ei kuitenkaan saatu vastausta siihen, miten kriteeristöä on tarkoitus käyttää julkishallinnon toimijoiden ja niiden lukuun toimivien muiden tahojen turvallisuuden arvioinnissa.

Asiasanat: tietoturvallisuus, kyberturvallisuus, tietoturvallisuuden hallinta, lainsäädäntö, tietoturvallisuuden arviointi, auditointi

ABSTRACT

Laitila, Rami
Julkri as a tool for information security evaluations
Jyväskylä: University of Jyväskylä, 2023, 63 pp.
Cyber Security, Master's Thesis
Supervisor: Siponen, Mikko

The research aimed to find out how Julkri (the public administration's information security evaluation criteria) works as a tool for information security evaluations and how it relates to previously published information security management system standards and information security evaluation criteria.

The research was carried out as a literature review of previous research related to information security management systems and information security regulation. Julkri assessment criteria and the legislation that affects it were also studied. Julkri was compared to other national and international data security evaluation criteria and the requirements presented in them.

As a result of the research, a tool was created, in which the administrative and technical verification methods suitable for evaluation of each requirement of the criteria have been determined. These verification methods can be used to reliably verify compliance as part of an independent evaluation performed by an external party.

Based on the findings of the study, Julkri is a comprehensive set of criteria that combines the requirements of several existing information security evaluation criteria with other requirements set forth in legislation. However, the research did not provide an answer as to how Julkri is intended to be used in the evaluation of the safety of public administration operators and other parties acting on their behalf.

Keywords: information security, cyber security, information security management, legislation, information security assessment, auditing

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tämän tutkimuksen tavoitteena on arvioida, miten Julkisen hallinnon tietoturvallisuuden arviointikriteeristö toimii tietoturva-arviointien välineenä. Tutkimuksessa Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön viitataan lyhenteellä Julkri, jota käytetään myös tiedonhallintalautakunnan omassa julkaisussa.

1.1 Aihepiirin kuvaus

Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttämistä. Joissain yhteyksissä saatavuuden sijasta käytetään termiä käytettävyys. Näihin kolmeen osa-alueeseen voidaan yhdistää myös tiedon kiistämättömyys (Suomen Standardisoimisliitto SFS, 2017).

Tietoturvallisuus voidaan joissain tilanteissa mieltää pelkiksi tietoteknisiksi kontrolleiksi, kuten haittaohjelmasuojausohjelmistoiksi, palomuureiksi tai tietojärjestelmien salasanoiksi. Tietoaineistojen suojaaminen laajassa merkityksessään vaatii kuitenkin myös muita kontrolleja ja kokonaishallintaa. Tätä tarkoitusta varten on muodostunut useita viitekehyksiä tietoturvallisuuden hallintajärjestelmille. Nämä hallintajärjestelmät perustuvat tietoturva-alan yleisesti hyväksyttyihin parhaisiin käytäntöihin ja toimintamalleihin. Tietoturvallisuuden hallintajärjestelmiä on sekä yleisluontoisia kansainvälisiä että kansallisia valtion oman erityislainsäädännön huomioivia.

Julkisessa keskustelussa sekä tämänkin tutkimuksen lähdeaineistossa ja tarkastelluissa kriteeristöissä käytetään myös termiä kyberturvallisuus. Kyberturvallisuuden sanaston (2018) mukaisesti kyberturvallisuus tarkoittaa tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa. Tietoturva on keskeisessä roolissa kyberturvallisuutta tavoiteltaessa, mutta laajempaan kokonaisuuteen liittyy myös digitaalisen ja

verkottuneen yhteiskunnan tai organisaation turvallisuus sekä näiden vaikutus toimintaan (Kyberturvallisuuden sanasto, 2018).

Todistaakseen tietoturvallisen toimintansa asiakkailleen, kumppaneilleen ja muille sidosryhmille, ei useinkaan riitä, että organisaatio itse kertoo noudattavansa jotain tiettyä tietoturvallisuuden hallintajärjestelmille määriteltyä kriteeristöä tai standardia, vaan organisaation toimintaan on kohdistettava riippumaton ulkoinen auditointi. Auditoinnilla tarkoitetaan järjestelmällistä, riippumatonta ja dokumentoitua prosessia, jossa arvioidaan kerättyä näyttöä objektiivisesti ja arvioidaan, missä määrin sovitut kriteerit täyttyvät (Suomen Standardisoimisliitto SFS, 2017). Tämän tutkimuksen lähdeaineistossa käytetään terminä sekä auditointia että arviointia, molempien termien kuitenkin tarkoittaessa ulkopuolisen hyväksytyn tahon suorittamaa riippumatonta katselmointia. Tutkimuksessa käytetään niin ikään molempia termejä ja mikäli niiden välille on tarpeen määritellä käsitteellinen ero, on tämä erikseen huomioitu.

1.2 Laki viranomaisten toiminnan perustana

Suomessa tietoturvallisuus on vahvasti läsnä julkishallinnon toimijoiden toiminnassa, sillä nämä toimijat ovat lakisääteisesti velvoitettuja luokittelemaan käsittelemänsä tietoaineiston ja käsittelemään sitä turvallisesti luokituksenn mukaisesti. Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) on säädetty tietoturvallisuustoimenpiteisiin liittyvistä vastuista julkisen hallinnon tiedonhallintayksiköille ja viranomaisille.

Vaatimukset koskevat myös muita kuin viranomaisena toimivia julkisoikeudellisia yhteisöjä. Vaatimukset velvoittavat esimerkiksi yrityksiä, siltä osin kuin ne hoitavat julkista hallintotehtävää. Laissa säädetään myös tietoturvallisuustoimenpiteiden vähimmäistasosta sekä toimijoiden velvoitteesta seurata toimintaympäristönsä tietoturvallisuuden tilaa ja varmistua tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta koko niiden elinkaaren ajan.

Suomessa on käytössä kokonaisturvallisuuden malli, johon yhteiskunnan elintärkeät toiminnot liittyvät (Turvallisuuskomitea, 2017). Malli perustuu viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyöhön, ja sen tavoitteena on varautua erilaisiin häiriötilanteisiin ja varmistaa yhteiskunnan elintärkeiden toimintojen toiminnan edellytykset. Kokonaisturvallisuuden mallin mukaisesti elinkeinoelämän toimijoilla on merkittävä rooli yhteiskunnan kriittisten toimintojen ylläpidossa. Tästä näkökulmasta onkin perusteltua, että tiukkoja tietoturvakriteerejä sovelletaan toimijoihin, jotka vastaavat esimerkiksi huoltovarmuuskriittisten tietojärjestelmien tai infrastruktuurin ylläpidosta, vaikka nämä toimijat eivät viranomaisia olisikaan. Kokonaisturvallisuuden mallin käytännön toteutus perustuu hallinnonalakohtaisiin sekä poikkihallinnollisiin strategioihin ja niiden toimeenpano-ohjelmiin. Tällaisia strategioita ovat esimerkiksi kyberturvallisuusstrategia.

Kokonaisturvallisuuden sanaston (2017) mukaisesti kokonaisturvallisuus voidaan määritellä malliksi ja periaatteeksi, jonka pohjalta asioita tarkastellaan valtioneuvoston tasolla.

Tiedonhallintalain mukaisesti organisaatioiden on tunnistettava olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteensä riskiarvioinnin tulosten mukaisesti. Vaatimus koskee myös hankintoja, joiden osalta organisaation tulisi varmistaa, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. (Valtiovarainministeriö, 2022).

Valtiovarainministeriön alainen tiedonhallintalautakunta hyväksyi 11.5.2022 käyttöön suosituskokoelman, josta käytetään nimeä Julkisen hallinnon tietoturvallisuuden arviointikriteeristö. Kriteeristöstä käytetään lyhennettä Julkri. Tiedonhallintalautakunnan mukaan 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.

Jo ennen Julkrin julkaisua Suomessa on hyväksytty käyttöön Katakri - Tietoturvallisuuden auditointityökalu viranomaisille. Tämän kriteeristön ylläpidosta vastaa ulkoministeriön alaisuudessa toimiva kansallinen turvallisuusviranomainen, NSA. Tutkimuksen kirjoitushetkellä Katakrista on käytössä versio Katakri 2020. Viranomaisten turvallisuusluokitellun tiedon suojaamisen arviointiin voidaan käyttää myös muita kriteeristöjä, joita ovat muun muassa Traficomin ylläpitämä Pilviturvallisuuskriteeristö PiTuKri sekä Digi- ja väestötietoviraston VAHTI-ohjeistukset. Tietoturvallisuuden arviointiin voidaan käyttää myös kansainvälisiä viitekehyksiä, kuten ISO/IEC 27000 -standardisarjaa tai luottokorttitoimijoiden maksuliikenteen turvallisuustarpeisiin luomaa PCI-DSS -standardia. Nämä kansainväliset standardit eivät kuitenkaan huomioi suomalaisen lainsäädännön erityispiirteitä. Tästä syystä voidaan todeta, että julkishallinnon toimijat soveltavat toimintaansa ensisijaisesti kansallisia viitekehyksiä, joiden vaatimukset perustuvat Suomen lainsäädäntöön ja muuhun sääntelyyn. Kansainvälisiä viitekehyksiä ja standardeja sekä niiden mukaisia auditointeja ja sertifiointeja voidaan käyttää kansallisten viitekehysten tukena.

2 TUTKIMUKSEN MOTIIVIT

Suomessa sovelletaan tietoturvallisuuteen useita näennäisen päällekkäisiä arviointikriteeristöjä ja ohjeita, joissa linjataan vaatimuksista viranomaisille ja julkishallinnon muille toimijoille. Osa vaatimuksista perustuu selkeästi suoraan lainsäädäntöön, mutta osa on johdettu kriteeristöihin lakien ja asetusten pohjalta kriteeristön valmistelijoiden tulkintaan perustuen.

Tietoturvallisuuskriteeristöjen käyttöön liittyy keskeisesti myös organisaatiosta itsestään riippumaton ulkoinen arviointi ja sen perusteella myönnetyt todistukset, hyväksynnät tai sertifikaatit. Suomessa arviointia voivat tehdä toimivaltaiset viranomaiset, joita ovat Suojelupoliisi, Puolustusvoimat sekä Liikenne- ja viestintävirasto Traficom. Näiden lisäksi tietoturvallisuutta voivat arvioida hyväksytyt tietoturvallisuuden arviointilaitokset arviointilaitoslain (1405/2011) mukaisesti. Viranomainen tai tietoturvallisuuden arviointilaitokset eivät kuitenkaan myönnä todistuksia tai hyväksyntiä kaikkien aiemmissa luvuissa mainittujen kriteeristöjen mukaisesti. Traficom ylläpitää listaa hyväksytyistä tietoturvallisuuden arviointilaitoksista ja näille myönnetyistä pätevyysalueista. Tämän julkisesti saatavilla olevan luettelon perusteella arviointilaitosten pätevyysalueisiin kuuluvat ISO/IEC 27001, Vahti sekä Katakri 2020 turvallisuusluokkien IV ja III osalta (Traficom, 2023).

Tämän tutkimuksen motiivina on selvittää, miten vuonna 2022 julkaistua Julkria voidaan soveltaa arviointityökaluna ja onko sitä tarkoitettu käytettävän muiden kriteeristöjen rinnalla vai niiden korvaajana. Lisäksi tutkimuksen tavoitteena on selvittää, onko Julkri tarkoitettu kriteeristöksi, jonka pohjalta voidaan myöntää hyväksyntiä tai todistuksia riippumattomaan arviointiin perustuen, vai onko Julkri tarkoitettu vain julkishallinnon organisaatioiden itsearviointityökaluksi tukemaan niitä velvoittavien vaatimusten tunnistamisessa.

Tutkimuksessa vertaillaan Julkria muihin kansallisiin ja kansainvälisiin tietoturvallisuuskriteeristöihin ja tietoturvallisuuden hallinnan viitekehyksiin. Vertailuun on valittu kriteeristöjä, jotka asettavat vaatimuksia tietoturvallisuuden hallinnalle ja tutkimuksen ulkopuolelle on rajattu muut kriteeristöt, joita käytetään esimerkiksi tuotteiden turvallisuuden arvioinnissa.

2.1 Tutkimusongelmat

Aiemmissa luvuissa esitellyn taustan perusteella tutkimukselle määritettiin kolme tutkimuskysymystä:

1. Mikä on eri kriteeristöjen rooli julkishallinnon toimijoiden tai niiden lukuun toimivien muiden yhteisöjen turvallisuuden arvioinnissa?
2. Tuleeko Julkri korvaamaan olemassa olevat toimivaltaisten viranomaisten sekä tietoturvallisuuden arviointilaitosten tietoturvallisuuden arviointityökalut?
3. Miten Julkrin vaatimusten täyttymistä voidaan todentaa luotettavasti?

Tutkimuksessa pyritään selvittämään, mitä uusia vaatimuksia tai tietoturvallisuuden hallintakeinojen toteutusesimerkkejä Julkri tuo mukanaan toimijoille, joiden toimintaan kriteeristön taustalla vaikuttavan lainsäädännön velvoitteita sovelletaan. Erityishuomiota tutkimuksessa tullaan käyttämään Julkrin ja Katakri 2020 -kriteeristöjen väliseen vertailuun. Traficomin ylläpitämän tietoturvallisuuden arviointilaitoslistauksen sekä pätevyysalueluettelon perusteella Katakri on se vaatimuskehikko, jonka mukaisesti tietoturvallisuutta tällä hetkellä arvioidaan toimivaltaisten viranomaisten ja arviointilaitosten toimesta (Traficom, 2023). Vertailua muihin kriteeristöihin, kuten PiTuKriin tai ISO/IEC 27001 -standardiin tullaan tekemään soveltuvin osin.

Toiseen tutkimuskysymykseen siitä, tuleeko Julkri korvaamaan olemassa olevat arviointityökalut pyritään löytämään vastaus ensisijaisesti vertailemalla kriteeristöjä keskenään, jotta voidaan varmistua niiden välisistä eroista ja siitä, onko Julkri ensinnäkään käytettävissä arviointikriteeristönä vai jättääkö se joitain keskeisiä lainsäädännön vaatimuksia huomiotta. Tämän lisäksi vastaus pyritään hakemaan julkisesti saatavilla olevasta materiaalista, kuten Traficomin tai muiden viranomaisten julkaisuista ja tiedotteista. Tutkimuksen tavoitteena ei ole selvittää miten kukin toimivaltaisista viranomaisista on sisäisesti suorittanut arviointikriteeristöjen vertailua tai valmistautunut Julkrin mahdolliseen käyttöönottoon.

3 KIRJALLISUUSKATSAUS

Tutkimus kohdistuu Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön, joka julkaistiin vuonna 2022. Julkaisun tuoreudesta johtuen suoraan Julkriin liittyvää tutkimusta ei ole saatavilla tämän tutkimuksen lähdemateriaaliksi. Kirjallisuuskatsauksessa lähdeaineistoksi on tästä syystä valikoitu tietoturvallisuuden hallintajärjestelmistä tehtyä aiempaa tutkimusta. Muina kirjallisuuslähteinä on käytetty Julkria ja sen tausta-aineistoa sekä muita tietoturvallisuuden arviointikriteeristöjä ja vaatimuskokoelmia. Tutkimuksen lähdeaineistona on käytetty myös kansallista lainsäädäntöä sekä tietoturvallisuuden sääntelyyn liittyvää aiempaa tutkimusta, sillä Julkrin sekä muista kriteeristöistä muun muassa Katakrin perustana toimivat viranomaisten toiminnasta säädetyt lait ja asetukset.

3.1 Tietoturvallisuuden hallintajärjestelmiin liittyvä tutkimus

Aiempi tietoturvallisuuden hallintajärjestelmiin liittyvä tutkimus on jaoteltu julkaisuissa havaittujen teemojen mukaisesti. Tutkimusten teemoissa havaittiin yhteneväisyyttä, vaikka tulokset tutkimusten välillä eivät olisikaan olleet toisiaan tukevia. Seuraavissa alaluvuissa aiempi tutkimus on jaoteltu seuraavasti:

1. Tietoturvallisuuden hallintajärjestelmien tarkoitus ja tärkeys
2. Tietoturvallisuuden hallintajärjestelmien sekä standardien historia ja vertailu
3. Tietoturvallisuuden hallintajärjestelmiin sekä standardeihin liittyvät ongelmat ja kritiikki

3.1.1 Tietoturvallisuuden hallintajärjestelmien tarkoitus ja tärkeys

Szczepaniuk, Rokicki ja Klepacki ovat tutkineet tietoturvallisuuden arviointia julkishallinnossa (2019). Heidän mukaansa tieto- tai kyberturvallisuuden hallinta on toimintaa, joka tähtää organisaatioiden tieto-omaisuuden ja

tietojenkäsittelyjärjestelmien turvallisuuden varmistamiseen riskien estämisellä tai minimoinnilla. Tähän tarkoitukseen tutkijat esittävät käytettävän tietoturvallisuuden hallintajärjestelmiä erottamattomana osana organisaation muusta johtamisjärjestelmästä. On kuitenkin huomattava, että tietoturvallisuuden hallintajärjestelmät voivat olla eri organisaatioissa erilaisia, sillä ne tulisi perustaa organisaation rakenteeseen, tietoturvallisuuspolitiikkaan, prosesseihin ja resursseihin

Tietoturvallisuuden hallintajärjestelmästandardien vertailussaan Susanto, Amunawar ja Tuan (2006) toteavat tietoturvallisuuden hallintajärjestelmän olevan tieto-omaisuuden suojaamiseksi organisaatioille lähes välttämättömyys. Tutkijat kuitenkin korostavat, että täydellisen turvallisuuden saavuttamiselle ei ole olemassa yhtä kaikille organisaatioille soveltuvaa reseptiä.

Humphreys (2008) korostaa tutkimuksessaan tietoturvallisuuden hallinnan roolia organisaation turvallisuuskulttuurin ja turvallisen työympäristön luomisessa. Koko organisaation laajuista johtamismallia voidaan käyttää kulttuurin ja ympäristön kehittämiseksi siten, että jokainen työntekijä tietää oman roolinsa ja ymmärtää toimintansa merkityksen turvallisuuden ylläpidossa. Mikäli organisaatio epäonnistuu turvallisen ja yhtenäisen turvallisuuskulttuurin luomisessa, voi riski tahattomille tai tahallisille tietoturvapoikkeamille kasvaa.

Standardien tärkeyttä tietoturvallisuuden hallinnassa on tutkinut muun muassa von Solms (1999). Von Solms käyttää aiheen tärkeyden esittelyyn vertausta ajoneuvoihin ja tieliikenteen normeihin. Artikkelissa esitetyn vertauksen mukaisesti kaikilta yleisellä tiellä kulkevilta moottoriajoneuvoilta edellytetään voimassa olevaa katsastustodistusta. Todistus osoittaa, että ajoneuvossa on kaikki tarvittavat turvamekanismit ja -ominaisuudet ja ne toimivat asianmukaisesti. Todistuksen lisäksi ajoneuvon kuljettaja tarvitsee ajokortin, joka osoittaa, että hän on oppinut ohjaamaan ajoneuvoa turvallisesti. Tämän lisäksi tieliikenteessä ajoneuvoja ja kuljettajia valvotaan jatkuvasti sen varmistamiseksi, että ajoneuvojen turvallisuusominaisuudet toimivat oikein ja kuljettajat noudattavat tieliikenteen määräyksiä. Edellä kuvatun vertauskuvan mukaisesti tietojärjestelmien hyväksynnät voidaan rinnastaa katsastustodistuksiin. Tietoturvallisuuden hallintajärjestelmistä myönnetyt sertifikaatit vastaavat ajokorttia ja ulkopuoliset arvioijat, kuten viranomaiset ja tietoturvallisuuden arviointilaitokset seuraavat jatkuvasti toiminnan oikeellisuutta poliisin tai katsastuslaitosten tavoin. Tutkimuksessaan von Solms korostaa myös sitä, että tietoturvallisuus ei ole vain yksittäisen organisaation käsissä, vaan siihen liittyvät keskeisesti myös muut toimijat, joiden turvallisuudesta on varmistuttava tai joille organisaation on itse pystyttävä osoittamaan turvallisuutensa.

Shameli-Sendi, Aghababaei-Barzegar ja Cheriet (2016) ovat tutkineet riskien arviointia ja hallintaa ja sitä, miten nämä on määritelty tietoturvallisuuden hallintajärjestelmien kontekstissa. Tutkijoiden mukaan tietoturvallisuuteen liittyvien riskien hallinnan tulisi olla jatkuva prosessi, joka

tukee liiketoimintaa ja tuottaa organisaatioille ymmärryksen niiden tieto-omaisuuteen kohdistuvista uhkista ja riskeistä. Tutkimuksen tuloksissa kirjoittajat kritisoivat tietoturvallisuuden hallintajärjestelmästandardien ja muiden vastaavien viitekehysten riskienhallintamallien yleistä luonnetta sekä yksityiskohtien puutetta, mikä estää organisaatioita viemästä malleja käytäntöön. Koska riskitekijät ovat jatkuvassa muutoksessa, on riskienhallinta ennalta määritetyn ja yleisluontoisen mallin avulla haastavaa (Shameli-Sendi ym., 2016).

Wiander (2007) on tutkinut tietoturvallisuuden hallintajärjestelmiin liittyvien standardien käyttökokemuksia pienissä ja keskisuurissa organisaatioissa. Wiander haastatteli tutkimustaan varten pienten tai keskisuurten yritysten tietoturvallisuuden hallintajärjestelmistä vastaavia henkilöitä tai henkilöitä, jotka olivat osallistuneet hallintajärjestelmien rakentamiseen. Haastateltavat valittiin organisaatioista, joilla oli ISO/IEC 17799 sertifikaatti. ISO/IEC 17799 on myöhemmin korvattu ISO/IEC 27001 standardilla ja sertifioinnilla. Wianderin tutkimuksen perusteella haastateltavat kokivat, että standardi vastasi hyvin heidän organisaatioidensa tarpeeseen ja toimintaympäristöön ja ISO/IEC 17799 -sertifiointia pidettiin toimivan tietoturvallisuuden hallintajärjestelmän peruspilarina pienissä ja keskisuurissa organisaatioissa.

Eri tutkimuksissa korostetaan kokonaisvaltaisen turvallisuuden hallinnan ja johtamismallin tärkeyttä kaikentyyppisten organisaatioiden toiminnassa. Turvallisuusjohtamisen tulisi olla tutkimusten mukaan erottamaton osa organisaation muuta johtamisjärjestelmää, mihin tarkoitukseen tietoturvallisuuden hallintajärjestelmät ovat kehittyneet.

3.1.2 Eri standardien vertailu ja historia

Tietojärjestelmiin, tietoturvallisuuteen ja tietoturvallisuuden hallintaan liittyvät standardit ovat kehittyneet yhdessä tietojärjestelmien kanssa. Kehitykseen on vaikuttanut myös muiden hallintajärjestelmä- ja johtamisjärjestelmästandardien kehitys. Analyysissään tietoturvallisuuden hallinnan kehitysmenetelmistä Siponen (2004) toteaa, että tietoturvamallien kehitystä ovat haitanneet eri tahojen toisistaan riippumaton ja siksi osin päällekkäinenkin toiminta. Lisäksi kehityksessä on keskitytty pääosin teknologiaratkaisuihin, joten sosiotekniset ja ihmisestä riippuvat tietoturvanäkökulmat ovat jääneet kehityksessä taka-alalle tai ne on kokonaan sivuutettu.

Siponen (2006B) on tutkinut myös tietoturvallisuuden hallintaan liittyvien standardien kehitystä. Tutkimuksen mukaan tietoturvallisuuden hallintaan liittyvät standardit ovat saaneet alkunsa tietokoneiden ja tietojärjestelmien alkuajoilta, jolloin tietoturvallisuuden varmistaminen perustui yksinkertaisiin tarkastuslistoihin. Ensimmäisiä esimerkkejä tällaisista tarkastuslistoista ovat 1970-luvulta peräisin olevat The American Federation of Information Processing Societies (AFIPS) sekä SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems.

Tarkastuslistojen jälkeen syntyivät ensimmäiset standardit, joihin kuuluivat BS1799 sekä Generally Accepted Information Security Principles. BS1799 muuttui myöhemmin ISO/IEC 17799 -standardiksi, joka sittemmin on toiminut pohjana myös nykyisin käytössä olevalle ISO/IEC 27001 -standardille. Tarkastuslistojen ja standardien keskeiseksi eroksi Siponen mainitsee standardien kunnianhimoisuuden, mikä näkyi niiden pyrkimyksenä olla kansainvälisesti ja yleisesti sovellettavia kaikenlaisissa organisaatioissa. Tästä geneerisyydestä johtuen ne eivät olleet sovellettavissa käytäntöön yhtä helposti kuin aiemmat tarkastuslistat.

Ensimmäisten tietoturvallisuusstandardien keskeinen heikkous oli oletus siitä, että kaikkien organisaatioiden tulisi ottaa käyttöön tiettyjä teknisiä ratkaisuja tietojärjestelmissään. Tätä ongelmaa pyrittiin korjaamaan uudenlaisilla standardeilla, jotka ottavat huomioon myös organisaation kypsyyden. Kypsyysarvion pohjalta organisaatio voi määritellä pitäisikö sen ottaa käyttöön yleisiä standardien esittämiä ratkaisuja vai keskittyä oman toimintansa kannalta merkittävimpiin vaatimuksiin. Kypsyysarvioon perustuvien mallien perustavana ajatuksena on resurssien suuntaaminen oikeisiin asioihin. Niiden ongelmana kuitenkin on, että luotettavan arvioinnin tekeminen vaatii merkittävää osaamista niin organisaation toiminnasta kuin tietoturvallisuuden eri turvallisuuskontrolleista ja uhistakin.

Tutkimuksen tuloksissa todetaan, että toimiakseen paremmin osaan organisaatioiden muuta toimintaa, tietoturvallisuuden hallintajärjestelmästandardien, tietoturvakriteeristöjen ja muiden vastaavien viitekehysten tulisi mahdollistaa jo käytössä olevien järjestelmien käyttö ja integroitua osaksi esimerkiksi tietojärjestelmien ja ohjelmistojen kehitysmenetelmiä. Jos tietoturvakriteeristöjen käyttö organisaatiossa tarkoittaa olemassa olevien prosessien merkittävää hidastumista, hankaloitumista tai heikentää järjestelmien toimintakykyä, on todennäköistä, että niistä poiketaan ja organisaation tietoturvallisuus heikentyy kokonaisuutena. (Siponen, 2006B.)

Tietoturvallisuuden hallintajärjestelmästandardien vertailussaan Susanto, Amunawar ja Tuan (2011) vertailevat viittä tunnettua viitekehystä tietoturvallisuuden hallintajärjestelmille; ISO/IEC 27001, BS 7799, PCI DSS, ITIL ja COBIT. Tutkijoiden mukaan jokaisella standardilla on oma roolinsa ja asemansa. Standardeista ISO/IEC 27001 ja BS 7799 keskittyvät nimenomaan tietoturvan hallintajärjestelmää, kun taas PCI DSS keskittyy hyvin rajoitettuun osa-alueeseen, joka kyseisen standardin kohdalla on maksukorttien ja maksutapahtumien turvallisuus. Vertailuun valituista standardeista ITIL ja COBIT keskittyvät projektinhallintaan ja IT-hallintaan, ja näin ollen niiden näkemys tietoturvallisuuden hallinnasta on hyvin projekti- ja palvelukeskeinen. Yhteenvetona tutkijat toteavat ISO/IEC 27001 -standardin olevan muita vertailuun valittuja helpommin käyttöönotettavissa ja sen tunnettuus sidosryhmien, kuten organisaation ylimmän johdon, toimittajien ja kumppaneiden oli muita standardeja parempi.

ISO/IEC 27001 -standardia on vertailtu muihin standardeihin myös Royn (2020) toimesta. Julkaisussaan Roy vertailee ISO/IEC 27001 -standardia

yhdysvaltalaisen National Institute of Standards and Technologyn (NIST) kyberturvallisuuden viitekehykseen. NIST:n kyberturvallisuuuden viitekehys on erityisesti kriittisen infrastruktuurin kyberturvallisuuden riskien hallintaan kehitetty työkalu. Sen käyttö on vapaaehtoista ja vaikka sen kohdeyleisöä ovatkin kriittisen infrastruktuurin toimijat, voidaan viitekehystä käyttää myös erilaisten organisaatioiden tarpeisiin. Vertailussaan Roy päätyy johtopääkseen, että standardi ja vapaaehtoinen viitekehys eivät ole ristiriidassa tai kilpaile keskenään. Tutkimuksen tuloksissa todetaankin, että yhdistämällä nämä kaksi mallia toisiinsa, organisaatio voi saavuttaa parhaat tulokset, sillä ISO/IEC 27001 lähtökohta on hyvin geneerinen, kun taas NIST:n viitekehys sisältää enemmän teknisiä tietoturvallisuuden hallintakeinoja.

Aiemman tutkimuksen perusteella tietoturvallisuuden hallintajärjestelmiin liittyvät standardit ja viitekehykset ovat kehittyneet vuosikymmenten aikana yhdessä tietojärjestelmien kehittymisen kanssa. Ensimmäiset vaatimuskokoelmat olivat tarkastuslistojen muodossa, mutta niiden jälkeen standardit ovat kehittyneet laajemmiksi ja ne pyrkivät huomioimaan erilaisten organisaatioiden erilaiset tarpeet ja soveltumaan kunkin organisaation toimintaympäristöön ja turvallisuusvaatimuksiin. Sovellettavien vaatimusten valinta voi perustua organisaation omaan kypsyysarvioon tai riskien arviointiin, mikä vaatii kattavaa organisaation toiminnan sekä siihen kohdistuvien uhkien tuntemusta.

3.1.3 Tietoturvallisuusstandardeihin kohdistuva kritiikki

Tietoturvallisuuden hallintajärjestelmästandardeihin ja niiden soveltamiseen tietoturvallisuuden toteutuskehyksinä ja arviointikriteeristöinä liittyy ongelmia ja rajoitteita, joita ovat tutkineet muun muassa Siponen ja Willison (2009). Julkaisussaan Information security management standards: Problems and solutions kirjoittajat ovat analysoineet BS7799, GAISP/GASSP sekä SSE-CMM -standardeja.

Todisteellinen sitoutuminen ja standardoitu toiminta ovat merkki ulkopuolisille toimijoille siitä, että organisaatio pyrkii määrätietoisesti suojaamaan oman toimintansa. Siponen ja Willison toteavatkin organisaatioiden pyrkivän noudattamaan tietoturvallisuuden hallinnassaan standardeja osoittaakseen sitoutumistaan liiketoimintansa turvaamiseen.

Tutkijat havaitsivat, että tutkitut standardit olivat luonteeltaan geneerisiä eivätkä huomioineet organisaatioiden erilaisia toimintaympäristöjä tai vaihtelevia turvallisuustarpeita. Yleisemmin sovelletut standardit ovat luonteeltaan sellaisia, että ne soveltuvat kaikentyyppisten organisaatioiden sovellettavaksi. Organisaatiot kuitenkin tarvitsivat omaan toimintaansa paremmin räätälöityjä viitekehyksiä ja ohjeistuksia.

Toinen artikkelissa esiin nostettu ongelma liittyy standardien esittämien vaatimusten auktoriteettiin ja sen perustaan. Standardeihin valitut turvallisuusvaatimukset ja toteutusesimerkit perustuvat ”yleisesti hyväksyttyihin periaatteisiin” tai ”alan parhaisiin käytäntöihin”. Standardien laatijat eivät kuitenkaan ole tuoneet omaa valmistelutyötään julkiseksi tai

tarkemmin avanneet standardien taustalla vaikuttavaa päätöksentekoprosessia. Näin ollen standardien käyttäjillä ei ole mahdollisuutta arvioida väitteiden paikkansapitävyyttä ja standardeja soveltavien organisaatioiden on luotettava niihin lähes sokeasti (Siponen & Willison, 2009).

Tietoturvallisuusstandardeja on kritisoitu myös siitä, että ne keskittyvät prosessien olemassaoloon eivätkä prosessien sisältöön, toimivuuteen tai vaikuttavuuteen. Artikkelissaan *Information Security Standards Focus on the Existence of Process, Not Its Content* Siponen (2006A) käyttää esimerkkinä vaatimusta riskianalyysien tekemisestä tai tietoturvatietoisuusohjelman asettamisesta. Kyseiset vaatimukset eivät ota kantaa siihen, miten riskejä tulisi arvioida, millä laajuudella ja millä menetelmin. Vastaavasti pelkkä tietoturvatietoisuusohjelman olemassaolo ei kerro siitä, ovatko organisaation työntekijät saaneet riittävää ja tehtäviinsä soveltuvaa koulutusta tai onko koulutus ollut kattavaa. Standardien näkökulmasta näiden kontrollien olemassaolo riittää, eikä niiden sisällölle tai vaikuttavuudelle aseteta vaatimuksia.

Artikkelissa kritisoidaan myös sitä, että vaatimukset eivät anna ohjeita niiden taustalla vaikuttavien tavoitteiden saavuttamiseen. Nämä ongelmat tulisikin tunnistaa ja huomioida, kun organisaatiot soveltavat standardeja toiminnassaan. Myös tietoturvallisuuden hallintajärjestelmästandardien kehittäjillä on merkittävä vastuu entistä toimivampien viitekehysten ja vaatimusten asettamisessa (Siponen, 2006A).

Tietoturvallisuuden hallintajärjestelmästandardeihin liittyy keskeisesti myös ulkoisten arvioijien tekemät auditoinnit, joita varten organisaatioiden on tehtävä sisäistä valmistelutyötä. Hsu (2009) on tutkinut organisaation eri rooleissa toimivien henkilöiden tulkintoja standardien asettamista vaatimuksista. Tutkimuksen tulosten perusteella esimerkiksi johdon, sertifiointia valmistelevien turvallisuusasiantuntijoiden sekä organisaation muiden työntekijöiden tulkinta eri vaatimuksista eroaa merkittävästi. Hsun tulosten perusteella muut työntekijät esimerkiksi kokevat sertifikaatin myöntämisen negatiivisesti, sillä he kokevat sen johtavan kiristyviin tietoturvavaatimuksiin ja heikompaan käytettävyyteen. Vastaavasti taas organisaation johto kokee sertifikaatin positiivisesti, sillä se kertoo onnistuneesta sisäisestä projektista (Hsu, 2009).

Niemimaa ja Niemimaa (2017) ovat todenneet, että tietoturvallisuuteen ja sen hallintaan liittyviä käytännön sovellutuksia ei ole juurikaan tutkittu, vaikka standardit ja muut yleisesti tunnistetut parhaat käytännöt onkin useissa tutkimuksissa nostettu keskeiseen rooliin organisaatioiden turvallisuuskulttuurin kehittämisessä. Niemimaa ja Niemimaa tutkivat käytännössä, miten yhdessä organisaatiossa sovellettiin käytäntöön tietoturvallisuuden parhaita käytäntöjä ja pyrittiin luomaan organisaatiolle tietoturvallisuuspolitiikka siihen perustuen. Tutkijoiden löydösten perusteella on keskeistä, ketkä organisaatiossa osallistuvat standardien tulkintaan ja ”kääntämiseen”, jotta ne saadaan soveltumaan parhaalla mahdollisella tavalla organisaation toimintaympäristöön ja olemassa olevaan johtamisjärjestelmään.

Aiemman tutkimuksen perusteella ISO/IEC 27001 -standardia pidetään yhtenä merkittävimmistä kansainvälisistä tietoturvallisuuden hallintajärjestelmiin liittyvistä standardeista. Tästä syystä se esiintyy laajasti myös aiheeseen liittyvässä tutkimuksessa. Culot, Nassimbeni, Podrecca ja Sartor (2021) ovat tehneet laajan kirjallisuuskatsauksen ISO/IEC 27001 -standardiin liittyvästä tutkimuksesta ja julkaisuista. Heidän tulostensa perusteella standardia käsitellään edelleen akateemisessa tutkimuksessa hyvin teknisestä näkökulmasta ja standardin sovellettavuutta tai käyttöä organisaatioiden johtamisen näkökulmasta on tutkittu hyvin rajallisesti. Tutkijoiden esittämien tulosten perusteella niin standardia soveltavat organisaatiot kuin tutkijatkin keskittyvät standardiin ja sen esittämiin vaatimuksiin yksittäisen organisaation näkökulmasta, vaikka kasvavaa vauhtia digitalisoituva ja verkottuva maailma voisikin vaatia kriteeristön esittämien vaatimusten huomiointia ja hallintaa organisaatioiden välillä (Culot ym., 2021).

Tietoturvallisuuden hallintajärjestelmiin liittyviä standardeja ja viitekehyksiä on kritisoitu niiden yleismaailmallisesta lähestymistavasta. Etenkin kansainväliset standardit pyrkivät olemaan kaiken kokoisten ja tyyppisten organisaatioiden sovellettavissa, mistä johtuen niiden esittämistä vaatimuksista ja toteutusesimerkeistä puuttuu konkretiaa. Toisaalta standardeja ja kriteeristöjä on kritisoitu niiden asettamien vaatimusten läpinäkyvyyden puutteesta. Vaatimusten voidaan todeta perustuvan tietoturva-alan parhaisiin käytäntöihin, mutta standardien laatijat eivät ole julkaisseet valintaperusteitaan tai perustelujaan. Toisaalta tieteellisessä tutkimuksessa tietoturvallisuuden hallintajärjestelmiä sekä niihin liittyvää standardointia ja arviointitoimintaa on käsitelty hyvin rajallisesti. Aiempi tutkimus keskittyy kriteeristöjen teknisiin vaatimuksiin, vaikka nimitys ”tietoturvallisuuden hallintajärjestelmä” viittaa jo itsessäänkin teknisiä turvallisuuskontrolleja laajempaan ja organisaatiota kokonaisvaltaisesti koskevaan ilmiöön.

3.2 Tietoturvallisuuden sääntelyyn liittyvä tutkimus

Tietoturvallisuus ja kyberturvallisuus ovat verrattain uusia ilmiöitä, joiden sääntelyyn ei ole pitkiä historiallisia perinteitä. Koska tietoturvallisuus liittyy keskeisesti tietojärjestelmiin ja tietojenkäsittelyyn, on myös tällä alalla tapahtuva kehitys jatkuvaa ja nopeaa. Kehittyvien teknologioiden sääntelyyn liittyy useita ongelmia, sillä perinteinen lainsäädäntökoneisto ei pysy teknologia-alan muutosten tahdissa. Tapahtuvaa kehitystä on myös mahdotonta ennustaa, joten lainsäädännöllä ei voida varautua tuleviin muutoksiin, vaan regulaatio on lähes poikkeuksetta reaktiivista.

Lewallen (2020) on tutkinut kehittyvien teknologioiden sääntelyyn liittyviä haasteita ja korostaa julkaisussaan niistä neljä keskeistä. Ensimmäinen haaste liittyy epävarmuuteen. Olemassa olevan sääntelyn suhde uusiin teknologioihin ja ongelmiin ei ole selkeää, minkä lisäksi uuteen sääntelyyn liittyvä toimivalta ei aina ole selvästi määritettävissä ja tunnistettavissa.

Toinen haaste liittyy niinikään toimivaltaan, joka muun muassa tietoturvallisuuteen liittyen on pirstoutunut useille eri toimijoille ja hajautettu toimivalta vaatii hallinnon sisäistä koordinaatiota. Haasteita aiheuttavat kokonaisuuden hallinnan koordinoinnin lisäksi eri toimijoiden ohjaus ja toimintakyky; toiset toimijat voivat olla hyvin joustavia ja proaktiivisia, kun taas toiset hitaammin mukautuvia. Tutkimuksessa kuitenkin korostetaan, että hajautettu sääntely ei välttämättä ole vain negatiivinen asia tilanteissa, joissa säätelijät ovat epävarmoja päätösten vaikutuksesta.

Lewallen nostaa kolmanneksi haasteeksi tavoitteista tai päämääristä johtuvan vastustuksen koordinoinnille. Eri osatekijöiden keskinäinen yhdistäminen toimivaksi kokonaisuudeksi vaatii hallinnon sisäistä ja poikkihallinnollista koordinointia sekä uusia järjestelyjä.

Neljäs julkaisussa esiin nostettu haaste on lainsäätäjien kokema epävarmuus, joka vaikuttaa byrokraattisuuden lisääntymiseen. Kirjoittaja toteaa, että epävarmuus sääntelyn mahdollisista seurauksista voi johtaa siihen, että toimijat välttävät kokonaan uutta sääntelyä. Sen sijaan he pyrkivät vetoamaan olemassa olevaan sääntelyyn, joka kuitenkin voi olla huonosti soveltuvaa tai vaikeasti uuden teknologian osalta tulkittavaa (Lewallen, 2020).

Myös Johnson, Lincke, Imhof ja Lim (2014) ovat tutkineet lainsäädännön merkitystä tieto- ja kyberturvallisuudelle. Heidän kansainvälisen vertailunsa perusteella valtioiden lähestymistavoissa tietoturvallisuuden sääntelyyn on eroja. Osa vertailuun valituista valtioista painottaa sääntelyssään tiedon käytettävyyttä ja saatavuutta, pyrkien takaamaan tiedon käytettävyyden ja tietojenkäsittelyn jatkuvuuden. Osa maista taas painottaa turvallisuutta, erityisesti tiedon eheyden ja luottamuksellisuuden varmistamista, tarvittaessa tiedon saatavuuden ja käytettävyyden kustannuksella.

Lainsäädäntöä tietoturvallisuuden näkökulmasta on tutkittu myös ulkoistamisen ja siihen liittyvien uhkien osalta. Dhillon, Syed ja de Sá-Soares (2016) ovat tutkineet ulkoistamiseen liittyviä ulkoistavien organisaatioiden sekä toimittajien näkökulmia ja näiden organisaatioiden kohtaamia ongelmia. Tutkijat esittävät tutkimuksen perusteella mallia, jossa ulkoistamiseen liittyvä tietoturvallisuus ja toimittajien turvallisuuskyvykkyys varmistetaan kolmen osa-alueen avulla.

Tutkijoiden mukaan toimittajien kyvykkyyden muodostavat teknologinen kypsyys sekä tietoturvallisuusosaaminen ja -kompetenssi. Toinen mallin osa-alue koostuu lainsäädännön noudattamisesta, minkä lisäksi tärkeään rooliin nostetaan asiakkaan toimittajilleen asettamien politiikkojen noudattaminen. Kolmas osa-alue on luottamus siitä, että tarvittavat turvallisuuden hallintakeinot on asetettu toimintaan asiakkaan tiedon suojaamiseksi (Dhillon ym., 2016).

Dhillonin, Syedin ja de Sá-Soaresin esittämä malli on huomionarvoinen myös tämän tutkimuksen näkökulmasta, sillä julkishallinnon tietoturvallisuus ja siihen kohdistuvat vaatimukset koskevat viranomaisten lisäksi myös julkisen ja yksityisen sektorin toimijoita, jotka toimivat tiedonkäsittelijöinä viranomaisten lukuun tai ylläpitävät tietojärjestelmiä, joissa

turvallisuusluokiteltua tai salassapidettävää tietoaineistoa käsitellään. Tutkimuksessa kehitetyn mallin kolmannen osa-alueen eli luottamuksen todistamisen voidaan myös nähdä liittyvän hyvin kiinteästi tietoturvallisuuden ulkoisiin arviointeihin tai auditointeihin ennalta määrättyjen kriteeristöjen mukaan.

Tietoturvallisuuden sääntelyyn liittyvän tutkimuksen perusteella tietoturvallisuuden sääntelyllä ei ole pitkiä perinteitä ja kansainvälisten vertailujen perusteella eri valtioiden lähtökohdat tietoturvallisuuden sääntelyyn vaihtelevat merkittävästi. Koska teknologia ja tietoturvallisuus ovat jatkuvassa ja nopeassa muutoksessa, on tietoturvallisuuden sääntely lähtökohtaisesti reaktiivista.

3.3 Julkisen hallinnon tietoturvallisuuden arviointikriteeristö

Tiedonhallintalautakunta hyväksyi toukokuussa 2022 suosituksen julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä. Valtiovarainministeriön alaisuudessa toimivan tiedonhallintalautakunnan mukaan Julkri tukee tietoturvallisuuden kehittämisen ja arvioinnin tarpeita koko julkishallinnossa ja kriteeristöä tulisi käyttää apuna arvioitaessa lainsäädännössä asetettujen vaatimusten täyttymistä. Suosituksen laadinnassa on huomioitu erityisesti Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) (turvallisuusluokitteluasetus), laki viranomaisen toiminnan julkisuudesta (621/1999) (julkisuuslaki) sekä EU:n yleinen tietosuoja-asetus ((EU) 2016/679) (GDPR).

Edellä mainituissa laissa ja asetuksissa säädetään tietoturvallisuustoimenpiteiden vähimmäistasosta ja velvoitetaan toimijoita seuraamaan toimintaympäristönsä tietoturvallisuuden tilannekuvaa. Tietoa käsittelevien organisaatioiden, olivatpa ne sitten viranomaisia tai muita organisaatioita, jotka käsittelevät turvallisuusluokiteltua tietoaineistoa, tulee vaatimusten mukaan tunnistaa keskeiset tietojenkäsittelyyn liittyvät riskit ja mitoittaa tietoturvallisuustoimenpiteensä riskiarvion mukaisesti.

Julkrissa mainitaan, että viranomaisen tietojärjestelmien turvallisuuden arviointiin voidaan soveltaa lakia viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) (arviointilaki). Suosituksessa viitataan liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen ohjeeseen tietojärjestelmien arviointi- ja hyväksyntäprosesseista. Kyseisessä ohjeessa ei kuitenkaan mainita, mitä kriteeristöä arvioinneissa ja hyväksyntäprosessissa käytetään (Traficom, 2021).

3.3.1 Julkrin osa-alueet

Tiedonhallintalautakunnan suosituksessa tietoturvallisuuden arviointikriteerit on ryhmitelty viiteen osa-alueeseen, joista jokaisella on nimi ja tunniste: hallinnollinen turvallisuus (HAL), fyysinen turvallisuus (FYY), tekninen

turvallisuus (TEK), varautuminen ja jatkuvuudenhallinta (VAR) ja tietosuoja (TSU). Osa-alueet koostuvat pääkriteereistä ja niitä täydentävistä alikriteereistä.

Suosituksen ensimmäinen osa-alue on hallinnollisen turvallisuuden osa-alue, josta käytetään lyhennettä tai tunnistetta HAL. Osa-alue koostuu vaatimuksista, jotka koskevat tietoturvallisuuden hallinnan jalkauttamista osaksi koko organisaation toimintaa.

Fyysinen turvallisuus (FYY) sisältää toimitiloihin ja säilytysratkaisuihin liittyviä kriteereitä, joiden tavoitteena on estää tai rajoittaa luvattomien henkilöiden pääsy suojattavaan tietoaineistoon. Julkrissa todetaan, että tähän osa-alueeseen kuuluvat kriteerit perustuvat Katakrissa esitettyihin vaatimuksiin hallinnollisille alueille, turva-alueille ja teknisille turva-alueille.

Tekninen osa-alue (TEK) pitää sisällään tietojärjestelmien ja tietoliikenneyhteyksien teknisiin ominaisuuksiin, turvalliseen käyttöön ja toimintamalleihin liittyviä vaatimuksia. Osa-alueen kuvauksessa viitataan myös Kyberturvallisuuskeskuksen NCSA-toiminnon suorittamiin salausratkaisuiden yleis- ja erillishyväksyntiin.

Varautuminen ja jatkuvuudenhallinta (VAR) osa-alueelle on koottu normaaliolojen varautumista ja jatkuvuudenhallintaa koskevia vaatimuksia, jotka perustuvat tiedonhallintalain ohella muun muassa ISO/IEC 27002 -standardin esittämiin hallintakeinoihin tietoturvallisuuden jatkuvuuden varmistamiseksi.

Tietosuoja-osa-alueen kriteerit koskevat henkilötietojen käsittelyä. Osa-alueeseen kuuluu muun muassa käsittelyn lainmukaisuutta, tietosuojaperiaatteita sekä rekisteröidyn oikeuksia koskevia kriteereitä (Valtiovarainministeriö, 2022).

3.3.2 Kriteerien rakenne

Jokainen julkisen hallinnon tietoturvallisuuden arviointikriteeristössä esitetty arviointikriteeri koostuu seuraavista osista:

- kriteerin yksilöllinen tunniste
- kriteerin luokittelu (luottamuksellisuus, eheys, saatavuus, henkilötieto)
- kriteerin sisältökappale
    - nimi
    - vaatimus
    - yleiskuvaus
    - mahdollinen toteutusesimerkki
- viittaukset eri lähteisiin

Kunkin kriteerin kohdalla kriteeristön laatijat ovat pyrkineet tunnistamaan kriteerin taustalla vaikuttavan lainsäädännön. Tämän lisäksi kriteeristö sisältää viittauksia myös muihin lähteisiin, kuten Katakriin, PiTuKriin sekä tiedonhallintalautakunnan muihin suosituksiin.

3.4 Muut tietoturvallisuuskriteeristöt

Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä ei ole luotu tyhjästä, vaan sen vaatimukset perustuvat jo aiemmin käytössä olleisiin ja julkaistuihin tietoturvallisuuden vaatimuskokoelmiin ja viitekehyksiin. Seuraavissa kappaleissa on esitelty niistä Julkrin kannalta keskeisimmät. Huomioitavaa kuitenkin on, että tietoturvallisuuden hallintajärjestelmiin liittyviä kriteeristöjä, ohjeita ja vaatimuskokoelmia on myös useita muita, kuten maksuliikenteeseen keskittyvä kansainvälisesti laajasti käytetty PCI-DSS sekä kansalliset Digi- ja väestötietoviraston VAHTI-ohjeet.

Julkri sisältää viittauksia lähinnä Katakriin, PiTuKriin sekä ISO/IEC 27000 -standardiperheeseen, mutta tämä ei tarkoita, että se olisi ristiriidassa muiden standardien kanssa. Organisaation toiminnasta riippuen voi myös olla, että tietoturvallisuuden kokonaishallinta kehittyy, mikäli Julkrin lisäksi sovelletaan käytäntöön jotain muutakin standardia.

3.4.1 Katakri

Ulkoministeriön alaisuudessa toimii Suomen kansallinen turvallisuusviranomainen -toiminto (NSA), joka ylläpitää Katakri-auditointityökalua. Katakri on viranomaisten työkalu, jota voidaan käyttää kohdeorganisaation arviointiin, kun selvitetään sen kykyä suojata viranomaisen salassa pidettävää tietoa (Ulkoministeriö, 2020). Katakrista on tällä hetkellä käytössä versio Katakri 2020. Kriteeristön ensimmäinen versio on julkaistu vuonna 2009 ja aiemmat päivitetyt versiot vuosina 2011 sekä 2015.

Kriteeristö ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin ja vähimmäisvaatimuksiin. Katakrin vaatimukset on jaettu kolmeen osa-alueeseen: turvallisuusjohtaminen (T), fyysinen turvallisuus (F) sekä tekninen tietoturvallisuus (I).

3.4.2 PiTuKri

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) on Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen laatima ja julkaisema kriteeristö, jonka tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta silloin, kun tietoaineistoa käsitellään pilvipalveluissa (Traficom, 2020).

Traficomin mukaan kriteeristö on laadittu Suomen kansallisten tarpeiden näkökulmasta ja sen valmistelussa on huomioitu Valtiovarainministeriön julkisen hallinnon pilvipalveluiden linjaukset sekä vuonna 2020 uusiutunut lainsäädäntö. Kriteerit perustuvat lainsäädännön vaatimusten lisäksi BSI:n pilviturvallisuuskriteeristöön, CSA-pilviturvallisuusyhteisön suojausmatriisiin sekä ISO/IEC 27015 ja ISO/IEC 27017 -standardeihin.

3.4.3 ISO/IEC 27001

ISO/IEC 27000 -standardisarjalla viitataan ryhmään standardeja, joiden yhteinen otsikko on *Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät* (Suomen Standardisoimisliitto SFS, 2017). Standardiperheeseen kuuluvat standardit tarjoavat suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin tietoturvallisuuden hallintajärjestelmissä. Standardiperhe sisältää yleisiä vaatimusstandardeja, ohjestandardeja sekä toimialakohtaisia standardeja.

ISO/IEC 27001 -standardissa määritellään vaatimukset tietoturvallisuuden hallintajärjestelmän luomiselle, toteuttamiselle, käyttämiselle, seurannalle, katselmoinnille, ylläpidolle ja parantamiselle. ISO/IEC 27001 -standardi on se osa tästä kansainvälisestä standardiperheestä, jota vasten tietoturvallisuuden hallintajärjestelmää käyttävät organisaatiot voivat hankkia järjestelmän vaatimustenmukaisuuden auditoinnin ja sertifioinnin.

4 TUTKIMUSMENETELMÄ

Tätä pro gradu -tutkielmaa lähdettiin koostamaan Jyväskylän yliopiston (2022) ohjeiden mukaisesti siten, että tutkimuksen teoriaosuus perustuu kirjallisuuskatsaukseen tai -kartoitukseen. Tämän teoriapohjan ympärille oli tarkoitus luoda uusi malli tai viitekehys tietoturvallisuuden todennusmenetelmistä, joiden avulla ulkopuolinen taho voi arvioida Julkrin vaatimusten täyttymistä hallinnollisin ja teknisin menetelmin osana tietoturvallisuuden arviointi- ja hyväksyntäprosessia.

Aineistoa haettaessa huomattiin, että tutkimuksen kohteena olevan julkishallinnon tietoturvallisuuden kriteeristön uutuudesta johtuen, siihen liittyvää aiempaa tieteellistä tutkimusta ei ole julkaistu. Aineiston haku laajennettiinkin koskemaan myös muita tietoturvallisuuden hallintajärjestelmiä ja niihin liittyviä standardeja koskevaan tutkimukseen ja kirjallisuuteen. Koska Julkri-kriteeristön perustalla vaikuttaa lainsäädäntö ja sitä käytäntöön soveltavat organisaatiot ovat lähtökohtaisesti julkishallinnon toimijoita, valittiin katsaukseen myös tietoturvallisuuden sääntelyyn liittyvää aiempaa tutkimusta. Aiemman tutkimuksen ja julkaisujen lisäksi tämän tutkimuksen lähdeaineistona käytettiin julkisen hallinnon tietoturvallisuuden arviointikriteeristöä, siihen liittyvää lainsäädäntöä sekä muita tietoturvallisuuden arviointikriteeristöjä.

Aineiston ja tutkimusaiheen perusteella havaittiin, että kirjallisuuskatsausta paremmin tutkimukseen soveltuva menetelmä on käsiteanalyysi. Käsiteanalyysiä sovelletaan Pertti Järvisen (2004) *conceptual analytical approach* mallin mukaisesti.

4.1 Tutkimusmenetelmän kuvaus

Käsiteanalyysi on tutkimusmenetelmä, jossa pyritään tutkimuksen keskeisten käsitteiden ja niiden välisten suhteiden analysointiin (Jyväskylän yliopisto, 2023). Järvinen (2004) kuvaa käsiteanalyysin menetelmänä, jota voidaan

soveltaa kahdella tavalla. Ensimmäisessä menetelmässä tutkija johtaa teorian tai mallin aiempiin uskomuksiin ja lähtökohtiin perustuen. Toinen lähestymistapa on tunnistaa aiemmassa tutkimuksessa esitellyt teoriat, mallit ja viitekehykset, joiden pohjalta tutkija pyrkii tunnistamaan, onko ilmiöiden taustalla yhteisiä nimittäjiä. Käsiteanalyysin tavoitteena on järjestää eri tavoin saatua käsitetietoa yhtenäisiksi, johdonmukaisiksi kokonaisuuksiksi käsitesuhteita selvittämällä. Käsiteanalyysissä ei olla niinkään kiinnostuneita tietyn sanan tarkoituksesta, vaan sanojen todellisista ja mahdollisista käyttötarkoituksista.

Puusa (2008) on käsitellyt julkaisussaan käsiteanalyysin erilaisia käyttötarkoituksia. Hänen mukaansa käsiteanalyysin avulla jäsennetään yleisesti tutkittavaa käsitettä, pyritään ymmärtämään käsitteeseen liitettyjä merkityksiä ja selkeyttämään sen suhdetta lähikäsitteisiin. Käsiteanalyysin avulla pyritään tunnistamaan tutkittavasta käsitteestä sen ominaispiirteet perehtymällä laajasti saatavilla olevaan kirjalliseen lähdeaineistoon. Puusan (2008) mukaan käsiteanalyysin avulla voidaan ymmärtää käsitteen kuvaamaan ilmiötä ja analyysin lopputuotosta voidaan käyttää tutkimuksen hypoteesina.

Kirjallisuuskatsaus voidaan tutkimusmenetelmänä jakaa kolmeen erilaiseen alatyyppiin, joita ovat kuvaileva krijallisuuskatsaus, systemaattinen kirjallisuuskatsaus sekä meta-analyysi (Salminen, 2011). Tässä tutkimuksessa on käytetty yhdistelmää kuvailevavasta ja systemaattisesta kirjallisuuskatsauksesta. Kuvaileva kirjallisuuskatsauksen voidaan todeta olevan yleiskatsaus ilman tiukkoja ja tarkkoja sääntöjä. Siinä hyödynnetyt aineistot ovat laajoja ja aineiston valintaa ei ole rajattu, mutta tutkittava ilmiö pystytään silti kuvaamaan laaja-alaisesti.

Systemaattinen kirjallisuuskatsaus on kirjallisuuskatsauksen toinen perustyyppi, jonka tavoitteena on tiivistelmän luominen perustuen tietyn aihepiirin aiempien tutkimusten olennaiseen sisältöön. Sen tarkoituksena on kartoittaa keskustelua ja seuloa esiin tieteellisten tulosten kannalta mielenkiintoisia ja tärkeitä tutkimuksia (Salminen, 2011).

Tutkimuksen aineistoksi valittiin tutkimuksen kohteena oleva julkisen hallinnon tietoturvallisuuden arviointikriteeristö. Arviointikriteeristössä on viitattu useisiin julkishallinnon toimijoita velvoittaviin lakeihin ja asetuksiin, joita myös hyödynnettiin tutkimuksen tausta-aineistona. Aiempaa tutkimusta haettiin tietojenkäsittelyn, tietoturvallisuuden ja johtamisen alan julkaisuista, kuten Information & Management, Computers & Security sekä European Journal of Information Systems. Osa aineistosta perustuu myös tutkielman ohjaajan suosituksiin tutkimusaiheeseen perustuen.

Edellä kuvatuin menetelmin on pyritty tunnistamaan aiemmassa tutkimuksessa esiintyvät keskeiset havainnot ja niiden mahdollisesti muodostamat teemat. Järvisen (2004) käsiteanalyysimallin mukaisesti aiemmasta tutkimuksesta on pyritty löytämään yhteiset nimittäjät ja tunnistamaan niiden vaikutus tutkimuksen kohteena olevaan Julkriin.

4.2 Oma kontribuutio

Tutkimuksen lopputuotteena on tarkoitus määritellä todennusmenetelmät siihen, miten kukin Julkrin vaatimus voitaisiin luotettavasti todentaa. Pääsääntönä voidaan pitää, että luotettavaan todennukseen tarvitaan kaksi eri menetelmää, jotka voivat olla hallinnollisia tai teknisiä. Hallinnollisiin menetelmiin kuuluvat haastattelut sekä dokumentaation katselmointi. Teknisiä menetelmiä ovat muun muassa passiivinen tai aktiivinen rajapinta-analyysi, tietoliikennekuuntelut, haavoittuvuusskannaus sekä sovellustestaus.

Tutkimuksen tavoitteena on, että kunkin vaatimuksen todentamiseen olisi mahdollisuuksien mukaan määritetty sekä hallinnollisia että teknisiä todennusmenetelmiä. Tutkimuksen tavoitteena ei ole määritellä tarkalla tasolla yksittäisiä työkaluja tai komentoja, joilla todennus tulisi suorittaa, vaan tunnistaa vain menetelmä. Tämä rajaus tehdään siitä syystä, että esimerkiksi passiivinen rajapinta-analyysi voidaan toteuttaa useilla eri työkaluilla riippuen arvioitavasta järjestelmästä ja siinä käytössä olevasta käyttöjärjestelmästä.

Todennusmenetelmien valinnassa ja arviointityökalun valmistelussa käytettiin hyödyksi Julkrin liitteenä julkaistua taulukkotyökalua kriteeristön vaatimuksista. Jokaista vaatimusta verrattiin muissa kriteeristöissä esitettyihin vaatimuksiin ja jokaiselle vaatimukselle pyrittiin löytämään soveltuvat todennusmenetelmät perustuen Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen arviointilaitosohjeeseen ja siinä määritettyihin todennusmenetelmiin.

5 JULKRI TIETOTURVALLISUUDEN TYÖKALUNA LAINSÄÄDÄNNÖN JA SÄÄNTELYN NÄKÖKULMASTA

Tämä luku käsittelee Julkriin liittyvää lainsäädäntöä ja muuta sääntelyä, ja pyrkii vastaamaan kysymyksiin siitä, miten julkishallinnon toimijoiden ja niiden lukuun toimivien muiden organisaatioiden turvallisuutta tulisi suomalaisen sääntelyn mukaan arvioida. Alaluvussa pyritään selventämään Julkrin ja muiden kriteeristöjen välistä roolia sekä niiden yhteneväisyyksiä ja eroja sen tunnistamiseksi, voisiko Julkri korvata muut käytössä olevat kriteeristöt vai onko niille kaikille edelleen oma tarpeensa julkishallinnon toimijoiden turvallisuuden arvioinnissa.

5.1 Tietoturvallisuuden sääntely Suomessa

Julkri, eli valtiovarainministeriön alaisen tiedonhallintalautakunnan suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä perustuu julkisen hallinnon toimijoiden tietojenkäsittelyyn liittyviin lakeihin ja säädöksiin sekä niissä asetettuihin vaatimuksiin. Suosituksen laadinnassa huomioidut keskeiset lait ja asetukset ovat niin kutsuttu turvallisuusluokitteluasetus eli Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) sekä laki viranomaisen toiminnan julkisuudesta (621/1999) eli julkisuuslaki. Tietosuojan osalta suosituksessa on huomioitu Euroopan Unionin yleinen tietosuoja-asetus ((EU) 2016/679), josta käytetään myös nimityksiä tietosuoja-asetus tai GDPR. Tietosuojaan liittyviä vaatimuksia on asetettu myös tietosuojalaissa (1050/2018) (Valtiovarainministeriö, 2022).

Valtioneuvoston ohjesäännön 2003/262 mukaisesti valtiovarainministeriön vastuulla on huolehtia julkishallinnon yleisestä kehittämisestä ja julkisen hallinnon tietopolitiikan, tiedonhallinnan ja sähköisen asioinnin kehittämisestä. Käytännössä tämä vaatimus on pyritty toteuttamaan julkisen hallinnon tiedonhallinnasta säädetyllä lailla 906/2019.

Tiedonhallintalailla pyritään varmistamaan, että viranomaiset käsittelevät tietoaineistojaan yhdenmukaisesti ja turvallisesti. Tämän lisäksi valtiovarainministeriö ohjaa valtionhallinnon tietoteknisiä hankintoja ja on velvoittanut toimijoita käyttämään valtion yhteisiä tieto- ja viestintäteknisiä palveluita, jotka Valtori tuottaa (1226/2013). Turvallisuuskriittisiä toimijoita velvoitetaan käyttämään turvallisuusverkon palveluja julkisen hallinnon turvallisuusverkkotoiminnasta säädetyn lain (10/2015) mukaisesti. Turvallisuusverkkolain tarkoituksena on varmistaa valtion ylimmän johdon ja turvallisuusviranomaisten ja muiden toimijoiden viestinnän häiriöttömyys ja jatkuvuus.

Tiedonhallintalaissa (906/2019) määrätään, että valtion viranomaisten ja erikseen mainittujen muiden toimijoiden on turvallisuusluokiteltava asiakirjansa. Asiakirjoihin on tehtävä vastaavat merkinnät sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjan käsittelyyn on sovellettava. Tiedonhallintalain vaatimusten käytännön toteuttamista on tarkennettu turvallisuusluokitteluasetuksessa (1101/2019). Tiedonhallintalain mukaisesti vastuu turvallisuusluokittelusta, merkinnästä ja sen mukaisista käsittelyolosuhteista on tiedonhallintayksiköllä. Tiedonhallintayksikön tulee mitoittaa tietoturvallisuustoimenpiteet tietojenkäsittelyyn kohdistuvien arvioitujen riskien mukaisesti suhteuttaen ne omaan toimintaympäristöönsä ja tietoturvallisuuden tilaansa. Tiedonhallintayksikön johdon vastuulla on huolehtia tietojenkäsittelyyn liittyvien vastuiden määrittelystä, ohjeiden ajantasaisuudesta, riittävästä koulutuksesta ja osaamisesta sekä soveltuvista työkaluista. Näiden toimenpiteiden lisäksi turvallisuusluokitellun tiedon käsittelyyn tulee kohdistaa riittävästi valvontaa poikkeamien havaitsemiseksi ja niihin reagoimiseksi.

Julkisuuslain (621/1999) mukaan viranomaisten asiakirjat ovat julkisia, jollei laissa erikseen toisin säädetä. Lain tarkoitus on toteuttaa avoimuutta viranomaisten toiminnassa ja tarjota yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä. Julkisten asiakirjojen perusteella yksilöillä ja yhteisöillä on mahdollisuus muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan. Laissa määritellään hyvin tarkkaan ne asiakirjat, jotka ovat salassapidettäviä.

Viranomaisten käyttämien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista on säädetty niin kutsutussa arviointilaissa (1406/2011). Tämän lisäksi Suomessa on erikseen säädetty kansainvälisiin tietoturvallisuusvelvoitteisiin liittyen lailla 588/2004. Siitä, kuka tai mikä taho näissä laeissa mainittuja arviointeja voi tehdä, on säädetty arviointilaitoslaissa (1405/2011). Arviointilain mukaan tietoturvallisuuden arviointi voi perustua lailla tai asetuksella säädettyyn vaatimukseen, valtiovarainministeriön ohjeeseen, kansallisen turvallisuusviranomaisen ohjeeseen, Euroopan Unionin tai muun kansainvälisen toimielimen antamiin säännöksiin tai ohjeisiin, yleisesti tai alueellisesti sovellettuihin säännöksiin, määräyksiin tai ohjeisiin sekä vahvistettuun standardiin. Liikenne- ja viestintävirasto Traficomin

Kyberturvallisuuskeskuksella on merkittävä rooli arviointien toteuttajana sekä arviointilaitosten toimintaa ohjaavana ja valvovana tahona.

Kuten jo edellä todettiin, laki velvoittaa valtionhallinnon viranomaisia käyttämään Valtion tieto- ja viestintätekniikkakeskus Valtorin palveluja. Tämä velvoite tulee valtiovarainministeriön hallinnonalaan kuuluvasta laista Valtion talous- ja henkilöstöhallinnon palvelukeskuksesta (2019/179). Muita velvoittavia lakeja ovat lait valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (2013/1226), julkisen hallinnon turvallisuusverkkotoiminnasta annettu laki (2015/10) sekä talousarviolaki (1988/423). Valtioneuvoston asetuksessa valtion yhteisten tieto- ja viestintäteknisten palveluiden järjestämisestä (2014/132) määritellään perustietotekniikkapalveluihin kuuluvaksi laitteet, ohjelmistot, tietoliikenne- ja viestintäpalvelut sekä niiden tarvitsemat infrastruktuuri- ja tukipalvelut. Asetuksen voidaankin todeta koskevan niin yksittäisiä työasemia kuin kapasiteetti- ja konesalipalveluitakin.

Valtion viranomaisilla on käytössään myös tietojärjestelmiä, jotka ovat vain niiden käytössä. Nämä niin kutsutut toimialasidonnaiset järjestelmät eivät ole valtionhallinnon yhteisiä palveluita, joten Valtori ei suoraan tuota niitä. Edellä kuvattujen lainsäädännön ja asetusten vaatimusten perusteella on kuitenkin tulkittavissa, että myös toimialasidonnaiset järjestelmät on tuotava Valtorin konesali- ja kapasiteettipalveluiden piiriin, vaikka itse järjestelmän ja ohjelmistojen ylläpito olisikin toisen viranomaisen tai heidän lukuunsa toimivan muun tahon vastuulla.

Turvallisuusverkon toimintaa ja vaatimuksia on määritelty hallituksen esityksessä 54/2013. Turvallisuusverkko on viranomaisverkko, jonka tavoitteena on täyttää korkean turvallisuustason ja varautumisen vaatimukset hallinnollisin, toiminnallisin ja teknisin ratkaisuin. Näiden vaatimusten täyttämiseksi valtio omistaa tiettyjä keskeisiä osia kriittisestä infrastruktuurista. Korkea turvallisuustaso edellyttää henkilöstöturvallisuuden järjestelyjä, verkkoliikenteen valvontaa, salausta ja automaattista reititystä sekä fyysisen turvallisuuden kontrolleja, kuten murtosuojausta, varavoimaa sekä suojausta asevaikutukselta tai elektroniselta tiedustelulta ja sähkömagneettiselta hajasäteilyltä. Turvallisuusverkon käyttöön liittyy käyttövelvoite, joka koskee valtioneuvostoa, poliisia, rajavartiolaitosta ja puolustusvoimia sekä tiettyjä muita turvallisuuden kannalta kriittisiä viranomaisia, kuten Tullia. On huomioitava, että kaikki toimijat, jotka ovat velvollisia käyttämään turvallisuusverkon palveluita eivät ole velvollisia käyttämään Valtorin tuottamia toimialariippumattomia palveluita.

Tietoturvallisuutta ja kyberturvallisuutta on pyritty kehittämään valtioneuvoston periaatepäätöksillä, jotka ovat poliittisia tahdonilmauksia tai kannanottoja, mutta niillä ei ole säädöksen asemaa (Valtioneuvosto, 2020). Valtioneuvoston periaatepäätökset ovat Suomen hallituksen käyttämä työkalu, jolla pyrkii ohjaamaan viranomaisten toimintaa. Periaatepäätösten toimeenpano ja sitovuus perustuvat siihen, miten hyvin ne pystytään muuttamaan konkreettiseksi toiminnaksi tai huomioimaan lainsäädännössä. Keskeinen

tietoturvallisuuteen vaikuttava valtioneuvoston periaatepäätös on Kyberturvallisuusstrategia, jonka uusin versio julkaistiin vuonna 2019. Kyberturvallisuusstrategian toteutumista on seurattu vuosittain valtionhallinnon sisällä. Jokainen hallitus päättää kuitenkin itse toimikautensa alussa, mitkä aikaisempien hallitusten tekemistä periaatepäätöksistä ovat voimassa kuluvalla hallituskaudella, joten periaatepäätökset eivät johda säädösten kaltaiseen jatkuvaan kehitykseen.

Tietoturvallisuuden sääntelyyn liittyvät lait ja asetukset ja niissä säädetyt vaatimukset ovat pirstaloituneet useaan eri lakiin, mistä johtuen niissä esitettyjen vaatimusten vertailu ja tulkinta on haastavaa. Avoimuuden ja julkisen vallan käytön läpinäkyvyyden näkökulmasta julkisuuslain periaate viranomaisten asiakirjojen julkisuudesta on ihailtava, mutta turvallisuusnäkökulmasta linjaus on haastava, sillä tiedon suojaamiselle tulisi olla laissa määritelty selkeä peruste.

5.2 Tietoturvallisuuden sääntelyyn liittyvät ongelmat

Julkri on tarkoitettu työkaluksi erityisesti julkishallinnon toimijoille. Tietoturvavaatimukset näille toimijoille sekä niiden lukuun toimiville muille organisaatioille on kriteeristöön johdettu pääasiallisesti lainsäädännöstä. Suomalainen lainsäädäntö ja asetukset muodostavat laajan kokonaisuuden, jonka tulkinta on paikoitellen haastavaa. Tämä ongelma on tunnistettu myös valtionhallinnossa ja tietoturvallisuuden sääntelyyn liittyen on tehty kansallista selvitystyötä.

Keskeisimmät selvitykset on laadittu osana valtioneuvoston selvitys- ja tutkimustoimintaa. Tutkijaryhmä Lehto, Limnéll, Innola, Pöyhönen, Rusi, ja Salmela totesivat vuoden 2017 yhteenvedossaan, että tietoturvallisuuden sääntelyyn liittyvien perusasioiden nähtiin olevan Suomessa kunnossa, sillä sääntelyä on tehty jo useiden vuosikymmenten ajan. Selvityksen mukaan lainsäädännössä ei ole merkittäviä puutteita eikä se estä viranomaisten välistä yhteistoimintaa. Selvityksessä kuitenkin tunnistettiin, että tietoturvallisuuteen ja kyberturvallisuuteen liittyvän lainsäädännön kehittäminen on hankalaa, koska erityisesti kyberturvallisuus on ilmiönä useita eri hallinnon osa-alueita poikkileikkaava.

Osana valtioneuvoston selvitys- ja tutkimustoimintaa on laadittu myös toinen selvitys, joka julkaistiin vuonna 2018. Tutkimusryhmän kokoonpano oli osin sama kuin ensimmäisessä selvityksessä ja siihen kuuluivat Lehto, Limnéll, Kokkomäki, Pöyhönen ja Salminen. Tutkijat esittävät, että kyberturvallisuuden kokonaisvaltaiseen strategiseen johtamiseen liittyy selkeitä puutteita, jotka johtuvat ministeriöiden hyvin itsenäisestä toiminnasta omilla sektoreillaan. Valtioneuvoston tasolla millään taholla ei nähty olevan selkeää kokonaisvastuuta kyberturvallisuuden strategisesta johtamisesta ja siihen liittyvän säätelyn ohjaamisesta (Lehto ym., 2018).

Vuonna 2021 julkaistiin valtioneuvoston selvitys Tietoturvallisuuden ja tietosuojan kehittäminen yhteiskunnan kriittisillä toimialoilla, josta käytetään myös lyhennettä TITUKRI. Selvitystyön tekivät Lehtilä, Nyström, Ronikonmäki ja Sirviö. Selvityksen perusteella tietoturvallisuuden ja tietosuojan osalta kehitettävää on viranomaisten yhteistoiminnassa, lainsäädännössä, velvoittavissa tietoturvallisuusvaatimuksissa sekä näiden vaatimusten valvonnassa ja säännöllisessä arvioinnissa. Selvitys kohdistui yhteiskunnan kriittisiin toimialoihin, kuten energia- ja vesihuoltoon, liikenteeseen, rahoitussektorille ja terveydenhuoltoon. Tutkijaryhmän mukaan kaikilta näiltä aloilta löytyy kehitettävää, ja selvitys esittääkin kattavan tietoturvallisuuden hallintajärjestelmän kehittämistä, huomioiden sekä tekniset, johtamiseen liittyvät että henkilöstöön liittyvät näkökulmat (Lehtilä ym., 2021).

TITUKRI-selvityksessä korostetaan, että lainsäädännön kehittämisessä on keskeistä varmistua siitä, että tietoturvallisuuteen ja tietosuojaan liittyvät vaatimukset ovat tarpeeksi kattavia ja niiden noudattamiseen kohdistuu riittävästi valvontaa. Viranomaisten välinen yhteistyö on tärkeää etenkin kriittisillä toimialoilla, joihin selvityskin kohdistuu, sillä näillä toimialoilla toimii viranomaisten lisäksi myös muita organisaatioita, joiden toimintaan voi kohdistua useamman eri viranomaisen ohjausta ja valvontaa. Tällaisessa tilanteessa viranomaisten väliset toimintatapojen tietoturvan ja tietosuojan vaatimusten valvonnassa on oltava yhteneväiset.

Selvitys nostaa esiin tarpeen kriittisten toimialojen toimijoita velvoittavien tietoturvallisuusvaatimusten kehittämiselle. TITUKRI-selvityksen perusteella tietoturvallisuuteen liittyvät toimintavelvoitteet tai niiden arviointi ja valvonta säännöllisesti ei tällä hetkellä ole riittävää. Erityisesti henkilöstöturvallisuuteen liittyvät seikat, kuten koulutus ja tietoturvatietoisuuden lisääminen nostetaan selvityksessä kehityskohteiksi (Lehtilä ym., 2021).

Valtiontalouden tarkastusvirasto (VTV) on kohdistanut tarkastuksia aiemmissa luvuissa mainitun hallinnon turvallisuusverkon toimintaan sekä Valtorin tuottamiin palveluihin ja niiden tietoturvallisuuden arviointeihin. Vuonna 2016 tehdyn tarkastuksen perusteella hallinnon turvallisuusverkolle ja siihen liittyville hankkeille saavutettuja tavoitteita ei oltu pystytty saavuttamaan (VTV, 2016). Raportin perusteella riskinä nostettiin esiin turvallisuusverkkoon liittyvät merkittävät kustannukset. Turvallisuusverkkoon ja sen palveluihin liittyy lähtökohtainen vaatimus korkeasta turvallisuustasosta, sillä turvallisuusverkossa on pystyttävä käsittelemään luottamuksellista tietoaineistoa, mikä käytännössä edellyttää Katakrin TL III -vaatimusten täyttymistä niin hallinnollisten prosessien kuin tilojen ja tietojärjestelmien teknisten kontrollien osalta. VTV:n tarkastusraportin mukaan etenkin käyttövelvoitteen alaiset viranomaiset kokivat omien toimialasidonnaisten järjestelmiensä tuomisen Valtorin ylläpitämään turvallisuusverkkoon kalliiksi. Tarkastuksessa todettiin, että valtiovarainministeriön vaatimuksesta kaikki turvallisuusverkossa käytettävät palvelut tulee auditoida, mutta tähän tunnistetaan liittyvän merkittävä riski siitä, että auditoinneissa paljastuu

seikkoja, jotka poikkeavat merkittävästi turvallisuusverkolle asetetusta vaatimustasosta. VTV toteaa toisessa tarkastusraportissaan vuodelta 2017, että auditointeja vaikeuttaa sovellettavien vaatimusten tulkinnan epäselvyys. Turvallisuusverkon osalta on toisaalta sovellettu tieto- ja viestintäteknisille palveluille määriteltyä korkean varautumisen, valmiuden ja turvallisuuden kriteeristöä (VaVaTu), mutta toisaalta käytetty myös Katakria auditointityökaluna (VTV, 2017).

Voimassa olevan lainsäädännön ja siihen liittyvien aiempien tutkimusten ja selvitysten perusteella tietoturvallisuuden sääntelyyn Suomessa kohdistuu useita ongelmia. Turvallisuuskriittisten toimijoiden kenttä on pirstaloitunut ja ohjaus ja valvonta jakautuu useille eri ministeriöille tai viranomaisille. Lainsäädännön perusteella tietojärjestelmien ja tietoliikennepalveluiden, joissa käsitellään turvallisuusluokiteltua tietoaineistoa tulisi täyttää turvallisuusvaatimukset. On kuitenkin jokseenkin tulkinnanvaraista, mitkä nämä sovellettavat vaatimukset kulloinkin ovat. Lainsäädäntö sekä kriteeristöt, kuten Katakri itsessään korostavat myös turvallisuustoimenpiteiden riskiperusteisuutta ja niiden mitoittamista arvioituihin uhkiin nähden.

Käytännön tasolla riskiperusteisuus on kuitenkin vaikeasti tulkittavissa. Tässä tutkimuksessa selvitettyjen lähteiden ja aiemman tutkimuksen perusteella ei ole selkeää, onko riskien arviointi tietoaineiston omistajan vai tiedon käsittelijän vastuulla. Toisaalta voidaan myös tulkita, että turvallisuusverkon osalta Valtori ja operaattorina toimiva Suomen Erillisverkot Oy ovat vastuussa turvallisuusvaatimusten valvonnasta ja näin ollen ympäristöönsä liittyvien riskien tunnistamisesta ja hallinnasta. Tilannetta mutkistaa edelleen vaatimus tietoturvallisuuden arvioinneista; onko auditointia suorittavan tahon, eli Traficomin tai hyväksytyn tietoturvallisuuden arviointilaitoksen hyväksyttävä järjestelmälle laadittu riskiarvio ja perustettava arviointinsa siihen vai sovelletaanko auditointeihin aina esimerkiksi Katakrin kaikkein tiukimpia vaatimuksia riippumatta tiedon omistajan tai järjestelmän toimittajan riskiarviosta.

Edellä kuvattujen havaintojen pohjalta eri viranomaisten järjestelmät voivat näennäisesti täyttää TL III -tason vaatimukset, mutta käytännössä niiden arviointi on tehty eri perustein tai eri kriteeristöjä käyttäen. Julkrin julkaisu ei toistaiseksi ole selkeyttänyt tilannetta, sillä sen rooli olemassa oleviin kriteereihin, kuten Katakriin tai vanhempiin Vahti-ohjeisiin nähden on epäselvä.

6 JULKRIN VAATIMUKSET

Tässä luvussa käsitellään Julkisen hallinnon tietoturvallisuuden arviointikriteeristössä esitettyjä kriteereitä. Luvun tavoitteena on kuvata, mitkä Julkrin kriteereistä perustuvat muissa tietoturvallisuuskriteeristöissä, kuten Katakrissa tai PiTuKrissa asetettuihin vaatimuksiin ja mitkä kriteereistä ovat kokonaan uusia.

6.1 Sovellettavien arviointikriteerien määritys

Alla esitellyt tulokset perustuvat Julkrin liitteessä 2 olevaan taulukkomuotoiseen työkaluun, jota voidaan käyttää vaatimusten arviointiin. Työkalua voidaan käyttää vaatimusten rajoittamiseen arvioinnin kohteena olevan organisaation ja suojattavan tiedon mukaisesti. Työkalun avulla organisaatio voi määrittää arvioinnille esiehdot seuraavien luokkien mukaisesti ja määrittää niille arvot:

- Turvallisuustasot
    - Vaadittava luottamuksellisuuden taso
        - Julkinen
        - Salassa pidettävä
        - TL IV
        - TL III
        - TL II
        - TL I
    - Vaadittava eheyden taso
        - Vähäinen
        - Normaali
        - Tärkeä
        - Kriittinen
    - Vaadittava saatavuuden taso

        - Vähäinen
        - Normaali
        - Tärkeä
        - Kriittinen

- Henkilötiedot arvioinnin kohteessa
    - Ei henkilötietoja
    - Henkilötieto
    - Erityinen henkilötietoryhmä

- Arviointiin sisällytettävät osa-alueet
    - Hallinnollinen turvallisuus
    - Fyysinen turvallisuus
    - Tekninen turvallisuus
    - Tietosuoja
    - Varautuminen ja jatkuvuudenhallinta

Työkalulla voidaan määritellä myös kriteeristön käyttötapaus, jonka mukaisesti sovellettavat vaatimukset valikoituvat. Julkrissa on etukäteen määritelty neljä erilaista käyttötapausta, jotka ovat tiedonhallintayksikön hallinnollinen turvallisuusarviointi, SaaS (Software as a Service) -pilvipalvelun arviointi, asiantuntijatyön hankinta sekä tietojärjestelmän palvelutuotannon arviointi (Valtiovarainministeriö, 2022).

Käyttötapausten tarkoituksena on tukea viranomaisia ja muita tiedonhallintayksiköitä sovellettavien kriteerien tunnistamisessa etenkin hankintatilanteissa. Mikäli Julkria ja sen liitteenä olevaa työkalua voidaan soveltaa hankintoja tehtäessä, voidaan alihankkijoiden tai järjestelmätoimittajien toiminnan turvallisuuden arviointiin soveltaa vain kulloinkin relevantteja vaatimuksia sen mukaisesti, minkälaisesta toimijasta on kyse. Aiemmissa kriteeristöissä, kuten Katakrissa vastaavaa käyttötapauksen mukaista vaatimusmäärittelyä ei ole ollut, vaan soveltuvien vaatimusten määrittely on perustunut riskiarviointiin. Koska riskiarvioinnille ei ole määritelty selkeitä ja yhteneväisiä perusteita, on mahdollista, että eri viranomaiset ovat soveltaneet eri kriteereitä hankkiessaan samoja palveluita samalta toimittajalta. Tämä voi esimerkiksi tarkoittaa sitä, että toinen viranomainen on vaatinut kaikkien Katakrin vaatimusten täyttymistä toisen vaatiessa ainoastaan T- ja F-osioiden vaatimusten täyttämistä samalta toimittajalta palveluita hankkiessaan.

6.2 Vaatimusten vertailu muihin kriteeristöihin

Julkisen hallinnon tietoturvallisuuden arviointikriteeristössä on yhteensä 83 pääkriteeriä. Hallinnollisen turvallisuuden osa-alueeseen kuuluu 19 pääkriteeriä, fyysisen turvallisuuden osa-alueeseen 11, teknisen turvallisuuden

osa-alueeseen 23, varautumisen ja jatkuvuuden hallinnan osa-alueeseen 9 ja tietosuojan osa-alueeseen 21 pääkriteeriä. Osa pääkriteereistä jakautuu edelleen alakriteereihin, joissa täydennetään pääkriteerin vaatimusta. Kaikki pääkriteerit ja alakriteerit yhteenlaskettuna Julkrissa on yhteensä 222 vaatimuskohtaa.

Pääkriteerien edelleen alakriteereihin jaottelun perusteena voi olla esimerkiksi vain tiettyihin turvallisuusluokkiin kohdistuva vaatimus. Tällaisia vaatimuksia on esitetty muun muassa fyysisen turvallisuuden osa-alueella alakriteereissä FYY-04.3 ja FYY-04.4. Nämä vaatimuskohdat koskevat vain turvallisuusluokan III tai sitä korkeammin luokiteltua tietoaineistoa. Alakriteereitä on käytetty myös jakamaan laajoja vaatimuskokonaisuuksia pienempiin kokonaisuuksiin, kuten teknisen turvallisuuden vaatimuksessa TEK-16, jossa tiedon salaamiseen kohdistuvat vaatimukset on eroteltu alakriteereissä TEK-16.1 ja TEK-16.2 turvallisuusalueen sisällä tapahtuvaan salaukseen ja turvallisuusalueen ulkopuolella tapahtuvaan salaukseen.

6.2.1 Hallinnollinen turvallisuus

Julkisen hallinnon tietoturvallisuuden arviointikriteeristön vaatimusten tarkastelun perusteella hallinnollisen turvallisuuden osa-alueen vaatimukset perustuvat laajasti jo aiemmin Katakrin osa-alueessa T, Turvallisuusjohtaminen esitettyihin vaatimuksiin. Uudet vaatimukset hallinnollisen turvallisuuden osa-alueella ovat:

- HAL-04: Suojattavat kohteet
    - Vaatimus HAL-04 velvoittaa organisaatiot tunnistamaan suojattavat kohteensa ja pitämään niistä ajantasaista kirjanpitoa.
    - Pääkriteeri sekä alakriteerit perustuvat tiedonhallintalakiin, turvallisuusluokitusasetukseen sekä julkisuuslakiin.
    - Vastaavaa kriteeriä ei suoraan löydy Katakrista, mutta alakriteerit HAL-04.2, HAL-04.3 sekä HAL-04.4 perustuvat Katakrin vaatimukseen T-08. Vastaavankaltainen kriteeri löytyy myös ISO/IEC 27001 -standardista, joka velvoittaa organisaatioita pitämään yllä ajantasaista luetteloa suojattavasta omaisuudestaan.
- HAL-05: Vaatimukset
    - Vaatimus HAL-05 velvoittaa organisaatioita tunnistamaan toimintaansa vaikuttavat tietoturvavaatimukset. Näitä vaatimuksia voivat asettaa sidosryhmät, mutta ne voidaan johtaa myös lainsäädännöstä tai organisaation omasta toiminnasta.
    - Kriteeri perustuu tiedonhallintalakiin. Vastaavaa vaatimusta ei ole esitetty Katakrissa tai PiTuKrissa, mutta verrattavissa oleva vaatimus esiintyy ISO/IEC 27001 -standardissa.
- HAL-09.1: Dokumentointi - ajantasaisuus
    - Pääkriteeri HAL-09, Dokumentointi perustuu jo aiemmin julkaistuihin kriteeristöihin, kuten Katakriin ja siinä esitettyyn vaatimukseen T-01. Alakriteeri HAL09-1 edellyttää kuitenkin erikseen organisaatioilta prosessia dokumentaation

ajantasaisuuden ja kattavuuden seurantaan. Seurannan lisäksi vaatimus velvoittaa reagoimaan dokumentaatiossa havaittuihin puutteisiin.
    - Sekä pääkriteeri että alakriteeri perustuvat tiedonhallintalakiin. Vaatimuksen muissa lisätiedoissa mainitaan myös ISO/IEC 27001 -standardin vaatimus dokumentaation ajantasaisuuden seurannasta.
- HAL-17: Tietojärjestelmien toiminnallinen käytettävyys ja vikasietoisuus
    - Julkrissa on aiempia kriteeristöjä selkeämmin huomioitu käytettävyys ja toimintavarmuus osana viranomaisten kriittisiin tietojärjestelmiin kohdistuvia turvallisuusvaatimuksia. Vaatimuksen HAL-17 mukaisesti organisaatioiden on varmistuttava tehtäviensä kannalta olennaisten järjestelmien vikasietoisuudesta ja toiminnallisesta käytettävyydestä säännöllisin testauksin ja harjoituksin.
    - Vaatimus perustuu tiedonhallintalain pykälään 13.
    - Alakriteerissä HAL-17.1 velvoitetaan organisaatioita varmistamaan tarjoamiensa palveluiden saavutettavuus lain digitaalisten palvelujen tarjoamisesta (306/2019) mukaisesti.
- HAL-18: Asiakirjajulkisuuden toteuttaminen
    - Asiakirjajulkisuuden toteuttaminen on uusi vaatimus, jota ei ole aiemmissa kriteeristöissä huomioitu. Vaatimus HAL-18 edellyttää että organisaatiot ovat toteuttaneet tietojärjestelmänsä, tietovarantojensa tietorakenteen sekä tietojenkäsittelyn muut järjestelynsä siten, että julkisuusperiaatetta pystytään vaivatta noudattamaan.
    - Vaatimuksen perustana on tiedonhallintalaki. Vastaavaa vaatimusta ei ole esitetty muissa kriteeristöissä.

6.2.2 Fyysinen turvallisuus

Fyysisen turvallisuuden osa-alue perustuu kokonaisuudessaan Katakriin. Tiedonhallintalautakunnan suosituksessa esitetyn osa-alueen yleiskuvauksen perusteella tämä on tietoinen valinta ja vaatimukset on pyritty pitämään mahdollisimman lähellä Katakrin vastaavia vaatimuksia. Julkrin ja Katakrin esittämien fyysisen turvallisuuden vaatimusten välisenä keskeisenä erona on kansainvälisiin velvoitteisiin perustuvien vaatimusten jättäminen pois Julkrista. Tämän lisäksi joitain vaatimuksia on laajennettu koskemaan myös muuta kuin turvallisuusluokiteltua tietoa koskevaa tietojenkäsittelyä (Valtiovarainministeriö, 2022).

6.2.3 Tekninen turvallisuus

Julkrin teknisen turvallisuuden osa-alue perustuu hallinnollisen turvallisuuden ja fyysisen turvallisuuden osa-alueiden tapaan vahvasti Katakrin vaatimuksiin. Osa-alueessa on kuitenkin joitain uusia vaatimuskohtia, jotka ovat:

- TEK-06: Kasautumisvaikutus
    - Vaatimus TEK-06 velvoittaa organisaatioita arvioimaan tietoaineiston kasautumisvaikutusta. Tämä voi käytännössä tarkoittaa esimerkiksi merkittävää määrää TL IV luokiteltua aineistoa, joka kokonaisuudessaan tulisi suojata TL III -tason vaatimusten mukaisesti.
    - Huomioitavaa on, että kasautumisvaikutuksen johdosta kohonnut turvallisuustaso ei edellytä kaikkia korkeamman tason turvallisuuskontrolleja. Esimerkkinä tästä on vaatimus viranomaisen hyväksymän yhdyskäytäväratkaisun käytöstä.
    - Vaatimus perustuu tiedonhallintalakiin. Muina viitteinä vaatimuksen osalta mainitaan ISO/IEC 27001 sekä PiTuKrin vaatimus IP-01.
- TEK-21.1: Sähköisessä muodossa olevien tietojen tuhoaminen - arkistointi
    - Pääkriteeri TEK-21 perustuu Katakrin vaatimukseen I-21 sekä vaatimuksiin T-12, F-08.3 ja F-08.4. Alakriteerissä TEK-21.1 lisätään aiempiin vaatimuksiin tarkennuksia arkistointiin liittyen. Vaatimus velvoittaa organisaatioita huomioimaan toimintaansa kohdistuvat arkistointivelvoitteet tietoaineistojen elinkaaren hallinnassa.
    - Pääkriteeri ja alikriteerit perustuvat tiedonhallintalakiin.
- TEK-21.2: Sähköisessä muodossa olevien tietojen tuhoaminen - pilvipalveluissa olevan tiedon tuhoaminen
    - Pääkriteeri TEK-21 perustuu Katakrin vaatimukseen I-21 sekä vaatimuksiin T-12, F-08.3 ja F-08.4. Alikriteeri TEK-21.2 tarkentaa vaatimuksia pilvipalveluissa olevan tiedon tuhoamisen osalta. Vaatimuksen perusteella pilvipalveluissa voidaan säilyttää salattua turvallisuusluokittelematonta tietoa, mikäli sen tuhoamisen yhteydessä voidaan varmistua salaukseen käytettyjen avainten luotettavasta tuhoamisesta.
    - Vaatimus perustuu PiTuKrin vaatimukseen SA-03 sekä ISO/IEC 27001 -standardin vaatimuksiin.
- TEK-22: Tietojärjestelmien saatavuus
    - Vaatimus TEK-22 on Julkriin tuotu uusi vaatimus. Aiemmat kriteeristöt, kuten Katakri eivät ole ottaneet kantaa turvallisuusluokitellun tiedon tai sen käsittelyyn tarkoitettujen tietojärjestelmien käytettävyyteen tai saatavuuteen, vaan ovat olleet kiinnostuneempia tiedon eheydestä ja luottamuksellisuudesta.

    - Vaatimus velvoittaa organisaatioita määrittelemään saatavuusvaatimukset tietojärjestelmille. Tämän määrittelyn tulisi sisältää palautusaikatavoite, palautuspistetavoite, kuormituksen kesto, vikasietoisuus sekä aika, jonka järjestelmä voi olla poissa käytöstä. Saatavuuteen liittyvät toimenpiteet tulisi mitoittaa tämän määrittelyn mukaisesti.
    - Vaatimuksen perustana on tiedonhallintalaki. Vastaava vaatimus on standardissa ISO/IEC 27001. Pääkriteerissä viitataan myös Julkrin vaatimukseen VAR-02 ja alikriteereissä kohtiin VAR-06, VAR-07, VAR-08 ja HAL-07.
- TEK-23: Tietojärjestelmien toiminnallinen käytettävyys
    - Pääkriteeri TEK-23 liittyy samaan saatavuuden ja käytettävyyden kokonaisuuteen kriteerin TEK-22 kanssa. Vaatimus velvoittaa kuitenkin vikasietoisuuden varmistamisen lisäksi organisaatioita varmistamaan myös toiminnallisen käytettävyyden.
    - Vaatimuksen mukaan järjestelmiin tulisi kohdistaa käyttötestausta erilaisten käyttäjäryhmien käyttötarpeiden mukaisesti. Testauksen tavoitteena on varmistaa, että järjestelmä on helposti opittavissa, sen toimintalogiikka on helposti muistettava ja sen toiminta tukee käyttäjien työtehtäviä ja edistää virheetöntä käyttöä.
    - Vaatimus perustuu tiedonhallintalakiin. Vaatimuksen osalta mainitaan kuitenkin, että myös digitaalisten palveluiden tarjoamisesta säädetyn lain (306/2019) mukaisia toimenpiteitä voidaan soveltaa, vaikka järjestelmää ei tarjottaisikaan julkisesti yleisölle.

6.2.4 Varautuminen ja jatkuvuudenhallinta

Varautuminen ja jatkuvuudenhallinta on uusi kokonaisuus, jonka vaatimukset perustuvat tiedonhallintalakiin. Kriteereiden sisältöön ovat vaikuttaneet ISO/IEC 27001 ja ISO/IEC 27002 -standardeissa esitetyt vaatimukset ja toteutusesimerkit tietoturvallisuuden jatkuvuudenhallinnasta. Julkrin vaatimusten ulkopuolelle on rajattu toiminta, joka kuuluu valmiuslain piiriin.

Varautumisen ja jatkuvuudenhallinnana osa-alueeseen kuuluu yhdeksän pääkriteeriä. Koska koko osa-alue on uusi, ei vastaavia kriteereitä ole asetettu vaatimuskokoelmissa, kuten Katakrissa, PiTuKrissa tai VAHTI-ohjeissa. Vaatimuksissa on kuitenkin joitain yhtymäkohtia Katakrin vaatimuksiin:

- VAR-03: Jatkuvuussuunnitelmat
    - Vaatimuskohdan alakriteeri VAR-03.1, jatkuvuussuunnitelmien testaus ja harjoittelu perustuu osin Katakrin vaatimukseen I-13.
    - Kriteeri velvoittaa organisaatioita säännölliseen harjoitteluun ja testaukseen määrittelemiensä jatkuvuussuunnitelmien mukaisesti. Kriteerin toteutusesimerkin mukaisesti organisaatioiden tulee mitoittaa harjoitustoimintansa toimintansa kannalta merkittävään laajuuteen ja osallistua sisäisten harjoitusten lisäksi myös

kansalliseen tai alueelliseen jatkuvuusharjoitteluun muiden organisaatioiden kanssa.

- VAR-04: Resurssit ja osaaminen
  - Pääkriteeri VAR-04 vaatii organisaatioilta varautumiseen liittyvien resurssien nimeämistä ja näiden henkilöiden osaamisen varmistamista. Vaatimuksen mukaan jokaisen henkilön tulisi tuntea varautumissuunnittelun perusteet ja eri tilanteiden vaikutus heidän omiin tehtäviinsä.
  - Vaatimus on osin sama kuin Katakrin vaatimus T-04 ja se perustuu tiedonhallintalakiin. Vaatimuksessa viitataan myös Julkrin kriteeriin HAL-03.

6.2.5 Tietosuoja

Julkrin osa-alue tietosuojasta on kokonaisuudessaan uusi. Osa-alue koostuu 21 vaatimuksesta, jotka perustuvat pääasiallisesti Euroopan Unionin yleisen tietosuoja-asetuksen asettamiin vaatimuksiin henkilötietojen turvallisesta ja asianmukaisesta käsittelystä. Muina lähteinä mainitaan julkisuuslaki vaatimuksessa TSU-05.2, Tehtävät ja vastuut - Tietosuojavastaavan asema ja tehtävät. Vaatimuksessa mainitaan, että tietosuojavastaavaa koskee julkisuuslain mukainen salassapitovelvollisuus.

Vaatimuskohdissa TSU-07, TSU-10, TSU-13.1 ja TSU-19.1 mainitaan tietosuoja-asetuksen ohella vaatimusten perustaksi tietosuojalaki. Pääkriteeri TSU-07 käsittelee henkilötietojen käsittelyn lainmukaisuutta, kriteeri TSU-10 henkilötietojen minimointia ja alakriteeri TSU-13.1 velvoittaa organisaatioita huolehtimaan henkilötietojen käsittelyn turvallisuudesta. Alakriteeri TSU-19.1, Rekisteröidyn oikeudet - Rekisteröidyn käytettävissä olevien oikeuksien tunnistaminen, määrittää organisaatioiden velvollisuuden tunnistaa, mitä oikeuksia rekisteröity voi missäkin tilanteessa käyttää. Organisaatioiden on mahdollista kieltäytyä rekisteröidyn oikeuksien toteuttamisesta, mikäli niillä on muuhun lainsäädäntöön perustuva peruste toimia näin.

7 TIETOTURVALLISUUDEN TODENNUSMENETELMÄT VAATIMUSTENMUKAISUUDEN TODENTAMISEKSI

Tässä luvussa on pyritty kuvaamaan ne todennusmenetelmät, joilla Julkrissa asetettujen tietoturvavaatimusten toteutumista voitaisiin todentaa. Ensimmäisessä alaluvussa esitellään arviointilaitosohje, johon valitut todennusmenetelmät perustuvat. Tutkimuksen tuloksena on syntynyt arviointimalli, jota voidaan soveltaa työkaluna kriteeristön ohessa. Malliin valitut todennusmenetelmät on pyritty valitsemaan yleisellä tasolla siten, että todennus esimerkiksi teknisen tietoturvallisuuden osa-alueella ei riipu tietystä tuotteesta tai teknologiasta, soveltuen näin käytettäväksi erilaisissa organisaatioissa ja järjestelmissä sekä arviointia suorittavan tahon resurssien puitteissa.

7.1 Arviointilaitosohje

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus ohjaa ja valvoo tietoturvallisuuden arviointilaitosten toimintaa. Arviointilaitoslain mukaisten tietoturvallisuuden arviointilaitosten toimintaa ohjaamaan on julkaistu arviointilaitosohje. Ohjeessa on esitelty se keskeinen lainsäädäntö ja normit, joihin tietoturvallisuuden arviointilaitosten toiminta ja niiden tekemät arvioinnit ja auditoinnit sekä niiden pohjalta myönnettävät todistukset ja sertifikaatit perustuvat (Traficom, 2022).

Arviointilaitosten hyväksymisestä säädetään arviointilaitoslaissa (1405/2011). Samassa laissa säädetään myös arviointilaitosten valvonnasta ja toiminnasta. Arviointilaitoslaissa ei kuitenkaan suoraan säädetä niitä tehtäviä, joita Liikenne- ja viestintäviraston hyväksymä tietoturvallisuuden arviointilaitos voi hoitaa, vaan nämä tehtävät on johdettavissa useista muista laeista. Arviointilaitosohjeen mukaan näitä lakeja ovat laki viranomaisten

tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (arviointilaki 1406/2011) sekä laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015). Edellä mainitut lait liittyvät turvallisuus- ja huoltovarmuuskriittisten viranomaisten toimintaan ja tilanteisiin, joissa viranomaiset tai heidän lukuunsa toimivat muut tahot käsittelevät salassa pidettävää tai turvallisuusluokiteltua tietoaineistoa tietojärjestelmissään. Tietoturvallisuuden arviointilaitokset osallistuvat myös kansalaisten henkilötietojen suojaustoimien riittävyyden arviointiin. Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021) ja laissa sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) säädetään arkaluontoisia sosiaali- ja terveystietoja sisältävien tai käsittelevien järjestelmien arvioinnista, jota hyväksytyt tietoturvallisuuden arviointilaitokset tekevät.

Tässä tutkimuksessa ei ole keskitytty asiakastietolain tai toisiolain mukaisiin tietoturvallisuuden arviointeihin tai niiden todennusmenetelmiin, sillä niiden lainsäädäntöperusta on Julkrista erillään, eikä uuden kriteeristön julkaiseminen tuo muutoksia niihin liittyvään sääntelyyn tai arviointitoimintaan.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista velvoittaa valtionhallinnon viranomaiset käyttämään tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden arviointiin vain Liikenne- ja viestintävirasto Traficomia tai sen hyväksymää arviointilaitosta. Arviointilaitosohjeen mukaisesti luottamuksellisen tiedon turvallista käsittelyä koskevat vaatimukset todennetaan Katakrin kulloinkin voimassa olevan version avulla. Tämän tutkimuksen kirjoitushetkellä Katakrin uusin käytössä oleva versio on Katakri 2020. Traficomin Kyberturvallisuuskeskuksen ylläpitämän hyväksyttyjen tietoturvallisuuden arviointilaitosten luettelon perusteella kyseisen kriteeristön vaatimustenmukaisuuden arviointiin on pätevyys kahdella arviointilaitoksella, tasoille TLIV (Käyttö rajoitettu) ja TLIII (Luottamuksellinen). Arviointilaitokset eivät voi arvioida sellaisia viranomaisten tietojärjestelmiä, joissa käsitellään EU:n tai NATO:n turvallisuusluokiteltua tietoa.

Arviointilaitoslain sekä arviointilaitosohjeen mukaisesti tullakseen Traficomin hyväksymäksi tietoturvallisuuden arviointilaitokseksi, organisaation on todennettava pätevyytensä yhdenmukaisten kansainvälisten tai eurooppalaisten arviointiperusteiden mukaisesti. Tätä varten organisaation on saavutettava akkreditointi FINAS-akkreditointipalvelun suorittaman pätevyyden arvioinnin mukaisesti. Tämä akkreditointi mahdollistaa arviointilaitokselle ISO/IEC 27001 -standardin mukaisten arviointien suorittamisen.

Mahdollisuus muiden tietoturvallisuuskriteeristöjen vaatimustenmukaisuuden arviointiin perustuu erikseen haettaviin pätevyysalueisiin. Voidakseen arvioida luottamuksellisen tiedon turvallista käsittelyä koskevia vaatimuksia Katakria vasten, arviointilaitoksen on täytettävä omassa toiminnassaan Katakrin turvallisuusjohtamista, fyysistä turvallisuutta sekä teknistä tietoturvallisuutta koskevat vaatimukset.

Arviointilaitosohjeen mukaan arviointilaitosten toimintaan sovelletaan lähtökohtaisesti yhtä turvallisuusluokkaa korkeampaa vaatimustasoa, kuin mille laitos hakee hyväksyntää. Toisin sanoen, voidakseen arvioida vaatimustenmukaisuutta TL III -tasolle, on arviointilaitoksen täytettävä TL II -tason vaatimukset (Traficom, 2022).

Traficom ylläpitää ajantasaista ja julkista luetteloa hyväksytyistä tietoturvallisuuden arviointilaitoksista ja niiden pätevyysalueista. Mikäli pätevyysalueiden kriteeristöt muuttuvat, esimerkiksi uuden Katakrin version myötä, eivät arviointilaitosten pätevyysalueet automaattisesti muutu, vaan hyväksyntää on haettava erikseen ja arviointilaitoksen oma vaatimustenmukaisuus pystyttävä todentamaan.

Tämän tutkimuksen kannalta on huomionarvoista, että arviointilaitosohjeessa todetaan Traficomin julkaisseen Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) keväällä 2019. Ohjeen mukaisesti PiTuKri-pätevyyden hakeminen ei ole arviointilaitoksille mahdollista ja Traficom tulee ilmoittamaan erikseen, kun pätevyyden hakeminen on mahdollista arviointilaitoksille. Arviointilaitosohjeessa ei ole mainintaa Julkrista, sillä kriteeristön julkaisun jälkeen arviointilaitosohjeesta ei ole julkaistu uutta versiota. On todennäköistä, että Julkriin tullaan soveltamaan samoja periaatteita kuin PiTuKriin, mikäli se tulee käyttöön tietoturvallisuuden arviointilaitosten käyttämänä työkaluna. Arviointilaitosten on erikseen haettava pätevyyttä sen arviointiin Traficomin ohjeistusten mukaisesti. Tämän tutkimuksen kirjoitushetkellä keväällä 2023 on kulunut neljä vuotta PiTuKri-kriteeristön julkaisemisesta, eikä sitä voida vielä käyttää luottamuksellisten tietojen turvallisen käsittelyn todentamiseen. Mikäli Julkrin osalta kriteeristön julkaisun ja sen käyttöön siirtymisen välinen aika on yhtä pitkä, on vielä useita vuosia siihen, että kriteeristöä sovelletaan käytäntöön tietoturvallisuuden arvioinneissa.

Arviointilaitokset voivat arviointilaitoslain ja arviointilaitosohjeen puitteissa hoitaa myös muita kuin tässä luvussa mainitussa lainsäädännössä kuvattuja arviointitehtäviä. Arviointilaitokset voivat tarjota palveluitaan myös muille kuin viranomaisille. Viranomaisten tietojärjestelmiä arvioitaessa viranomaisten on kuitenkin aina käytettävä Traficomin hyväksymän arviointilaitoksen palveluita. Keskeisiä eroja hyväksytyn tietoturvallisuuden arviointilaitoksen tekemän arvioinnin tai arviointilaitosstatuksen ulkopuolisen palvelun välillä ovat valvonta sekä arvioinnin kattavuus. Mikäli arvioinnissa ei tähdätä arviointilaitoksen myöntämään todistukseen, voidaan siitä rajata joitain osa-alueita ulkopuolelle. Katakrin rakenteen vuoksi todistus on mahdollista myöntää osittaisesta Katakri-arvioinnista vain joko T-osiosta tai T+F-osioista. Pelkän F- tai I-osion arvioinnin perusteella ei ole mahdollista myöntää todistusta.

Mikäli arviointilaitos myöntää arvioinnin perusteella todistuksen, todistus on lähtökohtaisesti voimassa korkeintaan kolme vuotta. Tämän jälkeen todistuksen voimassaolon jatkaminen vaatii uudelleentarkastusta ja sitä, että todistuksen kohde täyttää vaaditut kriteerit. Todistuksen voimassaolon aikana

organisaation toimintaan ei kuitenkaan kohdistu määräaikaisia ulkopuolisen suorittamia auditointeja. On huomioitava, että esimerkiksi Katakrin osalta uusi arviointi tulee tehdä kulloinkin voimassa olevan kriteeristön mukaan. Jos siis organisaatiolla on entuudestaan ollut todistus Katakri 2015 vaatimustenmukaisuudesta, tullaan uusi arviointi tekemään Katakri 2020 mukaisesti ja todistus myöntämään sen perusteella.

Arviointilaitosohjeen mukaisesti arviointilaitoksilla on velvollisuus varmistua siitä, että arviointiin liittyvät tiedot ovat riittävässä määrin saatavilla myös arvioinnin jälkeen. Keskeiset arviointiin liittyvät tulokset ja todistusaineisto on säilytettävä kuusi vuotta arvioinnin päättymisen jälkeen, jotta ne ovat tarvittaessa arviointilaitoksen sekä Traficomin saatavilla.

7.2 Todennusmenetelmät

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus ylläpitää ohjetta tietoturvallisuuden arviointilaitoksille. Tämän tutkimuksen kirjoitushetkellä uusin versio ohjeesta on 210/2022. Tähän arviointilaitosohjeeseen on kerätty ne todentamiselle asetettavat vähimmäisvaatimukset, joita arviointilaitosten tulisi toiminnassaan käyttää tietoturvakriteeristöjen asettamien vaatimusten todentamiseksi.

Ohjeessa todennusmenetelmät on jaettu kahteen alaluokkaan, jotka ovat hallinnolliseen todentamiseen liittyvät menetelmät sekä tekniseen todentamiseen liittyvät menetelmät. Oheiseen taulukkoon on koottu arviointilaitosohjeen mukaiset todennusmenetelmät, niiden tunnisteet, sovellettavat turvallisuusluokituksen tasot sekä lyhyt kuvaus menetelmien käyttämisestä mukaillen arviointilaitosohjetta.

Tunniste	Todennusmenetelmä	Turvallisuus-luokat	Huomiot
H1	Haastattelut	IV ja III	Haastattelujen kohteiden tulisi edustaa kattavasti eri tahoja, jotka liittyvät arvioitavaan kohteeseen, näin ollen johdon sekä tietojärjestelmien asiantuntijoiden ja ylläpitäjien lisäksi haastatteluissa tulisi olla edustettuna myös organisaation loppukäyttäjät.

H2	Dokumentaatioon tutustuminen	IV ja III	Arvioinnissa katselmoitavan dokumentaation tulisi kattaa prosessikuvaukset, järjestelmä- tai ratkaisukuvaukset sekä erilaiset arkkitehtuurikuvat esimerkiksi tietoliikenneverkoista tai sovellusarkkitehtuurista.
T1	Passiivinen rajapinta-analyysi	IV ja III	Passiivisen rajapinta-analyysin tulisi sisällyttää tietoliikenteen analysointi ja sen pohjalta muodostuva kuva tietoliikenne- ja järjestelmäverkosta. Tietoliikenneanalyysin tulisi kattaa kaikki arviointikohteeseen liittyvät rajapinnat ja olla laajuudeltaan riittävän kattava.
T2	Järjestelmä-konfiguraatioiden turvallisuuden tarkastelu	IV ja III	Konfiguraatiot tulisi katselmoida kaikista arviointikohteen turvallisuuteen vaikuttavista osakokonaisuuksista.
T3	Aktiivinen rajapinta-analyysi	IV ja III	Aktiiviseen rajapinta-analyysiin tulisi sisällyttää porttiskannaukset sekä haavoittuvuusskannaukset tunnettujen haavoittuvuuksien ja tarpeettomien tietoliikenneavausten havaitsemiseksi. Menetelmän tulisi huomioida myös toimintavarmuustestauks

			et tuntemattomien haavoittuvuuksien varalta.
T4	Sovellus-turvallisuuden tarkastelut järjestelmätyypeittäin	IV ja III	Arviointikohteeseen liittyvät tai vaikuttavat sovelluskomponentit tulisi tarkastaa soveltuvin menettelyin. Tällaisia komponentteja voivat olla esimerkiksi web-sovellukset, palvelin- tai asiakasohjelmistot tai toiminnanohjausjärjestelmät. Näiden sovellusten arvioinnissa tulee varmistua järjestelmien sisäisten pääsynhallintamekanismien toiminnasta, riippuvuuksien ja komponenttien ajantasaisuudesta sekä sovellusten käyttämien oikeuksien tarpeenmukaisuudesta.
T5	Salausratkaisujen turvallisuuden todentaminen	IV ja III	Arviointilaitosohjeen mukaisesti tilanteissa, joissa kohteessa ei ole käytössä hyväksyttyä salausratkaisua, on ratkaisun turvallisuudelle haettava Traficomin NCSA:n arvio. Mikäli kohteeseen on valittu käyttöön salausratkaisu, joka on Traficomin NCSA-toiminnon hyväksymä, tulee arvioinnissa varmistua salausasetusten ja hallintakäytäntöjen turvallisuudesta. Mikäli hyväksytyllä

			salausratkaisulla on käyttöpolitiikka, tulee sen mukaisesta toiminnasta varmistua.
T6	Käytettävyys-testaukset	IV ja III	Käytettävyystestauksella tarkoitetaan arviointilaitosohjeessa testausta, jolla arviointikohteeseen kohdistetaan stressitestejä, jotka simuloivat esimerkiksi palvelunestohyökkäyksiä. Tätä todennusmenetelmää käytetään arviointilaitosohjeen mukaisesti vain järjestelmissä, joihin kohdistuu korkean käytettävyyden vaatimukset. Teknisten testauksen lisäksi arvioinnissa tulee varmistua jatkuvuuteen liittyvien prosessien toimivuudesta.
T7	Fyysisen turvallisuuden suojausten todentamis-menetelmät	IV ja III	Arviointilaitosohje ei ota kantaa tarkempiin fyysisen turvallisuuden suojausten todennusmenetelmiin.
T8	Yhdyskäytävä-ratkaisujen turvallisuuden testaukset	III	Yhdyskäytäväratkaisun TL III -tasoisen tietojenkäsittely-ympäristön ja alemman tasoisten ympäristöjen välillä tulee perustua Traficomin julkaisemaan yhdyskäytäväratkaisuohje eseen. Mikäli ratkaisu ei perustu em. ohjeeseen tai

			ei täytä siinä asetettuja vaatimuksia, tulee poikkeukselle hakea hyväksyntä Traficomin NCSA-toiminnolta.
T9	Poikkeama-havainnointikyvyn testaukset	IV ja III	Korkean turvallisuustason tietojenkäsittely-ympäristöissä edellytetään ympäristöjen valvontaa ja poikkeavan toiminnan havainnointia. Havainnointikyvyn varmistamiseksi tulisi ympäristössä tehdä tai yrittää tehdä poikkeuksellisia toimenpiteitä, kuten tietojen tuhoamista tai pääsyä tietoihin oikeudettomasti. Havainnointikykyyn tulisi sisällyttää myös haitallisten tiedostojen siirto korkean turvallisuustason ympäristöön.
T10	Hajasäteilysuojausten todentaminen	III	Vaatimus hajasäteilyltä suojautumiseen koskee vain TL III ja sitä korkeampia turvallisuusluokituksia sekä joissain tapauksissa kansainvälisen turvallisuusluokitellun tietoaineiston suojaamista.
T11	Luvattomien teknisten laitteiden olemassaolon todentaminen	III	Vaatimus kohdistuu kohdekohtaisesti tiedon omistajan tai omistajan valtuuttaman tahon riskiarvion mukaisesti. Arviointilaitosohjeen

			mukaisesti todentamista ei tyypillisesti edellytetä esimerkiksi palvelintiloihin, joissa ei keskustella salassa pidettävästä tiedosta.

Taulukko 1: Arviointilaitosohjeen mukaiset todennusmenetelmät

Luotettavan todentamisen lähtökohtana tulisi pitää todentamista vähintään kahdella menetelmällä. Vaatimuksesta riippuen todennusmenetelmien tulisi olla yhdistelmä hallinnollisia ja teknisiä menettelyitä. Tämä voi tarkoittaa esimerkiksi sitä, että passiivisella rajapinta-analyysillä todennetaan orgnanisaation dokumentaatiossaan kuvaaman arkkitehtuurin toteutuminen, tai haastatteluissa kuvattujen prosessien mukainen toiminta varmistetaan esimerkiksi muutoshallinnan osalta toiminnanohjausjärjestelmään tehdyistä kirjauksista ja muutoslokista.

Tässä tutkimuksessa analysoitiin Julkrin eri osa-alueiden vaatimuksia ja tunnistettiin niihin soveltuvat arviointilaitosohjeessa määritetyt todennusmenetelmät. Tutkimuksen liitteenä on taulukkomuotoinen työkalu Julkrin vaatimuksista, missä kunkin vaatimuksen kohdalle on kirjattu soveltuvien todennusmenetelmien tunnisteet arviointilaitosohjeen mukaisesti. Seuraavissa kappaleissa kuvataan yleiset havainnot kuhunkin osa-alueeseen liittyen.

7.2.1 Hallinnollinen turvallisuus

Hallinnollisen turvallisuuden osa-alueen vaatimukset ovat luonteeltaan sellaisia, että niihin on hankalaa tai mahdotonta kohdistaa teknistä tarkastelua. Tästä syystä suurin osa vaatimuksista on todennettavissa vain hallinnollisin keinoin. Vaatimustenmukaisuus tulisi todentaa haastatteluin sekä dokumentaatioon perustuen.

Vaatimusten tarkastelun perusteella teknisempiä todennusmenetelmiä tulisi soveltaa kahteen vaatimukseen. Alakriteeri HAL-07.1 vaatii organisaatioita tunnistamaan lokitietojen keräämisen vaatimukset ja järjestämään arvion perusteella riittävän lokitietojen keräämisen sekä siihen kohdistuvan seurannan ja valvonnan. Tämän vaatimuksen todentamiseksi tulisi dokumentaation ja haastatteluiden lisäksi suorittaa järjestelmien konfiguraatioiden katselmointia sekä sovellusturvallisuuden arviointia. Teknisen todentamisen tarkoituksena on varmistaa, että määritetyt lokipolitiikat ja -periaatteet toteutetaan tietojärjestelmissä ja esimerkiksi sovellusten lokiasetukset ovat päällä ja konfiguroitu siten, että ne tukevat riittävän kattavaa valvontaa.

7.2.2 Fyysinen turvallisuus

Julkrin vaatimukset fyysiseen turvallisuuteen liittyen tulisi todentaa hallinnollisin menetelmin haastatteluin sekä dokumentaatioon perustuen. Kaikkien vaatimusten kohdalla hallinnollisia todennusmenetelmiä tulee täydentää fyysisen turvallisuuden suojausten tarkastelulla. Fyysisen turvallisuuden kriteerien todentamismenetelmien määrittäminen arviointilaitosohjeen perusteella on haastavaa, sillä Traficomin arviointilaitosohjeessa kokonaisuus on yhdistetty tunnisteen T7 alle, eikä ohje ota kantaa tarkempiin fyysisen turvallisuuden suojausten todennusmenetelmiin.

Julkrin vaatimukset fyysisen turvallisuuden osa-alueella perustuvat Katakrin versioon 2020. Tämän lisäksi yksittäisten kriteerien ja alakriteerien lisätiedoissa ja toteutusesimerkissä viitataan muihin standardeihin, kuten SFS-EN-1627 vaatimuksen FYY-04.1 kohdalla. Todennusmenetelmien tulisi perustua Julkrissa mainittuihin standardeihin niiden vaatimusten osalta, joissa muihin standardeihin viitataan.

Vaatimusten analysoinnin ja arviointilaitosohjeen tulkinnan perusteella fyysisen turvallisuuden kriteerit ja niiden todennusmenetelmät ovat ristiriidassa muihin Julkrin osa-alueisiin nähden. Ensimmäisen ongelman muodostaa ennalta määritettyjen ja yleisesti arviointia suorittavien tahojen ja arvioitavien tahojen saatavilla olevaa tietoa vaatimusten toteuttamisesta tai todentamisesta ei ole. Tämä voi johtaa tilanteeseen, jossa eri organisaatiot noudattavat samoja menettelyjä fyysisen turvallisuuden suojauksissaan, mutta arvioinnissa vain toisen tahon menetelmät hyväksytään vaatimustenmukaisiksi.

Toinen ongelma liittyy Julkrin taulukkomuotoisessa työkalussa viitattuihin muihin standardeihin. Viittaukset ovat otsikon "Toteutusesimerkki" alla, joten niiden velvoittavuus jää epäselväksi. Esimerkiksi vaatimuskohdassa FYY-05.1 äänieristyksen osalta viitataan standardeihin SFS-EN-ISO 717-1 sekä SFS-EN-ISO 16283-1. Viittaukset ovat kuitenkin konditionaalissa ja toteutusesimerkkejä. Mikäli kyseisiä standardeja ei noudateta, jää tulkinta vaatimustenmukaisuudesta täysin arviointia suorittava tahon vastuulle, eikä perustu yleisesti tunnistettuun tai julkiseen linjaukseen.

7.2.3 Tekninen turvallisuus

Kuten hallinnollisen turvallisuuden ja fyysisen turvallisuudenkin osa-alueilla, myös teknisen turvallisuuden osa-alueen vaatimustenmukaisuuden todentamisessa tulisi käyttää hallinnollisia menetelmiä. Arviointilaitosohjeen mukaiset menetelmät H1 ja H2, eli haastattelut ja dokumentaation katselmointi soveltuvat lähes kaikkiin osa-alueen pää- ja alikriteereihin. Vaikka osa-alueen nimi onkin tekninen turvallisuus, eivät Julkrin vaatimukset määritä tarkkaan tiettyjä teknologioita tai teknisiä kontrolleja, vaan kriteerit keskittyvät myös ylläpidon ja hallinnan prosesseihin sekä niiden turvallisuuteen.

Dokumentaation rooli korostuu muun muassa tietoturvallisuuteen liittyvien poikkeamien havaitsemisessa. Tietojärjestelmien normaalitila tulisi olla dokumentoitu selkeästi järjestelmän itsensä ulkopuolelle, että muutokset esimerkiksi tietoliikenneyhteyksissä tai suodatussäännöissä voidaan havaita. Teknisen turvallisuuden osa-alueen kriteerit keskittyvät tietoturvallisuuden osalta tiedon eheyteen ja luotettavuuteen, mutta dokumentaation rooli korostuu arvioitaessa tiedon ja tietojärjestelmien käytettävyyttä. Kattava dokumentaatio toteutetuista tietoturvallisuuskontrolleista auttaa organisaatiota varautumisessa ja jatkuvuuden hallinnassa, kun tieto järjestelmän yksityiskohdista ja ylläpidosta ei ole vain yksittäisten henkilöiden varassa.

Teknisen turvallisuuden osa-alueella useiden kriteerien vaatimustenmukaisuuden todentamiseen tulisi käyttää passiivista rajapinta-analyysia, järjestelmän konfiguraatioiden katselmointia sekä aktiviista rajapinta-analyysia, eli arviointilaitosohjeen mukaisia todennusmenetelmiä T1, T2 ja T3. Esimerkiksi vaatimuksen TEK-01 mukaan tietojenkäsittely-ympäristön yhteyksien julkiseen verkkoon tai alemman turvallisuusluokan ympäristöihin tulisi olla toteutettu turvallisesti. Tämän vaatimuksen todentaminen vaatii tietojärjestelmän tietoliikenteen nauhoittamista ja analysointia. Näin voidaan varmistua siitä, että liikenne muihin tietojenkäsittely-ympäristöihin kulkee vain tunnistettujen rajapintojen kautta ja on toteutettu turvallisuusluokasta riippuen joko palomuurien tai viranomaisen hyväksymän yhdyskäytäväratkaisun läpi. Turvallisuusluokkaan III kuuluvien tietojenkäsittely-ympäristöjen osalta todennusmenetelmänä tulisi käyttää myös yhdyskäytäväratkaisujen turvallisuuden testauksia.

Kunkin teknisen turvallisuuden osa-alueeseen kuuluvan vaatimuksen todentamiseen soveltuvat menetelmät on tunnistettu ja lueteltu tämän tutkimuksen liitteessä 1. Teknisen turvallisuuden osa-alueen osalta soveltuvien todennusmenetelmien valinta riippuu arvioitavasta kohteesta, sillä yksittäisen TL IV -tasolle määritellyn erillistyöaseman tai turvallisuusluokkaan III kuuluvan satojen loppukäyttäjien tietojenkäsittely-ympäristön todentaminen vaatii erilaisia toimenpiteitä ja työkaluja. Lähtökohtana kuitenkin on, että jokaisen järjestelmän osakomponentin turvallisuudesta tulisi varmistua, olipa kyseessä sitten tietoliikennelaite, palvelin, valmisohjelmisto, päätelaite tai mikään muu komponentti.

7.2.4 Varautuminen ja jatkuvuudenhallinta

Varautumisen ja jatkuvuudenhallinnan osa-alue on Julkrissa uusi verrattuna kolmeen ensimmäiseen osa-alueeseen, joiden sisältö vastaa Katakrin vaatimuksia. Tästä syystä arviointia suorittavilla tahoilla ei ole valmiita työkaluja vaatimusten luotettavaan todentamiseen.

Vaatimusten analysoinnin perusteella VAR-osa-alueen pää- ja alikriteereiden todentamiseen soveltuvimmat menetelmät ovat haastattelut ja dokumentaation katselmointi, sillä teknisten todennusmenetelmien kohdentaminen vaatimuksiin on haastavaa tai mahdotonta. Poikkeuksen muodostavat vaatimukset VAR-03.1 sekä VAR-04.

Alivaatimus VAR-03.1 edellyttää organisaatioilta jatkuvuussuunnitelmien testaamista ja säännöllistä harjoittelua. Tähänkin vaatimukseen liittyvät todennusmenetelmät H1 ja H2, mutta haastatteluita ja dokumentaatiota tulisi täydentää myös teknisillä todennusmenetelmillä, kuten järjestelmäkonfiguraatioiden tarkastelulla (T2), aktiiviseen rajapinta-analyysiin sisältyvillä toimintavarmuustestauksilla (T3) sekä sovellusturvallisuuden tarkasteluilla (T4). Teknisellä tarkastelulla voidaan varmistaa, että suunnitellut jatkuvuustoimenpiteet ovat mahdollisia myös järjestelmien teknisen toteutuksen ja ominaisuuksien puitteissa.

Varautumisen ja jatkuvuudenhallinnan osa-alueen todentamisessa tulisi huomioida soveltuvin osin myös arviointilaitosohjeen mukainen menetelmä T11, luvattomien teknisten laitteiden olemassaolon todentaminen. Organisaation toiminnan kannalta kriittisten tilojen ja laitteiden eheydestä tulisi varmistua osana arviointia. Arviointilaitosohjeen mukaisesti tietoturvallisuuden arviointilaitokset eivät käytä todennusmenetelmää T11, vaan sen mukaisista tarkastuksista vastaavat arviointeja suorittavat viranomaistahot.

7.2.5 Tietosuoja

Tietosuoja-osa-alueen vaatimukset pohjautuvat lainsäädäntöön ja muihin asetuksiin, joista keskeisin on Euroopan Unionin yleinen tietosuoja-asetus. Julkrin esittämät vaatimukset tietosuojaan liittyen kohdistuvat organisaation prosesseihin ja vastuumäärittelyyn. Tästä syystä vaatimusten todentaminen on mahdollista lähinnä hallinnollisin menetelmin, eli haastatteluin ja dokumentaatioon tutustumalla.

Tietosuojan vaatimuksiin liittyvät teknisen turvallisuuden osa-alueella määritetyt vaatimukset tiedon eheydelle ja luottamuksellisuudelle. Teknisessä todentamisessa tulisikin huomioida henkilötietojen suojaus ja varmistua tietojenkäsittely-ympäristön pääsyoikeuksista, turvallisista konfiguraatioista sekä turvallisuusluokan mukaisesta salauksesta niin tietoliikenteessä kuin tiedon säilytyksessäkin. Näiden vaatimusten todentamiseen tulisi hallinnollisten menettelyiden lisäksi soveltaa todennusmenetelmiä T2 ja T5, eli järjestelmäkonfiguraatioiden tarkastelu sekä salausratkaisujen turvallisuuden todentaminen.

8 YHTEENVETO

Tutkimukselle määritettiin kolme keskeistä tutkimuskysymystä. Tämän Yhteenveto-luvun tarkoituksena on tiivistää tutkimuksen keskeiset havainnot, arvioida niiden luotettavuutta ja arvoa käytännön tietoturvallisuustyön kannalta. Luvun lopussa on tunnistettu tutkimuksen perusteella heränneitä ajatuksia jatkotutkimuksen aiheista Julkriin, tietoturvallisuuden arviointitoimintaan sekä tietoturvallisuuden hallintajärjestelmästandardeihin ja -kriteeristöihin liittyen.

Tämän tutkimuksen tavoitteena oli arvioida, miten Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) toimii tietoturva-arviointien välineenä. Tavoitteen saavuttamiseksi tutkimukselle määritettiin seuraavat tutkimuskysymykset:

1. Mikä on eri kriteeristöjen rooli julkishallinnon toimijoiden tai niiden lukuun toimivien muiden yhteisöjen turvallisuuden arvioinnissa?
2. Tuleeko Julkri korvaamaan olemassa olevat toimivaltaisten viranomaisten sekä tietoturvallisuuden arviointilaitosten tietoturvallisuuden arviointityökalut?
3. Miten Julkrin vaatimusten täyttymistä voidaan todentaa luotettavasti?

8.1 Eri kriteeristöjen rooli

Tutkimuksen tulosten perusteella Julkrin vaatimukset perustuvat voimassa olevaan lainsäädäntöön sekä muihin julkisen sektorin toimijoita velvoittavaan sääntelyyn. Aiemmista kriteeristöistä esimerkiksi Katakri on perustunut samaan tapaan lainsäädäntöön, mistä johtuen Julkrin ja Katakrin vaatimukset ovat pääosin samoja. Merkittävänä muutoksena Julkriin on kuitenkin tuotu lisäksi varautumisen ja jatkuvuudenhallinnan osa-alue sekä tietosuojaa koskevat vaatimukset, jotka perustuvat tietosuojalakiin sekä tietosuoja-asetukseen.

Keskeinen ero Julkrin ja aiempien kansallisten tietoturvallisuuden arviointikriteeristöjen välillä on se, että Julkri on tarkoitettu soveltuvaksi paremmin myös niille julkishallinnon toimijoille, jotka eivät lain mukaan itse pysty luokittelemaan tietoaineistoaan turvallisuusluokitusasetuksen mukaisesti. Julkri mahdollistaa vaatimusten kohdistamisen myös niiden organisaatioiden toimintaan, jossa tietoaineiston korkein luokka on salassa pidettävä tai käsittely kohdistuu vain henkilötietoihin.

8.2 Julkri suhteessa aiempiin kriteeristöihin

Tutkimuksen toisen pääkysymyksen mukaisesti pyrittiin selvittämään, tuleeko Julkri korvaamaan olemassa olevat viranomaisten sekä tietoturvallisuuden arviointilaitosten arviointityökalut. Traficomin Kyberturvallisuuskeskuksen ylläpitämän hyväksyttyjen arviointilaitosten luettelon perusteella arviointikriteeristöinä käytetään tällä hetkellä ISO/IEC 27001 -standardia sekä Katakri-kriteeristöä tasoille TLIV ja TLIII.

Kansainväliset ISO-standardit ovat vakiinnuttaneet roolinsa yritysmaailmassa, eikä standardissa ole mahdollista huomioida suomalaisia erityistarpeita. Voidaankin todeta, että Julkri ei tule vaikuttamaan ISO/IEC 27001 -standardin mukaisesti tehtyihin arviointeihin, sillä ISO-standardit eivät sovellu lainsäädännössä esitettyjen julkishallinnon toimijoita koskevien erityisten tietoturvavaatimusten todentamiseen. Osana tutkimusta suoritetun kirjallisuuskatsauksen havaintojen perusteella eri standardien soveltaminen voi kuitenkin parantaa tietoturvallisuuden kokonaishallintaa, joten julkishallinnon toimijat voivat saavuttaa merkittäviä hyötyjä ISO/IEC 27001 -standardin vapaaehtoisella soveltamisella muiden viitekehysten rinnalla.

Julkrin vaatimusten analysoinnin perusteella suosituksessa esitetyt kriteerit perustuvat etenkin hallinnollisen, fyysisen sekä teknisen turvallisuuden osalta Katakrin versiossa 2020 esitettyihin vaatimuksiin. Tämän tutkimuksen tulosten perusteella on vaikeaa tunnistaa syytä näiden kahden, lähes päällekkäisen kriteeristön olemassaololle ja itsenäiselle kehittämiselle. Tutkimuksen aikana tehtyjen havaintojen perusteella Julkri vastaa samoihin tarpeisiin kuin Katakri, mutta sen lisäksi huomioi tiedon saavutettavuuden ja käytettävyyden sekä tietosuojan.

Julkrissa ei oteta kantaa siihen, miten suosituksen julkaissut valtiovarainministeriön alainen tiedonhallintalautakunta on suunnitellut kriteeristöä käytettävän, eikä julkaisusta ole mahdollista päätellä, miten sitä tulisi soveltaa aiempiin kriteereihin, kuten Katakriin tai PiTuKriin nähden. Tietoturvallisuuden arviointeja tekevät tai niistä vastaavat viranomaistahot Traficomin Kyberturvallisuuskeskus, Puolustusvoimien pääesikunta tai Suojelupoliisi eivät ole julkisesti ottaneet kantaa Julkriin tai kertoneet, miten aikovat kriteeristöä mahdollisesti hyödyntää osana omaa arviointitoimintaansa. Traficom vastaa tietoturvallisuuden arviointilaitosten ohjaamisesta, joten niiden arvioinneissaan soveltamat kriteeristöt perustuvat Traficomin omiin linjauksiin.

Tämän tutkimuksen kannalta on huomionarvoista, että arviointilaitosohjeessa todetaan Traficomin julkaisseen Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) keväällä 2019 (Traficom, 2022). Ohjeen mukaisesti PiTuKri-pätevyyden hakeminen ei ole arviointilaitoksille mahdollista ja Traficom tulee ilmoittamaan erikseen, kun pätevyyden hakeminen on mahdollista arviointilaitoksille. On todennäköistä, että Julkriin tullaan soveltamaan samoja periaatteita, mikäli se tulisi käyttöön tietoturvallisuuden arviointilaitosten työkaluna. Arviointilaitosten on erikseen haettava pätevyyttä sen arviointiin Traficomin ohjeistusten mukaisesti. Tämän tutkimuksen kirjoitushetkellä keväällä 2023 on kulunut neljä vuotta PiTuKri-kriteeristön julkaisemisesta, eikä sitä voida vielä käyttää luottamuksellisten tietojen turvallisen käsittelyn todentamiseen. Mikäli Julkrin osalta kriteeristön julkaisun ja sen käyttöön siirtymisen välinen aika on yhtä pitkä, on vielä useita vuosia siihen, että kriteeristöä sovelletaan käytäntöön.

8.3 Vaatimusten todentaminen

Kolmannen tutkimuskysymyksen tavoitteena oli selvittää, miten Julkrissa esitettyjä vaatimuksia voitaisiin luotettavasti todentaa. Tutkimuksen myötä syntyi taulukkomuotoinen työkalu, jossa kullekin kriteeristön vaatimukselle on määritetty niiden arviointiin soveltuvat hallinnolliset ja tekniset todennusmenetelmät.

Vaatimusten analysoinnin ja arviointilaitosohjeen tulkinnan perusteella fyysisen turvallisuuden kriteerit ja niiden todennusmenetelmät ovat ristiriidassa muihin Julkrin osa-alueisiin nähden. Ensimmäinen ongelma on, että arviointilaitosohjeessa ei anneta tarkkaa tietoa vaatimusten toteuttamisesta tai todentamisesta. Tämä voi johtaa tilanteeseen, jossa eri organisaatiot noudattavat samoja menettelyjä fyysisen turvallisuuden suojauksissaan, mutta arvioinnissa vain toisen tahon menetelmät hyväksytään vaatimustenmukaisiksi, kun arviointia suorittavat tahot käyttävät eri todennusmenetelmiä, koska niille ei ole määritetty yhteistä perustasoa.

Toinen ongelma liittyy Julkrin taulukkomuotoisessa työkalussa viitattuihin muihin standardeihin. Viittaukset ovat otsikon "Toteutusesimerkki" alla, joten niiden velvoittavuus jää epäselväksi. Esimerkiksi vaatimuskohdassa FYY-05.1 äänieristyksen osalta viitataan standardeihin SFS-EN-ISO 717-1 sekä SFS-EN-ISO 16283-1. Viittaukset ovat kuitenkin konditionaalissa ja toteutusesimerkkejä. Mikäli kyseisiä standardeja ei noudateta, jää tulkinta vaatimustenmukaisuudesta täysin arviointia suorittava tahon vastuulle, eikä perustu yleisesti tunnistettuun tai julkiseen linjaukseen, vaikuttaen näin kriteeristön vaatimusten läpinäkyvyyteen arvioitavien organisaatioiden ja arviointitahojen välillä.

Tutkimuksessa esitelty malli Julkrin vaatimuksiin soveltuvista todennusmenetelmistä perustuu arviointilaitosohjeen mukaisiin teknisiin ja

hallinnollisiin menettelyihin. Tutkimuksen havaintojen perusteella etenkin TEK-osion vaatimusten todentaminen luotettavasti vaatii laajaa osaamista ja työkaluja. Kirjallisuuskatsauksen perusteella useissa selvityksissä on havaittu, että valtionhallinnon uudistukset eivät ole tuottaneet haluttuja tuloksia ja turvallisuuskriittisiä tietojärjestelmiä ei ole auditoitu ja hyväksytty riittävästi tai niiden turvallisuustaso ei ole ollut toivotulla tasolla. Julkrin ja Katakrin teknisten vaatimusten luotettavan todentamisen haastavuus voi olla yksi merkittävimmistä syistä siihen, miksi arviointilaitoksia ei ole enempää, edesauttaen näin järjestelmien arviointien viivästymistä. Toisaalta samasta syystä organisaatioilla ei itsellään ole kompetenssia rakentaa vaatimukset täyttäviä järjestelmiä ja tehdä niille itsearviointeja, jotka nopeuttaisivat ulkoisten arvioijien toimintaa.

8.4 Tulosten yhteys aiempaan tutkimukseen

Osana tätä pro gradu -tutkielmaa selvitettiin aiempaa aiheeseen liittyvää tutkimusta tietoturvallisuuden hallintajärjestelmiin, hallintajärjestelmien standardeihin sekä tietoturvallisuuden sääntelyyn liittyen. Tämän tutkimuksen kannalta huomattavaa on erityisesti aiemmassa tutkimuksessa esitetty kritiikki tietoturvallisuuden hallintajärjestelmästandardeja sekä muita tietoturvallisuuden arviointikriteeristöjä kohtaan. Havainnot on esitelty tämän tutkimuksen luvussa 3.

Aiemmissa julkaisuissa tietoturvallisuuden hallintajärjestelmiin liittyviä standardeja ja viitekehyksiä on kritisoitu niiden yleismaailmallisesta lähestymistavasta. Valituissa tutkimuksissa tarkastellut standardit ovat olleet kansainvälisiä ja niiden pyrkimyksenä on soveltua kaiken kokoisten ja tyyppisten organisaatioiden käyttöön, mistä johtuen niiden esittämistä vaatimuksista ja toteutusesimerkeistä puuttuu konkretiaa. Toisaalta standardeja ja kriteeristöjä on kritisoitu niiden asettamien vaatimusten läpinäkyvyyden puutteesta. Kriteeristöjen ja viitekehysten vaatimusten todetaan perustuvan tietoturva-alan parhaisiin käytäntöihin, mutta standardien laatijat eivät ole julkaisseet valintaperusteitaan tai perustelujaan.

Tämän tutkimuksen havaintojen perusteella samat ongelmat ovat tunnistettavissa myös Julkrissa, vaikka se ei olekaan tarkoitettu kansainväliseksi standardiksi, vaan pääasiallisesti suomalaisten julkishallinnon organisaatioiden käyttöön. Tästä rajauksesta huolimatta organisaatiot, joiden sovellettavaksi Julkri on tarkoitettu ovat hyvin eri kokoisia ja eri tyyppisiä, mistä johtuen osa Julkrissa esitetyistä vaatimuksista jää varsin ylätasolle, eikä julkaisu tarjoa käytännön toteutusesimerkkejä vaatimusten täyttämiseen.

Kirjallisuuskatsauksen perusteella tietoturvallisuuden sääntelyyn liittyvät lait ja asetukset ja niissä säädetyt vaatimukset ovat pirstaloituneet useaan eri lakiin, mistä johtuen niissä esitettyjen vaatimusten vertailu ja tulkinta on haastavaa. Julkriin on koottu eri laeissa ja asetuksissa esitettyjä vaatimuksia

samaan julkaisuun, mikä voi johtaa vaatimusten helpompaan tulkintaan ja täyttämiseen organisaatioissa, joita säädökset velvoittavat.

Vaikka Julkri ehkä helpottaakin vaatimusten tulkintaa, on huomionarvoista, että tietoturvallisuuden ja kyberturvallisuuden valvonta ja ohjaus on jakautunut useille eri toimijoille. Julkrin on julkaissut valtiovarainministeriön alainen tiedonhallintalautakunta. Tietoturvallisuuden arviointeja tekevät Puolustusvoimien pääesikunta sekä Suojelupoliisi, joita ohjaavat puolustusministeriö ja sisäministeriö. Lisäksi tietojärjestelmien arviointeja tekee ja tietoturvallisuuden arviointilaitoksia ohjaa Liikenne- ja viestintävirasto Traficom, jonka ohjaus on liikenne- ja viestintäministeriössä. Tietoturvallisuuden arviointikriteeristönä käytetään tällä hetkellä Katakria, jota ylläpitää ulkoministeriön alaisuudessa toimiva kansallinen turvallisuusviranomainen. Lyhyenkin yhteenvedon perusteella julkishallinnon turvallisuuden arviointiin liittyy ainakin viisi eri ministeriötä ja useita niiden alaisuudessa toimivia virastoja. Tutkimuksen havaintojen perusteella tämä valvonta- ja ohjausvastuun pirstaloituminen on Julkrin osalta johtanut tilanteeseen, jossa on luotu ja julkaistu arviointikriteeristö, jonka käytännön sovellustapoja ei ole mietitty etukäteen poikkihallinnollisesti.

8.5 Tutkimuksen merkitys ja luotettavuus

Tutkimuksessa pyrittiin selvittämään, miten Julkisen hallinnon tietoturvallisuuden arviointikriteeristö toimii tietoturva-arviointien välineenä ja miten se suhteutuu aiemmin julkaistuihin tietoturvallisuuden hallintajärjestelmästandardeihin ja tietoturvallisuuden arviointikriteeristöihin.

Tutkimuksen havaintojen perusteella Julkri on kattava kriteeristö, joka yhdistää useampien olemassa olevien tietoturvallisuuden arviointikriteeristöjen vaatimukset muihin lainsäädännössä esitettyihin vaatimuksiin. Julkaisun hyödyllisyys tarkoitetuille kohdeorganisaatioille jää kuitenkin rajalliseksi, mikäli kriteeristöä vastaan ei tehdä auditointeja. Tietoturvallisuuden ja teknologioiden kehittyessä on mahdollista, että kriteeristössä esitetyt vaatimukset vanhentuvat, eivätkä vastaa enää parhaita tietoturvallisuuden käytäntöjä. Tämän vuoksi Julkri olisi tärkeää saada organisaatioiden sovellettavaksi ja arviointitahojen todennettavaksi ennen kuin kriteeristössä esitetyt vaatimukset hapantuvat teknologioiden kehittyessä.

Osana tutkimusta syntyi taulukkomuotoinen työkalu, jossa kullekin kriteeristön vaatimukselle on määritetty niiden arviointiin soveltuvat hallinnolliset ja tekniset todennusmenetelmät. Tämä taulukko on tarkoitettu käytännön työkaluksi niin arvioinnin kohteena oleville organisaatioille kuin arviointia suorittaville tahoille. Arvioinnissa käytettävien todennusmenetelmien tunnistaminen jo arviointiin valmistauduttaessa auttaa auditoitavia organisaatioita valmistelemaan riittävän dokumentaation ja teknisen kyvykkyyden vaatimustenmukaisuuden osoittamiseksi.

Tutkimuksen luotettavuus pyrittiin varmistamaan perustamalla tutkimuksen havainnot käytettyihin lähteisiin. Tutkijan oma koulutus ei kuitenkaan ole lainsäädännön alalta, mikä voi näkyä tutkimuksen aineistona käytettyjen lakitekstien tulkinnassa. Tutkimuksen aiheeksi valittu Julkisen hallinnon tietoturvallisuuden arviointikriteeristö on julkaistu vuonna 2022, eikä siihen liittyen ole julkaistu aiempaa tieteellistä tutkimusta. Tältä osin tutkimuksessa nojauduttiin aiempaan tutkimukseen muista tietoturvallisuuden hallintajärjestelmästandardeista ja tietoturvallisuuden arviointikriteeristöistä. Koska näiden tutkimusten kohteet ovat Julkrista erillisiä julkaisuja, ei voida täysin varmistua siitä, että kaikki aiemmassa tutkimuksessa esitetyt havainnot pätevät myös Julkriin.

Tutkimuksen perusteella jatkotutkimusaiheeksi voidaan nostaa Julkrin ja muiden kriteeristöjen käytännön sovellutusten seuranta, kun kriteeristö on ollut pidempään julkaistuna. Kirjoitushetkellä tietoturvallisuuden arviointeja suorittavat tahot eivät olleet julkisesti ottaneet kantaa tiedonhallintalautakunnan suositukseen tai kertoneet, tulevatko ne käyttämään Julkria omassa arviointitoiminnassaan.

LÄHTEET

Culot, G., Nassimbeni, G., Podrecca, M. & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal Vol. 33 No. 7, 76-105

Dhillon, G., Syed, R. & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. Information & Management, 54, 452-464.

Dhillon, G., Syed, R. & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. Information & Management, 54, 452-464.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Annettu 27.4.2016. Haettu osoitteesta https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fi

Hallituksen esitys eduskunnalle laeiksi julkisen hallinnon turvallisuusverkkotoiminnasta ja viestintämarkkinalain 2 §:n muuttamisesta HE 54/2013. Haettu osoitteesta https://finlex.fi/fi/esitykset/he/2013/20130054

Hsu, C. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. European Journal of Information Systems 18, 140–150

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information security technical report 13, 247–255.

Johnson, J., Lincke, S. J., Imhof, R., & Lim, C. (2014). A comparison of international information security regulations. Interdisciplinary Journal of Information, Knowledge, and Management, 9, 89-116.

Jyväskylän yliopisto. (2022). Pro gradu -tutkielma. Haettu osoitteesta https://www.jyu.fi/it/fi/ohjeita-opiskelijalle/opiskelu/pro-gradu-tutkielma

Jyväskylän yliopisto. (2023). Käsiteanalyysi. Haettu osoitteesta https://openscience.jyu.fi/fi/opetus/perustutkinto-opiskelijat/opiskelumateriaalit/kirjastotuutori/1-tutustu-aiheeseesi-ja-tyosta-hakutermit/kasitenalyysi

Järvinen, P. (2004). Research Questions Guiding Selection of an Appropriate Research Method. University of Tampere.

Kokonaisturvallisuuden sanasto. (2017). TSK 50. Sanastokeskus TSK ry. Haettu osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Kyberturvallisuuden sanasto. (2018). TSK 52. Haettu osoitteesta https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Laki digitaalisten palvelujen tarjoamisesta 306/2019. Annettu Helsingissä 15.3.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190306

Laki julkisen hallinnon tiedonhallinnasta 2019/906. Annettu Naantalissa 9.8.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190906

Laki julkisen hallinnon turvallisuusverkkotoiminnasta 2015/10. Annettu Helsingissä 13.1.2015. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2015/20150010

Laki kansainvälisistä tietoturvallisuusvelvoitteista 2004/588. Annettu Naantalissa 24.6.2004. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021. Annettu Helsingissä 27.8.2021. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2021/20210784

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä 552/2019. Annettu Helsingissä 26.4.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190552

Laki tietoturvallisuuden arviointilaitoksista 2011/1405. Annettu Helsingissä 22.12.2011. Haettu osoitteesta https://finlex.fi/fi/laki/ajantasa/2011/20111405

Laki Valtion talous- ja henkilöstöhallinnon palvelukeskuksesta 2019/179. Annettu Helsingissä 8.2.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2019/20190179

Laki valtion talousarviosta 1988/423. Annettu Helsingissä 13.5.1988. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1988/19880423

Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä. 2013/1226. Annettu Helsingissä 30.12.2013. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2013/20131226

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 2011/1406. Annettu Helsingissä 22.12.2011. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20111406

Laki viranomaisten toiminnan julkisuudesta 1999/621. Annettu Helsingissä 21.5.1999. Haettu osoitteesta https://finlex.fi/fi/laki/ajantasa/1999/19990621

Lehtilä, O., Nyström, P., Ronikonmäki, N-M. & Sirviö, T-H. (2021). Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla.

Työryhmän loppuraportti. Helsinki: Liikenne- ja viestintäministeriö. Haettu osoitteesta https://julkaisut.valtioneuvosto.fi/handle/10024/162783

Lehto, M., Limnéll, J., Innola, Pöyhönen, J., Rusi, T., & Salmela, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisu 30/2017. Haettu osoitteesta https://tietokayttoon.fi/julkaisu?pubid=17805

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 28/2018. Haettu osoitteesta https://julkaisut.valtioneuvosto.fi/handle/10024/160717

Lewallen, J. (2020). Emerging technologies and problem definition uncertainty: The case of cybersecurity. Regulation & Governance. Volume 15, Issue 4.

Liikenne- ja viestintävirasto Traficom. (2020). Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Traficomin julkaisuja 13/2020.

Liikenne- ja viestintävirasto Traficom. (2021). Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit. Haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf

Liikenne- ja viestintävirasto Traficom. (2022). Ohje tietoturvallisuuden arviointilaitoksille 210/2022.

Liikenne- ja viestintävirasto Traficom. (2023). Hyväksytyt tietoturvallisuuden arviointilaitokset. Haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset

Niemimaa, E. & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. European Journal of Information Systems 26, 1–20

Puusa, A. (2008). Käsiteanalyysi tutkimusmenetelmänä. Premissi 4/2008.

Roy, P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 1-3.

Salminen, A. (2011). Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan Yliopiston julkaisuja, opetusjulkaisuja 62.

Shameli-Sendi, A., Aghababaei, R. & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14- 30.

Siponen, M. (2004). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. Information and Organization 15 (2005) 339–375.

Siponen, M. (2006A). Information Security Standards Focus on the Existence of Process, Not Its Content. Communication of the ACM. August 2006/Vol. 49, No. 8

Siponen, M. (2006B). Secure-System Design Methods: Evolution and Future Directions. IT Pro.

Siponen, M. & Willison, R. (2009). Information management standards: Problems and solutions. Information & Management, 46, 5, 267-270.

Suomen Standardisoimisliitto SFS. (2017). SFS-EN ISO/IEC 27001:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

Susanto, H., Amunawar, M. N. & Tuan, Y.C. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS, 11, 5, 23-29.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T. & Klepacki, B. (2019). Information security assessment in public administration. Computers & Security 90, 101709.

Tietosuojalaki 2018/1050. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Turvallisuuskomitea. (2017). Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös. Helsinki: Lönnberg Print. Haettu osoitteesta https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/

Turvallisuuskomitea. (2019). Suomen kyberturvallisuusstrategia 2019. Haettu osoitteesta https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Ulkoministeriö. (2020). Katakri – tietoturvallisuuden auditointityökalu viranomaisille. Haettu osoitteesta https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Valtioneuvosto. (2020). Periaatepäätökset. Haettu osoitteesta https://valtioneuvosto.fi/paatokset/periaatepaatokset

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Annettu Helsingissä 28.11.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20191101

Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 132/2014. Annettu Helsingissä 20.2.2014. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2014/20140132

Valtioneuvoston ohjesääntö 2003/262. Annettu Helsingissä 3.4.2003. Haettu osoitteesta https://finlex.fi/fi/laki/ajantasa/2003/20030262

Valtiontalouden tarkastusvirasto. (2016). Hallinnon turvallisuusverkkotoiminnan ohjaus. Valtiontalouden tarkastusviraston tarkastuskertomukset 14/2016. Dnro 172/54/2015.

Valtiontalouden tarkastusvirasto. (2017). Kybersuojauksen järjestäminen. Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017. Dnro 185/54/2016. Haettu osoitteesta https://www.vtv.fi/app/uploads/2018/05/22102159/kybersuojauksen-jarjestaminen-16-2017.pdf

Valtiovarainministeriö. (2022). Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) – Suositus ja kriteeristö. Valtiovarainministeriön julkaisuja – 2022:43.

von Solms, R. (1999). Information security management: why standards are important. Information Management & Computer Security, Vol. 7 Issue: 1, 50-58

Wiander, T. (2007). ISO/IEC 17799 Standard's Intended Usage and Actual Use by the Practitioners. ACIS 2007 Proceedings. Paper 74.

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-01	**Periaatteet**	Organisaatiolla on ylimmän johdon hyväksymät tietoturvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan sekä ovat tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset.	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.		TihL 4 § 2 mom, 13 §	ISO/IEC 27002:2022 5.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01		T-01	H1, H2
Hallinnollinen turvallisuus	HAL-02	**Tehtävät ja vastuut**	Organisaatio on määritellyt ja dokumentoinut tietoturvallisuuden hoitamisen tehtävät ja vastuut sisältäen myös palveluntuottajille kuuluvat vastuut.	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.	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	TihL 4 § 2 mom	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		T-02	H1, H2
Hallinnollinen turvallisuus	HAL-02.1	**Tehtävät ja vastuut - tehtävien eriyttäminen**	Organisaation on varmistettava, että henkilöillä ei ole tietoturvallisuuden kannalta vaarallisia työyhdistelmiä	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.	- Organisaatio on määritellyt vaaralliset työyhdistelmät - Vaaralliset työyhdistelmät tarkastetaan osana tehtävien määrittelyjä - Vaaralliset työyhdistelmät tarkastetaan osana käyttöoikeuksien hallintaa erityisesti pääkäyttäjä- ja valvontaroolien kohdalla	TihL 4 § 2 mom, 13 §	ISO/IEC 27002:2022 5.3		I-06	H1, H2
Hallinnollinen turvallisuus	HAL-03	**Resurssit**	Organisaatiolla on käytössään riittävät resurssit ja asiantuntemus tietoturvallisuuden varmistamiseksi.	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.	- 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	TihL 4 § 2 mom	SFS-EN ISO/IEC 27001:2017 7.1, 7.2, 5.1		T-05	H1, H2
Hallinnollinen turvallisuus	HAL-04	**Suojattavat kohteet**	Organisaatio tunnistaa suojattavat kohteet sekä pitää niistä ajantasaista dokumentaatiota.	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.		TihL 5 § 2 mom, 13 §	ISO/IEC 27002:2022 5.9; Suositus tiedonhallintamallista 2020:29			H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-04.1	**Suojattavat kohteet - vastuut**	Organisaatio määrittelee suojattavien kohteiden vastuut.			TihL 4 § 2 mom	ISO/IEC 27002:2022 5.9; Suositus tiedonhallintamallista VM 2020:29			H1, H2
Hallinnollinen turvallisuus	HAL-04.2	**Suojattavat kohteet - luokittelu**	Organisaation on luokiteltava tiedot sekä niihin liittyvät järjestelmät ja käsittelyprosessit niihin kohdistuvien vaatimusten perusteella.	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).	- 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.	TihL 4 § 2 mom, 5 §, 13 §, 18 §; TLA 3 §, 4 §; JulkL 24 §	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		T-08	H1, H2
Hallinnollinen turvallisuus	HAL-04.3	**Suojattavat kohteet - kasautumisvaikutus**	Kasautumisvaikutus on huomioitu suojattavien kohteiden luokittelussa.	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.		TihL 5 § 2 mom, 13 § 1 mom		HAL-06, TEK-06	T-08	H1, H2
Hallinnollinen turvallisuus	HAL-04.4	**Suojattavat kohteet - merkitseminen**	Organisaation on merkittävä tiedot lakisääteisten vaatimusten sekä organisaation määrittelemien luokitteluperiaatteiden mukaisesti.	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.		TihL 18 §; TLA 3 §, 4 §; JulkL 25 §	Suositus turvallisuusluokiteltavienasiakirjojen käsittelystä 2021:5 luku 3; ISO/IEC 27002:2022 5.13		T-08	H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-04.5	**Suojattavat kohteet - riippuvuudet**	Organisaatio on tunnistanut ja dokumentoinut suojattavien kohteiden väliset riippuvuudet.			TihL 5 §				H1, H2
Hallinnollinen turvallisuus	HAL-04.6	**Suojattavat kohteet - sidosryhmät**	Organisaatio on tunnistanut ja dokumentoinut suojattaviin kohteisiin liittyvät sidosryhmät.			TihL 5 §				H1, H2
Hallinnollinen turvallisuus	HAL-05	**Vaatimukset**	Organisaatio tunnistaa lainsäädännöstä, sidosryhmistä sekä organisaation toiminnasta johtuvat tietoturvavaatimukset.	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.		TihL 13 §	SFS-EN ISO/IEC 27001:2017 4.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luvut 2 ja 4			H1, H2
Hallinnollinen turvallisuus	HAL-05.1	**Vaatimukset - seuranta**	Organisaatio seuraa asetettujen tietoturvallisuusvaatimusten ja toimintaympäristön muutoksia ja tekee tarvittavat toimenpiteet niihin reagoimiseksi.	Lainsäädäntö, sopimusvaatimukset sekä muuttuvat tietoturvallisuusuhat edellyttävät säännöllistä vaatimusten ja uhkien seurantaa ja muutoksiin reagoimista.		TihL 4 § 2 mom, 13 § 1 mom	SFS-EN ISO/IEC 27001:2017 9.1; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 4.1			H1, H2
Hallinnollinen turvallisuus	HAL-05.2	**Vaatimukset - muutosvaikutukset**	Organisaatio arvioi olennaisten hallinnollisten uudistusten ja tietojärjestelmien käyttöönottojen muutosvaikutukset suhteessa tietoturvallisuusvaatimuksiin ja -toimenpiteisiin.	Olennaisten muutosten yhteydessä organisaatioilta edellytetään muutosvaikutusten arviointia. Osana muutosvaikutusten arviointia on arvioitava muutosten vaikutukset suhteessa tietoturvallisuusvaatimuksiin ja -toimenpiteisiin.		TihL 5 §	Suositus tiedonhallinnan muutosvaikutusten arvioinnista 2020: 53; ISO/IEC 27002:2022 5.31			H1, H2
Hallinnollinen turvallisuus	HAL-06	**Riskienhallinta**	Organisaatio toteuttaa tietoturvallisuusriskien hallintaa ja on arvioinut olennaiset tietoihin kohdistuvat riskit sekä mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.	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.	- 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.	TihL 13 § 1 mom; TLA 6 §, 7 §	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	FYY-01, TEK-01, TEK-14, TEK-16	T-03	H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-06.1	**Riskienhallinta - lainsäädäntöjohdannaiset riskit**	Palveluun liittyvät lainsäädäntöjohdannaiset riskit on tunnistettu, arvioitu ja niistä on huolehdittu.	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.	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.	TihL 13 § 1 mom; TLA 6 §, 7 §	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	FYY-01, TEK-01, TEK-14, TEK-16, TSU-18	T-03	H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-07	**Seuranta ja valvonta**	Organisaatiossa on järjestetty seuranta ja valvonta tietoturvallisuuteen liittyvien prosessien toimivuudesta ja vaatimusten täyttymisestä.	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).	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	TihL 4 § 2 mom, 13 § 1 mom	SFS-EN ISO/IEC 27001:2017 9.1; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 7		T-01, I-19	H1, H2
Hallinnollinen turvallisuus	HAL-07.1	**Seuranta ja valvonta - tietojen käyttö ja luovutukset**	Organisaatio on tunnistanut lokitietojen kerääimiseen liittyvät vaatimukset ja varmistanut niiden perusteella lokitietojen keräämisen ja seurannan riittävyyden.	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.	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.	TihL 17 §	Kyberturvallisuuskeskus, Näin kerään ja käytät lokitietoja; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65, luku 14; ISO/IEC 27002:2022 5.31, 8.15		I-10	H1, H2, T2, T4
Hallinnollinen turvallisuus	HAL-08	**Häiriöiden hallinta**	Organisaatiolla on tietoturvallisuushäiriöiden ja poikkeamatilanteiden käsittelyyn määritellyt prosessit ja ohjeet.	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 kerääimiseen, 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.	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	TihL 4 § 2 mom ja 13 §; TLA 7 §	ISO/IEC 27002:2022 5.24; PiTuKri TJ-04		T-07	H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-09	**Dokumentointi**	Tietoturvallisuuteen liittyvät politiikat, prosessit, ohjeet ja prosessien toteuttamisessa syntyvät tulokset on dokumentoitu.		- 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	TihL 5 §, 6 §, 13 § 1 mom	ISO/IEC 27002:2022 5.37		T-01	H1, H2
Hallinnollinen turvallisuus	HAL-09.1	**Dokumentointi - ajantasaisuus**	Tietoturvallisuuteen liittyvä dokumentaatio on ajantasaista.		- Organisaatiolla on prosessi, jonka avulla seurataan dokumentaation kattavuutta ja ajantasaisuutta - Dokumentaation puutteisiin reagoidaan	TihL 5 §, 6 §, 13 § 1 mom	ISO/IEC 27002:2022 5.37			H1, H2
Hallinnollinen turvallisuus	HAL-10	**Henkilöstön luotettavuuden arviointi**	Organisaatio tunnistaa ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta.	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.	- 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.	TihL 12 §;	Turvallisuusselvityslaki 726/2014; ISO/IEC 27002:2022 6.1		T-10	H1, H2
Hallinnollinen turvallisuus	HAL-10.1	**Henkilöstön luotettavuuden arviointi - turvallisuusselvitys**	Organisaatio arvioi turvallisuusselvityksen tarpeen ja mikäli sellaista edellytetään, myöntää henkilöille pääsyn suojattaviin kohteisiin vasta turvallisuusselvityksen jälkeen.	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.	- Rekrytointien, tehtävämuutosten sekä ulkoisten palveluhankintojen yhteydessä tarkastetaan, edellyttääkö tehtävä turvallisuusselvitystä, - tarvittaessa organisaatio on määritellyt turvallisuusselvitysten hakemiseen prosessin	TihL 12 §; TLA 9 §	Valtion virkamieslaki 750/1994 8 c §		T-10	H1, H2
Hallinnollinen turvallisuus	HAL-11	**Salassapito- ja vaitiolovelvollisuus**	Tietoa käsitteleville henkilöille on selvitetty tietojen suojaamista ja asiakirjojen käsittelyä koskevat tietoturvallisuusperiaatteet ja -toimenpiteet.		- 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	TihL 4 § 2 mom; TLA 6 §, 8 §; JulkL 25 §, 26 § 3 mom	ISO/IEC 27002:2022 6.6; PiTuKri HT-03		T-11	H1, H2
Hallinnollinen turvallisuus	HAL-12	**Ohjeet**	Organisaatiossa on ajantasaiset ja kattavat ohjeet tietoturvallisuuden varmistamiseksi.	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.	- 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.	TihL 4 § 2 mom, 13 § 1 mom; TLA 6 § ja 8 §	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	TEK-17.2	T-04	H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-13	**Koulutukset**	Organisaatio varmistaa perehdytyksillä, koulutuksilla ja viestinnällä, että henkilöstöllä ja organisaation lukuun toimivilla on tuntemus voimassa olevista tietoturvallisuutta koskevista määräyksistä ja ohjeista.	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.	- Tietoja käsittelevälle henkilölle on selvitetty tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt. - Koulutus toteutetaan henkilöstön työtehtävien tarpeet huomioiden. - Koulutuksen sisältö dokumentoidaan - Koulutuksiin osallistuneista pidetään kirjaa	TihL 4 § 2 mom; TLA 6 §, 8 §	ISO/IEC 27002:2022 6.3; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 5		T-12	H1, H2
Hallinnollinen turvallisuus	HAL-14	**Käyttö- ja käsittelyoikeudet**	Organisaatio varmistaa, että tietojärjestelmien käyttöoikeudet ja tietojen käsittelyoikeudet määritellään tehtäviin liittyvien tarpeiden mukaan sekä pidetään ajantasaisina.	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.	- 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	TihL 4 § 2 mom ja 16 §; TLA 8 §, 11 § 1 mom 3 k	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		T-13, I-6	H1, H2, T2
Hallinnollinen turvallisuus	HAL-14.1	**Käyttö- ja käsittelyoikeudet - ajantasainen luettelo**	Organisaatio varmistaa, että sillä on ajantasaiset luettelot henkilöiden käyttö- ja käsittelyoikeuksista.	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.		TLA 8 §	ISO/IEC 27002:2022 5.18; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 4.1		T-13	H1, H2
Hallinnollinen turvallisuus	HAL-14.2	**Käyttö- ja käsittelyoikeudet - päättyminen**	Organisaatio varmistaa, että se, joka ei enää toimi tehtävissä, joihin oikeus tietojen käsittelyyn perustuu, palauttaa tiedot tai tuhoaa ne asianmukaisella tavalla.			TihL 13 § 1 mom, 21 § 2 mom; TLA 8 §	ISO/IEC 27002:2022 5.18; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 4.1		T-13	H1, H2
Hallinnollinen turvallisuus	HAL-15	**Työskentelyn tietoturvallisuus koko palvelussuhteen ajan**	Organisaatio huolehtii työskentelyn tietoturvallisuudesta koko palvelussuhteen ajan.	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.	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.	TihL 4 § 2 mom, 12 §, 16 §; TLA 6 §, 8 §	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		T-09	H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-16	**Hankintojen turvallisuus**	Organisaatio varmistaa jo ennakolta, että hankittavat tietojärjestelmät ja palvelut ovat tietoturvallisia sekä varmistaa niiden turvallisuuden muutostilanteissa koko järjestelmän elinkaaren ajan.	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.	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.	TihL 13 § 4 mom; TLA:n 6 §; JulkL 26 §	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		I-13	H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-16.1	**Hankintojen turvallisuus - sopimukset**	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.	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 §).		TihL 13 §; TLA:n 6 §; JulkL 26 §; Tietosuoja-asetus artikla 28.4	ISO/IEC 27002:2022 5.20; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 6; PiTuKri TJ-07;		I-13	H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-17	**Tietojärjestelmien toiminnallinen käytettävyys ja vikasietoisuus**	Organisaatio varmistaa tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden riittävällä testauksella säännöllisesti.	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.	- 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.	TihL 13 § 2 mom	ISO/IEC 27002:2022 8.29, Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 7			H1, H2
Hallinnollinen turvallisuus	HAL-17.1	**Tietojärjestelmien toiminnallinen käytettävyys ja vikasietoisuus - saavutettavuus**	Organisaation on varmistettava digitaalisten palveluiden saavutettavuus lainsäädännön edellyttämässä laajuudessa.	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.		Laki digitaalisten palvelujen tarjoamisesta (306/2019)	www.saavutettavuusvaatimukset.fi			H1, H2
Hallinnollinen turvallisuus	HAL-18	**Asiakirjajulkisuuden toteuttaminen**	Organisaatio varmistaa, että tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvän tietojenkäsittely suunnitellaan siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.	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.	- 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.	TihL 13 § 3 mom				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Hallinnollinen turvallisuus	HAL-19	**Tietojen käsittely**	Organisaatio varmistaa, että tietoja käsitellään ja säilytetään siten, että pääsy tietoihin suojataan sivullisilta.	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.	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.	TihL 13 §, 15 § 2 mom; TLA 10 § 1 mom	ISO/IEC 27002:2022 5.15; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 4;	FYY-03, FYY-04, TEK-09	I-17	H1, H2
Fyysinen turvallisuus	FYY-01	**Fyysisen turvallisuuden riskien arviointi**	Fyysiset turvatoimet on mitoitettava riskien arvioinnin mukaisesti.	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.	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	TihL 13 § 1 mom, 15 § 2 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 36	HAL-06	F-02	H1, H2, T7
Fyysinen turvallisuus	FYY-01.1	**Fyysisen turvallisuuden riskien arviointi - TEMPEST**	Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös TEMPEST-riski.	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.		TLA 11 § 2 mom		TEK-15	F-05.8, F-06.10	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-02	**Fyysisten turvatoimien valinta (monitasoinen suojaus)**	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.	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.	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.	TihL 13 § 1 mom, 15 § 2 mom; TLA 7 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 33; ISO/IEC 27002:2022 7.1, 7.2, 7.3		F-03	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-03	**Tiedon käsittely**	Tietoja on käsiteltävä siten, että pääsy niihin suojataan sivullisilta.	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.		TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 29	HAL-19	F-04	H1, H2, T7
Fyysinen turvallisuus	FYY-03.1	**Tiedon käsittely - TL I**	Turvallisuusluokan I asiakirjaa saa käsitellä ainoastaan turva-alueella.			TLA 10 § 2 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 29	HAL-19	F-04	H1, H2, T7
Fyysinen turvallisuus	FYY-04	**Tiedon säilytys**	Tietoja on säilytettävä siten, että pääsy niihin suojataan sivullisilta.	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.		TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28- 29	HAL-19	F-04	H1, H2, T7
Fyysinen turvallisuus	FYY-04.1	**Tiedon säilytys - TL IV**	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.		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.	TLA 10 §			F-04	H1, H2, T7
Fyysinen turvallisuus	FYY-04.2	**Tiedon säilytys - Tietovarannot ja tietojärjestelmät - TL IV**	Turvallisuusluokan IV asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle (hallinnollinen alue tai turva-alue).			TLA 10 § 3 mom 3 kohta	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28- 29	HAL-19	F-04	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-04.3	**Tiedon säilytys - Tietovarannot ja tietojärjestelmät - TL III**	Turvallisuusluokan II tai III asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turva-alueelle.			TLA 10 § 3 mom 2 kohta	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28- 29	HAL-19	F-04	H1, H2, T7
Fyysinen turvallisuus	FYY-04.4	**Tiedon säilytys - TL III**	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.			TLA 10 §			F-04	H1, H2, T7
Fyysinen turvallisuus	FYY-04.5	**Tiedon säilytys - TL II**	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.			TLA 10 §			F-04	H1, H2, T7
Fyysinen turvallisuus	FYY-04.6	**Tiedon säilytys - TL I**	Turvallisuusluokan I asiakirjaa saa säilyttää ainoastaan turva-alueella.			TLA 10 § 2 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 29	HAL-19	F-04	H1, H2, T7
Fyysinen turvallisuus	FYY-05	**Turvallisuusalue**	Turvallisuusalueiden eli hallinnollisten alueiden sekä turva-alueiden on noudatettava tässä kriteerissä annettuja suosituksia.	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.		TihL 13 § 1 mom, 15 § 2 mom; TLA 9 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39		F-05.4, F-06.6	H1, H2, T7
Fyysinen turvallisuus	FYY-05.1	**Turvallisuusalue - Äänieristys**	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.	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.	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 ilmaääneneristävyyden lisäksi myös runkoääneneristävyys. Äänieristysvaatimus voidaan tarvittaessa saavuttaa esimerkiksi tilan uudelleen sijoittelulla, rakenteiden ja läpivientien eristävyyden parantamisella tai arvioitavan tilan ulkopuolisten tilojen taustamelulla.	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 § 1 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39		F-05.4, F-06.6	H1, H2, T7
Fyysinen turvallisuus	FYY-05.2	**Turvallisuusalue - Salaa katselun estäminen**	Jos tietoihin kohdistuu salaa tai vahingossa katselun riski, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet.		Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia.	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 § 1 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 40 ja 45	HAL-19	F-05.6, F-06.8	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-05.3	**Turvallisuusalue - Tila- ja laitetarkastukset**	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.	Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista luotettavasti (esim. matkapuhelimet, älykellot, jne.), laitteet tulee jättää tilan ulkopuolelle esimerkiksi tähän tarkoitukseen varattuun säilytysratkaisuun.		TLA 7 §, 10 § 1 mom, 11 § 2 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 40 ja 46		F-05.7, F-06.9	H1, H2, T7
Fyysinen turvallisuus	FYY-05.4	**Turvallisuusalue - Pääsyoikeuksien ja avaintenhallinnan menettelyt**	Organisaation on määriteltävä alueen pääsyoikeuksien ja avainhallinnan menettelyt ja roolit.	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.	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.	TihL 15 § 2 mom; TLA 9 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 39 ja 44; ISO/IEC 27002:2022 7.2		F-05.2, F-06.3	H1, H2, T7
Fyysinen turvallisuus	FYY-05.5	**Turvallisuusalue - Vierailijat**	Muilla kuin organisaation asianmukaisesti valtuuttamilla henkilöillä (vierailijoilla) on aina saattaja.	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.	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.	TLA 9 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 39 ja 44		F-05.3, F-06.4	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-06	**Hallinnollinen alue**	Hallinnollisen alueen tulee täyttää tässä osiossa esitetyt suositukset sekä riskilähtöisesti arvioidut tarkennukset siten, että turvatoimien tavoitteet saavutetaan.	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".		TihL 13 § 1 mom, 15 § 2 mom; TLA 9 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 38	FYY-05	F-05	H1, H2, T7
Fyysinen turvallisuus	FYY-06.1	**Hallinnollinen alue - alueen raja ja rakenteet**	Alueella on oltava selkeästi määritelty näkyvä raja, mutta aluetta rajaavalle rakenteelle (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet) ei aseteta erityisiä vaatimuksia.	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.	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	TihL 13 § 1 mom, 15 § 2 mom; TLA 9 § 1 mom 1 k	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 39		F-05.1	H1, H2, T7
Fyysinen turvallisuus	FYY-06.2	**Hallinnollinen alue - kulunvalvonta**	Alueelle pääsyä tulee valvoa, mikäli se on riskien arvioinnin perusteella tarkoituksenmukaista.	Kulunvalvonta voi olla tarkoituksenmukaista esimerkiksi, jos alueella käsitellään turvallisuusluokan III tai korkeamman luokan tietoa.	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.	TLA 7 §, 9 §			F-05.2	H1, H2, T7
Fyysinen turvallisuus	FYY-06.3	**Hallinnollinen alue - pääsyoikeuksien myöntäminen**	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.	Pääsyn rajaaminen alueelle voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen.		TLA 9 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39, PiTuKri FT-03	FYY-05.4	F-05.2	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-06.4	**Hallinnollinen alue - tunkeutumisen ilmaisujärjestelmät**	Tarvittaessa tunkeutumisen ilmaisujärjestelmää voidaan käyttää täydentävänä monitasoisen suojauksen riskienhallintakeinona.	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.	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	TLA 7 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 40		F-05.5	H1, H2, T7
Fyysinen turvallisuus	FYY-07	**Turva-alue**	Turva-alueen tulee täyttää tässä osiossa esitetyt suositukset sekä riskilähtöisesti arvioidut lisätarkennukset siten, että monitasoisen suojauksen tavoitteet saavutetaan.	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".		TLA 7 §, 9 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43	FYY-05	F-06	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-07.1	**Turva-alue - alueen raja ja rakenteet**	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.	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.	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	TLA 9 § 1 mom 2 k	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43		F-06.1	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-07.2	**Turva-alue - kulunvalvonta**	Alueen rajalla tulee valvoa kaikkea kulkua sisään ja ulos kulkulupien avulla tai tunnistamalla henkilöt henkilökohtaisesti.	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.	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.	TLA 9 § 1 mom 2 k	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43		F-06.2	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-07.3	**Turva-alue - pääsyoikeuksien myöntäminen**	Itsenäinen pääsyoikeus alueelle voidaan myöntää vain organisaation asianmukaisesti valtuuttamalle henkilölle, jonka luotettavuus on varmistettu ja jolla on erityinen lupa tulla alueelle.	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.		TLA 9 § 1 mom 2 k	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 44	FYY-05.4	F-06.3	H1, H2, T7
Fyysinen turvallisuus	FYY-07.4	**Turva-alue - vierailijat**	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.	Kriteeri täydentää kaikkia turvallisuusalueita koskevaa kriteeriä "Turvallisuusalue - Vierailijat".		TLA 9 § 1 mom 2 k, 10 § 1 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 44	FYY-05.5	F-06.4	H1, H2, T7
Fyysinen turvallisuus	FYY-07.5	**Turva-alue - turvallisuusohjeet**	Kullekin turva-alueelle on laadittava ohjeet noudatettavista turvallisuusmenettelyistä.	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.	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.	TihL 4 § 2 mom; TLA 10 § 1 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 45	HAL-12	F-06.5	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-07.6	**Turva-alue - tunkeutumisen ilmaisujärjestelmät**	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).	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.	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.	TLA 7 §, 9 § 1 mom 2 k	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 45		F-06.7	H1, H2, T7
Fyysinen turvallisuus	FYY-07.7	**Turva-alue - säilytysyksiköiden avaimet ja pääsykoodit**	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.			TLA 8 §, 9 § 1 mom 2, 10 § 1 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 46		F-06.10	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-08	**Tietojen kuljettaminen**	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.			TihL 13 § 1 mom; TLA 13 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 26-28	TEK-16, FYY-02	F-08.1	H1, H2, T7
Fyysinen turvallisuus	FYY-08.1	**Tietojen kuljettaminen - TL IV**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TLA 13 §			F-08.1	H1, H2, T7
Fyysinen turvallisuus	FYY-08.2	**Tietojen kuljettaminen - TL III**	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.		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.	TLA 13 §			F-08.1	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-08.3	**Tietojen kuljettaminen - TL II**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TLA 13 §			F-08.1	H1, H2, T7
Fyysinen turvallisuus	FYY-09	**Tietojen kopioiminen**	Kopioihin ja käännöksiin sovelletaan alkuperäistä tietoa koskevia turvatoimia.	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.	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.	TihL 13 § 1 mom; TLA 2 § 2 mom	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28		F-08.2	H1, H2, T7
Fyysinen turvallisuus	FYY-09.1	**Tietojen kopioiminen - TL II**	Tietojen kopiot ja niiden käsittelijät on luetteloitava. Tietojen kopiointia varten on hankittava tiedon laatineen viranomaisen lupa.		Vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraava toimenpide: 4) Kopiointi ja käsittelijät merkitään diaariin/rekisteriin tai luetteloidaan jollakin muulla vastaavalla menettelyllä.	TLA 14 § 1 mom 3 ja 4 k			F-08.2	H1, H2, T7
Fyysinen turvallisuus	FYY-10	**Tietojen kirjaaminen**	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).	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.		TLA 14 § 1 mom 1 ja 2 k	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 19-23		F-08.3	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Fyysinen turvallisuus	FYY-11	**Tietojen fyysinen tuhoaminen**	Ei-sähköisten tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.	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.		TihL 21 §; TLA 15 §	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 29-31	TEK-21	F-08.4	H1, H2, T7
Fyysinen turvallisuus	FYY-11.1	**Tietojen fyysinen tuhoaminen - TL IV**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		- 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).	TLA 15 §			F-08.4	H1, H2, T7
Fyysinen turvallisuus	FYY-11.2	**Tietojen fyysinen tuhoaminen - TL III**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		- 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).	TLA 15 §			F-08.4	H1, H2, T7
Fyysinen turvallisuus	FYY-11.3	**Tietojen fyysinen tuhoaminen - TL II**	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.		- 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).	TLA 15 §			F-08.4	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-01	**Verkon rakenteellinen turvallisuus**	Tietojenkäsittely-ympäristö on erotettu julkisista tietoverkoista ja muista heikomman turvallisuustason ympäristöistä riittävän turvallisella tavalla.	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.		TihL 13 § 1 mom; TLA 11 § 1 mom 1 k	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		I-01	H1, H2, T2, T1
Tekninen turvallisuus	TEK-01.1	**Verkon rakenteellinen turvallisuus - salaus yleisissä tietoverkoissa**	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.	Käytettävien salausvahvuuksien ja -asetusten valinnassa voidaan hyödyntää lähtökohtaisesti turvallisuusluokan IV mukaisia vahvuuksia ja asetuksia.		TihL 14 §; TLA 12 § ja 11 §:n 1 mom 7 k	ISO/IEC 27002:2022 8.24	FYY-7.1	I-01, I-12, I-15	H1, H2, T1, T2, T5
Tekninen turvallisuus	TEK-01.2	**Verkon rakenteellinen turvallisuus - palomuuri**	Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuustasojen ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä.			TihL 13 § 1 mom; TLA 11 §:n 1 mom 1 ja 2 k	PiTuKri TT-01		I-01	H1, H2, T1, T2, T5

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-01.3	**Verkon rakenteellinen turvallisuus - käsittely-ympäristöjen erottaminen**	Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä.		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.	TihL 13 § 1 mom; TLA 11 § 1 mom 1 ja 2 k			I-01, I-06, I-08, I-11, I-19	H1, H2, T1, T2, T5, T8
Tekninen turvallisuus	TEK-01.4	**Verkon rakenteellinen turvallisuus - salaaminen turva-alueiden ulkopuolella**	Hallitun fyysisen turvallisuusalueen ulkopuolelle menevä liikenne salataan riittävän turvallisella salausratkaisulla.			TihL 14 §; TLA 11 § 1 mom 7 k, 12 §			I-01	H1, H2, T1, T2, T5, T8

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-01.5	**Verkon rakenteellinen turvallisuus - yhdyskäytäväratkaisun käyttö**	Turvallisuusluokat III-II: Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää riittävän turvallisen yhdyskäytäväratkaisun käyttöä.	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.	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	TLA 11 § 1 mom 1 ja 2 k		TEK-04	I-01	H1, H2, T1, T2, T5, T8

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-01.6	**Verkon rakenteellinen turvallisuus - TL II käsittely**	Turvallisuusluokan II käsittely-ympäristöt ovat lähtökohtaisesti fyysisesti eristettyjä kokonaisuuksia.		Turvallisuusluokan ylittävä liikennöinti voidaan sallia vain datadiodien tai vastaavien OSI-mallin fyysisellä kerroksella toimivien yksisuuntaisten yhdyskäytäväratkaisujen kautta.	TLA 11 § 1 mom 1 ja 2 k			I-01	H1, H2, T1, T2, T5, T7, T8
Tekninen turvallisuus	TEK-01.7	**Verkon rakenteellinen turvallisuus - TL I käsittely**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TLA 11 § 1 mom 1 ja 2 k			I-01	H1, H2, T1, T2, T5, T7, T8

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-02	**Tietoliikenneverkon vyöhykkeistäminen**	Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava monitasoisen suojaamisen periaatteen mukaisesti.	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.	Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Tietoliikenneverkko on jaettu ko. turvallisuusluokan sisällä erillisiin verkko-alueisiin (vyöhykkeet, segmentit). 2) Verkkoalueiden välistä liikennettä rajoitetaan ja ympäristöön sisäänpäin tulevaan liikenteeseen noudatetaan default-deny sääntöä. 3) Tietojenkäsittely-ympäristössä on varauduttu yleisiin verkkohyökkäyksiin.	TihL 13 § 1 mom; TLA 11 § 1 mom 1 ja 2 k	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02		I-02	H1, H2, T1, T2, T3
Tekninen turvallisuus	TEK-02.1	**Tietoliikenneverkon vyöhykkeistäminen - vähimpien oikeuksien periaate**	Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien periaatteen mukaisesti ko. turvaluokan sisällä.	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.	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).	TLA 11 § 1 mom 1 ja 2 k	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02	TEK-03	I-02	H1, H2, T1, T2, T3

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-03	**Suodatus- ja valvontajärjestelmien hallinnointi**	Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan.	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).		TihL 13 § 1 mom; TLA 11 § 1 mom 2 k	ISO/IEC 27002:2022 8.21, 8.23		I-03	H1, H2, T2
Tekninen turvallisuus	TEK-03.1	**Suodatus- ja valvontajärjestelmien hallinnointi - vastuutus ja organisointi**	Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen, poistaminen ja valvonta on vastuutettu ja organisoitu.			TihL 4 § 2 mom 1 k; TLA 11 § 1 mom 2 k	ISO/IEC 27002:2022 5.35, PiTuKri MH-01		I-03, I-16	H1, H2, T1, T2, T3, T4, T9, T11
Tekninen turvallisuus	TEK-03.2	**Suodatus- ja valvontajärjestelmien hallinnointi - dokumentointi**	Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.			TihL 5 § 2 mom; TLA 11 § 1 mom 2 k		HAL-09	I-03	H1, H2, T2
Tekninen turvallisuus	TEK-03.3	**Suodatus- ja valvontajärjestelmien hallinnointi - tarkastukset**	Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.			TihL 13 § 1 mom; TLA 11 § 1 mom 2 k	ISO/IEC 27002:2022 8.32		I-03	H1, H2, T2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-04	**Hallintayhteydet**	Hallintapääsy tapahtuu rajattujen, hallittujen ja valvottujen pisteiden kautta.	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	Rajattu pääsy tulee toteuttaa esimerkiksi hyppykoneiden, hallintaportaalien ja vastaavien menettelyiden kautta.	TihL 13 § 1 mom, 14 § 1 mom; TLA 11 § 1 mom	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	TEK-12	I-04	H1, H2, T1, T2, T3, T5, T8

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-04.1	**Hallintayhteydet - vahva tunnistaminen julkisessa verkossa**	Hallintapääsyn julkisesta verkosta tai muun käytettävän etähallintaratkaisun tulee edellyttää vahvaa, vähintään kahteen todennustekijään pohjautuvaa käyttäjätunnistusta.	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.	Hallintayhteydet julkisesta verkosta edellyttävät esimerkiksi VPN-yhteyden muodostamista, jossa vähintään joko käyttäjä tai laite tunnistetaan vahvasti.	TihL 13 § 1 mom; TLA 11 § 1 mom 5 k	ISO/IEC 27002:2022 8.2; PiTuKri IP-03		I-04	H1, H2, T1, T2, T3, T5, T8
Tekninen turvallisuus	TEK-04.2	**Hallintayhteydet - hallintayhteyksen salaaminen**	Hallintaliikenne julkisessa verkossa on salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia.			TihL 13 § 1 mom; TLA 11 § 1 mom 4 ja 7 k	ISO/IEC 27002:2022 8.24		I-04	H1, H2, T1, T2, T3, T5, T8
Tekninen turvallisuus	TEK-04.3	**Hallintayhteydet - vähimmät oikeudet**	Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti.			TihL 16 §; TLA 11 § 1 mom 3 k	ISO/IEC 27002:2022 8.20	HAL-2.1	I-04	H1, H2, T1, T2, T3, T5, T8
Tekninen turvallisuus	TEK-04.4	**Hallintayhteydet - henkilökohtaiset tunnukset**	Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia.		Mikäli henkilökohtaisten tunnusten käyttäminen ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille.	TihL 13 § 1 mom, 16 §; TLA 11 § 1 mom 3 ja 5 k	PiTuKri IP-02		I-04	H1, H2, T1, T2, T3, T5, T8
Tekninen turvallisuus	TEK-04.5	**Hallintayhteydet - yhteyksien rajaaminen turvallisuusluokittain**	Hallintayhteydet on rajattu turvallisuusluokittain, ellei käytössä ole turvallisuusluokka huomioon ottaen riittävän turvallista yhdyskäytäväratkaisua.		Tietojenkäsittely-ympäristöön ei ole yhteenliitäntää hallintayhteyksille muiden turvallisuusluokkien ympäristöistä ilman turvallisuusluokan huomioon ottaen riittävän turvallista yhdyskäytäväratkaisua.	TLA 11 § 1 mom 1 k		TEK-01	I-04	H1, H2, T1, T2, T3, T5, T8
Tekninen turvallisuus	TEK-04.6	**Hallintayhteydet - turvallisuusluokiteltua tietoa sisältävät hallintayhteydet**	Hallintaliikenteen sisältäessä turvallisuusluokiteltua tietoa ja kulkiessa matalamman turvallisuusluokan ympäristön kautta, turvallisuusluokitellut tiedot on salattu riittävän turvallisella salaustuotteella.		Ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään vain riittävän turvallisen salausratkaisun kautta tilanteissa, joissa hallintaliikenne kulkee matalamman turvallisuusluokan ympäristön kautta.	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §			I-04, I-12	H1, H2, T1, T2, T3, T5, T8

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-04.7	**Hallintayhteydet - salaaminen turvallisuusluokan sisällä**	Hallintaliikenteen kulkiessa ko. turvallisuusluokan sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella.		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.	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §			I-04	H1, H2, T1, T2, T3, T5, T8
Tekninen turvallisuus	TEK-04.8	**Hallintayhteydet - TL III**	Turvallisuusluokan III käsittely-ympäristöjen etähallinta tulee suorittaa turva-alueelta.	Turvallisuusluokan III sekä muissa kriittisissä käsittely-ympäristöissä edellytetään etähallinnan teknistä sitomista hyväksyttyyn etähallintalaitteistoon (esim. laitetunnistus).	Etähallinta on estetty teknisesti muita kuin hyväksyttyjä laitteita käyttäen.	TLA 10 § 3 mom 1 k			I-18	H1, H2, T2
Tekninen turvallisuus	TEK-05	**Langaton tiedonsiirto**	Langattomassa tiedonsiirrossa tietoliikenne salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia.	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.	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.	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §	PiTuKri SA-01; ISO/IEC 27002:2022 8.22		I-05, I-08, I-09, I-12, I-15, I-16	H1, H2, T1, T2, T5
Tekninen turvallisuus	TEK-05.1	**Langaton tiedonsiirto - salaaminen**	Langattomassa tiedonsiirrossa tietoliikenne salataan kyseiselle turvaluokalle riittävän turvallisella salausratkaisulla.		TL IV -tasolla vaatimus voidaan toteuttaa esimerkiksi tunneloimalla liikenne riittävän turvallisella VPN-ratkaisulla tai käyttämällä hyväksyttyä sovellustason salausratkaisua.	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §	ISO/IEC 27002:2022 8.24; PiTuKri SA-01		I-05	H1, H2, T1, T2, T5

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-06	**Kasautumisvaikutus**	Kasautumisvaikutus on huomioitu tietojenkäsittely-ympäristön suojaamisessa.	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.		TihL 15 § 2 mom, 13 § 1 mom	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01	HAL-04.3		H1, H2
Tekninen turvallisuus	TEK-07	**Pääsyoikeuksien hallinnointi**	Tietojärjestelmien käyttöoikeudet on määritelty.	Käyttöoikeuksien hallinnan keskeinen tavoite on pystyä varmistumaan siitä, että vain oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään suojattavaan tietoon.	1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t). 2) Järjestelmän käyttäjistä on olemassa lista.	TihL 16 §; TLA 8 §, 11 § 1 mom 3 k	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01	HAL-14, HAL-14.1, HAL-19	I-06	H1, H2, T2
Tekninen turvallisuus	TEK-07.1	**Pääsyoikeuksien hallinnointi - pääsyoikeuksien myöntäminen**	Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käyttötarpeesta on varmistuttu.	Käyttöoikeuksien taustalla on suositeltavaa olla jokin sopimus tai muu dokumentoitu peruste, joka voidaan todentaa (esim. työsuhde, sopimus toteutettavasta työstä ympäristössä).	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).	TihL 16 §; TLA 8 §, 11 § 1 mom 3 k	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01	HAL-14, HAL-10.1	I-06	H1, H2, T2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-07.2	**Pääsyoikeuksien hallinnointi - pääsyoikeuksien rajaaminen**	Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.	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 tai 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 tai 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 tai 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,	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.	TihL 13 § 1 mom, 15 § 1 mom 1 k, 16 §; TLA 8 §, 11 §:n 1 mom 3 ja 4 k	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01, SA-03, KT-03		I-06	H1, H2, T2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-07.3	**Pääsyoikeuksien hallinnointi - pääsyoikeuksien ajantasaisuus**	Käyttöoikeudet on pidettävä ajantasaisina.		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.	TihL 16 §	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01	HAL-14.1	I-06	H1, H2, T2
Tekninen turvallisuus	TEK-07.4	**Pääsyoikeuksien hallinnointi - turvallisuusluokiteltujen tietojen erottelu**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TLA 11 § 1 mom 1 k			I-06	H1, H2, T2
Tekninen turvallisuus	TEK-07.5	**Pääsyoikeuksien hallinnointi - TL III**	Alikriteeri tarkentaa pääkriteerin vaatimusta.	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.	Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi.	TihL 13 § 1 mom; TLA 11 § 1 mom 3 k		HAL-2.1	I-06, I-12	H1, H2, T2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-08	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen**	Tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti.		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), tunnisteväline illä (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	TihL 14 §; TLA 11 § 1 mom 5 k	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.	HAL-19	I-07	H1, H2, T2, T4

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-08.1	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen**	Kaikki käyttäjät tunnistetaan ja todennetaan yksilöllisillä henkilökohtaisilla käyttäjätunnisteilla.			TihL 13 § 1 mom, 16 §; TLA 11 § 1 mom 3 ja 5 k	PiTuKri IP-02		I-07	H1, H2, T2, T4
Tekninen turvallisuus	TEK-08.2	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen**	Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti.			TihL 13 § 1 mom, 14 §, 16 §; TLA 11 § 1 mom 3 ja 5 k	ISO/IEC 27002:2022 8.5; PiTuKri IP-02		I-07	H1, H2, T2, T4
Tekninen turvallisuus	TEK-08.3	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen**	Käyttäjätunnukset lukittuvat tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin.			TihL 13 § 1 mom; TLA 7 §	ISO/IEC 27002:2022 8.5; PiTuKri IP-02		I-07	H1, H2, T2, T4
Tekninen turvallisuus	TEK-08.4	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen - TL IV**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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), tunnisteväline illä (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.	TLA 11 § 1 mom 5 k	ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02		I-07	H1, H2, T2, T4

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-08.5	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen - TL III**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TLA 11 § 1 mom 5 k			I-07	H1, H2, T2, T4
Tekninen turvallisuus	TEK-09	**Tietojärjestelmien fyysinen turvallisuus**	Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.	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.		TihL 15 § 2 mom; TLA 10 §	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	FYY-7.1, HAL-19	I-17	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-10	**Järjestelmäkovennus**	Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.	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.	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.	TihL 13 § 1 ja 4 mom; TLA 11 § 1 mom 6 k	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		I-08	H1, H2, T1, T2, T3

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-10.1	**Järjestelmäkovennus - käytössä olevien palveluiden minimointi**	Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut.	Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.		TihL 13 § 1 mom; TLA 11 § 1 mom 6 k			I-08	H1, H2, T1, T2, T3
Tekninen turvallisuus	TEK-10.2	**Järjestelmäkovennus - kovennusten varmistaminen koko elinkaaren ajan**	Kovennusten voimassaolosta ja vaikuttavuudesta huolehditaan koko tietojärjestelmän elinkaaren ajan.			TihL 13 § 1 ja 4 mom; TLA 11 § 1 mom 6 k			I-08	H1, H2, T1, T2, T3
Tekninen turvallisuus	TEK-10.3	**Järjestelmäkovennus - turvallisuusluokitellut ympäristöt**	Alikriteeri tarkentaa pääkriteerin vaatimusta.	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.	Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan toteuttaa siten, että kohtien 1-4 lisäksi kovennuksiin käytetään useita kovennusohjeita ja kovennusohjeiden toteutuksen tiukkuutta kiristetään.	TihL 13 § 1 ja 4 mom; TLA 11 § 1 mom 6 k			I-08	H1, H2, T1, T2, T3
Tekninen turvallisuus	TEK-11	**Haittaohjelmilta suojautuminen**	Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.	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).	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.	TihL 13 § 1 mom, 15 § 1 mom; TLA 11 § 1 mom 2 ja 3 k	ISO/IEC 27002:2022 8.7; PiTuKri JT-04		I-09	H1, H2, T1, T2, T3

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-11.1	**Haittaohjelmilta suojautuminen - TL IV**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan lisäksi: 1) On tunnistettu järjestelmät, joissa haittaohjelman torjuntaohjelmistoilla pystytään saamaan lisäsuojausta.	TLA 11 § 1 mom 2 k	ISO/IEC 27002:2022 8.7; PiTuKri JT-04		I-09	H1, H2, T2, T4
Tekninen turvallisuus	TEK-11.2	**Haittaohjelmilta suojautuminen - TL III**	Alikriteeri tarkentaa pääkriteerin vaatimusta.	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.	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.	TLA 11 § 1 mom 2 k			I-09	H1, H2, T2, T4
Tekninen turvallisuus	TEK-11.3	**Haittaohjelmilta suojautuminen - TL II**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, huomioidaan lisäksi yleensä turvallisuusluokasta II lähtien myös muistivälineen kontrolleritason räätälöinnin uhat.	TLA 11 § 1 mom 2 ja 5 k			I-09	H1, H2, T2, T4

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-12	**Turvallisuuteen liittyvien tapahtumien jäljitettävyys**	Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyden varmistamiseksi.	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 luovutusloikeille 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.	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).	TihL 17 §, 15 §; TLA 7 §,14 §	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	HAL-7.1	I-10	H1, H2, T2, T4

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-12.1	**Turvallisuuteen liittyvien tapahtumien jäljitettävyys - tietojen luovutukset**	Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.	Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.		TihL 17 §, 15 §; TLA 7 §, 14 §		HAL-07.1, TSU-18	I-10	H1, H2, T2, T4
Tekninen turvallisuus	TEK-12.2	**Turvallisuuteen liittyvien tapahtumien jäljitettävyys - TL III**	Turvallisuusluokan II–III tiedon käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi).	Turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvien lokitietojen säilytyksestä on annettu suositus VM 2021:5: "Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä".	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.	TihL 17 §, 15 §; TLA 7 §, 14 §	Valtiovarainministeriö: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5) 7.9.		I-10	H1, H2, T2, T4
Tekninen turvallisuus	TEK-12.3	**Turvallisuuteen liittyvien tapahtumien jäljitettävyys - TL I**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TihL 17 §, 15 §; TLA 7 §, 14 §			I-10	H1, H2, T2, T4

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-13	**Poikkeamien havainnointikyky ja toipuminen**	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.	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.	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.	TihL 13 § 1 mom, 15 § 1 mom, 17 §; TLA 7 §, 11 § 1 mom 2 k	ISO/IEC 27002:2022 5.25, 5.26, 8.15, 8.16; PiTuKri TT-02, JT-01, TJ-05	TEK-17	I-11, T-07, T-12	H1, H2, T9
Tekninen turvallisuus	TEK-13.1	**Poikkeamien havainnointikyky ja toipuminen - poikkeamien havainnointi lokitiedoista**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		Suositellaan toteuttamaan menettely, jolla kerätyistä tallenteista ja tilannetiedosta (esimerkiksi muutokset lokikertymissä) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan).	TihL 13 § 1 mom, 15 § 1 mom, 17 §; TLA 7 §, 11 § 1 mom 2 k	ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05		I-11	H1, H2, T9

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-13.2	**Poikkeamien havainnointikyky ja toipuminen - TL IV**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TihL 13 § 1 mom, 15 § 1 mom, 17 §; TLA 7 §, 11 § 1 mom 2 k	ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05		I-11	H1, H2, T9
Tekninen turvallisuus	TEK-13.3	**Poikkeamien havainnointikyky ja toipuminen - TL I**	Käyttäjien ja ylläpitäjien toimintaa seurataan poikkeuksellisen toiminnan havaitsemiseksi.		Turvallisuusluokan I tietojen käsittelyssä suositellaan tehostettua poikkeamien havainnointikykyä, painottaen muun muassa tietojenkäsittely-ympäristön käyttäjien ja ylläpitäjien toiminnan seurantaa.	TihL 13 § 1 mom, 15 § 1 mom, 17 §; TLA 7 §, 11 § 1 mom 2 k	ISO/IEC 27002:2022 8.16; PiTuKri JT-01, TJ-05		I-11	H1, H2, T9

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-14	**Ohjelmistojen turvallisuuden varmistaminen**	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.	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	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.	TihL 13 § 1 mom, 15 § 1 mom; TLA 11 § 1 mom 2, 3, 4, 5 ja 6 k	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	HAL-16	I-13	H1, H2, T2, T3, T4

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-15	**Hajasäteily (TEMPEST) ja elektroninen tiedustelu**	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.	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.	1) Hajasäteilyyn liittyvät riskit on tunnistettu ja arvioitu. 2) Turvatoimet tai korvaavat menettelyt on mitoitettu riskeihin, tiedon turvallisuusluokkaan ja hyväksyttävään jäännösriskitasoon.	TLA 11 § 2 mom	Traficom: Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet; ISO/IEC 27002:2022 7.12	FYY-5.6	I-14	H1, H2, T10
Tekninen turvallisuus	TEK-15.1	**Hajasäteily (TEMPEST) ja elektroninen tiedustelu - TL II**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		On toteutettu turvatoimet, jotka on mitoitettu riskeihin ja tiedon turvallisuusluokkaan. Kohteen hajasäteilyn vastatoimien riittävyys voidaan todentaa vyöhykemittauksella tai suojatun tilan mittauksella.	TLA 11 § 2 mom			I-14	H1, H2, T10
Tekninen turvallisuus	TEK-15.2	**Hajasäteily (TEMPEST) ja elektroninen tiedustelu - TL I**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TLA 11 § 2 mom			I-14	H1, H2, T10

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-16	**Tiedon salaaminen**	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.	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.	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.	TihL 13 § 1 mom, 14 §; TLA 11 § 1 mom 7 k, 12 §	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	TEK-01	I-01, I-12, I-15, I-18	H1, H2, T1, T2, T5
Tekninen turvallisuus	TEK-16.1	**Tiedon salaaminen - salaaminen turvallisuusalueen sisällä**	Kun salassa pidettävää tietoa siirretään viranomaisen sisäisessä verkossa, voidaan käyttää alemman tason salausta tai salaamatonta tiedonsiirtoa riskinhallintaprosessin tulosten perusteella.			TihL 13 § 1 mom; 14 §; TLA 11 § 1 mom 7 k, 12 §	ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03	FYY-7.1	I-15	H1, H2, T1, T2, T5

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-16.2	**Tiedon salaaminen - turvallisuusluokitellun tiedon siirto turvallisuusalueiden ulkopuolella**	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.	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.	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).	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §	ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03	FYY-7.1	I-01, I-12, I-15, I-18, F-08.1	H1, H2, T1, T2, T5
Tekninen turvallisuus	TEK-16.3	**Tiedon salaaminen - turvallisuusluokitellun tiedon siirto turvallisuusalueiden sisällä**	Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen.		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).	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §		FYY-7.1	I-15	H1, H2, T1, T2, T5

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-16.4	**Tiedon salaaminen - TL III**	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.			TLA 10 §		FYY-7.1	F-04, I-12, I-17, I-18	H1, H2, T1, T2, T5
Tekninen turvallisuus	TEK-16.5	**Tiedon salaaminen - TL I**	Alikriteeri tarkentaa pääkriteerin vaatimusta.	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.	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.	TihL 14 §; TLA 11 § 1 mom 7 k, 12 §			I-15	H1, H2, T1, T2, T5

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-17	**Muutoshallintamenettelyt**	Tietojenkäsittely-ympäristöön tehtäviin muutoksiin on käytössä turvallisuuden huomioiva muutostenhallintamenettely.	Tietojenkäsittely-ympäristön tietoturvallisuuden ja muutosten luotettava hallinta edellyttää, että ympäristön tekninen rakenne ja esimerkiksi kaikki siihen kuuluvat laitteistot ja ohjelmistot ovat tiedossa. Tietojärjestelmien asetuksien ja toiminnan muuttumista tulee valvoa ja havaittujen muutosten tulee johtaa niiden oikeellisuuden tarkistamiseen. Ajantasaista kirjanpitoa vasten tarvittavat muutokset kyetään koko elinkaaren ajan kohdistamaan täsmällisesti, muutosten vaikutukset ovat helpommin ennustettavissa ja ympäristön turvallisuuden tarkastelu on mahdollista suorittaa. Kirjanpidon toteuttamisessa voi hyödyntää esimerkiksi verkkokuvia, laite- ja ohjelmistokomponenttiluetteloita sekä konfiguraatiotietokantoja. Tietojenkäsittely-ympäristön tietoturvallisuudesta tulee pystyä varmistumaan koko elinkaaren ajan. Tämä edellyttää muutostarpeiden jatkuvaa seurantaa sekä säännöllisiä muutoksia. Muutostarpeita voi seurata esimerkiksi tietojenkäsittely-ympäristön järjestelmien elinkaaren päättymisestä tai nykyisten suojausten kyvyttömyydestä vastata uusiin hyökkäysmenetelmiin. Esimerkiksi ohjelmistojen päivitykset voivat aiheuttaa odottamattomia seurauksia, kuten turvallisuusasetusten ja käyttöoikeuksien muuttumista tai uusien turvattomien palvelujen mukaantuloa tietojenkäsittely-ympäristöön. Haitallisia seurauksia voidaan pyrkiä ennaltaehkäisemään esimerkiksi kattavalla testauksella ja muutoslokien (tyypillisesti esim. changelog, readme) tarkastelulla. Haitallisia seurauksia voidaan pyrkiä havainnoimaan 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 menetelmää, tulisi sinettien eheyden tarkastamiseen olla säännöllinen prosessi. Luvattomien muutosten tai laitteistojen tarkasteluun hyväksyttävissä oleva tarkastustiheys riippuu kyseessä olevassa 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 otettava huomioon, että päätelaitteisiin ei saa kytkeä muita kuin kyseisen turvallisuusluokan tietojenkäsittely-ympäristöön hyväksyttyjä oheislaitteita (esim. näyttö, näppäimistö, hiiri) ja medioita (esimerkiksi vain kyseiseen ympäristöön hyväksytty USB-muisti). Erityisesti tilanteissa, joissa päätelaitetta käytetään matalamman turvallisuusluokan fyysisessä tilassa, ei yleensä ole mahdollista käyttää ko. tilassa säilytettäviä oheislaitteita tai medioita.	1) Tietojenkäsittely-ympäristön kokoonpanosta on olemassa ajantasainen kirjanpito. Kirjanpidolla tarkoitetaan laitteisto- ja ohjelmistokirjanpitoa, sekä tietoa turvallisuuteen vaikuttavista konfiguraatioista ja menettelyistä. 2) Tietojenkäsittelyyn ja tietojenkäsittely-ympäristöön liittyviin muutoksiin on käytössä muutostenhallintamenettely. Muutokset ovat jäljitettävissä. 3) On olemassa menetelmät, joilla varmistetaan tietojenkäsittely-ympäristön turvallisuustason säilyminen tehtyjen muutosten yhteydessä.	TihL 13 §, 15 §	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		I-03, I-05, I-16, I-17, I-18, T-04, T-12	H1, H2, T1, T3, T4, T9, T11
Tekninen turvallisuus	TEK-17.1	**Muutoshallintamenettelyt - uudelleenarviointi**	Tietoturvallisuutta koskevat tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.			TihL 13 § 1 mom			I-16	H1, H2, T1, T3, T4, T9, T11

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-17.2	**Muutoshallintamenettelyt - dokumentointi**	Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten- ja asetustenhallintaprosessia.			TihL 5 § 2 mom	ISO/IEC 27002:2022 8.9, 8.32		I-16	H1, H2, T1, T3, T4, T9, T11
Tekninen turvallisuus	TEK-17.3	**Muutoshallintamenettelyt - TL IV**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TihL 5 § 2 mom, 13 § 1 mom	ISO/IEC 27002:2022 5.9, 8.8		I-16	H1, H2, T1, T3, T4, T9, T11
Tekninen turvallisuus	TEK-17.4	**Muutoshallintamenettelyt - TL II**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		1) Laitteistot suojataan luvattomien laitteiden (näppäilynauhoittimet, langattomat lähettimet ml. mobiililaitteet ja vastaavat) liittämistä vastaan.	TLA 11 § 1 mom 2 ja 5 k			I-16	H1, H2, T1, T3, T4, T9, T11
Tekninen turvallisuus	TEK-18	**Etäkäyttö**	Etäkäytössä käyttäjät ohjeistettu ja tunnistetaan riittävän luotettavasti.	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.	1) Etäkäytössä käyttäjät tunnistetaan luotettavasti. 2) Etäkäyttö on ohjeistettu ja sitä valvotaan.	TihL 4 § 2 mom, 13 § 1 mom; TLA 10 § 1 mom	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	HAL-12, HAL-13, HAL-19	I-17, I-18	H1, H2, T7

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-18.1	**Etäkäyttö - tietojen ja tietoliikenteen salaaminen**	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.	Siirrettävien tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) osalta voidaan sallia salaamattomien laitteiden käyttö siinä tapauksessa, että tietovälineitä ei koskaan jätetä valvomatta hyväksyttyjen turvallisuusalueen ulkopuolella.	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.	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §, 11 §, 12 §, 13 §	ISO/IEC 27002:2022 7.9, 7.10, 8.1	FYY-7.1	I-18	H1, H2, T2
Tekninen turvallisuus	TEK-18.2	**Etäkäyttö - turvallisuusluokitettujen tietojen ja tietoliikenteen salaaminen**	Turvallisuusalueen ulkopuolella etäkäytössä käytettävät päätelaitteet, muistivälineet ja tietoliikenneyhteydet ovat suojattu käyttäen ko. turvallisuusluokan huomioiden riittävän turvallisia salausratkaisuja.	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.	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.	TihL 13 § 1 mom, 15 § 2 mom; TLA 10 §, 11 §, 12 §, 13 §	ISO/IEC 27002:2022 7.9, 7.10, 8.1	FYY-7.1	I-18	H1, H2, T2
Tekninen turvallisuus	TEK-18.3	**Etäkäyttö - käyttäjien vahva tunnistaminen**	Etäkäytössä järjestelmien käyttäjät tunnistetaan käyttäen vahvaa, vähintään kahteen todennustekijään perustuvaa käyttäjätunnistusta.			TLA 10 §, 11 § 1 mom 5 k			F-04, I-18	H1, H2, T2
Tekninen turvallisuus	TEK-18.4	**Etäkäyttö - hyväksytyt laitteet**	Etäkäytössä käytetään vain käyttöympäristöön hyväksyttyjä ja tunnistettuja laitteita.		Vain käyttöympäristöön hyväksyttyjä laitteita ja etäyhteyksiä käytetään.	TLA 10 §, 11 § 1 mom 5 k			F-04, I-18	H1, H2, T2
Tekninen turvallisuus	TEK-18.5	**Etäkäyttö - turvallisuusluokitellun tiedon käyttö julkisella paikalla**	Turvallisuusluokiteltuja tietoja ei lueta tai muuten käsitellä matkalla tai julkisilla paikoilla.			TLA 10 § 1 mom, 13 §		FYY-7.1	I-18	H1, H2, T2
Tekninen turvallisuus	TEK-18.6	**Etäkäyttö - laitetunnistus**	Alikriteeri tarkentaa pääkriteerin vaatimusta.	Turvallisuusluokkien III ja II käsittely-ympäristöissä sekä muissa kriittisissä käsittely-ympäristöissä edellytetään käytön teknistä sitomista hyväksyttyyn etäkäyttölaitteistoon (esim. laitetunnistus).	Etäkäyttö on estetty teknisesti muita kuin hyväksyttyjä laitteita käyttäen.	TLA 10 §, 11 § 1 mom 5 k			I-18	H1, H2, T2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-18.7	**Etäkäyttö - TL III**	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.			TLA 10 § (TL III)			I-18	H1, H2, T2
Tekninen turvallisuus	TEK-18.8	**Etäkäyttö - etäkäyttö turvallisuusalueella**	Järjestelmien etäkäyttö rajataan toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle.	Tiedon käsittely edellyttää fyysisesti suojattua turvallisuusaluetta tai korvaavia menettelyjä, joilla saavutetaan vastaavat fyysisen turvallisuuden olosuhteet.		TLA 10 § (TL II)			I-18	H1, H2, T2
Tekninen turvallisuus	TEK-18.9	**Etäkäyttö - TL I**	Alikriteeri tarkentaa pääkriteerin vaatimusta.	Turvallisuusluokan I tietoa saa säilyttää tai muutoin käsitellä ainoastaan turva-alueilla (TLA, 10 §), mikä asettaa rajoitteet myös etäkäytön mahdollisuuksille.		TLA 10 § (TL I)			I-18	H1, H2, T2
Tekninen turvallisuus	TEK-19	**Ohjelmistohaavoittuvuuksien hallinta**	Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.	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.	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.	TihL 13 §; TLA 11 § 1 mom 2 k	ISO/IEC 27002:2022 8.8; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-04	HAL-16, HAL-16.1	I-19	H1, H2, T2, T3

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-19.1	**Ohjelmistohaavoittuvuuksien hallinta - TL IV**	Tietojenkäsittely-ympäristön laitteet tarkastetaan kattavasti ohjelmistohaavoittuvuuksien varalta vähintään vuosittain ja merkittävien muutosten yhteydessä.		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.	TihL 13 §; TLA 11 § 1 mom 2 k	ISO/IEC 27002:2022 8.8; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-04		I-19	H1, H2, T2, T3
Tekninen turvallisuus	TEK-19.2	**Ohjelmistohaavoittuvuuksien hallinta - TL III**	Tietojenkäsittely-ympäristön laitteet tarkastetaan kattavasti ohjelmistohaavoittuvuuksien varalta vähintään puolivuosittain ja merkittävien muutosten yhteydessä.		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.	TihL 13 §; TLA 11 § 1 mom 2 k			I-19	H1, H2, T2, T3
Tekninen turvallisuus	TEK-20	**Varmuuskopiointi**	Varmistus- ja palautusprosessit on suunniteltu, toteutettu, testattu ja kuvattu siten, että ne vastaavat lainsäädännön ja toiminnan vaatimuksia.	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 palautuminen 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.	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.	TihL 13 § 1 mom, 15 § 1 mom; TLA 2 § 2 mom, 7 §, 11 § 1 mom 4 k	ISO/IEC 27002:2022 8.13; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 5); PiTuKri KT-03	VAR-09	I-20	H1, H2, T1, T2
Tekninen turvallisuus	TEK-20.1	**Varmuuskopiointi -TL IV**	Alikriteeri tarkentaa pääkriteerin vaatimusta.	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).	Käsiteltäessä samalla varmistusjärjestelmällä tarkastusoikeuden varaavien eri omistajien tietoja, tarkastusoikeuden mahdollistavat erottelumenettelyt on toteutettava ko. turvallisuusluokan mukaisesti varmistusjärjestelmän liittymien ja tallennemedioiden osalta.	TihL 13 § 1 mom, 16 §; TLA 7 §, 10 § 1 mom, 11 § 1 mom 3 k	ISO/IEC 27002:2022 8.13; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 5); PiTuKri KT-03		I-06, I-20	H1, H2, T1, T2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-20.2	**Varmuuskopiointi - varmuuskopioiden rekisteröinti ja käsittelyn seuranta**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		Varmuuskopioista on rekisterit ja varmuuskopioiden käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai tietoon (esimerkiksi dokumentin osaksi).	TLA 14 §			F-08.3, I-20	H1, H2, T1, T2
Tekninen turvallisuus	TEK-21	**Sähköisessä muodossa olevien tietojen tuhoaminen**	Sähköisessä muodossa olevien tietojen tuhoaminen on järjestetty luotettavasti. Salassa pidettävien tietojen tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.	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	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.	TihL 21 § 2 mom; TLA 15 §	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	FYY-11, FYY-11.1, FYY-11.2, FYY-11.3	T-12, F-08.3, F-08.4, I-21	H1, H2, T2
Tekninen turvallisuus	TEK-21.1	**Sähköisessä muodossa olevien tietojen tuhoaminen - arkistointi**	Tietojen arkistointivelvollisuus on huomioitu tiedon elinkaaren hallinnassa.			TihL 21 §				H1, H2
Tekninen turvallisuus	TEK-21.2	**Sähköisessä muodossa olevien tietojen tuhoaminen - pilvipalveluissa olevan tiedon tuhoaminen**	Alikriteeri tarkentaa pääkriteerin vaatimusta.	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.		TihL 21 § 2 mom	ISO/IEC 27002:2022 5.23; PiTuKri SA-03			H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-21.3	**Sähköisessä muodossa olevien tietojen tuhoaminen - TL IV**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TihL 21 § 2 mom; TLA 15 §	Traficom: Kiintolevyjen elinkaaren hallinta (26.10.2016); Tiedonhallintalautakunta: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5)	FYY-11.1, FYY-11.2, FYY-11.3	I-21	H1, H2, T2
Tekninen turvallisuus	TEK-21.4	**Sähköisessä muodossa olevien tietojen tuhoaminen - toisen viranomaisen laatimat tiedot**	Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle.			TLA 15 § 2 mom			I-21	H1, H2, T2
Tekninen turvallisuus	TEK-21.5	**Sähköisessä muodossa olevien tietojen tuhoaminen - tuhoamisen suorittaja**	Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö.			TLA 15 § 2 mom			I-21	H1, H2, T2
Tekninen turvallisuus	TEK-21.6	**Sähköisessä muodossa olevien tietojen tuhoaminen - TL I**	Alikriteeri tarkentaa pääkriteerin vaatimusta.		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.	TLA 15 §			I-21	H1, H2, T2
Tekninen turvallisuus	TEK-22	**Tietojärjestelmien saatavuus**	Viranomaisen on varmistettava tietojärjestelmien saatavuus koko niiden elinkaaren ajan.	Saatavuusvaatimusten toteutuksen tulee huomioida tietojärjestelmältä edellytettävä kuormituksen kesto, vikasietoisuus ja palautumisaika.	Saatavuusvaatimukset on tunnistettu. On tunnistettu vähintään pisin aika, jonka järjestelmä voi olla pois käytöstä, palautusaikatavoite ja palautuspistetavoite.	TihL 13 § 1 mom, 15 § 1 mom 4 k	ISO/IEC 27002:2022 8.6, 8.14	VAR-02		H1, H2
Tekninen turvallisuus	TEK-22.1	**Tietojärjestelmien saatavuus - saatavuutta suojaavat menettelyt**	Saattavuutta suojaavien menettelyiden toteutus on suhteutettu palautusaikatavoitteeseen.		Saatavuutta suojaavat menettelyt on toteutettu järjestelmäkohtaisesti räätälöidyillä suojauksilla. Suojauksiin voi sisältyä esimerkiksi keskeisten verkkoyhteyksien, laitteistojen ja sovellusten ajoympäristöjen kahdentamiset.	TihL 13 § 1 mom, 15 § 1 mom 4 k	ISO/IEC 27002:2022 5.30	VAR-02, VAR-06, VAR-07, VAR-08		H1, H2
Tekninen turvallisuus	TEK-22.2	**Tietojärjestelmien saatavuus - palveluiden valvonta**	Palveluiden ja tietojärjestelmien saatavuutta seurataan ja valvotaan niiden kriittisyyden edellyttämällä tasolla.		1) Jos palvelulla on saatavuus vaatimuksia, seurataan sen saatavuutta valvontajärjestelmällä. 2) Valvontajärjestelmän tulee lähettää hälyttää havaitusta saatavuuspoikkeamista.	TihL 13 § 1 mom, 15 § 1 mom 4 k	ISO/IEC 27002:2022 8.16	HAL-07		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tekninen turvallisuus	TEK-23	**Tietojärjestelmien toiminnallinen käytettävyys**	Viranomainen on varmistanut tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden.	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.	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.	TihL 13 § 2 mom		HAL-17, HAL-17.1		H1, H2
Varautuminen ja jatkuvuudenhallinta	VAR-01	**Varautumista ohjaava lainsäädäntö**	Organisaatio on tunnistanut toimintaansa ja palveluihinsa liittyvät ICT-varautumista ohjaavan kansallisen ja EU-lainsäädännön sekä muut ICT-varautumiseen liittyvät normit.	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.	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.	TihL 4 § 2 mom 2 k; 13 § 1 mom	PiTuKri TJ-07, PiTuKri EE-02	HAL-05		H1, H2
Varautuminen ja jatkuvuudenhallinta	VAR-02	**Jatkuvuusvaatimusten määrittely**	Toiminnan ja siihen liittyvien olennaisten palvelujen ja tietojärjestelmien jatkuvuusvaatimukset on määritelty.	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.	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.	TihL 4 § 2 mom 1 k, 13 § 1 ja 2 mom, 15 § 1 mom.	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6 ja luku 11; ISO/IEC 27002:2022 5.30	HAL-05		H1, H2
Varautuminen ja jatkuvuudenhallinta	VAR-02.1	**Jatkuvuusvaatimusten määrittely - palveluiden siirrot**	Jatkuvuusvaatimuksissa on huomioitu palveluiden kotiuttamiset ja siirrot toiselle palveluntarjoajalle.	Palvelua hankittaessa tulee huomioida, että palvelua voi olla hankala kotiuttaa ja toimittajalukkoon jäänyttä palvelua vaikea siirtää toiselle palveluntarjoajalle. Erityisesti vaatimus tulee huomioida hankittaessa pilvipalveluita.		TihL 4 § 2 mom 1 k, 13 § 1, 2 ja 4 mom, 15 § 1 mom.	Pilvipalveluiden soveltamisohje 2020:73; ISO/IEC 27002:2022 5.23	HAL-05		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Varautuminen ja jatkuvuudenhallinta	VAR-03	**Jatkuvuussuunnitelmat**	Jatkuvuussuunnitelmat on laadittu ja otettu käyttöön.	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.	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.	TihL 4 § 2 mom 2 k,15 §	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11; ISO/IEC 27002:2022 5.23			H1, H2
Varautuminen ja jatkuvuudenhallinta	VAR-03.1	**Jatkuvuussuunnitelmien testaus ja harjoittelu**	Jatkuvuussuunnitelmia testataan ja harjoitellaan säännöllisesti.	Harjoittelemalla testataan suunnitelmien toimivuus erilaisissa tilanteissa. Havaintoja käytetään suunnitelmien kehittämiseen.	Organisaatiot vastaavat omasta harjoitustoiminnastaan ja määrittelevät jatkuvuussuunnitelmien testaamisen käytännöt. Organisaatio harjoittelee sisäisesti sekä valtakunnallisissa että alueellisissa ja paikallisissa harjoituksissa toiminnan edellyttämässä laajuudessa.	TihL 4 § 2 mom, 13 § 2 mom; 15 §	ISO/IEC 27002:2022 5.23		I-13	H1, H2, T2, T3, T4
Varautuminen ja jatkuvuudenhallinta	VAR-04	**Resurssit ja osaaminen**	Henkilöt tuntevat omaan toimintaan liittyvät jatkuvuus- ja toipumissuunnitelmat sekä osaavat toimia niiden mukaisesti. Varahenkilöt on nimetty ja heidän kykynsä hoitaa tehtävät normaalitilanteissa on varmistettu.		Jokainen koulutettu henkilö tuntee periaatteet organisaation varautumisesta sekä tietää eri tilannemallien vaikutuksen omaan tehtäväänsä. Heitä kannustetaan osallistumaan erilaisiin varautumista tukeviin yhteistyöryhmiin.	TihL 4 § 2 mom		HAL-03	T-04	H1, H2, T11
Varautuminen ja jatkuvuudenhallinta	VAR-05	**Henkilöstön saatavuus ja varajärjestelyt**	Kriittisten tehtävien suorittamiseksi on suunniteltu ja valmisteltu erityistilanteiden vaihtoehtoiset toimintatavat ja henkilöstön saatavuus ja varajärjestelyt.		Lainsäädännön mahdollistamat toimenpiteet on tunnistettu ja toteutettu tarvittavassa laajuudessa esimerkiksi lakko-oikeuksien poistamisen, hätätöiden käytön ja henkilövarausten (VAP) osalta.	TihL 4 § 2 mom 2 k; 13 § 1 mom, 15 § 1 mom 4 k	Työaikalaki 872/2019, 19 §; Valtion virkaehtosopimuslaki 664/1970 11 §; Asevelvollisuuslaki 1438/2007 89 §			H1, H2
Varautuminen ja jatkuvuudenhallinta	VAR-06	**Tietoliikenteen varmistaminen**	Tietoliikennepalveluissa ja -sopimuksissa on huomioitu toiminnan kannalta tärkeiden palveluiden saatavuus häiriötilanteissa.		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.	TihL 13 § 1, 2 ja 4 mom, 15 §	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11	HAL-16.1		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Varautuminen ja jatkuvuudenhallinta	VAR-07	**Tietoteknisten ympäristöjen varmentaminen**	Tietoteknisissä ympäristöissä ja niihin liittyvissä sopimuksissa on huomioitu toiminnan kannalta tärkeiden palveluiden saatavuus häiriötilanteissa.		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.	TihL 13 § 1, 2 ja 4 mom, 15 §	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11	HAL-16.1		H1, H2
Varautuminen ja jatkuvuudenhallinta	VAR-08	**Vikasietoisuus**	ICT-infrastruktuuri sekä olennaiset tietojärjestelmät on toteutettu riittävän vikasietoisiksi ja käyttövarmoiksi riskiarvioinnin perusteella.	Tietojärjestelmien häiriöihin on varauduttu nopean palautumisen varmistamiseksi. Palautumisessa hyödynnetään mekanismeja, joiden tavoitteena on reaaliaikainen tai lähes reaaliaikainen viansietokyky kriittisten järjestelmien saatavuuden ylläpitämiseksi.	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.	TihL 13 § 1 ja 2 mom, 15 §	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6			H1, H2
Varautuminen ja jatkuvuudenhallinta	VAR-08.1	**Vikasietoisuus - riippuvuudet**	Palvelujen riippuvuus muista palveluista ja toisista toimijoista on otettu huomioon koko tietojenkäsittely-ympäristön ja sen vikasietoisuuden suunnittelussa.		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.	TihL 13 § 1 ja 2 mom, 15 §	Yhteiskunnan turvallisuusstrategia 2017			H1, H2
Varautuminen ja jatkuvuudenhallinta	VAR-09	**Tietojärjestelmien toipumissuunnitelmat**	Tietojärjestelmien toipumissuunnitelmien tulee olla laadittu, otettu käyttöön ja yhteensovitettu keskenään.	Toipumissuunnitelmat on määritetty organisaation toiminnan kannalta tärkeiden tietojärjestelmien häiriötilanteista palautumiseen.	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.	TihL 4 § 2 mom 2 k, 13 § 1 ja 2 mom, 15 § 1 mom		VAR-02		H1, H2
Tietosuoja	TSU-01	**Käsiteltävien henkilötietojen tunnistaminen**	Organisaatio tunnistaa kaikki käsittelemänsä henkilötiedot.	Käsiteltävien henkilötietojen tunnistaminen on välttämätön edellytys henkilötietojen suojaamiselle ja liittyy läheisesti organisaation tiedonhallintamallin laatimiseen sekä sen yhteydessä tehtävään organisaation tietovarantojen tunnistamiseen.	Käsiteltävien henkilötietojen tunnistaminen ja dokumentointi voidaan tehdä osana organisaation suojattavien kohteiden tunnistamista, tehtäessä selostetta käsittelytoimista tai muodostettaessa tiedonhallintamallia.	TihL 5 §; Tietosuoja-asetus Art 5 (1) (c)		HAL-04		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-01.1	**Käsiteltävien henkilötietojen tunnistaminen - Erityiset henkilötietoryhmät tai rikostuomioihin ja rikoksiin liittyvät tiedot**	Organisaatio tunnistaa käsittelemiensä erityisiin henkilötietoryhmiin kuuluvat tai rikostuomioihin ja rikoksiin liittyvät tiedot.	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.	Näihin henkilötietoryhmiin kuuluvien henkilötietojen tunnistaminen ja dokumentointi voidaan tehdä osana organisaation suojattavien kohteiden tunnistamista, tehtäessä selostetta käsittelytoimista tai muodostettaessa tiedonhallintamallia.	Tietosuoja-asetus Art 9 ja 10		HAL-04.2		H1, H2
Tietosuoja	TSU-02	**Organisaation roolit**	Organisaatio määrittelee käsittelemiensä henkilötietojen osalta, toimiiko organisaatio rekisterinpitäjänä, yhteisrekisterinpitäjänä vai henkilötietojen käsittelijänä.	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.	Organisaation rooli voidaan dokumentoida yhdeksi lähtötiedoksi henkilötietojen käsittelyä kuvaavaan dokumentaatioon, esimerkiksi selosteisiin käsittelytoimista ja tiedonhallintamalliin.	Tietosuoja-asetus Art 4 (7-8), 26 ja 28				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-03	**Yhteisrekisterinpitäjät**	Toimiessaan yhteisrekisterinpitäjänä organisaatio määrittelee läpinäkyvällä järjestelyllä muiden yhteisrekisterinpitäjien kanssa rekisterinpitäjien velvoitteiden noudattamisesta sekä rekisteröityjen informoinnista.	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.	Organisaatio voi esimerkiksi tehdä sopimuksen eri yhteisrekisteripitäjien kanssa tai dokumentoida kirjallisesti yhteisrekisterinpitäjyyteen liittyvät menettelyt sekä julkaista ne verkossa ja asettaa saataville toimipisteissä.	Tietosuoja-asetus Art 26				H1, H2
Tietosuoja	TSU-04	**Henkilötietojen käsittelijä**	Organisaatio käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet.	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.	Organisaatio voi arvioida käsittelijän kyvykkyyttä esimerkiksi käsittelijän toimittaman dokumentaation, hyväksyttyjen käytännesääntöjen tai sertifiointien avulla.	Tietosuoja-asetus Art 28		HAL-16		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-04.1	**Henkilötietojen käsittelijä - Sopimukset**	Organisaatio laatii henkilötietojen käsittelijöiden kanssa tietosuoja-asetuksen vaatimukset täyttävät sopimukset.	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.	Organisaatio voi laatia henkilötietojen käsittelyä koskevan sopimuksen esimerkiksi hyödyntämällä dokumenttia: 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.	Tietosuoja-asetus Art 28		HAL-16.1		H1, H2
Tietosuoja	TSU-05	**Tehtävät ja vastuut**	Organisaatio määrittelee henkilötietojen käsittelyyn liittyvät tehtävät ja vastuut.	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.	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).	Tietosuoja-asetus Art 12, 24		HAL-02		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-05.1	**Tehtävät ja vastuut - Tietosuojavastaava**	Organisaatio nimeää tehtävään soveltuvan tietosuojavastaavan ja julkistaa hänen yhteystietonsa.	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.		Tietosuoja-asetus Art 37-39				H1, H2
Tietosuoja	TSU-05.2	**Tehtävät ja vastuut - Tietosuojavastaavan asema ja tehtävät**	Organisaatio määrittelee tietosuojavastaavan aseman, resurssit ja valtuudet siten, että hänellä on edellytykset hoitaa tietosuojavastaavalle kuuluvat tehtävät.	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 §)	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.	Tietosuoja-asetus Art 37-39; JulkL 22-23 §				H1, H2
Tietosuoja	TSU-06	**Henkilötietojen käsittelyn ohjeet**	Organisaatio laatii henkilötietojen käsittelyä koskevat ohjeet ja varmistaa, että henkilötietoja käsitellään näiden ohjeiden mukaisesti.	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.	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.	Tietosuoja-asetus Art 29, 32(4)		HAL-12		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-07	**Käsittelyn lainmukaisuus**	Organisaatio tunnistaa käsittelemiensä henkilötietojen lainmukaiset käsittelyperusteet ja dokumentoi ne.	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.	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.	Tietosuoja-asetus Art 5 (1)(a), 6, 7, 8, 10; Tietosuojalaki 4 §, 5 §, 7 §, 29 §				H1, H2
Tietosuoja	TSU-07.1	**Käsittelyn lainmukaisuus - Suostumus**	Jos henkilötietojen käsittely perustuu poikkeuksellisesti suostumukseen, organisaatio varmistaa, että suostumuksen tietosuoja-asetuksessa säädetyt edellytykset täyttyvät.	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.	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.	Tietosuoja-asetus Art 4(1)(11), Art 7				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-07.2	**Käsittelyn lainmukaisuus - Henkilötunnus**	Organisaatio tunnistaa henkilötunnuksen käsittelyperusteet ja dokumentoi ne.	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.	Organisaatio voi esimerkiksi erikseen määritellä kaikki ne käsittelytoimet, joissa henkilötunnusta käytetään ja varmistaa kunkin toimenpiteen kohdalla, että henkilötunnuksen käytölle on laissa hyväksytty peruste.	Tietosuojalaki 29 §				H1, H2
Tietosuoja	TSU-07.3	**Käsittelyn lainmukaisuus - Erityiset henkilötietoryhmät**	Organisaatio tunnistaa käsittelemiensä erityisten henkilötietoryhmien käsittelyperusteet ja dokumentoi ne.	Erityisten henkilötietoryhmien, kuten etnistä alkuperää tai terveyttä koskevien tietojen käsittely on lähtökohtaisesti kiellettyä. Käsittely on kuitenkin mahdollista silloin, kun käsittelykielto on säädetty poikkeus tietosuoja-asetuksessa tai kansallisessa lainsäädännössä.	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.	Tietosuoja-asetus Art 9; Tietosuojalaki 6 § 1 mom				H1, H2
Tietosuoja	TSU-07.4	**Käsittelyn lainmukaisuus - Rikostuomioihin ja rikoksiin liittyvät henkilötiedot**	Organisaatio tunnistaa käsittelemiensä rikostuomioihin ja rikoksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittelyperusteet ja dokumentoi ne.	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.	Ennen rikostuomioihin ja rikkomuksiin liittyvän henkilötietojen käsittelyn aloittamista organisaatio voi toimia esimerkiksi seuraavalla tavalla: - Organisaatio selvittää ja dokumentoi käsittelyn perusteet ja varmistaa niiden asianmukaisuuden.	Tietosuoja-asetus Art 10; Tietosuojalaki 7 §				H1, H2
Tietosuoja	TSU-08	**Tarpeellisuus ja oikeasuhtaisuus**	Organisaatio varmistaa, että henkilötietojen käsittely on tarpeellista ja oikeasuhtaista käsittelyn laillisten tarkoitusten saavuttamiseksi.	Henkilötietoja olisi käsiteltävä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoilla.	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.	Tietosuoja-asetus Art 5				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-09	**Käyttötarkoitussidonnaisuus**	Organisaatio kerää henkilötietoja vain tietyssä, nimenomaisessa ja laillisessa tarkoituksessa, eikä käsittele henkilötietoja alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin.	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	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.	Tietosuoja-asetus Art 5(1)(b), 6(4)				H1, H2
Tietosuoja	TSU-10	**Tietojen minimointi**	Organisaatio käsittelee henkilötietoja vain siinä määrin, kun se on tarpeellista käsittelyn tarkoituksen kannalta.	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.	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.	Tietosuoja-asetus Art 51(c), 25(2); Tietosuojalaki 29.4 §				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-11	**Säilytyksen rajoittaminen**	Organisaatio säilyttää henkilötietoja muodossa, josta rekisteröity on tunnistettavissa, ainoastaan niin kauan, kun on tarpeen tietojen käsittelyn tarkoitusten toteuttamista varten.	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.	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.	Tietosuoja-asetus Art 5(1) (e), 25(2)				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-12	**Täsmällisyys**	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.	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.	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.	Tietosuoja-asetus Art 5(1)(d)				H1, H2
Tietosuoja	TSU-13	**Käsittelyn turvallisuus**	Organisaatio varmistaa henkilötietojen turvallisuuden käyttäen asianmukaisia teknisiä tai organisatorisia toimia.	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.	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.	Tietosuoja-asetus Art 5, 32				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-13.1	**Käsittelyn turvallisuus - Erityiset henkilötietoryhmät tai rikostuomioihin ja rikoksiin liittyvät tiedot**	Käsiteltäessä erityisiin henkilötietoryhmiin kuuluvia tai rikostuomioihin ja rikoksiin liittyviä henkilötietoja organisaatio toteuttaa asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi.	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.	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.	Tietosuoja-asetus Art 5, 32; Tietosuojalaki 6 § 2 mom ja 7 § 2 mom				H1, H2
Tietosuoja	TSU-14	**Tietoturvaloukkaukset**	Organisaatio dokumentoi kaikki henkilötietojen tietoturvaloukkaukset, sekä määrittelee toimintatavat niistä ilmoittamiseen valvontaviranomaiselle ja rekisteröidyille.	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.	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.	Tietosuoja-asetus Art 33		HAL-08, HAL-09		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-15	**Osoitusvelvollisuus**	Organisaatio pystyy osoittamaan noudattavansa yleisen tietosuoja-asetuksen vaatimuksia.	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.	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.	Tietosuoja-asetus Art 5(2), 24		HAL-09		H1, H2
Tietosuoja	TSU-16	**Tietosuojariskien hallinta**	Organisaatio arvioi henkilötietojen käsittelyyn kohdistuvat olennaiset riskit sekä toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet riskiarvioinnin mukaisesti.	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.	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.	Tietosuoja-asetus Art 24, 25, 32-34, 35		HAL-06		H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-17	**Tietosuojan vaikutustenarviointi**	Organisaatio toteuttaa ennen henkilötietojen käsittelyä arvioinnin suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle silloin, kun henkilötietojen käsittelyyn liittyy korkeita riskejä rekisteröidylle.	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.	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.	Tietosuoja-asetus Art 35				H1, H2
Tietosuoja	TSU-17.1	**Tietosuojan vaikutustenarviointi - Ennakkokuuleminen**	Organisaatio kuulee tarvittaessa tietosuojavaltuutetun toimistoa ennen henkilötietojen käsittelyn aloittamista.	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.	Organisaatio voi määritellä ennakkokuulemisen tarpeen tarkastuksen ja ennakkokuulemisen suorittamisen esimerkiksi yhdeksi osaksi vaikutustenarvioinnin ja henkilötietojen käsittelyn aloittamisen prosesseja.	Tietosuoja-asetus Art 36				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-18	**Henkilötietojen siirto ETA:n ulkopuolelle**	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.	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.	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	Tietosuoja-asetus V luku				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-19	**Rekisteröidyn oikeudet**	Organisaatio toteuttaa rekisteröidyn oikeudet.	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.	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.	Tietosuoja-asetus Art 12-21				H1, H2
Tietosuoja	TSU-19.1	**Rekisteröidyn oikeudet - Rekisteröidyn käytettävissä olevien oikeuksien tunnistaminen**	Organisaatio on määritellyt tunnistamansa henkilötietojen lainmukaisen käsittelyperusteen mukaisesti, mitkä rekisteröidyn oikeudet liittyvät kyseessä olevaan käsittelyyn.	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.	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.	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 §				H1, H2
Tietosuoja	TSU-19.2	**Rekisteröidyn oikeudet - Läpinäkyvä informointi**	Organisaatio informoi rekisteröityjä henkilötietojen käsittelystä säädetyllä tavalla.	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.	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.	Tietosuoja-asetus Art 5, 13-14				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-19.3	**Rekisteröidyn oikeudet - Oikeus saada pääsy tietoihin**	Organisaatio toimittaa pyynnöstä rekisteröidylle jäljennöksen käsiteltävistä henkilötiedoista sekä informaatiota henkilötietojen käsittelystä.	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.	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.	Tietosuoja-asetus Art 15				H1, H2
Tietosuoja	TSU-19.4	**Rekisteröidyn oikeudet - Tietojen oikaiseminen, poistaminen, siirtäminen, käsittelyn rajoittaminen ja vastustaminen**	Organisaatio toteuttaa tietojen oikaisemiseen, poistamiseen, siirtämiseen, käsittelyn rajoittamisen ja vastustamiseen liittyvät pyynnöt.	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.	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.	Tietosuoja-asetus Art 16-21				H1, H2

Osa-alue	Tunniste	Nimi	Vaatimus	Yleiskuvaus	Toteutusesimerkki	Lainsäädäntö	Muita lisätietoja	Julkri-viite	Katakri-viite	Todennusmenetelmä ID
Tietosuoja	TSU-20	**Automatisoidut yksittäispäätökset**	Organisaatio tunnistaa tilanteet, joissa henkilötietojen käsittelyyn sisältyy automaattista päätöksentekoa sekä varmistaa että automaattista päätöksentekoa ei tehdä muutoin kuin tietosuoja-asetuksessa erikseen sallituissa tapauksissa.	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.	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	Tietosuoja-asetus Art 22				H1, H2
Tietosuoja	TSU-21	**Seloste käsittelytoimista**	Organisaatio laatii kirjallisen kuvauksen organisaation suorittamista henkilötietojen käsittelytoimista.	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.	Rekisterinpitäjä ja henkilötietojen käsittelijä voivat laatia selosteet käsittelytoimista esimerkiksi hyödyntämällä tietosuojavaltuutetun sivuilta löytyviä ohjeita ja mallipohjia.	Tietosuoja-asetus Art 30				H1, H2