xxx ministeriön julkaisusarja 2020:xx

# Julkri-kriteerit

## Liite 1A

Lautakunnat

xxxministeriö Helsinki 2020

# Sisältö

# 1 Kriteeristön rakenne ja osa-alueet

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

- hallinnollinen turvallisuus (HAL),
- fyysinen turvallisuus (FYY),
- tekninen turvallisuus (TEK),
- varautuminen ja jatkuvuudenhallinta (VAR) sekä
- tietosuoja (TSU) (kuvattu erillisessä liitteessä 1B).

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

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

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

# 2 Hallinnollinen turvallisuus

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

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

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

Osa-alueen tarkoituksenmukainen käyttö edellyttää arvioinnin kohdentamista siihen osaan organisaatiosta, jolla on vaikutus arvioinnin kohteena olevaan tietojen käsittelyyn. Tarkoituksenmukainen kohdennus voi olla esimerkiksi tietojenkäsittely-ympäristöä hallinnoiva organisaation osa.

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

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

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

| Tunniste | HAL-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto |
|---|---|
| **Nimi** | **Periaatteet** |
| **Vaatimus** | Organisaatiolla on ylimmän johdon hyväksymät tietoturvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan sekä ovat tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset. |
| **Yleiskuvaus** | Ylimmän johdon hyväksymillä tietoturvallisuusperiaatteilla osoitetaan, että johto on sitoutunut organisaation tietoturvallisuusperiaatteisiin ja periaatteet edustavat johdon tahtotilaa sekä tukevat organisaation toimintaa. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina tai osana yleisiä toimintaperiaatteita, politiikkaa tai strategiaa. |
| **Lainsäädäntö** | TiHL 4 § 2 mom, 13 § |
| **Viitteet** | T-01 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01 |

| Tunniste | HAL-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto |
|---|---|
| **Nimi** | **Tehtävät ja vastuut** |
| **Vaatimus** | Organisaatio on määritellyt ja dokumentoinut tietoturvallisuuden hoitamisen tehtävät ja vastuut. |
| **Yleiskuvaus** | Tietoturvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa.<br><br>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.<br><br>Tietoturvallisuuden vastuualueet määritellään yleensä osana turvallisuuden kokonaisvastuuta. |
| **Toteutusesimerkki** | Organisaatio on määritellyt turvallisuuden toteuttamisen tehtävät ja niihin liittyvät vastuut seuraavilta osin:<br>a) turvallisuusjohtaminen<br>b) fyysinen turvallisuus<br>c) tekninen turvallisuus<br>d) varautuminen ja jatkuvuudenhallinta<br>e) tietosuoja<br>f) riskienhallinta<br>g) turvallisuuden kokonaisvastuu |
| **Lainsäädäntö** | TiHL 4 § 2 mom |
| **Viitteet** | T-02 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.2; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3; PiTuKri TJ-02; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 3 |

| Tunniste | HAL-02.1, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä |
|---|---|
| **Nimi** | **Tehtävät ja vastuut - tehtävien eriyttäminen** |
| **Vaatimus** | Organisaation on varmistettava, että henkilöillä ei ole turvallisuuden kannalta vaarallisia työyhdistelmiä |

| | |
|---|---|
| **Yleiskuvaus** | Organisaation tehtävien ja vastuualueiden on oltava eriytettyjä, jotta vähennetään organisaation suojattavan omaisuuden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Tällaisia vaarallisia yhdistelmiä ovat esimerkiksi yksi henkilö pääsee muuttamaan sekä tietojärjestelmän tietoja että tietojärjestelmän seurannassa käytettäviä lokitietoja. |
| **Toteutusesimerkki** | - Organisaatio on määritellyt vaaralliset työyhdistelmät<br>- Vaaralliset työyhdistelmät tarkastetaan osana tehtävien määrittelyjä<br>- Vaaralliset työyhdistelmät tarkastetaan osana käyttöoikeuksien hallintaa erityisesti pääkäyttäjä- ja valvontaroolien kohdalla |
| **Lainsäädäntö** | TiHL 4 § 2 mom, 13 § |
| **Viitteet** | I-06 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.3 |
| **Tunniste** | **HAL-03, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Resurssit** |
| **Vaatimus** | Organisaatiolla on käytössään riittävät resurssit ja asiantuntemus turvallisuuden varmistamiseksi. |
| **Yleiskuvaus** | Resursoinnilla ja asiantuntemuksella varmistetaan, että turvallisuustyö voidaan toteuttaa määriteltyjen periaatteiden mukaisesti. Turvallisuustyön resursseilla tarkoitetaan sekä henkilöresursseja että taloudellisia panostuksia, kuten tietojärjestelmäinvestointeja.<br><br>Yleisinä vaatimuksina voidaan pitää, että organisaatiolla tulee olla henkilöitä turvallisuuden hallinnan edellyttämiin tehtäviin ja että henkilöillä osaamista ja aikaa vaadittujen tehtävien suorittamiseen.<br><br>Lisäksi organisaatiolla tulee olla kykyä ja halua tehdä sellaiset turvallisuuteen liittyvät investoinnit, jotka turvallisuusvaatimusten ja riskien arvioinnin perusteella on tunnistettu tarpeellisiksi. |
| **Toteutusesimerkki** | - Turvallisuustehtäviä hoitavilla on riittävä asiantuntemus sekä näistä on näyttöjä.<br>- Turvallisuustyön resurssit, tehtävät, vastuut ja valtuudet on määritelty organisaation toimintaan, kokoon ja riskeihin nähden riittävän kattavasti.<br>- Resurssit riittävät tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen.<br>- Resurssien riittävyyttä arvioidaan säännöllisesti.<br>- Organisaatio tekee tarvittavat päätökset turvallisuuden edellyttämistä laite- ja muista investoinneista |
| **Lainsäädäntö** | TiHL 4 § 2 mom |
| **Viitteet** | T-05 |
| **Muita lisätietoja** | SFS-EN ISO/IEC 27001:2017 7.1, 7.2, 5.1 |
| **Tunniste** | **HAL-04, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Suojattavat kohteet** |
| **Vaatimus** | Organisaatio tunnistaa suojattavat kohteet sekä pitää niistä ajantasaista dokumentaatiota. |

| | |
|---|---|
| **Yleiskuvaus** | Suojattavien kohteiden luettelointi on yksi turvallisuuden hallinnan perusvaatimuksista. Suojattavia kohteita ovat tiedot, tietojärjestelmät, tietojenkäsittelyprosessit, tilat sekä muut mahdollisestii organisaation turvallisuuteen vaikuttavat kohteet.<br><br>Suojattavien kohteiden luettelointi on välttämätön edellytys suunnitelmallisen ja vaikuttavan tietoturvallisuuden hallinnan toteuttamiseksi. Ajantasaista luetteloa suojattavasta omaisuudesta hyödynnetään lähtötietona monilla tietoturvallisuuden hallinnan osa-alueilla. |
| **Lainsäädäntö** | TiHL 5 § 2 mom, 13 § |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.9; Suositus tiedonhallintamallista 2020:29 |
| **Tunniste** | **HAL-04.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Suojattavat kohteet - vastuut** |
| **Vaatimus** | Organisaatio määrittelee suojattavien kohtaiden vastuut. |
| **Lainsäädäntö** | TiHL 5 § 2 mom |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.9; Suositus tiedonhallintamallista VM 2020:29 |
| **Tunniste** | **HAL-04.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Suojattavat kohteet - luokittelu** |
| **Vaatimus** | Organisaation on luokiteltava tiedot sekä niihin liittyvät järjestelmät ja käsittelyprosessit niihin kohdistuvien vaatimusten perusteella. |
| **Yleiskuvaus** | Organisaation tulee tunnistaa lainsäädännöstä käsittelemänsä julkiset, salassa pidettävät, turvallisuusluokitellut ja henkilötiedot sekä niiden suojaamisen tarpeet. Luokittelulla tarkoitetaan erilaisista käsittelyvaatimuksista johtuvaa tarvetta suojata tietoa eri tasoilla.<br><br>Luokittelemalla tietojenkäsittely-ympäristöt tietoaineiston mukaisesti, pystytään helpommin osoittamaan ja perustelemaan kuhunkin tietojenkäsittely-ympäristöön liittyvät turvatoimet. Luokittelu olisi sisällytettävä organisaation prosesseihin ja sen olisi oltava johdonmukainen ja yhdenmukainen koko organisaatiossa.<br><br>Luokittelu toimii lähtötietona useille muille turvallisuuden prosesseille. Esimerkiksi järjestelmien saatavuusvaatimukset liittyvät järjestelmien vikasietoisuuden ja varautumisen suunnitteluun ja luottamuksellisuusvaatimukset järjestelmien turvallisuusvaatimusten määrittelyyn.<br><br>Tietojärjestelmän tai muun useita tietoaineistoja sisältävän kohteen luokitus määräytyy ensi sijassa korkeimman luokituksen aineiston mukaan. Mikäli tietoa on runsaasti, on arvioitava, onko kohteen luokittelu korkeampi kasautumisvaikutuksen johdosta. |

| | |
|---|---|
| **Toteutusesimerkki** | - Organisaatio määrittelee tietojen sekä niihin liittyvien tietojärjestelmien ja käsittelyprosessien luokittelussa käytettävät tasot luottamuksellisuuden, saatavuuden ja eheyden sekä näkökulmista. Tarvittaessa luokittelua voidaan laajentaa kattamaan myös muita näkökulmia kuten esimerkiksi sisältääkö tiedot henkilötietoja.<br>- Organisaatio määrittelee kriteerit, joiden mukaan tiedot ja muut kohteet luokitellaan eri luokkiin.<br>- Luokat ja niihin liittyvät kriteerit perustuvat lakisääteisiin vaatimuksiin, mutta organisaatioiden tulee täsmentää kriteerit siten, että ne ovat tarkoituksenmukaisia organisaatiossa työskenteleville henkilöille.<br>- Luokittelu voidaan tehdä suojattavien kohteiden luetteloinnin yhteydessä ja sisällyttää luetteloon suojattavaista tiedoista - esimerkiksi tiedonhallintamalliin. |
| **Lainsäädäntö** | TiHL 4 § 2 mom, 5 §, 13 §, 18 §;<br>TLA 3 §, 4 §;<br>621/1999 24 § |
| **Viitteet** | T-08 |
| **Muita lisätietoja** | Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65, luku 4.1; Suositus turvallisuusluokiteltavienasiakirjojen käsittelystä 2021:5 luku 2, luku 5.3; ISO/IEC 27002:2022 5.9 |
| **Tunniste** | **HAL-04.3, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Suojattavat kohteet - merkitseminen** |
| **Vaatimus** | Organisaation on merkittävä tiedot lakisääteisten vaatimusten sekä organisaation määrittelemien luokitteluperiaatteiden mukaisesti. |
| **Yleiskuvaus** | Tiedon merkitsemistapojen pitää kattaa sekä fyysisessä että sähköisessä muodossa olevat tiedot ja niihin liittyvä suojattava omaisuus kuten tietovälineet.<br><br>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.<br><br>Tietyissä tapauksissa,kuten esimerkiksi julkisuuslain mukaisista salassa pitoa koskevista merkinnöistä tulee myös käydä ilmi, miltä osin asiakirja on salassa pidettävä sekä mihin salassapito perustuu. |
| **Lainsäädäntö** | TiHL 18 §;<br>TLA 3 §, 4 §;<br>621/1999 25 § |
| **Viitteet** | T-08 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavienasiakirjojen käsittelystä 2021:5 luku 3; ISO/IEC 27002:2022 5.13 |
| **Tunniste** | **HAL-04.4, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Suojattavat kohteet - riippuvuudet** |
| **Vaatimus** | Organisaatio on tunnistanut ja dokumentoinut suojattavien kohteiden väliset riippuvuudet. |
| **Lainsäädäntö** | TiHL 5 § |
| **Tunniste** | **HAL-04.5, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Suojattavat kohteet - sidosryhmät** |
| **Vaatimus** | Organisaatio on tunnistanut ja dokumentoinut suojattaviin kohteisiin liittyvät sidosryhmät. |
| **Lainsäädäntö** | TiHL 5 § |

| | |
|---|---|
| **Tunniste** | **HAL-05, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Vaatimukset** |
| **Vaatimus** | Organisaatio tunnistaa lainsäädännöstä, sidosryhmistä sekä organisaation toiminnasta johtuvat tietoturvavaatimukset. |
| **Yleiskuvaus** | Organisaation tulee tunnistaa ja yksilöidä lainsäädännöstä, eri sidosryhmien kanssa laadituista sopimuksista sekä organisaation toiminnasta johtuvat turvallisuutta koskevat vaatimukset.<br><br>Julkisessa hallinnossa noudatettavat tiedonhallintalakiin perustuvat tietoturvallisuuden vähimmäisvaatimukset, ja niiden noudattamisesta annetut suositukset on määritelty tiedonhallintalautakunnan suosituksen 2021:65 luvussa 2.<br><br>Organisaation tietoturvallisuusvaatimukset muodostuvat edellä mainituista vähimmäisvaatimuksista sekä muista tunnistetuista vaatimuksista. Kunkin vaatimuksen toteuttamisen menettely arvioidaan riskiarviointiprosessin avulla. |
| **Lainsäädäntö** | TiHL 13 § |
| **Muita lisätietoja** | SFS-EN ISO/IEC 27001:2017 4.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luvut 2 ja 4 |
| **Tunniste** | **HAL-05.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Vaatimukset - seuranta** |
| **Vaatimus** | Organisaatio seuraa asetettujen turvallisuusvaatimusten ja toimintaympäristön muutoksia ja tekee tarvittavat toimenpiteet niihin reagoimiseksi. |
| **Yleiskuvaus** | Lainsäädäntö, sopimusvaatimukset sekä muuttuvat turvallisuusuhat edellyttävät säännöllistä vaatimusten ja uhkien seurantaa ja muutoksiin reagoimista. |
| **Lainsäädäntö** | TiHL 4 §, 13 § |
| **Muita lisätietoja** | SFS-EN ISO/IEC 27001:2017 9.1; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 4.1 |
| **Tunniste** | **HAL-05.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Vaatimukset - muutosvaikutukset** |
| **Vaatimus** | Organisaatio arvioi olennaisten hallinnollisten uudistusten ja tietojärjestelmien käyttöönottojen muutosvaikutukset suhteessa tietoturvallisuusvaatimuksiin ja -toimenpiteisiin. |
| **Yleiskuvaus** | Olennaisten muutosten yhteydessä organisaatioilta edellytetään muutosvaikutusten arviointia. Osana muutosvaikutusten arviointia on arvioitava muutosten vaikutukset suhteessa tietoturvallisuusvaatimuksiin ja -toimenpiteisiin. |
| **Lainsäädäntö** | TiHL 5 § |
| **Muita lisätietoja** | Suositus tiedonhallinnan muutosvaikutusten arvioinnista 2020:53; ISO/IEC 27002:2022 5.31 |
| **Tunniste** | **HAL-06, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Riskienhallinta** |
| **Vaatimus** | Organisaatio toteuttaa tietoturvallisuusriskien hallintaa ja on arvioinut olennaiset tietoihin kohdistuvat riskit sekä mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. |

| | |
|---|---|
| **Yleiskuvaus** | Tietoturvallisuusriskien hallintaprosessi koostuu toimintaympäristön määrittämisestä, riskien arvioinnista (tunnistaminen, analysointi, merkityksen arviointi), riskien käsittelystä, riskien hyväksynnästä, riskejä koskevasta viestinnästä ja tiedonvaihdosta sekä riskien seurannasta ja katselmoinnista.<br><br>Tietoturvallisuusriskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa. Tietoturvallisuusriskien hallinnan avulla varmistetaan tietoturvallisuustoimenpiteiden riittävyys tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi.<br><br>Riskienhallinta vaikuttaa muihin tietoturvallisuuden hallinnan eri osa-alueisiin. Riskienhallinta tulee suunnitella ja ohjeistaa siten, että siinä käsitellään systemaattisesti ja suunnitelmallisesti erilaisia tietoturvallisuuteen liittyviä riskejä kuten tietosisällön virheellisyyksistä johtuvia riskejä, organisaation toiminnan keskeytyksiin liittyviä riskejä sekä henkilötietojen tietoturvaloukkauksiin liittyviä riskejä. |
| **Toteutusesimerkki** | - Tietoturvallisuusriskien arvioinnissa ja analysoinnissa käytetään yleisesti hyväksyttyä menetelmää.<br>- Tietoturvallisuusriskien arvioinneista laaditaan aikataulutettu ja vastuutettu vuosisuunnitelma<br>- Tietoturvallisuusriskien hallintaan osallistuu riittävästi asiantuntijoita.<br>- Tietoturvallisuusriskien hallinnassa on otettu huomioon sidosryhmistä ja toimitusketjuista aiheutuvat riskit.<br>- Tietoturvallisuusriskien arviointia hyödynnetään muissa tietoturvallisuuden hallinnan prosesseissa. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 6 §, 7 § |
| **Viitteet** | FYY-01, TEK-01, TEK-13, TEK-15<br>, T-03 |
| **Muita lisätietoja** | SFS-EN ISO/IEC 27001:2017 6.1 ja 8-10; SFS-EN ISO/IEC 27005:2018 luku 6; SFS ISO 31000:2018; PiTuKri TJ-03; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 5.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6 |
| **Tunniste** | **HAL-06.1, L:Salassa pidettävä, E:, S:, TS:Henkilötieto** |
| **Nimi** | **Riskienhallinta - lainsäädäntöjohdannaiset riskit** |
| **Vaatimus** | 1) Palveluun liittyvät lainsäädäntöjohdannaiset riskit on tunnistettu ja arvioitu.<br>2) Lainsäädäntöjohdannaiset riskit eivät rajoita kyseisen palvelun soveltuvuutta kyseiseen käyttötapaukseen ja kyseisiin tietoihin.<br>3) Kyseiset tiedot ovat luovutettavissa kyseiseen palveluun määräysvallassa oleviin maihin. |
| **Yleiskuvaus** | Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa palveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy palvelun asiakkaiden salassa pidettäviin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin sekä muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimusoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia. |

| | |
|---|---|
| **Toteutusesimerkki** | Riskienarvioinnin tulisi kattaa lainsäädäntöjohdannaiset riskit vähintään seuraavien tekijöiden osalta:<br>a) Palvelussa käsiteltävän tiedon fyysinen sijainti koko tiedon elinkaaren ajalta, kattaen myös mahdolliset alihankinta- ja ulkoistusketjut.<br>b) Palvelun eri toimintojen (esimerkiksi ylläpito- ja hallintaratkaisut, varmistukset) ja komponenttien fyysinen sijainti koko tiedon elinkaaren ajalta.<br>c) Mahdolliset muut palvelun tuottamiseen osallistuvat tahot, esimerkiksi mahdolliset alihankinta-ja ulkoistusketjut.<br>d) Palvelun käyttöön ja palvelussa käsiteltäviin tietoihin sovellettava lainsäädäntö ja oikeuspaikka.<br>e) Toimijat, joilla voi sovellettavasta lainsäädännöstä johtuen olla pääsy palvelussa käsiteltäviin tietoihin.<br><br>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.<br><br>Turvallisuusluokittelemattomien salassa pidettävien tietojen suojaamisessa on huomioitavaa, että tällaisten tietojen suojaamisessa voidaan hyväksyä turvallisuusluokiteltuun tietoon nähden laajemmin lainsäädäntöjohdannaisia riskejä. Viranomaisen riskienarviointiin pohjautuen voikin olla mahdollista hyödyntää esimerkiksi toisen maan viranomaisen määräysvallassa olevia järjestelmiä/ipalveluita turvallisuusluokittelemattoman salassa pidettävän tiedon käsittelyyn, mikäli kyseinen palvelu täyttää muutkin salassa pidettävään tietoon kohdistuvat suojausvaatimukset. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 6 §, 7 § |
| **Viitteet** | FYY-01, TEK-01, TEK-13, TEK-15, T-03 |
| **Muita lisätietoja** | SFS-EN ISO/IEC 27001:2017 6.1 ja 8-10; SFS-EN ISO/IEC 27005:2018 luku 6; SFS ISO 31000:2018; PiTuKri TJ-03 ja EE-02; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 5.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6 |
| **Tunniste** | **HAL-07, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Seuranta ja valvonta** |
| **Vaatimus** | Organisaatiossa on järjestetty seuranta ja valvonta tietoturvallisuuteen liittyvien prosessien toimivuudesta ja vaatimusten täyttymisestä. |

| | |
|---|---|
| **Yleiskuvaus** | Organisaation on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.<br><br>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.<br><br>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.<br><br>Mittarit voivat olla esimerkiksi numeerisia raja-arvoja (esim. palveluiden saatavuus vähintään 99 %) tai vaatimustenmukaisuuden todentamista (esim. vuosikellon mukaiset arvioinnit ja katselmoinnit on hoidettu suunnitellusti). |
| **Toteutusesimerkki** | Organisaation on määritellyt<br>a) mitä täytyy seurata ja mitata,<br>b) millä seuranta-, mittaus-, analysointi- tai arviointimenetelmillä varmistetaan kelvolliset tulokset<br>c) milloin seuranta ja mittaus on toteutettava<br>d) ketkä toteuttavat seurannan ja mittaamisen<br>e) milloin seurannan ja mittauksen tuloksia on analysoitava ja arvioitava<br>f) ketkä analysoivat ja arvioivat saadut tulokset |
| **Lainsäädäntö** | TiHL 4 § 2 mom, 13 § 1 mom |
| **Viitteet** | T-01, I-19 |
| **Muita lisätietoja** | SFS-EN ISO/IEC 27001:2017 9.1; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 7 |
| **Tunniste** | **HAL-07.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Seuranta ja valvonta - tietojen käyttö ja luovutukset** |
| **Vaatimus** | Organisaatio on tunnistanut lokitietojen keräämiseen liittyvät vaatimukset ja varmistanut niiden perusteella lokitietojen keräämisen ja seurannan riittävyyden. |
| **Yleiskuvaus** | Lokitiedot ovat yksi keskeisimmistä keinoista tietojen käytön ja luovutusten seurantaan. Tiedonhallintalain mukaan lokitiedot tulee kerätä, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lisäksi tietosuoja-asetuksen osoitusvelvollisuus henkilötietojen käsittelyn turvallisuudesta edellyttää usein käytännössä lokitietojen keruuta ja seurantaa.<br><br>Lokitiedot tulee kerätä tietojärjestelmän käytöstä ja tietojen luovutuksista, mutta tietojen kerääminen on sidottu tarpeellisuuteen. Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, tulee luovuttavassa järjestelmässä kerätä luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen perusteensa. Lisäksi käyttölokitiedot tulee kerätä ainakin tietojärjestelmistä, joissa käsitellään henkilötietoja tai salassa pidettäviä tietoja. |

| | |
|---|---|
| **Toteutusesimerkki** | - Organisaatio määrittelee osana palvelujen ja tietojärjestelmien hankintaa niihin liittyvät lokitietojen keruun vaatimukset ja varmistaa niiden täyttymisen.<br>- Organisaatio määrittelee tietojärjestelmittäin tietojen käytön ja luovutusten seurannan tarpeet ja menettelyt.<br>- Seurannan menettelyitä arvioidaan määräajoin.<br>- Organisaatio määrittelee lokitietojen säilyttämiseen, hävittämiseen ja suojaamiseen liittyvät vastuut ja varmistaa niiden täyttymisen.<br>- Mikäli lokitietojen käyttö on laaja-alaista, organisaatio voi harkita keskitettyyn lokitietojen hallintaan (SIEM) siirtymistä. |
| **Lainsäädäntö** | TiHL 17 § |
| **Viitteet** | I-10 |
| **Muita lisätietoja** | Kyberturvallisuuskeskus, Näin keräät ja käytät lokitietoja; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65, luku 14; ISO/IEC 27002:2022 5.31, 8.15 |
| **Tunniste** | **HAL-08, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Häiriöiden hallinta** |
| **Vaatimus** | Organisaatiolla on tietoturvallisuushäiriöiden ja poikkeamatilanteiden käsittelyyn määritellyt prosessit ja ohjeet. |
| **Yleiskuvaus** | Tietourvallisuushäiriöiden 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.<br><br>Organisaatiolla tulee olla häiriöiden käsittelyprosessi, joka ottaa kantaa vähintään tilanteen vakavuuden määrittelemiseen, lisävahinkojen estämiseen, todisteiden keräämiseen, tilanteen selvittämiseen, tilanteesta viestimiseen, korjaavien toimenpiteiden toteuttamiseen ja tilanteesta oppimiseen.<br><br>Käsittelyprosessissa tulee ottaa huomioon palvelun aikakriittisyys ja sitä suunniteltaessa tulee arvioida tarpeet virka-ajan ulkopuolella tapahtuvien häiriöiden hallinnalle.<br><br>Organisaatiossa on myös selvitetty, mitkä kansalliset ja kansainväliset säädökset tai organisaation tekemät sopimukset edellyttävät tietoturvapoikkeamista tai niiden epäilystä ilmoittamista viranomaisille. Ilmoittamisen kriteerit, vastuut, yhteystideot sekä tiedottamisen määräajat on määritetty ja dokumentoitu. |
| **Toteutusesimerkki** | Tietoturvallisuushäiriöiden hallinta on<br>- suunniteltu ottaen huomioon koko palveluketju sekä virka-ajan ulkopuolella tapahtuvat häiriöt,<br>- ohjeistettu ja koulutettu,<br>- dokumentoitu riittävällä tasolla,<br>- harjoiteltu, sekä<br>- viestintäkäytännöt ja vastuut on sovittu |
| **Lainsäädäntö** | TiHL 4 § 2 mom ja 13 §;<br>TLA 7 § |
| **Viitteet** | T-07 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.24; PiTuKri TJ-04 |
| **Tunniste** | **HAL-09, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |

| Nimi | Dokumentointi |
|---|---|
| **Vaatimus** | Tietoturvallisuuteen liittyvät politiikat, prosessit, ohjeet ja prosessien toteuttamisessa syntyvät tulokset on dokumentoitu. |
| **Toteutusesi-merkki** | - Organisaatio on määritellyt tietoturvallisuuden hallinnan edellyttämät sekä tietoturvallisuuden hallinnan eri prosesseissa syntyvät dokumentit.<br>- Dokumentaatiolle on määritelty ylläpito- ja jakeluprosessit<br>- Dokumentaation oikeudet ja suojaukset on määritelty |
| **Lainsäädäntö** | TiHL 5 §, 6 §, 13 § 1 mom |
| **Viitteet** | T-01 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.37 |
| **Tunniste** | **HAL-09.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Dokumentointi - ajantasaisuus** |
| **Vaatimus** | Tietoturvallisuuteen liittyvä dokumentaatio on ajantasaista. |
| **Toteutusesi-merkki** | - Organisaatiolla on prosessi, jonka avulla seurataan dokumentaation kattavuutta ja ajantasaisuutta<br>- Dokumentaation puutteisiin reagoidaan |
| **Lainsäädäntö** | TiHL 5 §, 6 §, 13 § 1 mom |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.37 |
| **Tunniste** | **HAL-10, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Henkilöstön luotettavuuden arviointi** |
| **Vaatimus** | Organisaatio tunnistaa ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. |
| **Yleiskuvaus** | Erityistä luotettavuutta edellyttäviä tehtäviä voidaan tunnistaa esimerkiksi määrittämällä tilanteet, joissa henkilö käsittelee turvallisuusluokiteltavia tai merkittävässä määrin ja säännöllisesti salassa pidettäviä tietoja tai työskentelee tiloissa, joissa henkilön tietoon voi tulla muutoin kuin satunnaisesti turvallisuusluokiteltavia tai salassa pidettäviä tietoja. |
| **Toteutusesi-merkki** | - Organisaatio laatii kuvauksen sellaisista tietoaineistojen käsittelyyn liittyvistä tehtävistä, jotka edellyttävät erityistä luotettavuutta.<br>- Näihin tehtäviin nimettävistä henkilöistä haetaan turvallisuusselvitys, mikäli tähän on turvallisuusselvityslain mukaan peruste.<br>- Lisäksi tiedonhallintayksikkö ylläpitää luetteloa näistä tehtävistä. |
| **Lainsäädäntö** | TiHL 12 §; Turvallisuusselvityslaki 726/2014 |
| **Viitteet** | T-10 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 6.1 |
| **Tunniste** | **HAL-10.1, L:Salassa pidettävä, E:Kriittinen, S:Kriittinen, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Henkilöstön luotettavuuden arviointi - turvallisuusselvitys** |
| **Vaatimus** | Organisaatio arvioi turvallisuusselvityksen tarpeen ja mikäli sellaista edellytetään, myöntää henkilöille pääsyn suojattaviin kohteisiin vasta turvallisuusselvityksen jälkeen. |

| | |
|---|---|
| **Yleiskuvaus** | Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014).<br><br>Henkilöturvallisuusselvitys voidaan tehdä ihmisestä, joka työssään pääsee esimerkiksi turvallisuuden kannalta tärkeään tilaan tai käsittelee salassa pidettävää tietoa.<br><br>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.<br><br>Turvallisuusselvityksen hakee useimmiten työnantaja ja työntekijä täyttää aluksi turvallisuusselvitykseen liittyvät lomakkeet. |
| **Toteutusesimerkki** | - Rekrytointien, tehtävämuutosten sekä ulkoisten palveluhankintojen yhteydessä tarkastetaan, edellyttääkö tehtävä turvallisuusselvitystä |
| **Lainsäädäntö** | TiHL 12 §;<br>TLA 9 §;<br>Valtion virkamieslaki 8 c § |
| **Viitteet** | T-10 |
| **Tunniste** | **HAL-11, L:Salassa pidettävä, E:, S:, TS:Henkilötieto** |
| **Nimi** | **Salassapito- ja vaitiolovelvollisuus** |
| **Vaatimus** | Tietoa käsitteleville henkilöille on selvitetty tietojen suojaamista ja asiakirjojen käsitteyä koskevat tietoturvallisuusperiaatteet ja -toimenpiteet. |
| **Toteutusesimerkki** | - Henkilölle selvitetään tietojen suojaamista koskevat periaatteet ennen pääsyä tietoihin,<br>- Henkilö voi allekirjoittaa kirjallisen vaitiolositoumuksen ja allekirjoitus luetteloidaan "vaitiolositoumusluetteloon" tai<br>- Sitoumuksen antamiseen on sähköinen menettely, joka hoidetaan automaattisesti ensimmäisen sisäänkirjautumisen yhteydessä<br>- Salassapito- tai vaitiolositoumusmenettely on käytössä, kun tietoa käsittelee henkilö, jota virkavastuu ei koske |
| **Lainsäädäntö** | TiHL 4 § 2 mom;<br>TLA 6 §, 8 §;<br>Julkisuuslaki 25 §, 26 § 3 mom |
| **Viitteet** | T-11 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 6.6; PiTuKri HT-03 |
| **Tunniste** | **HAL-12, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Ohjeet** |
| **Vaatimus** | Organisaatiossa on ajantasaiset ja kattavat ohjeet tietoturvallisuuden varmistamiseksi. |
| **Yleiskuvaus** | Ohjeistamalla turvallisuuden kannalta keskeiset asiat pyritään varmistumaan siitä, että toiminta ei ole henkilöriippuvaista.<br><br>Organisaatiolla tulisi olla ajantasaiset ohjeet tietojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta sekä tietoturvallisuustoimenpiteistä. Ohjeet kattavat tietoihin liittyvät prosessit ja käsittely-ympäristöt tietojen koko elinkaaren ajalta. |

| | |
|---|---|
| **Toteutusesimerkki** | - Tietojen suojaamiseksi ja tietoturvallisuuden varmistamiseksi tarvittavat menettelyt ja ohjeet on dokumentoitu.<br>- Turvallisuusohjeistus toteutetaan henkilöstön työtehtävien tarpeet huomioiden.<br>- Turvallisuusohjeiden kattavuutta ja ajantasaisuutta seurataan säännöllisesti ja se on tarvittavien tahojen saatavilla. |
| **Lainsäädäntö** | TiHL 4 § 2 mom, 13 § 1 mom;<br>TLA 6 § ja 8 § |
| **Viitteet** | TEK-16.2, T-04 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.37; SFS-EN ISO/IEC 27001:2017 7.5; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 4 |
| **Tunniste** | **HAL-13, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Koulutukset** |
| **Vaatimus** | Organisaatio varmistaa perehdytyksillä, koulutuksilla ja viestinnällä, että henkilöstöllä ja organisaation lukuun toimivilla on tuntemus voimassa olevista turvallisuutta koskevista määräyksistä ja ohjeista. |
| **Yleiskuvaus** | Johdon on huolehdittava siitä, että organisaatiossa on tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja organisaation lukuun toimivilla on tuntemus voimassa olevista tietoturvallisuutta, tiedonhallintaa, tietojenkäsittelyä sekä tietojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja organisaation ohjeista sekä organisaation vastuulla oleviin tietoihin kohdistuvista riskeistä ja uhista.<br><br>Erityisesti koulutuksissa on huomioitava etäkäyttöön, tietojärjestelmien hallinnointiin sekä muihin korkeamman riskin käsittelytilanteisiin liittyvät uhat ja ohjeet. |
| **Toteutusesimerkki** | - Tietoja käsittelevälle henkilölle on selvitetty tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt.<br>- Koulutus toteutetaan henkilöstön työtehtävien tarpeet huomioiden.<br>-Koulutuksen sisältö dokumentoidaan<br>- Koulutuksiin osallistuneista pidetään kirjaa |
| **Lainsäädäntö** | TiHL 4 § 1 mom, 13 § 1 mom;<br>TLA 6 §, 8 § |
| **Viitteet** | T-12 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 6.3; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 5 |
| **Tunniste** | **HAL-14, L:Salassa pidettävä, E:Vähäinen, S:, TS:Henkilötieto** |
| **Nimi** | **Käyttö- ja käsittelyoikeudet** |
| **Vaatimus** | Organisaatio varmistaa, että tietojärjestelmien käyttöoikeudet ja tietojen käsittelyoikeudet määritellään tehtäviin liittyvien tarpeiden mukaan sekä pidetään ajantasaisina. |
| **Yleiskuvaus** | Käyttö- ja käsittelyoikeuksien hallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään niiden luvatonta käyttöä.<br><br>Käyttäjälle annetaan tietojärjestelmiin vain sellaiset käyttöoikeudet ja -valtuudet, jotka ovat työtehtävien kannalta tarpeellisia.<br><br>Käsittelyoikeus tietoihin voidaan antaa vain sille, jolla työtehtäviensä vuoksi on tarve saada tietoja tai muutoin käsitellä niitä, jolle on selvitetty tietojen suojaamista koskevat ohjeet ja joka tuntee tietojen käsittelyä koskevat velvoitteet. |

| | |
|---|---|
| **Toteutusesimerkki** | - Organisaatio on määritellyt periaatteet, joiden mukaan käyttö- ja käsittelyoikeudet myönnetään<br>- Oikeuksien hyväksymiseen on määritelty vastuut ja menettelyt<br>- Oikeuksien toteuttamiseen on määritelty vastuut ja menettelyt |
| **Lainsäädäntö** | TiHL 4 § 2 mom ja 16 §;<br>TLA 8 §, 11 § 1 mom 3 k |
| **Viitteet** | T-13, I-6 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.15, 5.18; PiTuKri HT-05; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65, luku 13; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5, luku 7.6 |
| **Tunniste** | **HAL-14.1, L:TL III, E:, S:, TS:** |
| **Nimi** | **Käyttö- ja käsittelyoikeudet - ajantasainen luettelo** |
| **Vaatimus** | Organisaatio varmistaa, että sillä on ajantasaiset luettelot henkilöiden käyttö- ja käsittelyoikeuksista. |
| **Yleiskuvaus** | Valtionhallinnon viranomaisen on pidettävä luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan I, II tai III asiakirjoja. Luettelossa on mainittava henkilön tehtävä, johon turvallisuusluokitellun tiedon käsittelytarve perustuu. |
| **Lainsäädäntö** | TLA 8 § |
| **Viitteet** | T-13 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.18; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 4.1 |
| **Tunniste** | **HAL-14.2, L:Salassa pidettävä, E:Kriittinen, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Käyttö- ja käsittelyoikeudet - päättyminen** |
| **Vaatimus** | Organisaatio varmistaa, että se, joka ei enää toimi tehtävissä, joihin oikeus tietojen käsittelyyn perustuu, palauttaa tiedot tai tuhoaa ne asianmukaisella tavalla. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 8 § |
| **Viitteet** | T-13 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.18; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 4.1 |
| **Tunniste** | **HAL-15, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Työskentelyn tietoturvallisuus koko palvelussuhteen ajan** |
| **Vaatimus** | Organisaatio huolehtii työskentelyn tietoturvallisuudesta koko palvelussuhteen ajan. |
| **Yleiskuvaus** | Erityisesti tulee huomioida toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja palvelussuhteen päättyessä.<br><br>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.<br><br>Palvelussuhteen päättymiseen liittyviä menettelyjä ovat esimerkiksi avainten, tunnusten sekä aineistojen ja materiaalien luovutus, sekä käsittely-, käyttö- ja pääsyoikeuksien poistaminen. Palvelussuhteen päättyessä on myös oleellista muistuttaa salassapito- ja vaitiolovelvollisuudesta. |

| | |
|---|---|
| **Toteutusesimerkki** | Toimenpiteet edellyttävät tyypillisesti menettelyohjeita, jotka on koulutettu ja saatavilla tarvittavilla henkilöstöryhmillä. Menettelyohjeet voidaan jakaa esimerkiksi palvelussuhteen elinkaaren mukaisiin kokonaisuuksiin.<br><br>Ohjekokonaisuuksia voivat olla esimerkiksi rekrytointiohjeet, perehdyttämisohjeet, palvelussuhteen aikaisten muutosten ohjeet, palvelussuhteen päättymisen ohjeet ja ohjeet yksityiskohtaisempiin toimiin kuten esimerkiksi ohjeet käsittely-, käyttö- ja pääsyoikeuksien muutoksiin. |
| **Lainsäädäntö** | TiHL 4 § 2 mom, 12 §, 16 §;<br>TLA 6 §, 8 § |
| **Viitteet** | T-09 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 6.1, 6.2, 6.3, 6.5; PiTuKri HT-01,Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 5; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 |
| **Tunniste** | **HAL-16, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Hankintojen turvallisuus** |
| **Vaatimus** | Organisaatio varmistaa jo ennakolta, että hankittavat tietojärjestelmät ja palvelut ovat tietoturvallisia. |
| **Yleiskuvaus** | Hankinnoissa on varmistettava, että hankittavat tietojärjestelmät ja palvelut täyttävät käsiteltävien tietoaineistojen mukaiset tietoturvallisuusvaatimukset ja että tietojärjestelmät on soveltuvia viranomaisen tehtävien hoitamiseksi tuloksekkaasti ja tehokkaasti.<br><br>Ennen hankintapäätöstä on suositeltavaa kartoittaa vaihtoehtoja ja karsia vaihtoehtoista 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.<br><br>Eräs yleisesti käytetty menetelmä palveluiden turvallisuuden varmistamiseen on tietojärjestelmien ja niiden palveluntarjoajien arvioinnit, jota on kuvattu yksityiskohtaisesemmin suosituksen "Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa" luvussa 4.<br><br>Osa palveluntarjoajista tarjoaa asiakkailleen mahdollisuuden ottaa käyttöönsä uusia toiminnallisuuksia, jotka ovat esikatselu- tai testausvaiheessa. Mikäli tällaisia toiminnallisuuksia halutaan ottaa käyttöön salassa pidettävän tiedon käsittelyyn, suositellaan riskienarvioinnissa huomioitavaksi muun muassa käyttöönottoon liittyvät vastuut. Uusien toiminnallisuuksien toteutuksessa voi vielä olla turvallisuuspuutteita, joista mahdollisesti aiheutuvien vahinkojen korvaaminen on sopimuksissa usein osoitettu asiakkaalle. |

| | |
|---|---|
| **Toteutusesimerkki** | Organisaatio määrittelee hankinta- ja kehitysprosesseissa tietoturvavaatimukset sekä varmistaa niiden täyttymisen.<br><br>Vaatimusten riittävyyden takaamiseksi organisaatio edellyttää, että tietoturvavaatimukset määritellään, katselmoidaan ja hyväksytään ennen hankinnan etenemistä ja tietoturvatestaus on suoritettu hyväksytysti ennen tietojärjestelmien käyttöönottoja.<br><br>Hankittavan palvelun tai järjestelmän tarjoajan/toimittajan tulee pystyä selvittämään vähintään seuraavat:<br>1) Palvelusta on järjestelmäkuvaus. Palveluntarjoajan kuvauksen perusteella on pystyttävä arvioimaan kyseisen palvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Järjestelmäkuvauksesta tulee käydä ilmi vähintään:<br>a) Palvelun palvelu- ja toteutusmallit, sekä näihin liittyvät palvelutasosopimukset (Service Level Agreements, SLAs).<br>b) Palvelun tarjoamisen elinkaaren (kehittäminen, käyttö, käytöstä poisto) periaatteet, menettelyt ja turvatoimet, valvontatoimet mukaan lukien.<br>c) Palvelun kehittämisessä, ylläpidossa/hallinnassa ja käytössä käytettävän infrastruktuurin, verkon ja järjestelmäkomponenttien kuvaus.<br>d) Muutostenhallinnan periaatteet ja käytännöt, erityisesti turvallisuuteen vaikuttavien muutosten käsittelyprosessit.<br>e) Käsittelyprosessit merkittäville normaalikäytöstä poikkeaville tapahtumille, esimerkiksi toimintatavat merkittävissä järjestelmävikaantumisissa.<br>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.<br>g) Alihankkijoille siirretyt tai ulkoistetut toiminnot.<br><br>Infrastruktuurin, verkon ja järjestelmäkomponenttien kuvauksen tulee olla riittävän yksityiskohtainen, jotta kuvauksen pohjalta pystytään arvioimaan palvelun yleistä soveltuvuutta ja riskejä suhteessa asiakkaan käyttötapaukseen. Vrt. PiTuKri KT-01 (Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi). Infrastruktuurin kuvauksessa voidaan tietyin rajauksin hyödyntää myös ohjelmistokoodia, jonka pohjalta kyseinen infrastruktuuri rakennetaan. |
| **Lainsäädäntö** | TiHL 13 § 4 mom;<br>TLA:n 6 §;<br>621/1999:n 26 § |
| **Viitteet** | I-13 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.19, 5.20, 5.21, 8.29, 8.30; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 6; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 8; Suositus turvallisuusluokiteltujen asiakirjojen käsittelystä pilvipalveluissa 2022:4 luku 4; PiTuKri EE-01 ja KT-01 |
| **Tunniste** | **HAL-16.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Hankintojen turvallisuus - sopimukset** |
| **Vaatimus** | Organisaatio varmistaa, että tietoturvallisuuteen sisältyvät vaatimukset ja niiden säilyminen koko elinkaaren ajan on otettu huomioon sopimuksissa. Sopimusehdot eivät myöskään saa rajoittaa palvelun soveltuvuutta kyseiseen käyttötapaukseen. |

| | |
|---|---|
| **Yleiskuvaus** | Erityisesti pilvipalvelut ovat jatkuvan muutoksen alaisia. Pilvipalveluille ominaista on nopea ja voimakas kehittyminen, mikä edellyttää jatkuvaa sopimusten seurantaa ja valvontaa sekä muutoshallintaa. Muutokset kasvattavat riskiä siitä, että palvelu, sen tarjoaja tai jokin uusi ominaisuus muuttuu sopimuksen- tai vaatimustenvastaiseksi tai toteutuu määräysvaltamuutosriskejä. 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.<br><br>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. Vrt. PiTuKri / TJ-07 (Vaatimustenmukaisuus ja tietosuoja).<br><br>Arvioinnissa tulee huomioida EU:n yleisen tietosuoja-asetuksen 28 artiklan 4. kohdan sekä rikosasioiden tietosuojalain 17 §:n 2 momentin vaatimukset niin sanottuja alikäsittelijöitä käytettäessä. Palveluntarjoajan (rekisterinpitäjän) tulee tehdä henkilötietojen käsittelijän kanssa kirjallinen sopimus.<br><br>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) tai rikosasioiden tietosuojalaissa (7 luku) säädettyjen edellytysten mukaisesti.<br><br>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.<br><br>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 §). |
| **Lainsäädäntö** | TiHL 13 §;<br>TLA:n 6 §;<br>621/1999 26 §;<br>(EU) 679/2016 artikla 28.4 |
| **Viitteet** | I-13 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.20; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa 2020:18, luku 6; PiTuKri TJ-07; |
| **Tunniste** | **HAL-17, L:, E:Tärkeä, S:Tärkeä, TS:** |
| **Nimi** | **Tietojärjestelmien toiminnallinen käytettävyys ja vikasietoisuus** |
| **Vaatimus** | Organisaatio varmistaa tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden riittävällä testauksella säännöllisesti. |

| | |
|---|---|
| **Yleiskuvaus** | Olennaisilla tietojärjestelmillä tarkoitetaan sellaisia tietojärjestelmiä, jotka ovat kriittisiä viranomaisen lakisääteisten tehtäviä toteuttamisen kannalta erityisesti hallinnon asiakkaille palveluja tuotettaessa.<br><br>Toiminnallisella käytettävyydellä tarkoitetaan tietojärjestelmän käyttäjän kannalta sen varmistamista, että tietojärjestelmä on helposti opittava ja käytössä sen toimintalogiikka on helposti muistettava, sen toiminta tukee niitä työtehtäviä, joita käyttäjän pitää tehdä tietojärjestelmällä ja tietojärjestelmä edistää sen käytön virheettömyyttä. |
| **Toteutusesimerkki** | - Organisaatio tunnistaa ja luetteloi tehtävien hoitamisen kannalta olennaiset tietojärjestelmät esimerkiksi osana suojattavien kohteiden luettelointia ja tiedon luokittelua.<br>- Organisaatio määrittelee olennaisten tietojärjestelmien saatavuuskriteerit, joita vasten vikasietoisuus voidaan testata. Järjestelmäkohtaiste saatavuuskriteerien määrittelyssä voidaan hyödyntää tietojärjestelmien saatavuusluokittelua.<br>- Organisaatio määrittelee toiminnallisen käytettävyyden kriteerit.<br>- Organisaation hankintaprosesseissa ja hankintaohjeissa on huomioitu toiminnalliseen käytettävyyteen ja vikasietoisuuteen liittyvät vaatimukset.<br>- Organisaatio dokumentoi vikasietoisuuden testaukset. |
| **Lainsäädäntö** | TiHL 13 § 2 mom |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.29, JHS 212, Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 7 |
| **Tunniste** | **HAL-17.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Tietojärjestelmien toiminnallinen käytettävyys ja vikasietoisuus - saavutettavuus** |
| **Vaatimus** | Organisaation on varmistettava digitaalisten palveluiden saavutettavuus lainsäädännön edellyttämässä laajuudessa. |
| **Yleiskuvaus** | Saavutettavuus tarkoittaa sitä, että mahdollisimman moni erilainen ihminen voi käyttää verkkosivuja ja mobiilisovelluksia mahdollisimman helposti. Saavutettavuus on ihmisten erilaisuuden ja moninaisuuden huomiointia verkkosivujen ja mobiilisovelluksien suunnittelussa ja toteutuksessa. Saavutettavan digipalvelun suunnittelussa ja toteutuksessa pitää huomioida kolme osa-aluetta: tekninen toteutus, helppokäyttöisyys ja sisältöjen selkeys ja ymmärrettävyys.<br><br>Koska saavutettavuus ei kuulu tiedonhallintalautakunnan toimivallan piiriin, on saavutettavuus mukana Julkri-kriteeristössä ainoastaan ylätason varmistus-kriteerinä. 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. |
| **Lainsäädäntö** | Laki digitaalisten palvelujen tarjoamisesta 306/2019 |
| **Muita lisätietoja** | www.saavutettavuusvaatimukset.fi |
| **Tunniste** | **HAL-18, L:Julkinen, E:, S:, TS:** |
| **Nimi** | **Asiakirjajulkisuuden toteuttaminen** |

| | |
|---|---|
| **Vaatimus** | Organisaatio varmistaa, että tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvän tietojenkäsittely suunnitellaan siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa. |
| **Yleiskuvaus** | Vaatimus kohdistuu viranomaisiin, jotka käytännössä vastaavat tietoaineistoissa olevien tietojen saatavuudesta. Vaatimus korostaa sitä, että viranomaisen tietojärjestelmissä olevista tiedoista on pystyttävä muodostamaan tietojärjestelmässä olevilla hakutoiminnoilla viranomaisen asiakirjoja viranomaisen toiminnan julkisuuden toteuttamiseksi. |
| **Toteutusesimerkki** | - Organisaatiot määrittelevät vastuullaan oleviin tietoaineistoihin kohdistuvat tiedonsaantitarpeet ottaen huomioon erityisesti viranomaisten tietojen julkisuuteen kohdistuvat vaatimukset.<br>- Organisaatiot huomioivatn toteutus- ja hankintaprosesseissa vaatimukset asiakirjajulkisuuden vaivattomasta toteuttamisesta.<br>- Organisaatio seuraa asiakirjajulkisuuden toteuttamiseen liittyviä tarpeita ja ylläpitää vanhoja tietojärjestelmiä tarpeen mukaan. |
| **Lainsäädäntö** | TiHL 13 § 3 mom |
| **Tunniste** | **HAL-19, L:Julkinen, E:, S:, TS:Henkilötieto** |
| **Nimi** | **Tietojen käsittely** |
| **Vaatimus** | Organisaatio varmistaa, että tietoja käsitellään ja säilytetään siten, että pääsy tietoihin suojataan sivullisilta. |
| **Yleiskuvaus** | Tietojen käsittelyn ja säilytyksen turvallisuuteen vaikuttavat muun muassa fyysisten tilojen turvallisuus, tietojen käsittelyssä käytettävien tietojärjestelmien ja päätelaitteiden turvallisuus sekä tietoja käsittelevien henkilöiden ohjeet ja koulutus.<br><br>Organisaation turvallisuuden hallinnan prosessien avulla tulee varmistaa, että tarvittavat toimenpiteet kaikkien edellä lueteltujen osa-alueiden suhteen on tehty.<br><br>Yksityiskohtaisempia kriteerit eri turvallisuustasoille luokiteltujen tietojen käsittelemisestä ja säilyttämisestä on esitetty fyysisen turvallisuuden ja teknisen turvallisuuden osa-alueilla. |
| **Toteutusesimerkki** | Organisaatio on varmistanut tietojen käsittelyn turvallisuuden esimerkiksi seuraavilla toimenpiteillä:<br>- 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.<br>- Organisaatio on ohjeistanut missä tiloissa eri turvallisuustasoille luokiteltuja tietoja saa käsitellä ja säilyttää.<br>- Organisaatio on ohjeistanut, miten tietoihin pääsy tulee suojata sivullisilta eri käsittelyympäristöissä<br>- Organisaatio on määritellyt miten eri tietojen käsittelyyn tarkoitetut tietojärjestelmät tulee säilyttää<br>- Organisaatio on määritellyt tietojen käsittelyssä käytettävien päätelaitteiden vaatimukset. |
| **Lainsäädäntö** | TiHL 13 §, 15 § 2 mom;<br>TLA 10 § 1 mom |
| **Viitteet** | FYY-03, Fyy-04, I-17 |

| | |
|---|---|
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.15; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 4; |

# 3 Fyysinen turvallisuus

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

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

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

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

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

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

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

Työskentely on mahdollista järjestää myös eri organisaatioille yhteisissä toimitiloissa. Tällöin yhteisissä toimitiloissa tulee noudattaa yhteisiä toimitilaturvallisuuteen liittyviä periaatteita, jotka mahdollistavat salassa pidettävän tiedon asianmukaisen käsittelyn ja säilyttämisen. Kunkin tietoja käsittelevän organisaation tulee lisäksi varmistaa, että yhteisten toimitilojen tarjoama turvallisuus on riittävä suhteessa organisaatioon kohdistettuihin fyysisen turvallisuuden vaatimuksiin.

| | |
|---|---|
| **Tunniste** | **FYY-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Fyysisen turvallisuuden riskien arviointi** |
| **Vaatimus** | Fyysiset turvatoimet on mitoitettava riskien arvioinnin mukaisesti. |
| **Yleiskuvaus** | Riskien arvioinnissa tulee ottaa huomioon esimerkiksi pääsyoikeuksien hallintaan ja muihin turvallisuusjärjestelyihin liittyviin prosesseihin sisällytettävät tiedonsaantitarpeen, tehtävien eriyttämisen ja vähimpien oikeuksien periaatteet. Fyysisiä turvatoimia koskevan riskien arvioinnin tulee olla säännöllistä ja osa organisaation riskienhallinnan kokonaisuutta. Arvioiduilla riskeillä on nimetyt omistajat. Hyväksyttyjen fyysisten turvatoimien muutoksiin liittyvät riskit tulee arvioida muutosten yhteydessä. Erityisesti korvaavien fyysisten turvatoimien osalta tulee pystyä osoittamaan perustelut valituille turvatoimille. |
| **Toteutusesimerkki** | Riskien arvioinnissa on otettava huomioon kaikki asiaan kuuluvat tekijät, erityisesti seuraavat:<br>a) Tietojen turvallisuusluokka ja salassapitoperuste;<br>b) Tietojen käsittely- ja säilytystapa sekä määrä ottaen huomioon, että tietojen suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista;<br>c) Tietojen käsittely- ja säilytysaika<br>d) Tietojen käsittely- ja säilytyspaikan ympäristö: rakennuksen ympäristö, sijoittuminen rakennuksessa, tilassa tai sen osassa;<br>e) Hälytystilanteisiin liittyvä vasteaika<br>f) Ulkoistetut toiminnot, kuten huolto-, siivous-, kiinteistö- ja turvallisuuspalvelut<br>g) Tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu uhka tiedoille |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom |
| **Viitteet** | HAL-06, F-02 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 36 |
| **Tunniste** | **FYY-01.1, L:TL III, E:, S:, TS:** |
| **Nimi** | **Fyysisen turvallisuuden riskien arviointi - TEMPEST** |
| **Vaatimus** | Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös TEMPEST-riski. |
| **Yleiskuvaus** | Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös TEMPEST-riski, eli sähkömagneettisen hajasäteilyn aiheuttama riski. TEMPEST-riskiä voidaan yleensä pienentää muuttamalla tiedon käsittelypaikan sijaintia kiinteistössä. |
| **Lainsäädäntö** | TLA 11 § 2 mom |
| **Viitteet** | TEK-14, F-05.8, F-06.10 |
| **Tunniste** | **FYY-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Fyysisten turvatoimien valinta (monitasoinen suojaus)** |
| **Vaatimus** | Turvallisuusalueilla ja niitä ympäröivissä tiloissa on toteutettava turvallisuusalueen suojausta vaarantavia tekoja ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä, toimenpiteitä suojausta vaarantavien tekojen havaitsemiseksi ja jäljittämiseksi sekä toimenpiteitä vaarantanutta tekoa edeltäneen turvallisuustason palauttamiseksi viipymättä monitasoista suojausperiaatetta soveltaen.<br><br>Laitteet on tarkastettava ja huollettava säännöllisin väliajoin. |

| | |
|---|---|
| **Yleiskuvaus** | Salassa pidettäviä tietoja ja asiakirjoja sisältävät tietovarannot sekä niiden käsittelyyn käytetyt tietojärjestelmät on sijoitettava viranomaisen tähän tarkoitukseen määrittelemälle suojatulle-alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa kuvattu hallinnollinen alue tai tieto pitää suojata riskiperusteisesti muilla turvakontrolleilla.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>Salassa pidettävien tietojen käsittely on mahdollista myös yhteisissä työympäristöissä, joissa voi työskennellä useita eri organisaatioita. Tällöin fyysisen turvallisuuden tasosta sovitaan tarvittaessa etukäteen, jotta tilat mahdollistavat salassa pidettävän tiedon asianmukaisen käsittelyn ja säilyttämisen jokaisen organisaation tarpeet huomioiden. Olennaista näissä tapauksissa on tiedon käsittelijän vastuu käsitellä tietoja niin, ettei tietoon oikeudeton saa haltuunsa tietoja. |

| | |
|---|---|
| **Toteutusesimerkki** | Monitasoinen suojaus muodostuu hallinnollisista, toiminnallisista ja fyysisistä keinoista, kuten:<br>a) rakenteelliset esteet: fyysinen este, jolla turvallisuusalueet ja sitä ympäröivät tilat rajataan ja luvatonta tunkeutumista vaikeutetaan ja hidastetaan;<br>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.<br>c) tunkeutumisen ilmaisujärjestelmä: rakenteellisen esteen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisen ilmaisujärjestelmää (murtohälytysjärjestelmä). Järjestelmää voidaan käyttää myös vartiointihenkilöstön tekemän valvonnan asemasta tai tueksi.<br>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.<br>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.<br>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.<br>g) valaistus: mahdollinen tunkeutuja voidaan havaita valaistuksen avulla ja vartiointihenkilöstö voi valvoa aluetta tehokkaasti, joko suoraan tai kameravalvontajärjestelmää hyödyntämällä.<br>h) muut asianmukaiset fyysiset toimenpiteet, joiden tarkoituksena on estää ja havaita luvaton pääsy tai ehkäistä turvallisuusluokiteltujen tietojen katoaminen tai vahingoittuminen. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 7 § |
| **Viitteet** | F-03 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 33; ISO/IEC 27002:2022 7.1, 7.2, 7.3 |
| **Tunniste** | **FYY-03, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tiedon käsittely** |
| **Vaatimus** | Tietoja on käsiteltävä siten, että pääsy niihin suojataan sivullisilta. |

| | |
|---|---|
| **Yleiskuvaus** | Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen tietoon että laittomalta tiedustelulta. Suojaaminen tarkoittaa käytännössä esimerkiksi suoran näkö- tai kuuloyhteyden estämistä turvallisuusluokiteltuun tietoon.<br><br>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.<br><br>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. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 10 § |
| **Viitteet** | HAL-19, F-04 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 29 |
| **Tunniste** | **FYY-04, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tiedon säilytys** |
| **Vaatimus** | Tietoja on säilytettävä siten, että pääsy niihin suojataan sivullisilta. |
| **Yleiskuvaus** | Suojaaminen tarkoittaa käytännössä esimerkiksi tiedon tai tietoa sisältävän päätelaitteen riittävän turvallista säilyttämistä. Tietojen käsittelyssä on huomioitava lisäksi toiminta työskentelytaukojen aikana, jolloin asiakirjat ja päätelaitteet on turvallisuusluokan perusteella sijoitettava soveltuvalle turvallisuusalueelle ja/tai säilytysyksikköön tauon ajaksi. Tiedon säilytyksellä viitataan tilanteeseen, jossa tieto ei ole sen käsittelijän välittömässä valvonnassa. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 10 § |
| **Viitteet** | HAL-19, F-04 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28- 29 |
| **Tunniste** | **FYY-04.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Tiedon säilytys - TL IV** |
| **Vaatimus** | Organisaatio säilyttää paperiasiakirjat<br>- turva-alueella tai hallinnollisella alueella soveltuvaksi arvioidussa toimistokalusteessa tai<br>- tilapäisesti turvallisuusalueiden ulkopuolella jos tiedon käsittelijä on sitoutunut noudattamaan annetuissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä.<br><br>Organisaatio säilyttää sähköisessä muodossa olevat tiedot<br>- turva-alueella tai hallinnollisella alueella vaatimukset täyttävässä laitteessa tai sähköisessä tietovälineessä tai<br>- turvallisuusalueiden ulkopuolella vaatimukset täyttävässä päätelaitteessa tai sähköisessä tietovälineessä valvotussa tilassa tai soveltuvassa lukitussa toimistokalusteessa turvapussissa tai vastaavalla tavalla. |

| | |
|---|---|
| **Toteutusesimerkki** | Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, tulisi alueen seinien, lattian, katon, ikkunoiden ja ovien täytettävä vähintään standardin SFS-EN-1627 luokkaa RC3 vastaava suoja.<br><br>Mikäli turvallisuusluokitellun tiedon säilytysyksikkönä käytetään lukittua toimistokalustetta, on varmistuttava siitä, että tunkeutumisesta jää murtojälki. |
| **Lainsäädäntö** | TLA 10 § |
| **Viitteet** | F-04 |
| **Tunniste** | **FYY-04.2, L:TL III, E:, S:, TS:** |
| **Nimi** | **Tiedon säilytys - TL III** |
| **Vaatimus** | Organisaatio säilyttää paperiasiakirjat turva-alueella soveltuvaksi arvioidussa säilytysratkaisussa.<br><br>Organisaatio säilyttää sähköisessä muodossa olevat tiedot<br>- turva-alueella vaatimukset täyttävässä laitteessa tai sähköisessä tietovälineessä tai<br>- turva-alueiden ulkopuolella vaatimukset täyttävässä päätelaitteessa valvotussa tilassa tai soveltuvassa lukitussa toimistokalusteessa turvapussissa tai vastaavalla tavalla. |
| **Lainsäädäntö** | TLA 10 § |
| **Viitteet** | F-04 |
| **Tunniste** | **FYY-04.3, L:TL II, E:, S:, TS:** |
| **Nimi** | **Tiedon säilytys - TL II** |
| **Vaatimus** | Organisaatio säilyttää paperiasiakirjat turva-alueella soveltuvaksi arvioidussa säilytysratkaisussa.<br><br>Organisaatio säilyttää sähköisessä muodossa olevat tiedot turva-alueella vaatimukset täyttävässä laitteessa tai sähköisessä tietovälineessä. |
| **Lainsäädäntö** | TLA 10 § |
| **Viitteet** | F-04 |
| **Tunniste** | **FYY-05, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Turvallisuusalue** |
| **Vaatimus** | Turvallisuusalueiden eli hallinnollisten alueiden sekä turva-alueiden on noudatettava tässä kriteerissä annettuja suosituksia. |
| **Yleiskuvaus** | Monet fyysisen turvallisuuden suositukset ovat yhteisiä sekä hallinnollille alueille että turva-alueille. Tähän kriteeriin on koottu yhteiset suositukset, jotka tulee ottaa huomioon sekä hallinnollisten alueiden että turva-alueiden arvioinneissa. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 9 § |
| **Viitteet** | F-05.4, F-06.6 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39 |
| **Tunniste** | **FYY-05.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Turvallisuusalue - Äänieristys** |
| **Vaatimus** | Alueen äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selvänaisena suojattavaan tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan suojattavista tiedoista, joihin kaikilla ei ole tiedonsaantitarvetta. |

| | |
|---|---|
| **Yleiskuvaus** | Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta kyseiseen keskusteltavaan tietoon että laittomalta tiedustelulta. Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan suojattavista tiedoista.<br><br>Äänieristystä voidaan arvioida esimerkiksi kuuntelemalla keskustelua tilan ulkopuolelta ovien, seinien sekä ilmastointiputkien ja muiden läpivientien kohdalta. Tilan äänieristystä voidaan myös tarvittaessa verrata rakenteille annettavaan ilmaääneneristävyysvaatimukseen. |
| **Toteutusesimerkki** | Vaatimus voidaan määrittää standardin SFS-EN-ISO 717-1 mukaisesti. Ilmaääneneristävyys voidaan todeta standardin SFS-EN-ISO 16283-1 mukaisesti tehdyllä mittauksella. Arvioinnissa tulee huomioida ilmanääneneristävyyden lisäksi myös runkoääneneristävyys.<br><br>Äänieristysvaatimus voidaan tarvittaessa saavuttaa esimerkiksi tilan uudelleen sijoittelulla, rakenteiden ja läpivientien eristävyyden parantamisella tai arvioitavan tilan ulkopuolisten tilojen taustamelulla. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 10 § 1 mom |
| **Viitteet** | F-05.4, F-06.6 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39 |
| **Tunniste** | **FYY-05.2, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Turvallisuusalue - Salaa katselun estäminen** |
| **Vaatimus** | Jos tietoihin kohdistuu salaa tai vahingossa katselun riski, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet. |
| **Toteutusesimerkki** | Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 10 § 1 mom |
| **Viitteet** | HAL-19, F-05.6, F-06.8 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 40 ja 45 |
| **Tunniste** | **FYY-05.3, L:TL II, E:, S:, TS:** |
| **Nimi** | **Turvallisuusalue - Tila- ja laitetarkastukset** |
| **Vaatimus** | Organisaation on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella alueella, jossa käsitellään turvallisuusluokan II tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi.<br><br>Myös alue on tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin sekä mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta. |
| **Yleiskuvaus** | Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista luotettavasti (esim. matkapuhelimet, älykellot, jne.), laitteet tulee jättää tilan ulkopuolelle esimerkiksi tähän tarkoitukseen varattuun säilytysratkaisuun. |
| **Lainsäädäntö** | TLA 7 §, 10 § 1 mom, 11 § 2 mom |
| **Viitteet** | F-05.7, F-06.9 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 40 ja 46 |

| | |
|---|---|
| **Tunniste** | **FYY-05.4, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Turvallisuusalue - Pääsyoikeuksien ja avaintenhallinnan menettelyt** |
| **Vaatimus** | Organisaation on määriteltävä alueen pääsyoikeuksien ja avainhallinnan menettelyt ja roolit. |
| **Yleiskuvaus** | Pääsyn rajaaminen alueelle voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien ja avainhallinnan menettelyistä.<br><br>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.<br><br>Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua: Lukot heloineen: SFS 7020+5970, luokat 1-4, tavoitetaso 3; Elektroniset kulunvalvontajärjestelmät: SFS-EN 60839-11-1 ja 2, Huomioitava esimerkiksi SFS-EN 50131-standardin vaatimukset, mikäli kulunvalvontajärjestelmä on osa tunkeutumisen ilmaisujärjestelmää. |
| **Toteutusesimerkki** | Alueelle on nimetty vastuuhenkilö, joka huolehtii seuraavista pääsyoikeuksien ja avainhallinnan menettelyistä.<br>- pääsyoikeuksien ja avainten hallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu.<br>- pääsyoikeuksien ja avainten haltijoista on lista.<br>- pääsyoikeudet tarkastetaan säännöllisesti ja ne pidetään ajan tasalla.<br>- avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet on vastuutettu.<br>- avainkortteja, jakamattomia avaimia ja kulkutunnisteita säilytetään asianmukaisesti.<br>- avaimen luovutusperuste kirjataan dokumenttiin.<br>- avaimet luovutetaan vain itsenäisen pääsyoikeuden alueelle saaneelle henkilölle.<br>- henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa avainten hallintaoikeuteen. |
| **Lainsäädäntö** | TiHL 15 § 2 mom;<br>TLA 9 § |
| **Viitteet** | F-05.2, F-06.3 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 39 ja 44; ISO/IEC 27002:2022 7.2 |
| **Tunniste** | **FYY-05.5, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Turvallisuusalue - Vierailijat** |
| **Vaatimus** | Muilla kuin organisaation asianmukaisesti valtuuttamilla henkilöillä (vierailijoilla) on aina saattaja. |

| | |
|---|---|
| **Yleiskuvaus** | Vieraiden isännällä tulee olla itsenäinen pääsyoikeus turvallisuusalueelle, jolle hän vie vieraat sekä oikeus isännöidä vieraita. Vierailumenettelyillä on varmistuttava, ettei vierailulla vaaranneta alueella käsiteltävän tai säilytettävän tiedon luottamuksellisuutta.<br><br>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.<br><br>Saattamaton vierailijamenettely (unescorted visitor) on mahdollista hyväksyä alueen niille vierailijoille, jotka täyttävät pääsyoikeuksien myöntämisen vaatimukset. |
| **Toteutusesimerkki** | Organisaation on hyväksynyt menettelyohjeen vierailijoita varten. Vierailijaohje voi käsitellä muun muassa seuraavia asioita:<br>- Vieras tunnistetaan ja varustetaan vieraskortilla.<br>- Vierailu kirjataan.<br>- Vierailijoita ei päästetä tai jätetä alueille valvomatta ja isäntä vastaa ulkopuolisista henkilöistä koko vierailun ajan.<br>- Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten.<br>- Huolehtiminen siitä, ettei vieras pääse oikeudettomasti näkemään, kuulemaan tai muutoin saa haltuunsa suojattavaa tietoa.<br>- Henkilökunta on ohjeistettu reagoimaan ilman tunnistetta liikkuviin henkilöihin. |
| **Lainsäädäntö** | TLA 9 § |
| **Viitteet** | F-05.3, F-06.4 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 39 ja 44 |
| **Tunniste** | **FYY-06, L:Salassa pidettävä, E:, S:, TS:** |
| **Nimi** | **Hallinnollinen alue** |
| **Vaatimus** | Hallinnollisen alueen tulee täyttää tässä osiossa esitetyt suositukset sekä riskilähtöisesti arvioidut tarkennukset siten, että turvatoimien tavoitteet saavutetaan. |
| **Yleiskuvaus** | Salassa pidettäviä tietoja ja asiakirjoja sisältävät tietovarannot sekä niiden käsittelyyn käytetyt tietojärjestelmät on sijoitettava viranomaisen tähän tarkoitukseen määrittelemälle suojatulle-alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa kuvattu hallinnollinen alue tai tieto pitää suojata riskiperusteisesti muilla turvakontrolleilla.<br><br>Hallinnollisella alueella tarkoitetaan normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta.<br><br>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.<br><br>Lisäksi hallinnollisen alueen tulee täyttää kaikki turvallisuusalueita koskevat yhteiset vaatimukset, jotka on kuvattu kriteerissä "Turvallisuusalue". |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 9 § |

| | |
|---|---|
| **Viitteet** | FYY-05, F-05 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 38 |
| **Tunniste** | **FYY-06.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Hallinnollinen alue - alueen raja ja rakenteet** |
| **Vaatimus** | Alueella on oltava selkeästi määritelty näkyvä raja, mutta aluetta rajaavalle rakenteelle (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet) ei aseteta erityisiä vaatimuksia. |
| **Yleiskuvaus** | Fyysisten turvatoimien tavoite tulee täyttyä ennen kuin turvallisuusalueet voidaan hyväksyä. Alueen rakenne voi olla normaalia toimistorakennetta. Aluetta rajaavia rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Näitä vahvennuksia tulee arvioida suhteessa alueen ympäröivien tilojen antamaan muuhun suojaan sekä vartiointihenkilöstön vasteaikaan. Alueen aukot, jotka eivät ole käytössä kulkemiseen, on voitava lukita tai sulkea, jotta alueelle kulkua voidaan hallinnoida asianmukaisesti. Mikäli hallinnollisen alueen rajoilla on käytetty mekaanista lukkoa, lukon avainten kopiointi tulisi olla estetty patenttisuojalla. Mikäli mahdollista, hätäpoistumistiet eivät saa kulkea turva-alueen kautta. Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät ratkaisut ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. |
| **Toteutusesimerkki** | Standardeja, joita voidaan käyttää referenssinä arvioitaessa aluetta rajaavia rakenteita: Seinät ja ovet sekä lattia- ja kattorakenteet: SFS-EN 1627, RC1-RC6; Ikkunat (suojauslasi): SFS-EN 356, P4A-P5A ja P6B-P8B |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 9 § 1 mom 1 k |
| **Viitteet** | F-05.1 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien<br>asiakirjojen käsittelystä 2021:5 sivut 39 |
| **Tunniste** | **FYY-06.2, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Hallinnollinen alue - kulunvalvonta** |
| **Vaatimus** | Alueelle pääsyä tulee valvoa, mikäli se on riskien arvioinnin perusteella tarkoituksenmukaista. |
| **Yleiskuvaus** | Kulunvalvonta voi olla tarkoituksenmukaista esimerkiksi, jos alueella käsitellään turvallisuusluokan III tai korkeamman luokan tietoa. |
| **Toteutusesimerkki** | Suositus kulunvalvonnan toteuttamisesta:<br>- Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita.<br>- Henkilöllä on vain ne kulkuoikeudet, joita hän tarvitsee työtehtäviensä hoitamiseksi.<br>- Kulkuoikeuden myöntämisperuste kirjataan dokumenttiin ja vain nimetyillä henkilöillä on kulkuoikeudet alueelle.<br>- Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa kulkuoikeuksiin.<br>- Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu, jos se on hyvin hallinnoitu. |
| **Lainsäädäntö** | TLA 7 §, 9 § |
| **Viitteet** | F-05.2 |
| **Tunniste** | **FYY-06.3, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Hallinnollinen alue - pääsyoikeuksien myöntäminen** |
| **Vaatimus** | Ainoastaan asianmukaisesti valtuutetuilla henkilöillä on itsenäinen pääsy alueelle. |
| **Yleiskuvaus** | Pääsyn rajaaminen alueelle voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. |

| | |
|---|---|
| **Lainsäädäntö** | TLA 9 § |
| **Viitteet** | FYY-05.4, F-05.2 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 39 |
| **Tunniste** | **FYY-06.4, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Hallinnollinen alue - tunkeutumisen ilmaisujärjestelmät** |
| **Vaatimus** | Tarvittaessa tunkeutumisen ilmaisujärjestelmää voidaan käyttää täydentävänä monitasoisen suojauksen riskienhallintakeinona. |
| **Yleiskuvaus** | Alue ja sinne johtavat ovet voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa lukittavassa toimistokalusteessa ja murtoriski arvioidaan todennäköiseksi.<br><br>Alue tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Alueen mahdollista tunkeutumisen ilmaisujärjestelmää tai korvaavaa järjestelyä arvioitaessa tulee ottaa huomioon alueen rakenteita koskevan vaatimuksen yhteydessä käsitelty vasteaika-arvio. Mikäli alue on valvottu tunkeutumisen ilmaisujärjestelmällä, alueen suositellaan olevan valvottu järjestelmän avulla, kun alueella ei työskennellä. Tunkeutumisen ilmaisujärjestelmän sijoitustilan tulisi sijaita sen suojaamalla turvallisuusalueella. |
| **Toteutusesimerkki** | Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua:<br><br>Tunkeutumisen ilmaisujärjestelmät: SFS-EN 50131 luokat 1 – 4, tavoitetaso 2; Tunkeutumisen ilmaisujärjestelmän ilmoituksensiirto: SFS-EN 50136-1 luokat DP1 - DP4 ja SP5 - SP6; Vartioimisliikkeen hälytyskeskus: SFS-EN 50518 |
| **Lainsäädäntö** | TLA 7 § |
| **Viitteet** | F-05.5 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 40 |
| **Tunniste** | **FYY-07, L:TL III, E:, S:, TS:** |
| **Nimi** | **Turva-alue** |
| **Vaatimus** | Turva-alueen tulee täyttää tässä osiossa esitetyt suositukset sekä riskilähtöisesti arvioidut lisätarkennukset siten, että monitasoisen suojauksen tavoitteet saavutetaan. |
| **Yleiskuvaus** | Turva-alueella tarkoitetaan organisaation työskentelyyn tarkoitettuja, hallinnollista aluetta paremmin suojattuja alueita ja tiloja, joissa turvallisuusluokiteltuja tietoja käsitellään ja säilytetään. Turva-alue voidaan tilapäisesti perustaa hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten.<br><br>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.<br><br>Lisäksi turva-alueen tulee huomioida kaikki turvallisuusalueita koskevat yhteiset suositukset, jotka on kuvattu kriteerissä "Turvallisuusalue". |
| **Lainsäädäntö** | TLA 7 §, 9 § |
| **Viitteet** | FYY-05, F-06 |

| | |
|---|---|
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43 |
| **Tunniste** | **FYY-07.1, L:TL III, E:, S:, TS:** |
| **Nimi** | **Turva-alue - alueen raja ja rakenteet** |
| **Vaatimus** | Alueella on oltava selkeästi määritelty näkyvä raja. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen säilytyksen edellyttämä turvallisuustaso. |
| **Yleiskuvaus** | Alueen aukot, joita ei käytetä kulkemiseen, on voitava lukita tai sulkea kalteroinnilla tai vahvoilla terässäleiköillä, 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.<br><br>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.<br><br>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.<br><br>Hätäpoistumistiet eivät saa kulkea turva-alueen kautta. Mikäli hätäpoistumistien on välttämätöntä kulkea turva-alueen kautta, tulee varmistua, että hätäpoistumistie on varustettu tunkeutumisen ilmaisujärjestelmällä. Turva-aluetta jonka läpi kulkee hätäpoistumistie ei voida hyväksyä, mikäli turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin tai alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua. |
| **Toteutusesimerkki** | Seinät ja ovet sekä lattia- ja kattorakenteet: SFS-EN 1627, RC1-RC6, tavoitetaso RC3; Ikkunat (suojauslasi): SFS-EN 356, P4A-P5A ja P6B-P8B, tavoitetaso P5A |
| **Lainsäädäntö** | TLA 9 § 1 mom 2 k |
| **Viitteet** | F-06.1 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43 |
| **Tunniste** | **FYY-07.2, L:TL III, E:, S:, TS:** |
| **Nimi** | **Turva-alue - kulunvalvonta** |
| **Vaatimus** | Alueen rajalla tulee valvoa kaikkea kulkua sisään ja ulos kulkulupien avulla tai tunnistamalla henkilöt henkilökohtaisesti. |

| | |
|---|---|
| **Yleiskuvaus** | Kulunvalvonta voidaan toteuttaa joko elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Alueen rajalla voidaan käyttää kaksipuoleista kulunvalvontaa. Suosituksena on käyttää kaksoistunnistusta sisään ja/tai ulos mentäessä.<br><br>Kulunvalvontajärjestelmän etäyhteydet ja lukijalaitteiden asennus tulee toteuttaa riskienarvioinnin perusteella riittävän tietoturvallisesti siten, että järjestelmään pääsy on vain valtuutetuista päätelaitteista ja verkoista ja että tietoliikenneyhteys ja kulunvalvontajärjestelmän rajapinnat on suojattu siten, että ulkopuolisilla ei ole pääsyä välitettyihin tietoihin. Kulunvalvontajärjestelmän sijoitustilan tulisi sijaita sen suojaamalla turvallisuusalueella. |
| **Toteutusesimerkki** | Suositus kulunvalvonnan toteuttamisesta:<br>- Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita.<br>- Turva-alueen kulkuoikeudet myöntää nimetty vastuuhenkilö organisaatiossa<br>- Kulunvalvonnan hallintajärjestelmän menettelytavat on ohjeistettu ja dokumentoitu:<br>-- Myönnetyistä kulkuoikeuksista laaditaan dokumentti ja sitä ylläpitää nimetty vastuuhenkilö.<br>-- Henkilöllä on vain ne kulkuoikeudet, joita hän tarvitsee työtehtäviensä hoitamiseksi.<br>-- Kulkuoikeuden myöntämisperuste kirjataan dokumenttiin ja vain nimetyillä henkilöillä on kulkuoikeudet alueelle.<br>-- Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa kulkuoikeuksiin.<br>-- Organisaatioon kuuluvan henkilöstön ja ulkopuolisten henkilöiden luettelot pidetään erillään.<br>-- Kulkuoikeudet katselmoidaan säännöllisin väliajoin esimerkiksi 6kk:n välein organisaatiosta nimetyn vastuuhenkilön toimesta.<br>-- Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu, jos se on hyvin hallinnoitu<br>-- Peruskäyttäjän työasemalta tapahtuva oven avaus turva-alueelle pitää olla estetty<br>- Turva-alueelle kulkuoikeus on vain alueelle oikeutetulla henkilöllä. Kulku alueelle pitää olla myöhemmin todennettavissa.<br>- Kulku tilaan pitää olla myöhemmin todennettavissa.<br>- Tunnisteiden tulee käyttää nykyaikaista ja salattua lukutekniikkaa tai edellyttää kaksoistunnistusta<br><br>Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia: Elektroniset kulunvalvontajärjestelmät: SFS-EN 60839-11-1 ja 2, luokat 1-4. Kameravalvontajärjestelmät: SFS-EN 62676, Suunnittelu Finanssialan K-menetelmän mukaisesti. Kameravalvontajärjestelmän tallenteiden säilymisaika määritellään riskiperusteisesti organisaation poikkeamien havainnointikyvyn mukaisesti huomioiden ennakoivat ja reagoivat menettelyt. Suositeltava vähimmäisaika tallenteille on 1 kk. Lisäksi kameravalvontajärjestelmä voidaan liittää tunkeutumisen ilmaisujärjestelmään. |
| **Lainsäädäntö** | TLA 9 § 1 mom 2 k |
| **Viitteet** | F-06.2 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 43 |
| **Tunniste** | **FYY-07.3, L:TL III, E:, S:, TS:** |
| **Nimi** | **Turva-alue - pääsyoikeuksien myöntäminen** |
| **Vaatimus** | Itsenäinen pääsyoikeus alueelle voidaan myöntää vain organisaation asianmukaisesti valtuuttamalle henkilölle, jonka luotettavuus on varmistettu ja jolla on erityinen lupa tulla alueelle. |

| | |
|---|---|
| **Yleiskuvaus** | Luotettavuus tulisi ensisijaisesti varmistaa henkilöturvallisuusselvitysmenettelyn avulla.<br><br>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. |
| **Lainsäädäntö** | TLA 9 § 1 mom 2 k |
| **Viitteet** | FYY-05.4, F-06.3 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 44 |
| **Tunniste** | **FYY-07.4, L:TL III, E:, S:, TS:** |
| **Nimi** | **Turva-alue - vierailijat** |
| **Vaatimus** | Jos turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin:<br>- alueella tavanomaisesti säilytettyjen tietojen korkein turvallisuusluokka on ilmoitettava selkeästi sekä<br>- kaikilla vierailijoilla on oltava erityinen lupa tulla alueelle, heillä on aina oltava saattaja ja heidän luotettavuutensa on oltava varmistettu asianmukaisesti, paitsi jos on varmistettu, ettei vierailijoilla ole pääsyä turvallisuusluokiteltuihin tietoihin. |
| **Yleiskuvaus** | Kriteeri täydentää kaikkia turvallisuusalueita koskevaa kriteeriä "Turvallisuusalue - Vierailijat". |
| **Lainsäädäntö** | TLA 9 § 1 mom 2 k, 10 § 1 mom |
| **Viitteet** | FYY-05.5, F-06.4 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 44 |
| **Tunniste** | **FYY-07.5, L:TL III, E:, S:, TS:** |
| **Nimi** | **Turva-alue - turvallisuusohjeet** |
| **Vaatimus** | Kullekin turva-alueelle on laadittava määräykset noudatettavista turvallisuusmenettelyistä. |
| **Yleiskuvaus** | Turvallisuusohjeet kattavat turvallisuusluokiteltuun tietoon liittyvät prosessit ja turvallisuusalueet koko tiedon elinkaaren ajalta. Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti. Turvallisuusohjeiden ajantasaisuus sekä jalkautuminen varmistetaan säännöllisesti, vähintään vuosittain. |
| **Toteutusesimerkki** | Kullekin turva-alueelle on laadittava turvallisuusmenettelyt, joissa on määräykset seuraavista asioista:<br>a) Tiedon säilyttäminen ja käsitteleminen alueella: turvallisuusluokka tiedoille, joita alueella voidaan käsitellä ja säilyttää.<br>b) Sovellettavat valvonta- ja suojatoimenpiteet.<br>c) Pääsyoikeuksien myöntäminen alueelle: henkilöt, joilla on pääsy alueelle ilman saattajaa erityisen luvan ja luotettavuuden varmistamisen perusteella.<br>d) Vierailijat: tarvittaessa menettelyt saattajien käyttämiseksi tai turvallisuusluokiteltujen tietojen suojaamiseksi silloin, kun muille henkilöille myönnetään pääsy alueelle.<br>e) Muut asiaan kuuluvat toimenpiteet ja menettelyt. |
| **Lainsäädäntö** | TiHL 4 § 2 mom;<br>TLA 10 § 1 mom |
| **Viitteet** | HAL-12, F-06.5 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 45 |

| Tunniste | FYY-07.6, L:TL III, E:, S:, TS: |
|---|---|
| **Nimi** | **Turva-alue - tunkeutumisen ilmaisujärjestelmät** |
| **Vaatimus** | Alue, jolla ei ole henkilöstöä palveluksessa vuorokauden ympäri, on tarvittaessa tarkastettava normaalin työajan päätteeksi ja satunnaisiin aikoihin työajan ulkopuolella, paitsi jos alueelle on asennettu tunkeutumisen ilmaisujärjestelmä (murtohälytysjärjestelmä). |
| **Yleiskuvaus** | Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet) ja/tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Alueen mahdollista tunkeutumisen ilmaisujärjestelmää tai korvaavaa järjestelyä arvioitaessa tulee ottaa huomioon alueen rakenteita koskevan vaatimuksen yhteydessä käsitelty vasteaika-arvio. Mikäli alue on valvottu tunkeutumisen ilmaisujärjestelmällä, alueen suositellaan olevan valvottu järjestelmän avulla, kun alueella ei työskennellä.<br><br>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.<br><br>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.<br><br>Vartiointihenkilöstön tulee olla kohdekoulutettu alueella toimimiseen. Vartiointihenkilöstön osaamisen ja<br>työvälineiden tulee olla riittävät suhteessa toimintaympäristön riskeihin. Hälytystilanteessa alueelle voidaan edellyttää saapuvan kaksi henkilöä samanaikaisesti, mikäli turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin tai alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua. |
| **Toteutusesimerkki** | Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia: Tunkeutumisen ilmaisujärjestelmät: SFS-EN 50131, luokat 1 – 4, tavoitetaso 3; Tunkeutumisen ilmaisujärjestelmän ilmoituksensiirto: SFS-EN 50136-1, luokat DP1 - DP4 ja SP5 - SP6, tavoitetaso DP3-DP4 (dual path) tai SP5-SP6 (single path); Vartioimisliikkeen hälytyskeskus: SFS-EN 50518, Liikkeen on oltava standardin mukaisesti pätevä ja lisäksi ylläpidettävä SFS-EN ISO 9001:n mukaista sertifioitua laadunhallintajärjestelmää tai liikkeen tulee olla arvioitu soveltuvin osin tätä standardia vastaavaksi. |
| **Lainsäädäntö** | TLA 7 §, 9 § 1 mom 2 k |
| **Viitteet** | F-06.7 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 45 |
| **Tunniste** | **FYY-07.7, L:TL III, E:, S:, TS:** |

| | |
|---|---|
| **Nimi** | **Turva-alue - säilytysyksiköiden avaimet ja pääsykoodit** |
| **Vaatimus** | Säilytysyksiköiden avaimet tai pääsykoodit ovat sellaisten henkilöiden hallussa, joilla on tiedonsaantitarve säilytysyksikössä säilytettävään tietoon. Kyseisten henkilöiden on osattava numeroyhdistelmät ulkoa.<br><br>Turvallisuusluokiteltuja tietoja sisältävien säilytysyksiköiden numeroyhdistelmät on vaihdettava:<br>- tehdaskoodit on vaihdettava uuden turvallisen säilytyspaikan vastaanoton yhteydessä<br>- aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos.<br>- aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen.<br>- kun jokin lukoista on huollettu tai korjattu. |
| **Lainsäädäntö** | TLA 8 §, 9 § 1 mom 2, 10 § 1 mom |
| **Viitteet** | F-06.10 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 46 |
| **Tunniste** | **FYY-08, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tietojen välitys postilla ja kuriirilla** |
| **Vaatimus** | 1. Tiedot tulee kuljettaa tietojen riittävän suojaamisen huomioivia, organisaation ohjeita noudattaen.<br>2. Tiedot on pakattava niin, että ne on suojattu luvattomalta ilmitulolta.<br>3. Tietoja saa kuljettaa turvallisuusalueiden ulkopuolelle suojaamalla sähköiset tietovälineet riittävän turvallisella salauksella.<br>4. Salaamattomia tietoja voidaan kuljettaa postipalvelujen välityksellä. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 13 § |
| **Viitteet** | TEK-15, FYY-02, F-08.1 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 26-28 |
| **Tunniste** | **FYY-08.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Tietojen välitys postilla ja kuriirilla - TL IV** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Turvallisuusluokan IV tiedoille vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:<br>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).<br>2) Tieto toimitetaan kotimaassa tavallisena postina, kirjattuna kirjeenä tai ko. turvallisuusluokalle hyväksytyn menettelyn mukaisesti. Ulkomaille toimitus postin välityksellä vain viranomaisen erillishyväksyntään pohjautuen.<br>3) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä.<br>4) Organisaatiossa on tunnistettu vaatimukset ja toteutettu menettelyt erityissuojattavien tietojen (esimerkiksi salausavaimet) välittämiseksi. |
| **Lainsäädäntö** | TLA 13 § |
| **Viitteet** | F-08.1 |
| **Tunniste** | **FYY-08.2, L:TL III, E:, S:, TS:** |
| **Nimi** | **Tietojen välitys postilla ja kuriirilla - TL III** |

| | |
|---|---|
| **Vaatimus** | Turvallisuusluokan II-III salaamaton tieto on kuljettamista varten pakattava asianmukaisesti sekä kuljetettava se jatkuvan valvonnan alaisuudessa vastaanottajalle. Mainitun tiedon saa kuljettaa vastaanottajalle myös muulla turvallisella tavalla, jolla tiedon luottamuksellisuus ja eheys varmistetaan kyseiselle turvallisuusluokalle riittävällä tavalla. |
| **Toteutusesimerkki** | Turvallisuusluokkien III tiedoille vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraavat toimenpiteet:<br>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).<br>6) Tieto toimitetaan ko. turvallisuusluokiteltuun tietoon oikeutetun organisaation henkilön toimesta jatkuvan valvonnan alaisuudessa vastaanottajalle. Vaihtoehtoisesti toimitus ko. turvallisuusluokalle hyväksytyn menettelyn mukaisesti.<br>7) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä turvallisuusselvitettyä henkilöstöä. |
| **Lainsäädäntö** | TLA 13 § |
| **Viitteet** | F-08.1 |
| **Tunniste** | **FYY-08.3, L:TL II, E:, S:, TS:** |
| **Nimi** | **Tietojen välitys postilla ja kuriirilla - TL II** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Turvallisuusluokan II tiedoille vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraavat toimenpiteet:<br>8) Tieto pakataan suljettavaan kaksinkertaiseen kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää turvallisuusluokasta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän turvallisuusluokiteltua tietoa (kirjekuorien tai vastaavien on oltava läpinäkymättömiä). Sisäkuoren on oltava sinetöity. Vastaanottaja on ohjeistettava tarkistamaan sinetöinnin eheys ja ilmoitettava välittömästi, mikäli eheyden vaarantumista epäillään. |
| **Lainsäädäntö** | TLA 13 § |
| **Viitteet** | F-08.1 |
| **Tunniste** | **FYY-09, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tietojen kopioiminen** |
| **Vaatimus** | Kopioihin ja käännöksiin sovelletaan alkuperäistä tietoa koskevia turvatoimia. |
| **Yleiskuvaus** | Tulostimet ja kopiokoneet tulkitaan tietojärjestelmiksi ja niiden tulee siten täyttää vaatimukset sekä teknisen, fyysisen että hallinnollisen tietoturvallisuuden osalta. Tekniset vaatimukset voi täyttää muun muassa erillislaiteratkaisulla. |
| **Toteutusesimerkki** | Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:<br>1) Kopioita käsitellään kuten alkuperäistä tietoa.<br>2) Kopion voi luovuttaa edelleen vain henkilölle, jolla on käsittelyoikeus tietoon ja tarve tietosisältöön.<br>3) Kopion/tulosteen saa ottaa vain ko. turvallisuustason vaatimukset täyttävällä laitteella. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 2 § 2 mom |
| **Viitteet** | F-08.2 |

| | |
|---|---|
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 28 |
| **Tunniste** | **FYY-09.1, L:TL II, E:, S:, TS:** |
| **Nimi** | **Tietojen kopioiminen - TL II** |
| **Vaatimus** | Tietojen kopiot ja niiden käsittelijät on luetteloitava.<br><br>Tietojen kopiointia varten on hankittava tiedon laatineen viranomaisen lupa. |
| **Toteutusesi-merkki** | Vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraava toimenpide:<br>4) Kopiointi ja käsittelijät merkitään diaariin/rekisteriin tai luetteloidaan jollakin muulla vastaavalla menettelyllä. |
| **Lainsäädäntö** | TLA 14 § 1 mom 3 ja 4 k |
| **Viitteet** | F-08.2 |
| **Tunniste** | **FYY-10, L:TL III, E:, S:, TS:** |
| **Nimi** | **Tietojen kirjaaminen** |
| **Vaatimus** | Turvallisuusluokan III tai sitä korkeamman luokan tiedon vastaanottaminen ja lähettäminen tulee kirjata.<br><br>Turvallisuusluokan III tietojen ja niitä korkeamman tason tietojen käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi). |
| **Yleiskuvaus** | Kirjaamisella tarkoitetaan sellaisten menettelyjen soveltamista, joilla rekisteröidään tiedon elinkaari, mukaan lukien sen jakelu ja hävittäminen. Jos kyseessä on tietojärjestelmä, kirjaamismenettelyt voidaan suorittaa järjestelmän omien prosessien avulla.<br><br>Tiedon elinkaaren rekisteröinnin käytännön toteutukset edellyttävät tyypillisesti muun muassa tapahtumien jäljitettävyydestä varmistumista. |
| **Lainsäädäntö** | TLA 14 § 1 mom 1 ja 2 k |
| **Viitteet** | F-08.3 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivu 19-23 |
| **Tunniste** | **FYY-11, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tietojen fyysinen tuhoaminen** |
| **Vaatimus** | Ei-sähköisten tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. |

| | |
|---|---|
| **Yleiskuvaus** | Tiedon suojaamisesta tulee huolehtia tiedon elinkaaren päättymiseen asti. Tämä tulee huomioida erityisesti tilanteissa, joissa käytetään kolmannen osapuolen palvelua tiedon tuhoamiseen. Käytännön toteutusmallina yleensä menettely, jossa tiedosta vastuussa oleva organisaatio valvoo tiedon tuhoamisprosessin aina elinkaaren päättymiseen saakka.<br><br>Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia.<br><br>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). |
| **Lainsäädäntö** | TiHL 21 §;<br>TLA 15 § |
| **Viitteet** | TEK-20, F-08.4 |
| **Muita lisätietoja** | Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 sivut 29-31 |
| **Tunniste** | **FYY-11.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Tietojen fyysinen tuhoaminen - TL IV** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | - Paperiaineistojen silppukoko on enintään 30 mm2 (DIN 66399 / P5 tai DIN 32757 / DIN 4).<br>- Magneettisten kiintolevyjen silppukoko on enintään 320 mm2 (DIN 66399 / H-5.<br>- SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm2 (DIN 66399 / E-5).<br>- Optisten medioiden silppukoko on enintään 10 mm2 (DIN 66399 / O-5). |
| **Lainsäädäntö** | TLA 15 § |
| **Viitteet** | F-08.4 |
| **Tunniste** | **FYY-11.2, L:TL III, E:, S:, TS:** |
| **Nimi** | **Tietojen fyysinen tuhoaminen - TL III** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | - Paperiaineistojen silppukoko on enintään 30 mm2 (DIN 66399 / P5 tai DIN 32757 / DIN 4).<br>- Magneettisten kiintolevyjen silppukoko on enintään 10 mm2 (DIN 66399 / H-6).<br>- SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm2 (DIN 66399 / E-5).<br>- Optisten medioiden silppukoko on enintään 5 mm2 (DIN 66399 / O-6). |
| **Lainsäädäntö** | TLA 15 § |
| **Viitteet** | F-08.4 |
| **Tunniste** | **FYY-11.3, L:TL II, E:, S:, TS:** |
| **Nimi** | **Tietojen fyysinen tuhoaminen - TL II** |
| **Vaatimus** | Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle.<br><br>Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö. |

| | |
|---|---|
| **Toteutusesi-merkki** | - Paperiaineistojen silppukoko on enintään 10 mm2 (DIN 66399 / P6).<br>- Magneettisten kiintolevyjen silppukoko on enintään 10 mm2 (DIN 66399 / H-6).<br>- SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 1 mm2 (DIN 66399 / E-6).<br>- Optisten medioiden silppukoko on enintään 5 mm2 (DIN 66399 / O-6). |
| **Lainsäädäntö** | TLA 15 § |
| **Viitteet** | F-08.4 |

# 4 Tekninen turvallisuus

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

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

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

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

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

| | |
|---|---|
| **Toteutusesimerkki** | Turvallisuusluokittelemattoman salassa pidettävän tiedon sekä myös turvallisuusluokan IV tietojenkäsittely-ympäristön yhdistäminen eri turvallisuusluokan ympäristöihin voidaan toteuttaa palomuuriratkaisuilla ja rajaamalla riskialttiiden alemman turvallisuusluokan ympäristöä käyttävien palvelujen (web-selailu, Internetin kautta reitittyvä sähköposti, ja vastaavat) liikenne kulkemaan erillisten sisältöä suodattavien välityspalvelinten kautta. Turvallisuusluokittelemattoman salassa pidettävän sekä myös turvallisuusluokan IV käsittely-ympäristöjä on mahdollista kytkeä Internetiin ja muihin ei-luotettuihin verkkoihin, edellyttäen että kytkennän tuomia riskejä pystytään muilla suojauksilla pienentämään riittävästi. Internet-kytkentäisyyden tuomien riskien pienentäminen turvallisuusluokittelemattomalle salassa pidettävälle tiedolle sekä turvallisuusluokalle IV edellyttää erityisesti ohjelmistopäivityksistä huolehtimista, vähimpien oikeuksien periaatteen mukaisia käyttöoikeuksia, järjestelmäkovennuksia sekä kykyä poikkeamien havainnointiin ja korjaaviin toimiin. Tyypillinen käyttötapa turvallisuusluokittelemattoman salassa pidettävän tai/ja turvallisuusluokan IV käsittely-ympäristölle on organisaation "toimistoverkon" tietojenkäsittely-ympäristön osa, joka voi muodostua esimerkiksi päätelaitepalveluista, sovelluspalveluista, tietoliikennepalveluista sekä niiden suojaamiseen liittyvistä järjestelyistä. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 § 1 mom 1 ja 2 k |
| **Viitteet** | I-01, I-06, I-08, I-11, I-19 |
| **Tunniste** | **TEK-01.3, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Verkon rakenteellinen turvallisuus - palomuuri** |
| **Vaatimus** | Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 §:n 1 mom 1 ja 2 k |
| **Viitteet** | I-01 |
| **Muita lisätietoja** | PiTuKri TT-01 |
| **Tunniste** | **TEK-01.4, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Verkon rakenteellinen turvallisuus - salaaminen turva-alueiden ulkopuolella** |
| **Vaatimus** | Hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne salataan riittävän turvallisella salausratkaisulla. |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | I-01 |
| **Tunniste** | **TEK-01.5, L:TL III, E:, S:, TS:** |
| **Nimi** | **Verkon rakenteellinen turvallisuus - yhdyskäytäväratkaisun käyttö** |
| **Vaatimus** | Turvallisuusluokat III-II:<br>Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää riittävän turvallisen yhdyskäytäväratkaisun käyttöä. |

| | |
|---|---|
| **Yleiskuvaus** | Tietojenkäsittely-ympäristöjen oletetaan lähtökohtaisesti olevan toisilleen ei-luotettuja myös tilanteissa, joissa yhdistetään eri organisaatioiden hallinnoimia tietojenkäsittely-ympäristöjä toisiinsa. Saman turvallisuusluokan käsittely-ympäristöjä voidaan liittää toisiinsa ko. turvallisuusluokalle riittävän turvallisen salausratkaisun avulla (esimerkiksi organisaation eri toimipisteiden ko. turvallisuusluokan käsittely-ympäristöjen yhteenliittäminen julkisen verkon ylitse).<br><br>Huom: Turvallisuusluokan ylitys hallintaliikenteen osalta edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymää yhdyskäytäväratkaisua. Käytännössä hallintaliikenne rajataankin lähes poikkeuksetta turvallisuusluokittain. Hallintaliikenteen suojausperiaatteet on käsitelty yksityiskohtaisemmin Katakri 2020:n kohdassa I-04. |
| **Toteutusesimerkki** | Turvallisuusluokasta III lähtien yhdistäminen eri turvallisuusluokkien ympäristöihin voidaan toteuttaa riittävän turvallisilla yhdyskäytäväratkaisuilla. Yhdyskäytäväratkaisun tulee luotettavasti estää ylemmän turvallisuusluokan tiedon kulkeutuminen matalamman turvallisuusluokan ympäristöön. Turvallisten, hyväksyttävissä olevien yhdyskäytäväratkaisujen suunnitteluperiaatteita ja yleisiä ratkaisumalleja on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa (www.ncsa.fi > "Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista").<br><br>Turvallisuusluokan III käsittely-ympäristöt ovat moniportaisesti loogisesti tai fyysisesti eiluotetuista verkoista/järjestelmistä eristettyjä kokonaisuuksia. Fyysisellä eristämisellä tarkoitetaan OSI-mallin fyysisen kerroksen tasolla tapahtuvaa erottelua. Turvallisuusluokan III käsittely-ympäristöihin ei pääsääntöisesti kytketä mitään muita verkkoja/järjestelmiä. Mikäli loppukäyttäjän työtehtävät edellyttävät pääsyä Internetiin tai muihin eri turvallisuusluokan järjestelmiin/verkkoihin, se on yleensä perustelluinta järjestää erillisellä tietokoneella, jota ei kytketä turvallisuusluokan III verkkoon. Toimivaltainen viranomainen voi tapauskohtaisesti hyväksyä myös turvallisuusluokan III käsittely-ympäristön fyysisen kytkemisen erikseen tarkastettuun ja hyväksyttyyn verkkoon/järjestelmään. Tällaiset erikseen hyväksytyt verkot/järjestelmät jakautuvat yleisimmin neljään käyttötilanteeseen:<br><br>A. Tiedonsiirtojärjestelmät<br>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.<br><br>B. Palvelujärjestelmät<br>Turvallisuusluokan III järjestelmä/verkko voi olla esimerkiksi tietokantapalvelu, jota käytetään useasta fyysisestä pisteestä. Verkkotason rajapinta on tällöin vastaava kuin käyttötilanne A:ssa.<br><br>C. Yhdyskäytäväratkaisut<br>C1. Turvallisuusluokan III tiedon käsittely-ympäristöön voidaan siirtää tietoa alemman turvallisuusluokan ympäristöstä yksisuuntaisen liikenteen sallivan yhdyskäytäväratkaisun (esim. datadiodi) kautta. Vastaavilla järjestelyillä voidaan toteuttaa myös turvallisuusluokan II mukainen ratkaisu. Turvallisuusluokkien IV ja III väliseen liikennöintiin voidaan hyödyntää myös alkiotunnistukseen perustuvaa sisältösuodatusratkaisua (Vrt. kohta C2 alla).<br>C2. Turvallisuusluokan III tiedon käsittely-ympäristöstä voidaan siirtää matalamman turvallisuusluokan tietoa matalamman turvallisuusluokan ympäristöön alkiotunnistukseen perustuvan sisältösuodatusratkaisun kautta. Sisältösuodatusratkaisun käyttö edellyttää tiedon tunnistamista ylemmän tason ympäristössä, ja vain matalamman tason tiedon siirtymisen sallimista ylemmän turvallisuusluokan ympäristöstä matalamman tason ympäristöön. |

| | |
|---|---|
| | D. Muut käsittely-ympäristöt<br>Muut turvallisuusluokan III käsittely-ympäristöt ovat yleisimmin organisaation tuotekehitysverkkoja tai muita turvallisuusluokan III tiedon käsittely-ympäristöjä. Tällaisiin järjestelmiin voidaan kytkeä esimerkiksi vain tätä ympäristöä palveleva päivityspalvelin. Päivityspalvelimelta voidaan sallia keskitetty turvapäivitysten ja haittaohjelmatunnisteiden jakelu tietyin rajauksin. Jaeltavat päivitykset ja tunnistekannat voidaan tuoda päivityspalvelimelle ilmaraon yli, tai vaihtoehtoisesti esimerkiksi datadiodin läpi. |
| **Lainsäädäntö** | TLA 11 § 1 mom 1 ja 2 k |
| **Viitteet** | I-01 |
| **Tunniste** | **TEK-01.6, L:TL II, E:, S:, TS:** |
| **Nimi** | **Verkon rakenteellinen turvallisuus - TL II käsittely** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Turvallisuusluokan II käsittely-ympäristöt ovat lähtökohtaisesti fyysisesti eristettyjä kokonaisuuksia, joihin sallitaan turvallisuusluokan ylittävä liikennöinti vain datadiodien tai vastaavien OSI-mallin fyysisellä kerroksella toimivien yksisuuntaisten yhdyskäytäväratkaisujen kautta. |
| **Lainsäädäntö** | TLA 11 § 1 mom 1 ja 2 k |
| **Viitteet** | I-01 |
| **Tunniste** | **TEK-01.7, L:TL I, E:, S:, TS:** |
| **Nimi** | **Verkon rakenteellinen turvallisuus - TL I käsittely** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |

| | |
|---|---|
| **Toteutusesimerkki** | Lähtökohtaisesti turvallisuusluokan I tietojenkäsittely-ympäristöt suositellaan pidettäväksi fyysisesti eriytettyinä kaikista muista ympäristöistä. Tyypillisenä toteutustapana on fyysisellä turva-alueella, hajasäteilysuojatussa tilassa tapahtuva kaikista muista ympäristöistä fyysisesti eriytetty tietojenkäsittely tähän tarkoitukseen varatulla päätelaitteella. Toteutustapana voi olla myös vastaavasti turva-alueella hajasäteilysuojattuun tilaan fyysisesti sijoitettu ja muista ympäristöistä fyysisesti eriytetty päätelaitteista, niitä yhdistävästä paikallisesta verkosta ja tähän tarkoitukseen varatusta erillistulostimesta koostuva tietojenkäsittely-ympäristö.<br><br>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.<br><br>Mikäli kansallisen turvallisuusluokan I tietojenkäsittely-ympäristö on toiminnallisten tarpeiden näkökulmasta ehdottoman välttämätöntä yhdistää matalamman turvallisuusluokan ympäristöön, tulisi yhdistäminen tapahtua turvallisuusluokalle I hyväksytyn yhdyskäytäväratkaisun kautta. Turvallisuusluokan I tietojenkäsittelyympäristöjen erotteluun hyväksyttyjä yhdyskäytäväratkaisuja on saatavilla rajoitetusti, keskittyen tyypillisesti vain yksisuuntaisen liikennöinnin (TL II --> TL I) mahdollistavien datadiodiratkaisujen moniportaisiin ratkaisumalleihin. Yhdyskäytäväratkaisuja on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa. |
| **Lainsäädäntö** | TLA 11 § 1 mom 1 ja 2 k |
| **Viitteet** | I-01 |
| **Tunniste** | **TEK-02, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tietoliikenne-verkon vyöhykkeistäminen** |
| **Vaatimus** | Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava monitasoisen suojaamisen periaatteen mukaisesti. |
| **Yleiskuvaus** | Tietoliikenneverkon jakaminen ko. turvallisuusluokan sisällä erillisille verkko-alueille (vyöhykkeet ja segmentit) voi tarkoittaa esimerkiksi tietojen suojaamisen näkökulmasta tarkoituksenmukaista työasema- ja palvelinerottelua, kattaen myös mahdolliset hankekohtaiset erottelutarpeet.<br><br>Kaikkia liitettyjä tietotekniikkajärjestelmiä tulisi lähtökohtaisesti käsitellä epäluotettavina ja varautua yleisiin verkkohyökkäyksiin. Yleisiin verkkohyökkäyksiin varautumiseen sisältyy esimerkiksi vain tarpeellisten toiminnallisuuksien pitäminen päällä. Toisin sanoen jokaiselle päällä olevalle toiminnallisuudelle tulisi olla perusteltu toiminnallinen tarve. Toiminnallisuus tulisi rajata suppeimpaan toiminnalliset vaatimukset täyttävään osajoukkoon (esimerkiksi toiminnallisuuksien näkyvyyden rajaus). Lisäksi tulisi ottaa huomioon esimerkiksi osoitteiden väärentämisen (spoofing) estäminen ja verkkojen näkyvyyden rajaaminen. |
| **Toteutusesimerkki** | Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:<br>1) Tietoliikenneverkko on jaettu ko. turvallisuusluokan sisällä erillisiin verkko-alueisiin (vyöhykkeet, segmentit).<br>2) Verkko-alueiden välistä liikennettä rajoitetaan ja ympäristöön sisäänpäin tulevaan liikenteeseen noudatetaan default-deny sääntöä.<br>3) Tietojenkäsittely-ympäristössä on varauduttu yleisiin verkkohyökkäyksiin. |

| | |
|---|---|
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 § 1 mom 1 ja 2 k |
| **Viitteet** | I-02 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02 |
| **Tunniste** | **TEK-02.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Tietoliikenne-verkon vyöhykkeistäminen - vähimpien oikeuksien periaate** |
| **Vaatimus** | Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien periaatteen mukaisesti. |
| **Yleiskuvaus** | Verkkoalueiden välisen liikenteen valvonnan ja rajoittamisen voi toteuttaa turvallisuusluokan IV verkon ulkorajalla esimerkiksi siten, että kaikki sisäänpäin tulevat yhteydenavausyritykset estetään ja ulospäin lähtevät yhteydet rajataan vain välityspalvelimen kautta tulevaan web-selailuun sekä sähköpostiliikenteeseen. Kaikkien turvallisuusluokkien verkoissa riittävä vähimpien oikeuksien periaatteen huomiointi edellyttää tyypillisesti myös sitä, että turvallisuusluokan sisällä eri verkkoalueiden välillä sallitaan vain tarpeelliset yhteydet (lähde-kohde-protokolla) ja että muut yhteysyritykset havaitaan. 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. Kytkentöjen ja konfiguraatioiden turvallisesta toiminnasta tulee varmistua säännöllisesti, vrt. I-03. Turvallisuusluokalla IV tulisi myös ottaa huomioon palvelunestohyökkäyksen uhka, mikäli järjestelmä liitetään ei-luotettuun verkkoon.<br><br>Suodatusten tulisi perustua vähimpien oikeuksien periaatteeseen ja suodatuksen tulisi sallia vain erikseen hyväksytty liikennöinti (default-deny). Suodatuksissa tulisi huomioida myös eri protokollien (esim. IPv4, IPv6, GRE, IPSec-tunnelit, reititysprotokollat, sekä myös ylempien kerrosten protokollat, esim. HTTP, SSH, FTP ja SMTP) toiminnallisuudet. Tarpeettomat protokollat tulisi poistaa käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa niille ei ole todellista käyttöperustetta, ja varmistettava liikennöinnin estyminen (verkko-, työasema- ja palvelintason) palomuurien suodatussäännöillä. Mikäli työasemissa, palvelimissa, verkkolaitteissa tai muissa vastaavissa järjestelmissä käytetään esimerkiksi IPv6-toiminnallisuutta, tulisi ottaa huomioon sen vaikutukset erityisesti liikenteen suodatukseen (palomuurauksen tulisi kattaa myös IPv6-liikenne) sekä reititykseen. Myös eri protokollien yhdistämis- ja yhteiskäyttöratkaisujen (esim. IPv4-IPv6-toteutukset, NAT-64, Teredo) vaikutukset tulisi ottaa huomioon verkon/järjestelmien turvallisuuden kokonaissuunnittelussa. |
| **Toteutusesimerkki** | Turvallisuusluokkien IV-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan aiemmin mainittujen toimenpideuden lisäksi:<br>4) Verkko-alueiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti sallitaan (default-deny). |
| **Lainsäädäntö** | TLA 11 § 1 mom 1 ja 2 k |
| **Viitteet** | I-02 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02 |
| **Tunniste** | **TEK-03, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Suodatus- ja valvontajärjestelmien hallinnointi** |
| **Vaatimus** | Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan. |

| | |
|---|---|
| **Yleiskuvaus** | Liikennettä suodattavia ja/tai valvovia järjestelmiä ovat tyypillisesti palomuurit, reitittimet, IDS- ja IPS-järjestelmät sekä vastaavia toiminnallisuuksia sisältävät verkkolaitteet, palvelimet ja sovellukset.<br><br>Riittävän dokumentaation toteutus edellyttää yleensä esimerkiksi verkkorakenteen kuvaamista verkkoalueineen (vyöhykkeet ja segmentit) sillä tarkkuudella, että dokumentaation pohjalta voidaan tarkastaa verkon vastaavan toimivaltaisen viranomaisen hyväksymää rakennetta.<br><br>Käytettävyyden ja riittävän dokumentoinnin varmistamisen kannalta tarkoituksenmukainen ratkaisu on usein suodatus- ja valvontajärjestelmien asetusten (konfiguraatioiden, ml. esimerkiksi palomuurisäännöstöt) varmuuskopiointi, ja varmuuskopioiden turvallisuusluokan mukainen säilytys.<br><br>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). |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 § 1 mom 2 k |
| **Viitteet** | I-03 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.21, 8.23 |
| **Tunniste** | **TEK-03.1, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Suodatus- ja valvontajärjestelmien hallinnointi - vastuutus ja organisointi** |
| **Vaatimus** | Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen, poistaminen ja valvonta on vastuutettu ja organisoitu. |
| **Lainsäädäntö** | TiHL 4 § 2 mom 1 k;<br>TLA 11 § 1 mom 2 k |
| **Viitteet** | I-03 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.35, Katakri 2020 I-16; PiTuKri MH-01 |
| **Tunniste** | **TEK-03.2, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Suodatus- ja valvontajärjestelmien hallinnointi - dokumentointi** |
| **Vaatimus** | Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia. |
| **Lainsäädäntö** | TiHL 5 § 2 mom;<br>TLA 11 § 1 mom 2 k |

| | |
|---|---|
| **Viitteet** | HAL-09, I-03 |
| **Tunniste** | **TEK-03.3, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Suodatus- ja valvontajärjestelmien hallinnointi - tarkastukset** |
| **Vaatimus** | Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 § 1 mom 2 k |
| **Viitteet** | I-03 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.32 |
| **Tunniste** | **TEK-04, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Hallintayhteydet** |
| **Vaatimus** | Hallintapääsy tapahtuu rajattujen, hallittujen ja valvottujen pisteiden kautta. |
| **Yleiskuvaus** | Laitteilla/liittymillä tarkoitetaan alla kuvatuissa toteutusesimerkeissä järjestelmiä, joihin pitäisi olla hallintaoikeudet vain ylläpitäjillä tai vastaavilla. Tällaisia ovat tyypillisesti esimerkiksi palomuurit, reitittimet, kytkimet, langattomat tukiasemat, palvelimet, työasemat, erilliset konsoliliittymät (esim. iLO, iDrac) ja Blade-runkojen hallintaliittymät.<br><br>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.<br><br>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 kansallisen 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 toimivaltaisen viranomaisen hyväksymän yhdyskäytäväratkaisun kautta tarjota joissain tapauksessa (read-only) valvontapääsy luokkaa matalamman turvallisuusluokan ympäristöön.<br><br>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. Katakri 2020 / I-10). Etähallinnan edellytyksiä on kuvattu tarkemmin vaatimuksessa Katakri 2020 / I-18.<br><br>Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa:<br>- 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<br>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.<br>- 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 päätelaitteista käsin. Turvallisuusluokiteltua tietoa sisältävän pilvipalvelualustan hallinnointi tuleekin rajata kyseisen turvallisuusluokan vaatimukset täyttäviin päätelaitteisiin. Huomioitava, että myös päätelaitteiden hallinnointiratkaisujen ja muiden niihin kytkeytyvien taustajärjestelmien tulee täyttää kyseisen turvallisuusluokan vaatimukset, kuten myös fyysiset tilat/alueet, joista hallintaa suoritaan.<br>- Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat<br>vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia. |
| **Toteutusesimerkki** | Rajattu pääsy tulee toteuttaa esimerkiksi hyppykoneiden, hallintaportaalien ja vastaavien menettelyiden kautta. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 14 § 1 mom;<br>TLA 11 § 1 mom |
| **Viitteet** | I-04 |
| **Muita lisätietoja** | Traficom: Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista (2.12.2021); ISO/IEC 27002:2022 8.2, 8.20, 8.21, 8.22; PiTuKri IP-03, TT-01 |
| **Tunniste** | **TEK-04.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Hallintayhteydet - vahva tunnistaminen julkisessa verkossa** |
| **Vaatimus** | Hallintapääsyn julkisesta verkosta tai muun käytettävän etähallintaratkaisun tulee edellyttää vahvaa, vähintään kahteen todennustekijään pohjautuvaa käyttäjätunnistusta. |
| **Yleiskuvaus** | Hallintayhteyksien suojaus on eräs kriittisimmistä tietojärjestelmien turvallisuuteen vaikuttavista tekijöistä. Erityisesti turvallisuusluokittelemattomia salassa pidettäviä sekä turvallisuusluokan IV järjestelmiä voi kuitenkin olla perusteltua pystyä hallinnoimaan myös fyysisesti suojattujen turvallisuusalueiden ulkopuolelta. Tilanteissa, joissa etähallinta nähdään perustelluksi, suositellaan se suojattavan etäkäyttöä kattavammilla turvatoimilla. Esimerkiksi turvallisuusluokan IV järjestelmän etähallintayhteydet voidaan rajata yksittäisiin fyysisiin ja loogisiin pisteisiin. |

| | |
|---|---|
| **Toteutusesimerkki** | Hallintayhteydet julkisesta verkosta edellyttävät esimerkiksi VPN-yhteyden muodostamista, jossa vähintään joko käyttäjä tai laite tunnistetaan vahvasti. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 § 1 mom 5 k |
| **Viitteet** | I-04 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.2; PiTuKri IP-03; Katakri 2020 I-04 |
| **Tunniste** | **TEK-04.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Hallintayhteydet - hallintayhteyksen salaaminen** |
| **Vaatimus** | Hallintaliikenne on salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 § 1 mom 4 ja 7 k |
| **Viitteet** | I-04 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.24 |
| **Tunniste** | **TEK-04.3, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Hallintayhteydet - vähimmät oikeudet** |
| **Vaatimus** | Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti. |
| **Lainsäädäntö** | TiHL 16 §;<br>TLA 11 § 1 mom 3 k |
| **Viitteet** | HAL-2.1, I-04 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.20 |
| **Tunniste** | **TEK-04.4, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Hallintayhteydet - henkilökohtaiset tunnukset** |
| **Vaatimus** | Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. |
| **Toteutusesimerkki** | Mikäli henkilökohtaiste tunnusten käyttäminen ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 16 §;<br>TLA 11 § 1 mom 3 ja 5 k |
| **Viitteet** | I-04 |
| **Muita lisätietoja** | PiTuKri IP-02 |
| **Tunniste** | **TEK-04.5, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Hallintayhteydet - yhteyksien rajaaminen turvallisuusluokittain** |
| **Vaatimus** | Hallintayhteydet on rajattu turvallisuusluokittain, ellei käytössä ole turvallisuusluokka huomioon ottaen riittävän turvallista yhdyskäytäväratkaisua. |
| **Toteutusesimerkki** | Tietojenkäsittely-ympäristöön ei ole yhteenliitäntää hallintayhteyksille muiden turvallisuusluokkien ympäristöistä ilman turvallisuusluokan huomioonottaen riittävän turvallista yhdyskäytäväratkaisua. |
| **Lainsäädäntö** | TLA 11 § 1 mom 1 k |
| **Viitteet** | TEK-01, I-04 |
| **Tunniste** | **TEK-04.6, L:TL IV, E:, S:, TS:** |

| | |
|---|---|
| **Nimi** | **Hallintayhteydet - turvallisuusluokiteltua tietoa sisältävät hallintayhteydet** |
| **Vaatimus** | Hallintaliikenteen sisältäessä turvallisuusluokiteltua tietoa ja kulkiessa matalamman turvallisuusluokan ympäristön kautta, turvallisuusluokitellut tiedot on salattu riittävän turvallisella salaustuotteella. |
| **Toteutusesimerkki** | Ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään vain riittävän turvallisen salausratkaisun kautta tilanteissa, joissa hallintaliikenne kulkee matalamman turvallisuusluokan ympäristön kautta. |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | I-04 |
| **Muita lisätietoja** | Katakri 2020 I-12 |
| **Tunniste** | **TEK-04.7, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Hallintayhteydet - salaaminen turvallisuusluokan sisällä** |
| **Vaatimus** | Hallintaliikenteen kulkiessa ko. turvallisuusluokan sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella. |
| **Toteutusesimerkki** | Tilanteissa, joissa hallintaliikenne kulkee ko. turvallisuusluokan sisällä (ko. turvallisuusluokalle riitävän salauksen sisällä tai/ja ko. turvallisuusluokan tiedon säilyttämiseen hyväksytyn turvallisuusalueen sisällä muista ympäristöistä fyysisesti eriytetyn verkon sisällä),<br>a) ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään fyysisesti (esim. konsolikaapeli), tai<br>b) ko. turvallisuusluokan hallintayhteyden liikennekanava on muuten luotettavasti fyysisesti suojattu (esim. turva-alueen sisäiset kaapeloinnit), tai<br>c) ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään matalamman tason salauksella (esim. SSH, HTTPS, SCP) suojatulla yhteydellä.<br>4) Laitteisiin/liittymiin sallitaan hallintayhteydenotot vähimpien oikeuksien periaatteen mukaisesti vain hyväksytyistä lähteistä ja määritellyin käyttäjäoikeuksin. |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | I-04 |
| **Tunniste** | **TEK-04.8, L:TL III, E:, S:, TS:** |
| **Nimi** | **Hallintayhteydet - TL III** |
| **Vaatimus** | Turvallisuusluokan III käsittely-ympäristöjen etähallinta tulee suorittaa turva-alueelta. |
| **Lainsäädäntö** | TLA 10 § 3 mom 1 k |
| **Viitteet** | I-18 |
| **Tunniste** | **TEK-05, L:Salassa pidettävä, E:, S:, TS:Henkilötieto** |
| **Nimi** | **Langaton tiedonsiirto** |
| **Vaatimus** | Langattomassa tiedonsiirrossa tietoliikenne salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia. |

| | |
|---|---|
| **Yleiskuvaus** | Radiorajapinnan käyttö langattomassa tiedonsiirrossa (esim. WLAN, Bluetooth) tulkitaan poistumiseksi fyysisesti suojatun turvallisuusalueen ulkopuolelle. Toisin sanoen radiorajapinnan käyttö rinnastetaan julkisen 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.<br><br>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.<br><br>Käytettävissä tuotteissa ja algoritmeissä ei saa olla tunnettuja korjaamattomia haavoittuvuuksia ja heikkouksia, jotka vaarantavat tietoturvallisuuden. Lisäksi käytettävien tuotteiden valmistajan tulee tarjota tuotteille tietoturvapäivityksiä. |
| **Toteutusesimerkki** | 1) Fyysisen turva-alueen ulkopuolelle kantautuva langaton tiedonsiirto salataan vaatimuksen mukaisesti.<br>2) Fyysisen turva-alueen sisällä tapahtuvan vaatimuksia heikommin suojattu langaton tiedonsiirto (esim. langattomat oheislaitteet) voidaan hyväksyä, kun varmistutaan, että tiedon luottamuksellisuus ei vaarannu näiden yhteyksien kautta.<br>3) Langattomia yhteyksiä sisältäviä matalamman turvallisuustason laitteita ei liitetä ympäristöön. |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | I-05 |
| **Muita lisätietoja** | PiTuKri SA-01; ISO/IEC 27002:2022 8.22; Katakri 2020 I-08, I-09, I-12, I-15 ja I-16 |
| **Tunniste** | **TEK-05.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Langaton tiedonsiirto - salaaminen** |
| **Vaatimus** | Langattomassa tiedonsiirrossa tietoliikenne salataan kyseiselle turvaluokalle riittävän turvallisella salausratkaisulla. |
| **Yleiskuvaus** | |
| **Toteutusesimerkki** | TL IV -tasolla vaatimus voidaan toteuttaa esimerkiksi tunneloimalla liikenne riittävän turvallisella VPN-ratkaisulla tai käyttämällä hyväksyttyä sovellustason salausratkaisua. |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | I-05 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.24; PiTuKri SA-01 |
| **Tunniste** | **TEK-06, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Pääsyoikeuksien hallinnointi** |
| **Vaatimus** | Tietojärjestelmien käyttöoikeudet on määritelty. |

| | |
|---|---|
| **Yleiskuvaus** | Käyttöoikeuksien hallinnan keskeinen tavoite on pystyä varmistumaan siitä, että vain oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään suojattavaan tietoon. |
| **Toteutusesimerkki** | 1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).<br>2) Järjestelmän käyttäjistä on olemassa lista. |
| **Lainsäädäntö** | TiHL 16 §;<br>TLA 8 §, 11 § 1 mom 3 k |
| **Viitteet** | HAL-14, HAL-14.1, HAL-19, I-06 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01 |
| **Tunniste** | **TEK-06.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Pääsyoikeuksien hallinnointi - pääsyoikeuksien myöntäminen** |
| **Vaatimus** | Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käyttötarpeesta on varmistuttu. |
| **Yleiskuvaus** | Käyttöoikeuksien taustalla on suositeltavaa olla jokin sopimus tai muu dokumentoitu peruste, joka voidaan todentaa (esim. työsuhde, sopimus toteutettavasta työstä ympäristössä). |
| **Toteutusesimerkki** | 3) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu.<br>4) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu.<br>5) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen). |
| **Lainsäädäntö** | TiHL 16 §;<br>TLA 8 §, 11 § 1 mom 3 k |
| **Viitteet** | HAL-14, HAL-10.1, I-06 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01 |
| **Tunniste** | **TEK-06.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Pääsyoikeuksien hallinnointi - pääsyoikeuksien rajaaminen** |
| **Vaatimus** | Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä. |

| | |
|---|---|
| **Yleiskuvaus** | Käyttöoikeudet tulee rajata vain toiminnallisen tarpeen edellyttämään osajoukkoon. Tarpeettoman laajat oikeudet mahdollistavat ko. käyttäjälle, prosessille tai edellä mainitut haltuun saavalle hyökkääjälle tarpeettoman laajat toimintamahdolliset. Käyttöoikeuksien rajaamisella vähimpien oikeuksien periaatteen mukaiseksi voidaan pienentää sekä tahallisten että tahattomien tekojen, kuin myös esimerkiksi haittaohjelmista aiheutuvia riskejä. Erityisesti tulee huomioida, että ylläpito-oikeuksia käytetään vain ylläpitotoimiin. Ylläpitotunnuksella varustettua käyttäjätiliä ei tule käyttää esimerkiksi web-selailuun tai sähköpostin käyttöön.<br><br>Tarkastusoikeuden ottaminen huomioon teknisessä toteutuksessa<br>Turvallisuusluokitellun tiedon omistajat varaavat usein itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti monihankeverkoissa ja muissa vastaavissa ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulisi varmistua siitä, että verkon/järjestelmän rakenne mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä.<br><br>Eri omistajien tietojen erottelumenetelmät jakautuvat kolmeen pääluokkaan.<br>a) Loogisen tason erotteluun (esim. palvelinten virtualisointi ja käyttöoikeuksin rajoitetut verkkolevykansiot) perustuvat menetelmät soveltuvat turvallisuusluokan IV tiedoille.<br>b) Luotettavaan loogiseen erotteluun (esim. hyväksytysti salatut virtuaalikoneet levyjärjestelmän asiakaskohtaisesti varatuilla fyysisillä levyillä, ja tiedon/tietoliikenteen hyväksytty salaus yhteiskäyttöisillä verkkolaitteilla) perustuvat menetelmät soveltuvat turvallisuusluokille IV ja III saman turvallisuusluokan sisäiseen erotteluun.<br>c) Fyysisen tason erotteluun (tiedonomistajakohtaisesti varatut fyysiset laitteet) perustuvat menetelmät soveltuvat turvallisuusluokille IV, III, II ja I.<br><br>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. Toteutukseen voidaan hyödyntää myös mallia, jossa kyseiseen tietojenkäsittely-ympäristöön voidaan ottaa tietoja vain sellaisilta tietojen omistajilta, jotka sitoutuvat olemaan käyttämättä teknistä tarkastusoikeutta kyseiseen tietojenkäsittely-ympäristöön.<br><br>Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa:<br>- 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.<br>- Erottelun toteuttaminen pilviteknogiaa hyödyntäen, huomioitavaa:<br>-- 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. Vrt. PiTuKri / SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella) ja PiTuKri / KT-03 (Varmistus- ja palautusprosessit).<br>-- Jos samaa laitteistoa käytetään useiden asiakkaiden tiedon käsittelyyn samanaikaisesti, tulee varmistua siitä, että tietojen fyysinen ja looginen erottelu on riittävän turvallinen. Mikäli asiasta ei saada riittävää varmuutta, tulee tietojen käsittelyyn käyttää erillisiä |

| | |
|---|---|
| | fyysisiä laitteita. Esimerkiksi turvallisuusluokitellut tiedot voidaan säilyttää fyysisesti erillisellä virtualisointialustalla, jossa esimerkiksi mahdollisiin prosessorihaavoittuvuuksiin liittyvät rajapinnat on rajattu vain turvallisuusluokiteltujen tietojen valtuutettujen käyttäjien saavutettaviksi.<br>-- Jos samaa laitteistoa käytetään useiden eri asiakkaiden tietojen käsittelyyn, mutta ei samanaikaisesti, tulee varmistua myös siitä, että edellisen asiakkaan tiedot on poistettu riittävän turvallisesti laitteistosta (ml. kaikki osat, BIOS, erilaisten muiden laitteiden välimuistit). Mikäli asiasta ei saada riittävää varmuutta, tulee tietojen käsittelyyn käyttää erillisiä fyysisiä laitteita. Vrt. PiTuKri / SI-02 (Tietoaineistojen tuhoaminen).<br>-- Turvallisuusluokitellun salassa pidettävän tiedon omistajat voivat varata itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulee varmistua siitä, että verkon/järjestelmän toteutustapa mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä.<br>Erityisesti palvelumalleilla IaaS ja PaaS, turvallisuusluokitellun tiedon erottaminen tulee varmistaa fyysisesti erillisillä verkoilla tai salatuilla virtuaalisilla tai ohjelmistopohjaisilla paikallisverkoilla. Vrt. PiTuKri / SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella). |
| **Toteutusesimerkki** | 6) Tietojärjestelmissä turvallisuusluokitellut tiedot on eritelty vähimpien oikeuksien periaatteen mukaisesti käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä.<br>7) Tietojärjestelmissä tarkastusoikeuden varaavien tiedon omistajien tiedot säilytetään toisistaan ko. turvallisuusluokalle toimivaltaisen viranomaisen hyväksymällä menetelmällä eroteltuna. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom 1 k, 16 §;<br>TLA 8 §, 11 §:n 1 mom 3 ja 4 k |
| **Viitteet** | I-06 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01 |
| **Tunniste** | **TEK-06.3, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Pääsyoikeuksien hallinnointi - pääsyoikeuksien ajantasaisuus** |
| **Vaatimus** | Käyttöoikeudet on pidettävä ajantasaisina. |

| | |
|---|---|
| **Yleiskuvaus** | Kaikkien käyttäjätunnusten osalta on huolehdittava tunnusten elinkaaresta siten, että vain tarpeelliset tunnukset ovat voimassa ja aktiivisia ja tarpeettomat käyttäjätunnukset poistetaan välittömästi.<br><br>Pääsyoikeuksien ajantasaisuudesta varmistuminen<br>Pääsyoikeuksien ajantasaisuudesta varmistuminen edellyttää yleensä sitä, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esim. 6 kuukauden välein. Lisäksi muutoksissa, kuten ylennyksissä, alennuksissa, työnkierron yhteydessä ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen/poistamiseen on oltava selkeä ja toimiva menettelytapa. Tämä voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan pidettyä ajantasaisina. Tämä voi edelleen tarkoittaa sitä, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen. |
| **Toteutusesimerkki** | 8) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen.<br>9) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti. |
| **Lainsäädäntö** | TiHL 16 § |
| **Viitteet** | HAL-14.1, I-06 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01 |
| **Tunniste** | **TEK-06.4, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Pääsyoikeuksien hallinnointi - turvallisuusluokiteltujen tietojen erottelu** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | 1) Kunkin turvallisuusluokan tiedot pidetään erillään julkisista ja muiden turvallisuusluokkien tiedoista, tai eri tason tietoja käsitellään korkeimman turvallisuusluokan mukaisesti.<br>2) Palvelimissa, työasemissa ja muissa tallennusvälineissä turvallisuusluokitellut tiedot säilytetään riittävän turvallisella menetelmällä salattuna, mikäli salausta käytetään tarkastusoikeuden varaavien eri tiedon omistajien tietojen erotteluun, tai/ja mikäli tallennusvälineitä viedään niiden elinkaaren aikana kyseisen turvallisuusluokan säilyttämiseen hyväksytyn turvallisuusalueen ulkopuolelle. |
| **Lainsäädäntö** | TLA 11 § 1 mom 1 k |
| **Viitteet** | I-06 |
| **Tunniste** | **TEK-06.5, L:TL III, E:, S:, TS:** |
| **Nimi** | **Pääsyoikeuksien hallinnointi - TL III** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |

| | |
|---|---|
| **Yleiskuvaus** | Tehtävien erottelun riittävä toteutus riippuu merkittävästi kyseessä olevan järjestelmän käyttötapauksista. Useimmissa järjestelmissä riittävä tehtävien erottelu on toteutettavissa järjestelmän ylläpitoroolien (ja henkilöiden) ja lokien valvontaan osallistuvien roolien (ja henkilöiden) erottelulla toisistaan. Usein käytettynä valvontamekanismina on myös se, että kriittiset ylläpito- ja vastaavat toimet vaativat kahden tai useamman henkilön hyväksynnän. |
| **Toteutusesimerkki** | Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 § 1 mom 3 k |
| **Viitteet** | HAL-2.1, I-06, I-12 |
| **Tunniste** | **TEK-07, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto** |
| **Nimi** | **Tietojenkäsittely-ympäristön toimijoiden tunnistaminen** |
| **Vaatimus** | Tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti. |
| **Toteutusesimerkki** | Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:<br><br>Henkilöiden tunnistaminen:<br>1) Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet.<br>2) Kaikki käyttäjät tunnistetaan ja todennetaan.<br>3) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti.<br>4) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen.<br>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.<br>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.<br><br>Tietojärjestelmien tunnistaminen:<br>7) Tietoa keskenään vaihtavat tietojärjestelmät tunnistetaan käyttötapaukseen soveltuvalla tekniikalla, kuten salasanoilla, avaimilla (esim. API-avain), tunnistevälineillä (tokeneilla, esim. oAuth) tai vastaavilla menetelmillä. Tunnistautuminen tehdään salattuja yhteyksiä pitkin.<br><br>Huomioitavaa<br>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.<br><br>Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa:<br>- Julkisen verkon yli saavutettavissa pilvipalveluissa käyttötapa tulkittavissa etäkäytöksi |

| | |
|---|---|
| | ja siten huomioitava esimerkiksi vaatimukset vahvasta, useaan todennustekijään pohjautuvasta tunnistaumisesta.<br>- Tilanteissa, joissa pilvipalveluun tunnistautumisessa hyödynnetään federoitua identiteetinhallintaa, tai/ja identiteetin- ja pääsynhallintajärjestelmiä (organisaation omia tai esimerkiksi pilvipalveluntarjoajan tuottamia), tulee arvioinnissa kiinnittää erityistä huomiota tunnistuspalvelun sekä attribuuttien välitysketjun luotettavuuteen. Salassa pidettävän tiedon käsittelyyn soveltuvat vain sellaiset tunnistuspalvelut, jotka tarjoavat vahvaan ensitunnistamiseen perustuvaa identiteettiä ja joiden attribuuttien välitysketju pystytään toteuttamaan riittävän turvallisesti tunnistukseen nojaavaan palveluun asti.<br>- Koska salassa pidettävän tiedon suojaus on yleensä suoraan riippuvainen tunnistuspalvelun luotettavuudesta, tunnistuspalvelun turvallisuudesta varmistuminen kuuluu lähes poikkeuksetta<br>osaksi pilvipalvelun turvallisuuden arviointia. Esimerkiksi attribuuttien välityksen salausteknistä suojausta on tyypillisesti perusteltua arvioida samansuuntaisesti kuin kyseessä olevan tietotyypin suojaamiseen sovellettavan salausratkaisun avainten välitystä.<br>- Identiteetinhallintamalleista organisaatiokeskeinen (organization-centric identity management) soveltuu yleensä esimerkiksi käyttäjäkeskeistä (user-centric) paremmin salassa pidettävän tiedon suojaamistarpeisiin, joissa on huomioitava myös käyttäjän sidonta tiettyyn organisaatioon sekä turvallisuustoteutuksen luotettavuudesta varmistuminen.<br>- Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia. |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 5 k |
| **Viitteet** | HAL-19, I-07 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02, SA-01, SA-02 ja SA-03. |
| **Tunniste** | **TEK-07.1, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto** |
| **Nimi** | **Tietojenkäsittely-ympäristön toimijoiden tunnistaminen** |
| **Vaatimus** | Kaikki käyttäjät tunnistetaan ja todennetaan yksilöllisillä henkilökohtaitaisilla käyttäjätunnisteilla. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 16 §;<br>TLA 11 § 1 mom 3 ja 5 k |
| **Viitteet** | I-07 |
| **Muita lisätietoja** | PiTuKri IP-02 |
| **Tunniste** | **TEK-07.2, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto** |
| **Nimi** | **Tietojenkäsittely-ympäristön toimijoiden tunnistaminen** |

| | |
|---|---|
| **Vaatimus** | Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 14 §, 16 §;<br>TLA 11 § 1 mom 3 ja 5 k |
| **Viitteet** | I-07 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.5; PiTuKri IP-02 |
| **Tunniste** | **TEK-07.3, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto** |
| **Nimi** | **Tietojenkäsittely-ympäristön toimijoiden tunnistaminen** |
| **Vaatimus** | Käyttäjätunnukset lukittuvat tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 7 § |
| **Viitteet** | I-07 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.5; PiTuKri IP-02 |
| **Tunniste** | **TEK-07.4, L:TL IV, E:Kriittinen, S:, TS:** |
| **Nimi** | **Tietojenkäsittely-ympäristön toimijoiden tunnistaminen - TL IV** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Laitteiden tunnistaminen: Turvallisuusluokitellun tiedon käsittelyyn käytetään vain organisaation tarjoamia ja hallinnoimia, kyseiselle turvallisuusluokalle hyväksyttyjä päätelaitteita. Kaikkien muiden laitteiden kytkeminen turvallisuusluokitellun tiedon käsittely-ympäristöön on yksiselitteisesti kielletty. Henkilöstö on ohjeistettu ja velvoitettu toimimaan ohjeistuksen mukaisesti.<br><br>Tietojärjestelmien tunnistaminen: Tietoa keskenään vaihtavat tietojärjestelmät tunnistetaan käyttötapaukseen soveltuvalla tekniikalla, kuten salasanoilla, avaimilla (esim. API-avain), tunnistevälineillä (tokeneilla, esim. oAuth) tai vastaavilla menetelmillä. Tunnistautuminen tehdään salattuja yhteyksiä pitkin.<br><br>Huomioitavaa: Turvallisuusluokan IV käsittely-ympäristöissä, joissa uhka palvelunestohyökkäyksen aiheuttamiseen (tunnusten lukitseminen esim. Internet-kytkentäisissä tunnistuspalveluissa) arvioidaan merkittäväksi, tunnuksen lukittuminen voidaan korvata jollain riskiä pienentävällä menettelyllä (esim. vastaamisen hidastamiseen, suodattamiseen tai väliaikaiseen lukitsemiseen perustuvat menettelyt). Turvallisuusluokan IV käsittely-ympäristöissä ei yleensä edellytetä päätelaitteen teknistä tunnistamista, mikäli käyttäjät tunnistetaan. |
| **Lainsäädäntö** | TLA 11 § 1 mom 5 k |
| **Viitteet** | I-07 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02 |
| **Tunniste** | **TEK-07.5, L:TL III, E:Kriittinen, S:, TS:** |
| **Nimi** | **Tietojenkäsittely-ympäristön toimijoiden tunnistaminen - TL III** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |

| | |
|---|---|
| **Toteutusesimerkki** | Turvallisuusluokkien III-II toteutetaan myös seuraavat toimenpiteet:<br>1) Edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta.<br>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 toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymän turva-alueen sisällä).<br><br>Huomioitavaa<br>Turvallisuusluokkien III ja II käsittely-ympäristöjen menetelmät vahvasta käyttäjätunnistuksesta ja päätelaitteen tunnistamisesta voidaan joissain tapauksissa toteuttaa siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisesti suojatulta alueelta (yleensä turva-alue, lukittu laitekaappi, tai vastaava), jonka pääsynvalvonnassa käytetään vahvaa, vähintään kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla. Tilanteissa, joissa käyttäjätunnistus nojaa fyysisen turvallisuuden menettelyihin, tulee myös fyysisen turvallisuuden menettelyjen täyttää jäljitettävyydelle asetetut vaatimukset erityisesti lokitietojen ja vastaavien tallenteiden säilytysaikojen suhteen. |
| **Lainsäädäntö** | TLA 11 § 1 mom 5 k |
| **Viitteet** | I-07 |
| **Tunniste** | **TEK-08, L:Salassa pidettävä, E:Kriittinen, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tietojärjestelmien fyysinen turvallisuus** |
| **Vaatimus** | Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia. |
| **Yleiskuvaus** | Hallinnolliselle alueelle, turva-alueille sekä esimerkiksi säilytysyksiköille asetetut vaatimukset on kuvattu fyysisen turvallisuuden osiossa. Turvallisuusalueen ulkopuolella tapahtuva käyttö on etäkäyttöä, johon sovelletaan kyseisen kohdan vaatimuksia.<br><br>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.<br><br>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. |
| **Lainsäädäntö** | TiHL 15 § 2 mom;<br>TLA 10 § |
| **Viitteet** | FYY-7.1, HAL-19, I-17 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 7.1, 7.3, 7.6, 7.8; Tiedonhallintalautakunta: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2020:19, luku 5); PiTuKri FT-02; CPNI: Physical Security Advice |

| Tunniste | TEK-09, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä |
|---|---|
| **Nimi** | **Järjestelmäkovennus** |
| **Vaatimus** | Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. |
| **Yleiskuvaus** | Järjestelmissä on usein paljon ominaisuuksia, jotka ovat yleensä oletusarvoisesti päällä ja helppo ottaa käyttöön. Ominaisuuksien oletusasetukset eivät usein ole riittävän turvallisia. Jos tarpeettomia ominaisuuksia ei poisteta käytöstä, nämä ovat myös pahantahtoisen toimijan käytettävissä. Jos välttämättömien palvelujen riskialttiita oletusasetuksia ei muuteta, ovat nämä myös pahantahtoisen toimijan käytettävissä. Järjestelmissä on oletusarvoisesti usein käytössä esimerkiksi ennalta määriteltyjä ylläpitosalasanoja, valmiiksi asennettuja tarpeettomia ohjelmistoja ja tarpeettomia käyttäjätilejä.<br><br>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.<br><br>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.<br><br>Koventamiseen ja kovennetun asennuksen ylläpitämiseen voidaan usein hyödyntää myös konfiguraationhallintatyökaluja.<br><br>Oleellista kovennuksista<br>1) Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin. Salasanoja säilytetään siten, että salasanat ovat suojattuna sekä saatavilla.<br>2) Ylimääräiset palvelut, sovellukset, yhteydet (myös BIOS-tasolla) ja laitteet on poistettu.<br>3) Käyttäjät, rajapinnat ja laitteet tunnistetaan (vrt. I-07).<br>4) Päällä olevat välttämättömät palvelut ovat saavutettavissa vain tarpeellisten verkkojen, laitteiden ja käyttäjätunnusten osalta.<br>5) Ohjelmistot (esim. laiteohjelmistot, sovellukset) pidetään ajantasaisina (vrt. I-19).<br>6) Kohteen yhteydet, mukaan lukien hallintayhteydet, ovat rajattuja, kovennettuja, käyttäjätunnistettuja sekä aikarajoitettuja (istunnon aikakatkaisu).<br>7) Käytössä olevat sovellukset, rajapinnat ja vastaavat on kovennettu, rajoitettu ja ominaisuudet on asetettu vähimpien oikeuksien periaatteen mukaiseksi.<br>8) Ohjelmistot, kuten käyttöjärjestelmät, sovellukset ja laiteohjelmistot, asetetaan keräämään tarvittavaa lokitietoa väärinkäytösten havaitsemiseksi (vrt. I-10).<br>9) Tietojärjestelmän käynnistäminen tuntemattomalta (muulta kuin ensisijaiseksi määritellyltä) laitteelta on estetty.<br><br>Korvaavia menetelmiä<br>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.<br><br>Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa: |

| | |
|---|---|
| | Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia. |
| **Toteutusesimerkki** | 1) Kovennettavat kohteet on tunnistettu.<br>2) Kovennusten toteutus on määritelty.<br>3) Kohteet on kovennettu määritysten mukaisesti.<br>4) Kovennusten pysyminen päällä varmistetaan säännöllisesti, erityisesti päivitysten jälkeen koko tietojärjestelmän elinkaaren ajan.<br><br>Erityisesti huomioitavaa:<br>a) Kovennukset kohdistetaan kaikkiin tietojenkäsittely-ympäristön laitteisiin, joita ovat muun muassa verkon aktiivilaitteet, palvelimet, työasemat, mobiililaitteet, tulostimet, oheislaitteet ja muut tietojärjestelmäksi käsitettävät laitteet.<br>b) Hyökkäyspinta-alan rajaamiseksi laitteissa on päällä vain tarvittavat palvelut, rajapinnat, yhteydet ja väylät, ja nämä toimivat vähimpien oikeuksien periaatteella.<br>c) Laitteen laiteohjelmisto (firmware, BIOS ja vastaavat), käyttöjärjestelmä, sovellukset sekä muut vastaavat komponentit kovennetaan vähintään valmistajan kovennussuosituksen mukaisesti ja/tai käyttäen yleisesti tunnettua kovennusohjetta. Tämän lisäksi kovennukset räätälöidään järjestelmäkohtaisesti käyttötarkoituksen ja riskien perusteella. Jollei kovennusohjetta käytetylle komponentille ole olemassa, sovelletaan vastaavalle tuotteelle tarkoitettua ohjetta. |
| **Lainsäädäntö** | TiHL 13 § 1 ja 4 mom;<br>TLA 11 § 1 mom 6 k |

| | |
|---|---|
| **Viitteet** | I-08 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.27; The United States Government Configuration Baseline (USGCB); DISA Security Technical Implementation Guides (STIGs); NIST - National Checklist Program Repository; Microsoft DSC Environment Analyzer; Microsoft Baseline Management; CIS benchmarks; PiTuKri JT-02 |
| **Tunniste** | **TEK-09.1, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Järjestelmäkovennus - käytössä olevien palveluiden minimointi** |
| **Vaatimus** | Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut. |
| **Yleiskuvaus** | Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi. |
| **Lainsäädäntö** | TiHL 13 § 1 mom;<br>TLA 11 § 1 mom 6 k |
| **Viitteet** | I-08 |
| **Tunniste** | **TEK-09.2, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Järjestelmäkovennus - kovennusten varmistaminen koko elinkaaren ajan** |
| **Vaatimus** | Kovennusten voimassaolosta ja vaikuttavuudesta huolehditaan koko tietojärjestelmän elinkaaren ajan. |
| **Lainsäädäntö** | TiHL 13 § 1 ja 4 mom;<br>TLA 11 § 1 mom 6 k |
| **Viitteet** | I-08 |
| **Tunniste** | **TEK-09.3, L:TL III, E:Kriittinen, S:, TS:** |
| **Nimi** | **Järjestelmäkovennus - turvallisuusluokitellut ympäristöt** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Yleiskuvaus** | Erityisesti korkeimpien turvallisuusluokkien ympäristöissä tarpeettomien komponenttien käytönesto on usein perusteltua toteuttaa fyysisesti kyseiset komponentit (esimerkiksi langattomat verkkokortit, kamerat, mikrofonit) laitteesta irrottaen. Tilanteissa, joissa kyseistä komponenttia ei voida fyysisesti irrottaa, korvaavana suojauksena voi joissain tapauksissa hyödyntää esimerkiksi kameroiden teippaamista sekä laitteiston ohjelmallista käytöstäpoistoa sekä käyttäjäasetus-, käyttöjärjestelmä- ja laiteohjelmistotasoilla. Joissain käyttöjärjestelmissä suojausta voidaan täydentää myös poistamalla kyseisen laitteen käyttöön liittyvät ohjelmisto-osiot (kernel module).<br><br>Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus tulee huomioida kovennusohjeiden mahdollisesti sisältämät tasot sekä useiden eri kovennusohjeiden, kuten esimerkiksi valmistajakohtaiset ohjeet, CIS Benchmark ja DISA STIG, hyödyntäminen kovennusten kattavuuden varmistamisessa. |
| **Toteutusesimerkki** | Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan toteuttaa siten, että kohtien 1-4 lisäksi kovennuksiin käytetään useita kovennusohjeita ja kovennusohjeiden toteutuksen tiukkuutta kiristetään. |
| **Lainsäädäntö** | TiHL 13 § 1 ja 4 mom;<br>TLA 11 § 1 mom 6 k |
| **Viitteet** | I-08 |
| **Tunniste** | **TEK-10, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä** |

| Nimi | Haittaohjelmilta suojautuminen |
|---|---|
| **Vaatimus** | Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen. |
| **Yleiskuvaus** | Haittaohjelmariskejä vastaan voidaan suojautua esimerkiksi järjestelmien kovennusmenettelyillä , käyttöoikeuksien rajauksilla, järjestelmien pitämisellä turvallisuuspäivitysten tasolla, poikkeamien havainnointikyvyllä, henkilöstön turvatietoisuudesta varmistumalla ja myös haittaohjelmantorjuntaohjelmistojen käytöllä. Riskejä voidaan pienentää myös riskialttiiden ympäristöjen eriyttämisellä tuotantoympäristöistä sekä muun muassa siirreltävien medioiden (esimerkiksi USB-muistien) käytön rajauksilla. Torjuntaohjelmistot voidaan jättää asentamatta ympäristöissä, joihin haittaohjelmien pääsy on muuten estetty (esim. järjestelmät, joissa ei ole mitään tiedon tuonti-/vientiliittymiä, tai joissa tarkasti rajatuissa liittymissä toteutetaan siirrettävän tiedon luotettava validointi/sanitointi). |
| **Toteutusesimerkki** | Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:<br>1) Järjestelmien käyttöoikeudet on rajattu vähimpien oikeuksien periaatteen mukaisesti.<br>2) Järjestelmät pidetään turvallisuuspäivitysten tasolla.<br>3) Järjestelmät on kovennettuja siten, että vain välttämättömät toiminnallisuudet ja ohjelmistokomponentit käytössä.<br>4) Henkilöstön turvatietoisuudesta on varmistuttu. Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta.<br>5) Haittaohjelmantorjuntaohjelmistot 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.<br>6) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä.<br>7) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja ja hälytyksiä.<br>8) Haittaohjelmatunnisteet (ja vast.) päivittyvät säännöllisesti.<br>9) Haittaohjelmahavaintoja sekä hälytyksiä seurataan säännöllisesti ja niihin reagoidaan. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom;<br>TLA 11 § 1 mom 2 ja 3 k |
| **Viitteet** | I-09 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.7; PiTuKri JT-04 |
| **Tunniste** | **TEK-10.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Haittaohjelmilta suojautuminen - TL IV** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan lisäksi:<br>1) On tunnistettu järjestelmät, joissa haittaohjelmantorjuntaohjelmistoilla pystytään saamaan lisäsuojausta. |
| **Lainsäädäntö** | TLA 11 § 1 mom 2 k |
| **Viitteet** | I-09 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.7; PiTuKri JT-04 |
| **Tunniste** | **TEK-10.2, L:TL III, E:, S:, TS:** |

| Nimi | Haittaohjelmilta suojautuminen - TL III |
|---|---|
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Yleiskuvaus** | Julkisista verkoista eristetyt ympäristöt<br>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.).<br><br>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.<br><br>Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, tapauskohtaisiin ehtoihin sisältyy usein myös määrittelyt siitä, millä menetelmillä pienennetään tämän aiheuttamaa riskiä. Menetelmänä voi esimerkiksi olla ei-luotetusta lähteestä tulevan muistivälineen kytkeminen eristettyyn tarkastusjärjestelmään, jonne siirrettävä tieto siirretään, ja josta siirrettävä tieto viedään edelleen luotettuun järjestelmään erillistä muistivälinettä käyttäen. |
| **Toteutusesimerkki** | Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että lisäksi toteutetaan seuraavat toimenpiteet:<br>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.<br>a) Tilanteissa, joissa liityntöjen käytölle ei ole kriittistä tarkastelua kestävää perustetta, liitynnät poistetaan käytöstä.<br>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.<br><br>Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, huomioidaan lisäksi yleensä turvallisuusluokalla III vähintään muistialueen tarkastaminen. |
| **Lainsäädäntö** | TLA 11 § 1 mom 2 k |
| **Viitteet** | I-09 |
| **Tunniste** | **TEK-10.3, L:TL II, E:, S:, TS:** |
| **Nimi** | **Haittaohjelmilta suojautuminen - TL II** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, huomioidaan lisäksi yleensä turvallisuusluokasta II lähtien myös muistivälineen kontrolleritason räätälöinnin uhat. |

| | |
|---|---|
| **Lainsäädäntö** | TLA 11 § 1 mom 2 ja 5 k |
| **Viitteet** | I-09 |
| **Tunniste** | **TEK-11, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Turvallisuuteen liittyvien tapahtumien jäljitettävyys** |
| **Vaatimus** | Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen. |
| **Yleiskuvaus** | Jäljitettävyydellä tarkoitetaan järjestelmäympäristön tapahtumien kirjaamista siten, että poikkeamatilanteessa voidaan selvittää mitä toimia ympäristössä on tehty, kenen toimesta ja mitä vaikutuksia toimilla on ollut. Keskeisiä tallenteita ovat tyypillisesti kirjautumistietojen lisäksi keskeisten verkkolaitteiden ja palvelinten lokitiedot. Myös esimerkiksi työasemien ja vastaavien lokitiedot kuuluvat tähän erittäin usein.<br><br>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.<br><br>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).<br><br>Lokitietojen säilytysajoissa tulee huomioida kyseessä olevan käyttötapauksen tarpeet. Esimerkiksi joidenkin tietojen käsittely- ja luovutuslokeille voi olla perusteltua edellyttää eroavia säilytysaikoja, kuin poikkeamatilanteiden selvittämiseksi kerättäville lokitiedoille. Esimerkiksi viranomaistoiminnassa rikosoikeudelliset vanhentumisajat voivat johtaa tyypillisesti vähintään viiden vuoden säilytysaikatarpeisiin. Usein käytettynä käytäntönä on, että 6 kuukauden lokitiedot ovat saatavilla reaaliaikaisesti, ja pidemmän aikavälin lokitiedot ovat tarvittaessa saatavissa muutamien työpäivien viiveellä. Lokitietojen erilaisia käyttötapauksia on käsitelty myös Tiedonhallintalautakunnan suosituksessa (2020:21, luku 7).<br><br>Toteutus edellyttää usein myös sen huomioon ottamista, että lokien säilytystilaa ja -aikaa kasvatetaan riittäviksi. Suositus: lokeille varataan tilaa ympäristössä riittäväksi arvioitava määrä. Riittävän ajan määritys voidaan tehdä esimerkiksi siten, että arvioidaan yhden kuukauden lokikertymän perusteella riittävä tila vaadittavalle säilytysaikajaksolle. Huom: tilalle on syytä varata reilusti ”puskuria”, sillä poikkeavat tilanteet ja myös tietyt hyökkäystyypit kasvattavat lokimäärää merkittävästi. |

| | |
|---|---|
| **Toteutusesimerkki** | Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:<br>1) Toimintaan on jalkautettu kirjallinen lokien keräys-, luovutus-, hälytys- ja seurantapolitiikka/-ohje, joka on muodostettu ottaen huomioon toiminnan vaatimukset.<br>2) Tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen.<br>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.<br>4) Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta). |
| **Lainsäädäntö** | TiHL 17 §, 15 §;<br>TLA 7 §,14 § |
| **Viitteet** | HAL-7.1, I-10 |
| **Muita lisätietoja** | The United States Government Configuration Baseline (USGCB); ISO/IEC 27002:2022 5.33, 8.15, 8.17; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 7); PiTuKri JT-01 |
| **Tunniste** | **TEK-11.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Turvallisuuteen liittyvien tapahtumien jäljitettävyys - tietojen luovutukset** |
| **Vaatimus** | Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. |
| **Yleiskuvaus** | Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. |
| **Lainsäädäntö** | TiHL 17 §, 15 §;<br>TLA 7 §, 14 § |
| **Viitteet** | HAL-07.1, TSU-18, I-10 |
| **Tunniste** | **TEK-11.2, L:TL III, E:, S:, TS:** |
| **Nimi** | **Turvallisuuteen liittyvien tapahtumien jäljitettävyys - TL III** |
| **Vaatimus** | Turvallisuusluokan II–III tiedon käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi). |
| **Yleiskuvaus** | Turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvien lokitietojen säilytyksestä on annettu suositus VM 2021:5: "Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä". |
| **Toteutusesimerkki** | Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että kohtien 1-4 lisäksi toteutetaan seuraavat toimenpiteet:<br>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.<br>6) Lokitiedot varmuuskopioidaan säännöllisesti.<br>7) Samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on synkronoitu sovitun ajanlähteen kanssa.<br>8) On olemassa menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen.<br>9) Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkinnät. |

| | |
|---|---|
| **Lainsäädäntö** | TiHL 17 §, 15 §;<br>TLA 7 §, 14 § |
| **Viitteet** | I-10 |
| **Muita lisätietoja** | Valtiovarainministeriö: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5) 7.9. |
| **Tunniste** | **TEK-11.3, L:TL I, E:, S:, TS:** |
| **Nimi** | **Turvallisuuteen liittyvien tapahtumien jäljitettävyys - TL I** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Turvallisuusluokan I tietojen käsittelyssä suositellaan riskiperustaisesti turvallisuusluokkaa II pidempiä säilytysaikoja lokitiedoille (esimerkiksi vähintään 10 vuotta).<br><br>Turvallisuusluokan I tietojenkäsittely-ympäristöt ovat tyypillisesti suppeita, koostuen esimerkiksi kaikista verkoista pysyvästi irtikytketyistä päätelaitteista. Toisaalta esimerkiksi 10 vuoden lokikertymän säilyvyys on haastava toteuttaa uskottavasti vain päätelaitteilla, joten tällaisten päätelaitteiden lokienkeräys sekä kerättyjen lokitietojen varmistukset edellyttävätkin yleensä suunniteltua säännöllistä prosessia. Käytännön toteutustapana voi olla esimerkiksi lokitietojen säännöllinen kerääminen irtomedialle, jota käsitellään ja säilytetään sen elinkaaren ajan kuin turvallisuusluokan I tietoa. Lisäksi huomioitava, että mikäli tietojärjestelmän pääsynhallinta tai esimerkiksi toimien jäljitettävyys nojautuu fyysisen turvallisuuden menettelyihin, myös näistä syntyviä tallenteita saattaa olla perusteltua säilyttää ja hallinnoida turvallisuusluokan I mukaisilla menettelyillä. |
| **Lainsäädäntö** | TiHL 17 §, 15 §;<br>TLA 7 §, 14 § |
| **Viitteet** | I-10 |
| **Tunniste** | **TEK-12, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Poikkeamien havainnointikyky ja toipuminen** |
| **Vaatimus** | Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely-ympäristön suojattu tilanne viipymättä. |

| | |
|---|---|
| **Yleiskuvaus** | Tekninen poikkeamien havainnointikyky pohjautuu yleensä kolmeen lähteeseen: 1) Verkkoliikenteessä näkyviin tapahtumiin, 2) kerättyihin tallenteisiin (lokeihin) ja 3) kohteilla (hosts) näkyviin tapahtuviin. Riittävä tekninen havainnointikyky pystytään yleensä toteuttamaan edellä mainittuja havainnointilähteitä yhdistelemällä. Mitä tarkemmin kyseinen tietojenkäsittely-ympäristö ja sen normaali toiminta tunnetaan, sitä paremmin pystytään myös havainnoimaan normaalista toiminnasta eroavia tapahtumia. Normaalista toiminnasta eroavien tapahtumien havainnointi tukee myös sellaisten hyökkäysten havainnointia, joista ei ole saatavilla hyökkäysten tunnistetietoja (IoC, Indicator of Compromise). Tietojenkäsittely-ympäristön normaali toiminta tulisi tuntea koko elinkaaren ajalta, aina alkuhetkistä käytöstä poistoon asti. Myös muutostenhallinta (vrt. Katakri 2020 / I-16) tukee poikkeamien havainnointikykyä, muun muassa laitteisto- ja ohjelmistokonfiguraatiomuutosten säännöllisen tarkastelun avulla.<br><br>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.<br><br>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.<br><br>Tietojenkäsittely-ympäristön palauttaminen takaisin suojattuun tilaan kohtuullisessa ajassa edellyttää yleensä suunniteltuja, kuvattuja, koulutettuja sekä harjoiteltuja prosesseja sekä teknisiä menetelmiä.<br><br>Poikkeamien havainnointikyvyn kehittämisessä ja ylläpitämisessä tulee huomioida myös koko henkilöstön rooli. Esimerkiksi loppukäyttäjien ilmoittamat havainnot voivat tuottaa arvokasta tietoa hyökkäysten tai niiden yritysten havainnointiin. |
| **Toteutusesimerkki** | Verkkoliikenteen normaali tila (liikennemäärät, protokollat ja yhteydet) on tiedossa. On olemassa menettely, jolla verkkoliikenteen normaaliin tilaan nähden eroavat tapahtumat (esimerkiksi poikkeavat yhteydet tai niiden yritykset) pyritään havaitsemaan. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom, 17 §;<br>TLA 7 §, 11 § 1 mom 2 k |
| **Viitteet** | I-11 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.25, 5.26, 8.15, 8.16; PiTuKri TT-02, JT-01, TJ-05; Katakri 2020 T-07 (Turvallisuuspoikkeamien hallinta) ja T-12 (Turvallisuuskoulutus). |
| **Tunniste** | **TEK-12.1, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Poikkeamien havainnointikyky ja toipuminen - poikkeamien havainnointi lokitiedoista** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |

| | |
|---|---|
| **Toteutusesimerkki** | Suositellaan toteuttamaan menettely, jolla kerätyistä tallenteista ja tilannetiedosta (esimerkiksi muutokset lokikertymissä) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan). |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom, 17 §;<br>TLA 7 §, 11 § 1 mom 2 k |
| **Viitteet** | I-11 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05 |
| **Tunniste** | **TEK-12.2, L:TL IV, E:Tärkeä, S:, TS:** |
| **Nimi** | **Poikkeamien havainnointikyky ja toipuminen - TL IV** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | 1) On olemassa menettely, jolla kerätyistä tallenteista ja tilannetiedosta (esimerkiksi muutokset lokikertymissä) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan).<br>2) On olemassa menettely, jolla tietojenkäsittely-ympäristön kohteista (hosts, esimerkiksi työasemat ja palvelimet) voidaan havainnoida poikkeamia.<br>3) On olemassa menettely havaituista poikkeamista toipumiseen. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom, 17 §;<br>TLA 7 §, 11 § 1 mom 2 k |
| **Viitteet** | I-11 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05 |
| **Tunniste** | **TEK-12.3, L:TL I, E:, S:, TS:** |
| **Nimi** | **Poikkeamien havainnointikyky ja toipuminen - TL I** |
| **Vaatimus** | Käyttäjien ja ylläpitäjien toimintaa seurataan poikkeuksellisen toiminnan havaitsemiseksi. |
| **Toteutusesimerkki** | Turvallisuusluokan I tietojen käsittelyssä suositellaan tehostettua poikkeamien havainnointikykyä, painottaen muun muassa tietojenkäsittelyympäristön käyttäjien ja ylläpitäjien toiminnan seurantaa. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom, 17 §;<br>TLA 7 §, 11 § 1 mom 2 k |
| **Viitteet** | I-11 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.16; PiTuKri JT-01, TJ-05 |
| **Tunniste** | **TEK-13, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Ohjelmistojen turvallisuuden varmistaminen** |
| **Vaatimus** | Sovellukset ja ohjelmointirajapinnat (API:t) suunnitellaan, kehitetään, testataan ja otetaan käyttöön alan hyvien turvallisuuskäytäntöjen mukaisesti. Sovellusten ja rajapintojen on kestettävä niitä vastaan käytettävissä olevat yleiset hyökkäysmenetelmät ilman, että käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus vaarantuu. |

| | |
|---|---|
| **Yleiskuvaus** | Ohjelmistot ja niiden käyttötarkoitukset eri tietojenkäsittely-ympäristöissä eroavat toisistaan merkittävästi. Vastaavasti myös tarpeet ohjelmistojen turvalliseen toteutukseen ja käyttöönottoon eroavat merkittävästi eri tietojenkäsittely-ympäristöissä ja käyttötarkoituksissa. Esimerkiksi kaikista verkoista fyysisesti eriytetyssä työasemassa käytettävän toimisto-ohjelmiston turvallisuudelle asetettavat tarpeet eroavat tarpeista, jotka kohdistuvat useiden käyttäjien saavutettavissa olevaan asianhallintajärjestelmään.<br><br>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.<br><br>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.<br><br>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.<br><br>Joskus voi tulla tarve käyttää palveluita, joiden ohjelmakoodin ja sen kehityskäytäntöjen näkyvyys on heikkoa tai jopa olematonta. Tällaisten ohjelmistojen luotettavuudesta voidaan pyrkiä saamaan näyttöä esimerkiksi tutkimalla päivitystiheyksiä, dokumentaatiota ja mahdollista muuta näkyvyyttä, kuten olemassa olevia testiraportteja. Tällaisissa tilanteissa voi turvallisen konfiguroinnin lisäksi hyödyntää myös korvaavia suojauksia. Turvallisessa konfiguroinnissa ja korvaavina suojauksina voi tietyin rajoituksin hyödyntää esimerkiksi tehostettua havainnointikykyä, kovennuksia, koodin suorituksenaikaista rajoittamista (esim. AppLocker, SELinux, AppArmor), sovelluspalomuureja (WAF), sekä koko ohjelmiston loogista eriyttämistä esimerkiksi virtualisointia hyödyntäen.<br><br>Ohjelmistojen turvallisuudesta varmistumiseen tulee hyödyntää aihepiirin tarkentavia ohjeita ja standardeja. Näitä ovat esimerkiksi VAHTI Sovelluskehityksen tietoturvaohje (VAHTI 1/2013), OWASP Application Security Verification Standard (ASVS) ja Kyberturvallisuuskeskuksen ohje "Turvallinen tuotekehitys: kohti hyväksyntää". |

| | |
|---|---|
| **Toteutusesimerkki** | 1) Ohjelmistojen (sovellukset, palvelut, järjestelmät) käyttötarkoitukset ja ohjelmistojen turvallisuutta mahdollisesti toteuttavat roolit on tunnistettu.<br>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.<br>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.<br>4) Kriittiset ohjelmistot (sovellukset, palvelut, järjestelmät) toteutetaan tai toteutus tarkastetaan mahdollisuuksien mukaan luotettavaa standardia vasten tai/ja turvallisen ohjelmoinnin ohjetta hyödyntäen.<br>5) On varmistettu, että ohjelmistojen (sovellukset, palvelut, järjestelmät) ohjelmakoodin laadun ylläpito, kehitys ja muutoshallinta vastaavat tarpeita koko elinkaaren ajan.<br>6) On varmistettu, että ohjelmistot (sovellukset, palvelut, järjestelmät) täyttävät lainsäädännöstä johdetut vaatimukset. Erityisesti huomioitava salauksiin, hallintaliittymiin, käyttäjähallintaan ja -tunnistukseen, kovennuksiin ja jäljitettävyyteen liittyvät kokonaisuudet. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom; TLA 11 § 1 mom 2, 3, 4, 5 ja 6 k |
| **Viitteet** | HAL-16, I-13 |
| **Muita lisätietoja** | OWASP Application Security Verification Standard (ASVS); CWE TOP 25 Most Dangerous Software Errors; The Building Security In Maturity Model; Software Assurance Maturity Model; ISO/IEC 27002:2022 5.8, 8.26, 8.27, 8.28, 8.29; Traficom: Turvallinen tuotekehitys: kohti hyväksyntää; PiTuKri MH-02 |
| **Tunniste** | **TEK-14, L:TL III, E:, S:, TS:** |
| **Nimi** | **Hajasäteily (TEMPEST) ja elektroninen tiedustelu** |
| **Vaatimus** | Turvatoimia toteutetaan turvallisuusluokiteltuihin tietoihin liittyvässä tietojenkäsittely-ympäristössä riittävän turvallisilla menetelmillä niin, että tahattomat sähkömagneettiset vuodot eivät vaaranna tietoja (TEMPEST-turvatoimet). Nämä turvatoimet on suhteutettava tiedon hyväksikäytön riskiin ja turvallisuusluokkaan. Käsiteltäessä turvallisuusluokan III tai II tietoja sähköisesti, on pidettävä huolta, että elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi. |
| **Yleiskuvaus** | Turvallisuusluokkien III-II käsittely-ympäristöissä raja-arvot ylittävän hajasäteilyn osalta suojautuminen toteutetaan ko. turvallisuusluokalle toimivaltaisen viranomaisen hyväksymillä menettelyillä.<br><br>Turvallisuusluokan III tietojen osalta on laajemmat mahdollisuudet hyväksyä korvaavia menettelyjä riittävän suojauksen saavuttamiseksi. |
| **Toteutusesimerkki** | 1) Hajasäteilyyn liittyvät riskit on tunnistettu ja arvioitu.<br>2) Turvatoimet tai korvaavat menettelyt on mitoitettu riskeihin, tiedon turvallisuusluokkaan ja hyväksyttävään jäännösriskitasoon. |
| **Lainsäädäntö** | TLA 11 § 2 mom |
| **Viitteet** | FYY-5.6, I-14 |

| | |
|---|---|
| **Muita lisätietoja** | Traficom: Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet; ISO/IEC 27002:2022 7.12 |
| **Tunniste** | **TEK-14.1, L:TL II, E:, S:, TS:** |
| **Nimi** | **Hajasäteily (TEMPEST) ja elektroninen tiedustelu - TL II** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | On toteutttu turvatoimet, jotka on mitoitettu riskeihin ja tiedon turvallisuusluokkaan. Kohteen hajasäteilyn vastatoimien riittävyys voidaan todentaa vyöhykemittauksella tai suojatun tilan mittauksella. |
| **Lainsäädäntö** | TLA 11 § 2 mom |
| **Viitteet** | I-14 |
| **Tunniste** | **TEK-14.2, L:TL I, E:, S:, TS:** |
| **Nimi** | **Hajasäteily (TEMPEST) ja elektroninen tiedustelu - TL I** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Turvallisuusluokan I tietojen suojaamisessa tulee huomioida turvallisuusluokan II tiedoista eroavat riskit ja suhteutettava nämä toteutettaviin turvatoimiin. Hajasäteilyä ja siltä suojautumisen periaatteita on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen hajasäteilyltä suojautumisen ohjeessa. |
| **Lainsäädäntö** | TLA 11 § 2 mom |
| **Viitteet** | I-14 |
| **Tunniste** | **TEK-15, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tiedon salaaminen** |
| **Vaatimus** | Kun salassa pidettävää tietoa siirretään yleisissä tietoverkoissa, tieto salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä turvallisuusluokittelemattomia salassa pidettäviä tietoja. |

| | |
|---|---|
| **Yleiskuvaus** | Salassa pidettävän tiedon sähköiseen välitykseen liittyy useita riskejä. Riskien pienentäminen hyväksyttävälle tasolle edellyttää sekä henkilöstöön että tekniseen toteutukseen liittyvien tekijöiden huomiointia. Tilanteissa, joissa salassa pidettävää tietoa on tarve välittää esimerkiksi kahden organisaation välillä julkisen verkon kautta, turvallinen välitys edellyttää turvallisia salausratkaisuja ja avainhallintakäytäntöjä, sekä niiden käyttöön harjaantunutta henkilöstöä. Tilanteissa, joissa salausratkaisun käyttö edellyttää henkilöstön toimia (esimerkiksi salassa pidettävän dokumentin välitys toiseen organisaatioon sähköpostin salattuna liitteenä), tulee kiinnittää erityistä huomiota salausratkaisun turvallisen käytön jalkautukseen henkilöstölle. Teknisesti turvallinen salausratkaisu ei tuota salassa pidettävälle tiedolle riittävää suojausta esimerkiksi tilanteissa, joissa avainhallintakäytännöt ovat puutteellisia, tai joissa henkilöstö ei käytä salausratkaisua siihen liittyvien turvallisen käytön periaatteiden mukaisesti.<br><br>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.<br><br>Internet, sekä operaattorin tarjoamat MPLS-verkot ja esimerkiksi niin sanotut mustat kuidut tulkitaan julkisiksi verkoiksi. Tämä kattaa puhelimen, telekopion (faksi), sähköpostin, pikaviestimet ja muut vastaavat tietoverkon kautta toimivat tiedonsiirtomenetelmät. |
| **Toteutusesimerkki** | 1) Siirrettäessä salassa pidettävää tietoa ko. tiedolle hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolella verkon kautta tulee ottaa huomioon erityisesti salauksen rooli keskeisenä suojauksena.<br>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.<br>b) Henkilöstön osaamisesta salausratkaisun turvalliseen käyttöön on varmistuttu (esimerkiksi ohjeistus, koulutus ja valvonta).<br>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.<br>3) Salausratkaisun toimitusketjun turvallisuudesta on varmistuttu riittävällä tasolla. Erityisesti salausratkaisun toimitusketju luotettavalta valmistajalta kohteen tietojenkäsittelyympäristöön on varmistettu. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | TEK-01, I-15 |

| | |
|---|---|
| **Muita lisätietoja** | Traficom: Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut; Traficom: Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat; Traficom: Turvallinen tuotekehitys: kohti hyväksyntää; Tiedonhallintalautakunta: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2020:19, luku 7); ISO/IEC 27002:2022 5.14, 5.31, 8.24; PiTuKri JT-05, SA-01, SA-02, SA-03; Katakri 2020 I-01, I-12, I-18 |
| **Tunniste** | **TEK-15.1, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Tiedon salaaminen - salaaminen turvallisuusalueen sisällä** |
| **Vaatimus** | Kun salassa pidettävää tietoa siirretään viranomaisen sisäisessä verkossa, voidaan käyttää alemman tason salausta tai salaamatonta tiedonsiirtoa riskinhallintaprosessin tulosten perusteella. |
| **Lainsäädäntö** | TiHL 13 § 1 mom; 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | FYY-7.1, I-15 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03 |
| **Tunniste** | **TEK-15.2, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Tiedon salaaminen - turvallisuusluokitellun tiedon siirto turva-alueiden ulkopuolella** |
| **Vaatimus** | Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella, tieto/tietoliikenne salataan riittävän turvallisella menetelmällä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä turvallisuusluokiteltuja tietoja. |
| **Yleiskuvaus** | Erityisesti turvallisuusluokitellun tiedon suojaamisessa korostuu tarve käyttää salausratkaisuja, joiden riittävästä turvallisuudesta on luotettavaa näyttöä. Salausratkaisujen arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salausratkaisun oikeellisesta toiminnasta varmistumisen lisäksi huomioidaan muun muassa salausratkaisun käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa merkittävästi tilanteeseen, jossa salausta käytetään liikennöintiin hallitun fyysisesti suojatun alueen sisällä (esimerkiksi kahden turva-alueen välinen liikennöinti hallinnollisen alueen kautta). Muihin salausratkaisujen arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi ko. käyttötapauksen vaatimukset tiedon salassapitoajalle ja kryptografiselle eheydelle.<br><br>Puhtaasti ohjelmistopohjaiset salausratkaisut ovat tyypillisesti hyväksyttävissä IV- ja joissain tilanteissa erityisehdoilla myös III-luokille. II-luokalle ja useimmin myös III-luokalle edellytetään tyypillisesti enemmän alustan luotettavuudelta. Salausratkaisujen hyväksyntäprosessia on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen ohjeessa salaustuotearvioinneista ja -hyväksynnistä. Salausratkaisun vähimmäisvaatimuksia on käsitelty myös Kyberturvallisuuskeskuksen ylläpitämässä salausvahvuuskuvauksessa, sekä turvallisen tuotekehityksen ohjeessa. |

| | |
|---|---|
| **Toteutusesimerkki** | 1) Organisaatiossa on tunnistettu käyttötapaukset, joissa turvallisuusluokitellun tiedon suojaamiseen on tarve käyttää salausratkaisuja. Tunnistetut käyttötapaukset kattavat kaikki tilanteet, joissa turvallisuusluokitellun tiedon suojaaminen nojaa täysin tai osittain salausratkaisuun. Erityisesti on huomioitu liikennöinti julkisen tai matalamman turvallisuusluokan verkon kautta, tiedon välitys toiseen organisaatioon, ja turvallisuusalueiden ulkopuolelle vietävät päätelaitteet.<br>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.<br>3) Siirrettäessä turvallisuusluokiteltua tietoa ko. turvallisuusluokalle hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella verkon kautta tulee ottaa huomioon erityisesti salauksen rooli keskeisenä suojauksena.<br>a) Henkilöstöllä on käytössä työvälineet ja menetelmät turvallisuusluokitellun tiedon suojaamiseksi toimivaltaisen viranomaisen hyväksymällä salausratkaisulla.<br>b) Henkilöstön osaamisesta toimivaltaisen viranomaisen hyväksymän salausratkaisun turvalliseen käyttöön on varmistuttu (esimerkiksi ohjeistus, koulutus ja valvonta). |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | FYY-7.1, I-15 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03; Katakri 2020 I-01, I-12, I-15, I-18, F-08.1 |
| **Tunniste** | **TEK-15.3, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Tiedon salaaminen - turvallisuusluokitellun tiedon siirto turva-alueiden sisällä** |
| **Vaatimus** | Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen. |
| **Toteutusesimerkki** | 2) Tilanteissa, joissa turvallisuusluokiteltua tietoa siirretään fyysisesti suojattujen turvallisuusalueiden sisäpuolella,<br>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<br>b) tieto suojataan toimivaltaisen viranomaisen erillishyväksyntään perustuen matalamman tason salauksella (esim. HTTPS ko. turvallisuusluokan verkon sisäisessä liikenteessä). |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | FYY-7.1, I-15 |
| **Tunniste** | **TEK-15.4, L:TL III, E:, S:, TS:** |
| **Nimi** | **Tiedon sähköinen välitys - TL III** |

| | |
|---|---|
| **Vaatimus** | Vain kansallisten turvallisuusluokan III sähköisten tietojen säilytys on mahdollista kyseisen turvallisuusluokan mukaisessa päätelaitteessa turva-alueen ulkopuolella edellyttäen, että a) tiedot on suojattu ko. turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla , ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle riittävästä luottamuksellisuudesta ja eheydestä on huolehdittu toimivaltaisen viranomaisen hyväksymällä menetelmällä. |
| **Viitteet** | FYY-7.1, I-17 |
| **Muita lisätietoja** | Katakri 2020 F-04, I-12, I-18 |
| **Tunniste** | **TEK-15.5, L:TL I, E:, S:, TS:** |
| **Nimi** | **Tiedon salaaminen - TL I** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Yleiskuvaus** | Katakri 2020:n kohta I-12 ottaa kantaa turvallisuusluokan II tietojenkäsittely-ympäristössä käytettäviin salausratkaisuihin. Fyysisten turva-alueiden ja matalamman turvallisuusluokan verkkojen yli liikennöinti on käsitelty kohdassa I-01.<br><br>Muissa tilanteissa, joissa turvallisuusluokan I tietojen suojaamiseen käytetään salausratkaisuja, esimerkiksi päätelaitteiden kiintolevyjen salaukseen tai eri tiedon omistajien tietojen erotteluun, suositellaan huomioitavaksi, että turvallisuusluokan I tietojen suojaamiseen riittävän luotettavia, hyväksyttyjä salausratkaisuja on saatavilla äärimmäisen rajoitetusti. Tällaisissa tilanteissa salausratkaisut ovatkin lähtökohtaisesti vain tukevassa roolissa muille suojauksille, erityisesti fyysiselle pääsynhallinnalle. |
| **Toteutusesimerkki** | Erityisesti huomioitava, että turvallisuusluokan I tietojen suojaamiseen riittävän luotettavia, hyväksyttyjä salausratkaisuja on saatavilla erittäin rajoitetusti. Tämä edellyttääkin tyypillisesti turvallisuusluokan I tietojen siirtämistä turvallisuusluokalle I hyväksytyllä kuriirimenettelyllä tilanteissa, joissa turvallisuusluokan I tietoa on tarve siirtää fyysisten turva-alueiden välillä. |
| **Lainsäädäntö** | TiHL 14 §;<br>TLA 11 § 1 mom 7 k, 12 § |
| **Viitteet** | I-15 |
| **Tunniste** | **TEK-16, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Muutoshallintamenettelyt** |
| **Vaatimus** | Tietojenkäsittely-ympäristöön tehtäviin muutoksiin on käytössä turvallisuuden huomioiva muutostenhallintamenettely. |

| | |
|---|---|
| **Yleiskuvaus** | Tietojenkäsittely-ympäristön tietoturvallisuuden ja muutosten luotettava hallinta edellyttää, että ympäristön 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.<br><br>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.<br><br>Laitteiston suojauksessa luvattomien laitteiden kytkemistä vastaan voidaan hyödyntää esimerkiksi<br>a) laitteiden sijoittamista sinetöityyn ja/tai hälytyslaitteella varustettuun turvakehikkoon tai vastaavaan,<br>b) peukalointia vastaan suojattujen laitteiden käyttämistä, tai<br>c) jotain vastaavaa menettelyä (esim. käytettävien laitteiden sinetöintiä). Käytettäessä sinetöintiin perustuvaa menetelmää, tulisi sinettien eheyden tarkastamiseen olla säännöllinen prosessi.<br><br>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.<br><br>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. |
| **Toteutusesimerkki** | 1) Tietojenkäsittely-ympäristön kokoonpanosta on olemassa ajantasainen kirjanpito. Kirjanpidolla tarkoitetaan laitteisto- ja ohjelmistokirjanpitoa, sekä tietoa turvallisuuteen vaikuttavista konfiguraatioista ja menettelyistä.<br>2) Tietojenkäsittelyyn ja tietojenkäsittely-ympäristöön liittyviin muutoksiin on käytössä muutostenhallintamenettely. Muutokset ovat jäljitettävissä.<br>3) On olemassa menetelmät, joilla varmistetaan tietojenkäsittely-ympäristön turvallisuustason säilyminen tehtyjen muutosten yhteydessä. |
| **Lainsäädäntö** | TiHL 13 §, 15 § |
| **Viitteet** | I-16 |

| | |
|---|---|
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.9, 5.36, 5.37, 8.19, 8.29, 8.32; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 5); PiTuKri MH-01; Katakri 2020 I-03, I-05, I-17, I-18, T-04. T-12 |
| **Tunniste** | **TEK-16.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Muutoshallintamenettelyt - uudelleenarviointi** |
| **Vaatimus** | Tietoturvallisuutta koskevat tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä. |
| **Lainsäädäntö** | TiHL 13 § 1 mom |
| **Viitteet** | I-16 |
| **Tunniste** | **TEK-16.2, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Muutoshallintamenettelyt - dokumentointi** |
| **Vaatimus** | Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten- ja asetustenhallintaprosessia. |
| **Lainsäädäntö** | TiHL 5 § 2 mom |
| **Viitteet** | I-16 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.9, 8.32 |
| **Tunniste** | **TEK-16.3, L:TL IV, E:Tärkeä, S:Tärkeä, TS:** |
| **Nimi** | **Muutoshallintamenettelyt - TL IV** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | 1) Tietojenkäsittely-ympäristö on dokumentoitu sellaisella tasolla, että siitä pystytään selvittämään tietojenkäsittely-ympäristössä käytetyt laitteet ja ohjelmistot versiotietoineen (laite-, käyttöjärjestelmä- ja sovellusohjelmistot) ja se tukee myös haavoittuvuuksien hallintaa.<br>2) Tietojenkäsittely-ympäristöjä tarkkaillaan luvattomien muutosten tai laitteistojen havaitsemiseksi. Tietojenkäsittely-ympäristön kirjanpito pidetään ajan tasalla koko elinkaaren ajan.<br>3) Tietojenkäsittely-ympäristön turvallisuuden toteuttamiseen liittyvän aineiston (dokumentaatiot, sähköiset kirjanpidot ja vast.) luokittelu- ja suojaamistarpeet on määritetty. |
| **Lainsäädäntö** | TiHL 5 § 2 mom, 13 § 1 mom |
| **Viitteet** | I-16 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.9, 8.8 |
| **Tunniste** | **TEK-16.4, L:TL II, E:Kriittinen, S:Kriittinen, TS:** |
| **Nimi** | **Muutoshallintamenettelyt - TL II** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | 1) Laitteistot suojataan luvattomien laitteiden (näppäilynauhoittimet, langattomat lähettimet ml. mobiililaitteet ja vastaavat) liittämistä vastaan. |
| **Lainsäädäntö** | TLA 11 § 1 mom 2 ja 5 k |
| **Viitteet** | I-16 |
| **Tunniste** | **TEK-17, L:Salassa pidettävä, E:Normaali, S:, TS:Henkilötieto** |
| **Nimi** | **Etäkäyttö** |

| | |
|---|---|
| **Vaatimus** | Etäkäytössä käyttäjät ohjeistettu ja tunnistetaan riittävän luotettavasti. |
| **Yleiskuvaus** | Etäkäytöllä ja -hallinnalla tarkoitetaan perinteisessä merkityksessään organisaation toimitilojen ulkopuolelta tapahtuvaa tietojärjestelmien käyttöä/hallintaa tätä tarkoitusta varten hankitulla päätelaitteella. Normaalisti päätelaitteena toimii organisaation henkilön käyttöön antama kannettava tietokone. Turvallisuusluokitellun tiedon osalta etäkäyttö soveltuu perinteisessä merkityksessään vain turvallisuusluokan IV tiedoille.<br><br>Henkilöstön koulutuksessa ja ohjeistuksessa on huomioitava erityisesti salassa pidettävien tietojen suojaaminen sivullisilta. Sivullisilta suojaamiseen sisältyy muun muassa mahdollisten käsittelypaikkojen valinta ja erilaisiin paikkoihin liittyvät rajoitteet käsittelylle (salakatselun ja salakuuntelun estäminen), päätelaitteiden ja muiden työvälineiden suojaaminen varkauksilta ja peukaloinneilta (säilytys vain lukitussa tilassa ja aina muistialueiden salaus aktivoituna, sekä esimerkiksi suojapakkausten ja -koteloiden käyttö), sekä muut kyseisten päätelaitteiden ja muiden työvälineiden turvallisen käytön menettelyt. |
| **Toteutusesimerkki** | 1) Etäkäytössä käyttäjät tunnistetaan luotettavasti.<br>2) Etäkäyttö on ohjeistettu ja sitä valvotaan. |
| **Lainsäädäntö** | TiHL 4 § 2 mom, 13 § 1 mom; TLA 10 § 1 mom |
| **Viitteet** | HAL-12, HAL-13, HAL-19, I-18 |
| **Muita lisätietoja** | CPNI: Personnel Security in Remote Working; CPNI: Configuring and managing Remote Access for Industrial Control Systems; CPNI: Physical Security Advice; ISO/IEC 27002:2022 5.10, 5.37, 6.3, 6.7, 7.1, 7.8, 7.9, 7.10, 8.1; PiTuKri IP-03, JT-05, SA-02; Katakri 2020 I-17:n Lisätietoja-kenttä |
| **Tunniste** | **TEK-17.1, L:Salassa pidettävä, E:Tärkeä, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Etäkäyttö - tietojen ja tietoliikenteen salaaminen** |
| **Vaatimus** | Turvallisuusalueen ulkopuolella etäkäytössä käytettävät päätelaitteet, muistivälineet ja tietoliikenneyhteydet ovat suojattu käyttäen sellaisia salausratkaisuja, joissa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat valmistajilta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia. |
| **Yleiskuvaus** | Siirrettävien tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) osalta voidaan sallia salaamattomien laitteiden käyttö siinä tapauksessa, että tietovälineitä ei koskaan jätetä valvomatta hyväksyttyjen turvallisuusalueen ulkopuolella. |
| **Toteutusesimerkki** | 1) Päätelaitteessa olevat tiedot tulee olla suojattu salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia.<br>2) Järjestelmien etäkäyttö edellyttää tietoliikenteen salausratkaisua, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia.<br>3) 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, tietovälineitä ei jätetä valvomatta. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 10 §, 11 §, 12 §, 13 § |

| | |
|---|---|
| **Viitteet** | FYY-7.1, I-18 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 7.9, 7.10, 8.1 |
| **Tunniste** | **TEK-17.2, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Etäkäyttö - turvallisuusluokitettujen tietojen ja tietoliikenteen salaaminen** |
| **Vaatimus** | Turvallisuusalueen ulkopuolella etäkäytössä käytettävät päätelaitteet, muistivälineet ja tietoliikenneyhteydet ovat suojattu käyttäen ko. turvallisuusluokan huomioiden riittävän turvallisia salausratkaisuja. |
| **Yleiskuvaus** | Siirrettävien tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) osalta voidaan sallia salaamattomien laitteiden käyttö siinä tapauksessa, että tietovälineitä ei koskaan jätetä valvomatta hyväksyttyjen turva-alueiden ulkopuolella. |
| **Toteutusesimerkki** | 1) Päätelaitteessa olevat tiedot tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella salausratkaisulla, ja päätelaitteen ko. turvallisuusluokalle riittävästä eheydestä tulee huolehtia.<br>2) Järjestelmien etäkäyttö edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokan tietojen suojaamiseen hyväksymää liikenteen salausta.<br>3) Elleivät turvallisuusalueiden ulkopuolelle viedyt turvallisuusluokiteltua tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu ko. turvallisuusluokalle riittävän turvallisella menetelmällä, tietovälineitä ei jätetä valvomatta. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 2 mom;<br>TLA 10 §, 11 §, 12 §, 13 § |
| **Viitteet** | FYY-7.1, I-18 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 7.9, 7.10, 8.1 |
| **Tunniste** | **TEK-17.3, L:TL IV, E:Tärkeä, S:, TS:** |
| **Nimi** | **Etäkäyttö - käyttäjien vahva tunnistaminen** |
| **Vaatimus** | Etäkäytössä järjestelmien käyttäjät tunnistetaan vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta. |
| **Yleiskuvaus** | |
| **Lainsäädäntö** | TLA 10 §, 11 § 1 mom 5 k |
| **Viitteet** | I-18 |
| **Muita lisätietoja** | Katakri 2020 F-04 |
| **Tunniste** | **TEK-17.4, L:TL IV, E:Kriittinen, S:, TS:** |
| **Nimi** | **Etäkäyttö - hyväksytyt laitteet** |
| **Vaatimus** | Etäkäytössä käytettään vain käyttöympäristöön hyväksyttyjä ja tunnistettuja laitteita. |
| **Toteutusesimerkki** | Vain käyttöympäristöön hyväksyttyjä laitteita ja etäyhteyksiä käytetään. |
| **Lainsäädäntö** | TLA 10 §, 11 § 1 mom 5 k |
| **Viitteet** | I-18 |
| **Muita lisätietoja** | Katakri 2020 F-04 |
| **Tunniste** | **TEK-17.5, L:TL III, E:, S:, TS:** |
| **Nimi** | **Etäkäyttö - turvallisuusluokitellun tiedon käyttö julkisella paikalla** |
| **Vaatimus** | Turvallisuusluokiteltuja tietoja ei lueta tai muuten käsitellä matkalla tai julkisilla paikoilla. |

| | |
|---|---|
| **Lainsäädäntö** | TLA 10 § 1 mom, 13 § |
| **Viitteet** | FYY-7.1, I-18 |
| **Tunniste** | **TEK-17.6, L:TL III, E:Kriittinen, S:, TS:** |
| **Nimi** | **Etäkäyttö - laitetunnistus** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Yleiskuvaus** | Turvallisuusluokkien III ja II käsittely-ympäristöissä sekä muissa kriittisissä käsittely-ympäristöissä edellytetään käytön teknistä sitomista hyväksyttyyn etäkäyttölaitteistoon (esim. laitetunnistus). |
| **Toteutusesimerkki** | Etäkäyttö on estetty teknisesti muita kuin hyväksyttyjä laitteita käyttäen. |
| **Lainsäädäntö** | TLA 10 §, 11 § 1 mom 5 k |
| **Viitteet** | I-18 |
| **Tunniste** | **TEK-17.7, L:TL III, E:Kriittinen, S:, TS:** |
| **Nimi** | **Etäkäyttö - TL III** |
| **Vaatimus** | Turvallisuusluokan III sähköisten tietojen etäkäyttö (käsittely) ja säilytys on mahdollista kyseisen turvallisuusluokan mukaisessa päätelaitteessa turva-alueiden ulkopuolella edellyttäen, että a) tiedot on suojattu ko. turvallisuusluokalle riittävän turvallisella salausratkaisulla, ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle riittävästä luottamuksellisuudesta ja eheydestä on huolehdittu toimivaltaisen viranomaisen hyväksymällä menetelmällä. |
| **Yleiskuvaus** | |
| **Lainsäädäntö** | TLA 10 § (TL III) |
| **Viitteet** | I-18 |
| **Tunniste** | **TEK-17.8, L:TL II, E:, S:, TS:** |
| **Nimi** | **Etäkäyttö - etäkäyttö turvallisuusalueella** |
| **Vaatimus** | Järjestelmien etäkäyttö ja -hallinta rajataan toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle. |
| **Yleiskuvaus** | Tiedon käsittely edellyttää fyysisesti suojattua turvallisuusaluetta tai korvaavia menettelyjä, joilla saavutetaan vastaavat fyysisen turvallisuuden olosuhteet. |
| **Lainsäädäntö** | TLA 10 § (TL II) |
| **Viitteet** | I-18 |
| **Tunniste** | **TEK-17.9, L:TL I, E:, S:, TS:** |
| **Nimi** | **Etäkäyttö - TL I** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Yleiskuvaus** | Turvallisuusluokan I tietoa saa säilyttää tai muutoin käsitellä ainoastaan turva-alueilla (TLA, 10 §), mikä asettaa rajoitteet myös etäkäytön mahdollisuuksille. |
| **Lainsäädäntö** | TLA 10 § (TL I) |

| | |
|---|---|
| **Viitteet** | I-18 |
| **Tunniste** | **TEK-18, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Ohjelmistohaavoittuvuuksien hallinta** |
| **Vaatimus** | Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi. |
| **Yleiskuvaus** | Ohjelmistohaavoittuvuuksien hyödyntäminen on useissa hyökkäystyypeissä jossain vaiheessa mukana. On huomioitava, että haavoittuvaa lähdekoodia on niin käyttöjärjestelmäohjelmistoissa, palvelinsovelluksissa, loppukäyttäjäsovelluksissa, kuin esimerkiksi laiteohjelmistotason (firmware) sovelluksissa ja ajureissa, BIOS:issa ja erillisissä hallintaliittymissä (esim. iLo, iDrac). Ohjelmistovirheiden lisäksi haavoittuvuuksia aiheutuu konfiguraatiovirheistä ja vanhoista käytänteistä, esimerkiksi vanhentuneiden salausalgoritmien käytöstä. Vastuulliset toimittajat korjaavat ohjelmistoistaan löytyneitä haavoittuvuuksia. Riskejä voidaan pienentää korjausten asennuksilla. Haavoittuvuuden hallintaa toteuttaessa tulee huolehtia haavoittuvuusskannerin, CMDB:n ja muiden järjestelmien ajantasaisuudesta ja tietoturvallisuudesta.<br><br>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.<br><br>Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa:<br>- 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.<br>- Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia. |

| | |
|---|---|
| **Toteutusesimerkki** | Vaatimus voidaan toteuttaa siten, että haavoittuvuuksien hallintaan on olemassa prosessi, joka sisältää vähintään alla mainitut toimenpiteet:<br>1) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan aktiivisesti ja tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti.<br>2) Päivitysten asentumisen onnistumista tarkastellaan säännöllisesti, vähintään kuukausittain.<br>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.<br>4) Löytyneiden haavoittuvuuksien sekä päivitysmenettelyjen puutteiden käsittely on järjestetty siten, että tietojenkäsittely-ympäristön suojaamiseen oleellisesti vaikuttavat heikkoudet poistetaan, korjataan tai muuten rajoitetaan siten, että turvallisuusluokiteltujen tietojen käsittely ei tarpeettomasti vaarannu. |
| **Lainsäädäntö** | TiHL 13 §;<br>TLA 11 § 1 mom 2 k |
| **Viitteet** | HAL-16, HAL-16.1, I-19 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.8; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-04 |
| **Tunniste** | **TEK-18.1, L:TL IV, E:Tärkeä, S:Tärkeä, TS:** |
| **Nimi** | **Ohjelmistohaavoittuvuuksien hallinta - TL IV** |
| **Vaatimus** | Tietojenkäsittely-ympäristön laitteet tarkastetaan kattavasti ohjelmistohaavoittuvuuksien varalta vähintään vuosittain ja merkittävien muutosten yhteydessä. |
| **Toteutusesimerkki** | 1) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti vähintään (haavoittuvuusskannaus, CMDB jne.) vuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi.<br>2) Laitteisto- ja ohjelmistokirjanpidon (ml. CMDB) sekä skannausohjelmiston ajantasaisuudesta ja tietoturvallisuudesta on huolehdittu. |
| **Lainsäädäntö** | TiHL 13 §;<br>TLA 11 § 1 mom 2 k |
| **Viitteet** | I-19 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.8; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-04 |
| **Tunniste** | **TEK-18.2, L:TL III, E:Kriittinen, S:Kriittinen, TS:** |
| **Nimi** | **Ohjelmistohaavoittuvuuksien hallinta - TL III** |
| **Vaatimus** | Tietojenkäsittely-ympäristön laitteet tarkastetaan kattavasti ohjelmistohaavoittuvuuksien varalta vähintään puolivuosittain ja merkittävien muutosten yhteydessä. |

| | |
|---|---|
| **Toteutusesimerkki** | Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti vähintään (haavoittuvuusskannaus, CMDB jne.) puolivuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. "Merkittäviin muutoksiin" voidaan laskea esimerkiksi verkkotopologian muutokset, uusien järjestelmien käyttöönotot ja/tai vanhojen service pack -tason päivitykset, palomuurien ja vastaavien suodatussääntöjen merkittävät muutokset, jne. |
| **Lainsäädäntö** | TiHL 13 §;<br>TLA 11 § 1 mom 2 k |
| **Viitteet** | I-19 |
| **Tunniste** | **TEK-19, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Varmuuskopiointi** |
| **Vaatimus** | Varmistus- ja palautusprosessit on suunniteltu, toteutettu, testattu ja kuvattu siten, että ne vastaavat palvelutasosopimusten ja<br>lainsäädännön velvoitteisiin sekä muihin liiketoiminnallisiin vaatimuksiin. |
| **Yleiskuvaus** | Varmuuskopiointi suositellaan aina mitoitettavan toimintavaatimuksiin. Toimintavaatimuksiin nähden riittävässä varmuuskopioinnissa tulisi huomioida ainakin seuraavat:<br>1) Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää (recovery point objective, RPO).<br>2) Varmuuskopiot kattavat kaiken järjestelmän toiminnan jatkuvuuden kannalta olennaisen tiedon.<br>3) Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palautuminen voi kestää (recovery time objective, RTO).<br>4) Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti.<br>5) Palautusprosessin dokumentointi on riittävällä tasolla.<br>6) Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä, jne.).<br>Huom: Varmuuskopiot tulisi suojata fyysisen ja loogisen pääsynhallinnan menetelmin vähintään tiedon (mahdollisesti kasautumisvaikutuksen nostaman) turvallisuusluokan mukaisesti. |
| **Toteutusesimerkki** | Vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:<br>1) Varmuuskopiot käsitellään ja säilytetään niiden elinkaaren ajan vähintään vastaavan turvallisuustason järjestelmissä.<br>2) Mikäli varmuuskopioita siirretään ko. turvallisuusluokan fyysisesti suojatun turvallisuusalueen ulkopuolelle, on menettelyt toteutettava kohtien TEK-15:ssa (sähköinen välitys) ja/tai FYY-08 (posti/kuriiri) sekä TEK-17 (kuljetus fyysisesti suojatun alueen ulkopuolelle).<br>3) Varmistusmediat hävitetään luotettavasti.<br>4) Järjestelmän ja tiedon palauttamista testataan säännöllisesti esimerkiksi automatisoidusti, jotta tieto voidaan palauttaa oikeaan tilaansa eheyden varmistamiseksi. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom;<br>TLA 2 § 2 mom, 7 §, 11 § 1 mom 4 k |
| **Viitteet** | VAR-09, I-20 |

| | |
|---|---|
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.13; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 5); PiTuKri KT-03; Katakri 2020 I-20 |
| **Tunniste** | **TEK-19.1, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Varmuuskopiointi -TL IV** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Yleiskuvaus** | Käsiteltäessä samalla varmistusjärjestelmällä eri omistajien tietoja, tarkastusoikeuden mahdollistavat erottelumenettelyt on toteutettava varmistusjärjestelmän liittymien ja tallennemedioiden osalta (esim. omistaja-/hankekohtaiset eri avaimilla salatut nauhat, joita säilytetään asiakaskohtaisissa kassakaapeissa/kassakaappilokeroissa). |
| **Toteutusesimerkki** | Käsiteltäessä samalla varmistusjärjestelmällä tarkastusoikeuden varaavien eri omistajien tietoja, tarkastusoikeuden mahdollistavat erottelumenettelyt on toteutettava ko. turvallisuusluokan mukaisesti varmistusjärjestelmän liittymien ja tallennemedioiden osalta. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 16 §;<br>TLA 7 §, 10 § 1 mom, 11 § 1 mom 3 k |
| **Viitteet** | I-20 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.13; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 5); PiTuKri KT-03; Katakri 2020 I-06 |
| **Tunniste** | **TEK-19.2, L:TL III, E:, S:, TS:** |
| **Nimi** | **Varmuuskopiointi - varmuuskopioiden rekisteröinti ja käsittelyn seuranta** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Varmuuskopioista on rekisterit ja varmuuskopioiden käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai tietoon (esimerkiksi dokumentin osaksi). |
| **Lainsäädäntö** | TLA 14 § |
| **Viitteet** | I-20 |
| **Muita lisätietoja** | Katakri 2020 F-08.3 |
| **Tunniste** | **TEK-20, L:Salassa pidettävä, E:, S:, TS:Erityinen henkilötietoryhmä** |
| **Nimi** | **Sähköisessä muodossa olevien tietojen tuhoaminen** |
| **Vaatimus** | Sähköisessä muodossa olevien tietojen tuhoaminen on järjestetty luotettavasti. Salassa pidettävien tietojen tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. |
| **Yleiskuvaus** | Tiedon suojaamisesta tulee huolehtia tiedon elinkaaren päättymiseen asti. Tämä tulee huomioida erityisesti tilanteissa, joissa käytetään kolmannen osapuolen palvelua tiedon tuhoamiseen, esimerkiksi kiintolevyjen sulattamiseen. Käytännön toteutusmallina yleensä menettely, jossa tiedosta vastuussa oleva organisaatio valvoo tiedon tuhoamisprosessin aina elinkaaren päättymiseen saakka.<br><br>Myös henkilöstön rooli on syytä huomioida tuhoamisprosesseissa. Organisaation tulee järjestää henkilöstölle yksikäsitteinen tapa tietojen tuhoamiseen. |

| | |
|---|---|
| **Toteutusesimerkki** | Tuhoaminen eri menetelmiä yhdistäen<br>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.<br><br>Sähköisessä muodossa olevien tietojen tuhoamisessa huomioon otettavaa<br>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 toimivaltaisen viranomaisen hyväksymä ylikirjoitusmenettely) ei ole mahdollista, turvallisuusluokiteltua tietoa sisältävää osaa ei tule luovuttaa kolmansille osapuolille. Tilanteissa, joissa laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä, tulisi kolmannen osapuolen suorittamia huoltotoimenpiteitä valvoa, ja pyrkiä varmistumaan siitä, että turvallisuusluokiteltua tietoa ei viedä huoltotoimenpiteen yhteydessä. |
| **Lainsäädäntö** | TiHL 21 § 2 mom;<br>TLA 15 § |
| **Viitteet** | FYY-11, I-21 |
| **Muita lisätietoja** | Traficom: Kiintolevyjen elinkaaren hallinta (26.10.2016); CPNI: Secure destruction of sensitive items (2017); ISO/IEC 27002:2022 7.10, 7.14; Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 4); PiTuKri SI-02; Katakri 2020 T-12, F-08.3, F-08.4 (ei-sähköisten tietojen osalta). |
| **Tunniste** | **TEK-20.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Sähköisessä muodossa olevien tietojen tuhoaminen - arkistointi** |
| **Vaatimus** | Tietojen arkistointivelvollisuus on huomioitu tiedon elinkaaren hallinnassa. |
| **Lainsäädäntö** | TiHL 21 § |
| **Tunniste** | **TEK-20.2, L:Salassa pidettävä, E:, S:, TS:Henkilötieto** |
| **Nimi** | **Sähköisessä muodossa olevien tietojen tuhoaminen - pilvipalveluissa olevan tiedon tuhoaminen** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Yleiskuvaus** | Huomioitavaa erityisesti pilviteknologiaa hyödyntävissä toteutuksissa:<br>- 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. |
| **Lainsäädäntö** | TiHL 21 § 2 mom |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.23; PiTuKri SA-03 |
| **Tunniste** | **TEK-20.3, L:TL IV, E:, S:, TS:** |
| **Nimi** | **Sähköisessä muodossa olevien tietojen tuhoaminen - TL IV** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |

| | |
|---|---|
| **Toteutusesimerkki** | Tuhoaminen ylikirjoittamalla<br>Tuhottaessa turvallisuusluokiteltua materiaalia ylikirjoittamalla, suositellaan noudatettavaksi Kyberturvallisuuskeskuksen ohjeen "Kiintolevyjen elinkaaren hallinta" mukaisia vaatimuksia ylikirjoitukselle sekä muistivälineiden uusiokäytölle.<br><br>Tuhoaminen silppuamalla<br>Tuhottaessa turvallisuusluokiteltua materiaalia silppuamalla, noudatetaan suosituksen "VM 2021:5 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä" mukaisia vaatimuksia kyseisen turvallisuusluokan aineiston silppukoolle. |
| **Lainsäädäntö** | TiHL 21 § 2 mom;<br>TLA 15 § |
| **Viitteet** | FYY-11.1, FYY-11.2, FYY-11.3, I-21 |
| **Muita lisätietoja** | Traficom: Kiintolevyjen elinkaaren hallinta (26.10.2016); Tiedonhallintalautakunta: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5) |
| **Tunniste** | **TEK-20.4, L:TL II, E:, S:, TS:** |
| **Nimi** | **Sähköisessä muodossa olevien tietojen tuhoaminen - toisen viranomaisen laatimat tiedot** |
| **Vaatimus** | Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle. |
| **Lainsäädäntö** | TLA 15 § 2 mom |
| **Viitteet** | I-21 |
| **Tunniste** | **TEK-20.5, L:TL II, E:, S:, TS:** |
| **Nimi** | **Sähköisessä muodossa olevien tietojen tuhoaminen - tuhoamisen suorittaja** |
| **Vaatimus** | Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö. |
| **Lainsäädäntö** | TLA 15 § 2 mom |
| **Viitteet** | I-21 |
| **Tunniste** | **TEK-20.6, L:TL I, E:, S:, TS:** |
| **Nimi** | **Sähköisessä muodossa olevien tietojen tuhoaminen - TL I** |
| **Vaatimus** | Alikriteeri tarkentaa pääkriteerin vaatimusta. |
| **Toteutusesimerkki** | Turvallisuusluokan I sähköisessä muodossa olevan tiedon tuhoamisessa voidaan hyödyntää "VM 2021:5 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä" koottuja turvallisuusluokan II silppukokoja, mikäli suojausta täydennetään viranomaisen hyväksymillä menettelyillä. Tällaisia menettelyihin sisältyvät tyypillisesti muun muassa silpun jatkokäsittely valvotusti polttamalla tai sulattamalla. |
| **Lainsäädäntö** | TLA 15 § |
| **Viitteet** | I-21 |
| **Tunniste** | **TEK-21, L:, E:, S:Normaali, TS:** |
| **Nimi** | **Tietojärjestelmien saatavuus** |
| **Vaatimus** | Viranomaisen on varmistettava tietojärjestelmien saatavuus koko niiden elinkaaren ajan. |

| | |
|---|---|
| **Yleiskuvaus** | Saatavuusvaatimusten toteutuksen tulee huomioida tietojärjestelmältä edellytettävä kuormituksen kesto, vikasietoisuus ja palautumisaika. |
| **Toteutusesimerkki** | Saatavuusvaatimukset on tunnistettu. On tunnistettu vähintään pisin aika, jonka järjestelmä voi olla pois käytöstä, palautusaikatavoite ja palautuspistetavoite. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom 4 k |
| **Viitteet** | VAR-02, |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.6, 8.14 |
| **Tunniste** | **TEK-21.1, L:, E:, S:Normaali, TS:** |
| **Nimi** | **Tietojärjestelmien saatavuus - saatavuutta suojaavat menettelyt** |
| **Vaatimus** | Saattavuutta suojaavien menettelyiden toteutus on suhteutettu palautusaikatavoitteeseen. |
| **Toteutusesimerkki** | Saatavuutta suojaavat menettelyt on toteutettu järjestelmäkohtaisesti räätälöidyillä suojauksilla. Suojauksiin voi sisältyä esimerkiksi keskeisten verkkoyhteyksien, laitteistojen ja sovellusten ajoympäristöjen kahdentamiset. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom 4 k |
| **Viitteet** | VAR-02, VAR-06, VAR-07, VAR-08, |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.30 |
| **Tunniste** | **TEK-21.2, L:, E:, S:Normaali, TS:** |
| **Nimi** | **Tietojärjestelmien saatavuus - palveluiden valvonta** |
| **Vaatimus** | Palveluiden ja tietojärjestelmien saatavuutta seurataan ja valvotaan niiden kriittisyyden edellyttämällä tasolla. |
| **Toteutusesimerkki** | 1) Jos palvelulla on saatavuus vaatimuksia, seurataan sen saatavuutta valvontajärjestelmällä.<br>2) Valvontajärjestelmän tulee lähettää hälyttää havaitusta saatavuuspoikkeamista. |
| **Lainsäädäntö** | TiHL 13 § 1 mom, 15 § 1 mom 4 k |
| **Viitteet** | HAL-07, |
| **Muita lisätietoja** | ISO/IEC 27002:2022 8.16 |
| **Tunniste** | **TEK-22, L:, E:Tärkeä, S:Tärkeä, TS:** |
| **Nimi** | **Tietojärjestelmien toiminnallinen käytettävyys** |
| **Vaatimus** | Viranomainen on varmistanut tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden. |

| | |
|---|---|
| **Yleiskuvaus** | Toiminnallisen käytettävyyden varmistamisessa on suositeltavaa käyttää niin teknisiä käytettävyystestauksia kuin käyttäjillä suoritettavia käytettävyystestejä tai heuristisia asiantuntija-arviointeja.<br><br>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.<br><br>Tiedonhallintalain täyttämistä voi tukea myös digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) mukaisilla, yleisölle tarjottavien palvelujen saavutettavuutteen liittyvillä menettelyillä. |
| **Toteutusesimerkki** | 1) Viranomaisen tehtävien hoitamisen kannalta olennaiset tietojärjestelmät on tunnistettu. Olennaisiksi tunnistetuista tietojärjestelmistä on olemassa lista.<br>2) Olennaisiksi tunnistettujen tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys varmistetaan testauksen avulla niin hankintavaiheessa kuin merkittävien ylläpitotoimien yhteydessä. Varmistamisessa huomioidaan erityisesti, että<br>a) tietojärjestelmä on helposti opittava,<br>b) tietojärjestelmän toimintalogiikka on helposti muistettava,<br>c) tietojärjestelmän toiminta tukee niitä työtehtäviä, joissa käyttäjä järjestelmää hyödyntää ja<br>d) tietojärjestelmä edistää sen käytön virheettömyyttä. |
| **Lainsäädäntö** | TiHL 13 § 2 mom |
| **Viitteet** | HAL-17, HAL-17.1, |

# 5 Varautuminen ja jatkuvuudenhallinta

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

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

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

| Tunniste | VAR-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto |
|---|---|
| **Nimi** | **Varautumista ohjaava lainsäädäntö** |
| **Vaatimus** | Organisaatio on tunnistanut toimintaansa ja palveluihinsa liittyvä ICT-varautumista ohjaavan kansallisen ja EU-lainsäädännön sekä muut ICT-varautumiseen liittyvät normit. |
| **Yleiskuvaus** | Lainsäädäntö ja normit määrittävät minimitason ICT-varautumisen toteuttamiselle. Tämän lisäksi organisaation on huomioitava oman toimintansa erityispiirteistä nousevat tarpeet. Toimintojen sisäisten ja ulkoisten riippuvuussuhteiden ymmärtäminen on perusedellytys varautumisen kustannustehokkaalle johtamiselle. |
| **Toteutusesimerkki** | Organisaatiossa selvitetään ICT-varautumiseen ja jatkuvuudenhallintaan liittyvä lainsäädäntö, määräykset, ohjeet, standardit ja sopimukset sekä mahdolliset kansainväliset velvoitteet. Erityisen tärkeää on, että sekä palvelua hankkiva että palvelua tuottava organisaatio tuntee palveluun vaikuttavat määräykset ja pitävät toisensa näistä tietoisina.<br><br>Organisaation toimintaa ohjaava lainsäädäntö ja muut ohjaavat asiakirjat on useimmiten tunnistettu ja listattu tietoturva- ja riskienhallintapolitiikan perusteissa. Strategioissa, periaatteissa ja toiminnan suunnittelussa on huomioitu valtioneuvostotason ohjausasiakirjoissa asetetut ICT-varautumista ohjaavat linjaukset. |
| **Lainsäädäntö** | TiHL 4 § 2 mom 2 k; 13 § 1 mom |
| **Viitteet** | HAL-05, |
| **Muita lisätietoja** | PiTuKri TJ-07, PiTuKri EE-02 |
| **Tunniste** | **VAR-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Jatkuvuusvaatimusten määrittely** |
| **Vaatimus** | Toiminnan ja siihen liittyvien olennaisten tietojärjestelmien jatkuvuusvaatimukset on määritelty. |
| **Yleiskuvaus** | Järjestelmän palautumisajan tavoitteet tulee määrittää sen mukaisesti, miten pitkään organisaation toiminnan näkökulmasta järjestelmä voi pisimmillään olla poissa käytöstä. Toiminnan näkökulmasta tulee määrittää, miten paljon tai miten pitkältä ajalta tietoa voidaan menettää. |
| **Toteutusesimerkki** | Organisaation tulee määrittää jatkuvuusvaatimukset yhteistyössä riskienhallinnan, tietoturvan sekä arkkitehtuurien kanssa.<br>Ydintoimintojen ja -prosessien suojattavat palvelut ja järjestelmät on tunnistettu ja niille on asetettu saatavuustavoitteet ydintoimintojen tai ydinprosessien vaatimusten mukaisesti.<br>Palautumistoimenpiteiden käynnistämiskyky on määritetty palveluittain. |
| **Lainsäädäntö** | TiHL 4 § 2 mom 1 k, 13 § 1 ja 2 mom, 15 § 1 mom. |
| **Viitteet** | HAL-05, |
| **Muita lisätietoja** | Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6 ja luku 11; ISO/IEC 27002:2022 5.30 |
| **Tunniste** | **VAR-02.1, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto** |
| **Nimi** | **Jatkuvuusvaatimusten määrittely - palveluiden siirrot** |
| **Vaatimus** | Jatkuvuusvaatimuksissa on huomioitu palveluiden kotiuttamiset ja siirrot toiselle palveluntarjoajalle. |

| | |
|---|---|
| **Yleiskuvaus** | Palvelua hankittaessa tulee huomioida, että palvelua voi olla hankala kotiuttaa ja toimittajalukkoon jäänyttä palvelua vaikea siirtää toiselle palveluntarjoajalle. Erityisesti vaatimus tulee huomioida hankittaessa pilvipalveluita. |
| **Lainsäädäntö** | TiHL 4 § 2 mom 1 k, 13 § 1, 2 ja 4 mom, 15 § 1 mom. |
| **Viitteet** | HAL-05, |
| **Muita lisätietoja** | Pilvipalveluiden soveltamisohje 2020:73; ISO/IEC 27002:2022 5.23 |
| **Tunniste** | **VAR-03, L:, E:, S:Tärkeä, TS:** |
| **Nimi** | **Jatkuvuussuunnitelmat** |
| **Vaatimus** | Jatkuvuussuunnitelmat on laadittu ja otettu käyttöön. |
| **Yleiskuvaus** | Organisaation jatkuvuussuunnitelma sisältää periaatteet siitä miten toiminta järjestetään suunnitelmallisesti eri tilanteissa. Organisaation jatkuvuussuunnittelussa tunnistetaan ne palvelut, joista organisaation ydintoiminnot ovat riippuvaisia, arvioidaan mitä vaikutuksia eripituisilla ICT-palvelujen katkoilla on organisaation ydintoimintoihin.<br><br>Jatkuvuussuunnitelmissa tulee huomioida myös tietoturvallisuuden vaaditun tason säilyminen poikkeustilanteiden aikana. |
| **Toteutusesimerkki** | Jatkuvuussuunnitelmaan on kirjattu käytettävissä oleva henkilöstö, avainhenkilöt ja varahenkilöt sekä arvio heidän saatavuudestaan.<br>Jatkuvuussuunnitelmissa on kuvattu miten toimitaan häiriötilanteiden aikana sekä kuinka niiden jälkeen siirrytään takaisin normaaliin toimintaan.<br>Organisaatiolla on tarvittaessa suunnitelma ICT-palvelujen tuotannon siirtämisestä toisiin tiloihin mikäli nykyiset tilat muuttuvat käyttökelvottomiksi.<br>Jatkuvuussuunnitelmat yhteensovitetaan sidosryhmien kanssa riittävän laajasti koko toimintaketjussa.<br>Häiriötilanteiden viestinnän suunnittelu on osa jatkuvuussuunnitelmaa. |
| **Lainsäädäntö** | TiHL 4 § 2 mom 2 k,15 § |
| **Muita lisätietoja** | Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11; ISO/IEC 27002:2022 5.23 |
| **Tunniste** | **VAR-03.1, L:, E:, S:Tärkeä, TS:** |
| **Nimi** | **Jatkuvuussuunnitelmien testaus** |
| **Vaatimus** | Jatkuvuussuunnitelmia testataan säännöllisesti. |
| **Yleiskuvaus** | Harjoittelemalla testataan suunnitelmien toimivuus erilaisissa tilanteissa. Havaintoja käytetään suunnitelmien kehittämiseen. |
| **Toteutusesimerkki** | Organisaatiot vastaavat omasta harjoitustoiminnastaan ja määrittelevät jatkuvuussuunnitelmien testaamisen käytännöt. Organisaatio harjoittelee sisäisesti sekä valtakunnallisissa että alueellisissa ja paikallisissa harjoituksissa toiminnan edellyttämässä laajuudessa. |
| **Lainsäädäntö** | TiHL 4 § 2 mom,13 § 2 mom; 15 § |
| **Viitteet** | I-13 |
| **Muita lisätietoja** | ISO/IEC 27002:2022 5.23 |
| **Tunniste** | **VAR-04, L:, E:, S:Tärkeä, TS:** |
| **Nimi** | **Resurssit ja osaaminen** |

| | |
|---|---|
| **Vaatimus** | Henkilöt tuntevat omaan toimintaan liittyvät jatkuvuus- ja toipumissuunnitelmat sekä osaavat toimia niiden mukaisesti.<br><br>Varahenkilöt on nimetty ja heidän kyky hoitaa tehtävät normaalitilanteissa on varmistettu. |
| **Toteutusesimerkki** | Jokainen koulutettu henkilö tuntee periaatteet organisaation varautumisesta sekä tietää eri tilannemallien vaikutuksen omaan tehtäväänsä.<br>Heitä kannustetaan osallistumaan erilaisiin varautumista tukeviin yhteistyöryhmiin. |
| **Lainsäädäntö** | TiHL 4 § 2 mom |
| **Viitteet** | HAL-03, T-04 |
| **Tunniste** | **VAR-05, L:, E:, S:Tärkeä, TS:** |
| **Nimi** | **Henkilöstön saatavuus ja varajärjestelyt** |
| **Vaatimus** | Kriittisten tehtävien suorittamiseksi on suunniteltu ja valmisteltu erityistilanteiden vaihtoehtoiset toimintatavat ja henkilöstön saatavuus ja varajärjestelyt. |
| **Toteutusesimerkki** | Lainsäädännön mahdollistamat toimenpiteet on tunnistettu ja toteutettu tarvittavassa laajuudessa esimerkiksi lakko-oikeuksien poistamisen, hätätöiden käytön ja henkilövarausten (VAP) osalta. |
| **Lainsäädäntö** | TiHL 4 § 2 mom 2 k; 13 § 1 mom, 15 § 1 mom 4 k |
| **Muita lisätietoja** | Työaikalaki 872/2019, 19 §; Valtion virkaehtosopimuslaki 664/1970 11 §; Asevelvollisuuslaki 1438/2007 89 § |
| **Tunniste** | **VAR-06, L:, E:, S:Tärkeä, TS:** |
| **Nimi** | **Tietoliikenteen varmistaminen** |
| **Vaatimus** | Tietoliikennepalveluissa ja -sopimuksissa on huomioitu toiminnan kannalta tärkeiden palveluiden saatavuus häiriötilanteissa. |
| **Yleiskuvaus** | |
| **Toteutusesimerkki** | Tärkeiden palvelujen verkkoympäristöt ja tietoliikennepalvelut varmennetaan esimerkiksi kahdentamalla. Tietoliikenne voidaan kahdentaa fyysisesti kahta eri reittiä pitkin kahden eri operaattorin toimesta.<br>Tärkeissä ympäristöissä varmistetaan, että yksittäisen tietoliikennekomponentin vikaantuminen ei keskeytä palvelun toimintaa.<br>Erikseen valittuihin työasemiin voidaan esimerkiksi asentaa erillinen tietoliikenneyhteys jonka kautta voi päästä yleiseen tietoverkkoon.<br>Sopimusvaiheessa tulisi huomioida myös Suomen ulkopuolisten yhteyksien vikasietoisuus. |
| **Lainsäädäntö** | TiHL 13 § 1, 2 ja 4 mom, 15 § |
| **Viitteet** | HAL-16.1, |
| **Muita lisätietoja** | Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11 |
| **Tunniste** | **VAR-07, L:, E:, S:Tärkeä, TS:** |
| **Nimi** | **Tietoteknisten ympäristöjen varmentaminen** |
| **Vaatimus** | Tietoteknisissä ympäristöissä ja niihin liittyvissä sopimuksissa on huomioitu toiminnan kannalta tärkeiden palveluiden saatavuus häiriötilanteissa. |

| | |
|---|---|
| **Toteutusesimerkki** | Tärkeiden palvelujen tietotekniset ympäristöt varmennetaan esimerkiksi kahdentamalla siten, että yksittäisten komponenttien vikaantumiset eivät aiheuta toiminnan edellyttämää palvelutasoa pidempiä käyttökatkoja..<br>Tietotekniset ympäristöt voidaan varmentaa varavoimalla tai varavoimaliitännöillä siten, että sähkönjakelu voidaan käynnistää riittävän nopeasti ja ylläpitää sitä riittävän ajan suhteessa toiminnan vaatimuksiin. |
| **Lainsäädäntö** | TiHL 13 § 1, 2 ja 4 mom, 15 § |
| **Viitteet** | HAL-16.1, |
| **Muita lisätietoja** | Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 11 |
| **Tunniste** | **VAR-08, L:, E:, S:Kriittinen, TS:** |
| **Nimi** | **Vikasietoisuus** |
| **Vaatimus** | ICT-infrastruktuuri sekä olennaiset tietojärjestelmät on toteutettu riittävän vikasietoisiksi ja käyttövarmoiksi riskiarvioinnin perusteella. |
| **Yleiskuvaus** | Tietojärjestelmien häiriöihin on varauduttu nopean palautumisen varmistamiseksi. Palautumisessa hyödynnetään mekanismeja, joiden tavoitteena on reaaliaikainen tai lähes reaaliaikainen viansietokyky kriittisten järjestelmien saatavuuden ylläpitämiseksi. |
| **Toteutusesimerkki** | Kriittisten palvelujen verkko-, palvelin- ja laiteympäristöt varmennetaan esimerkiksi kahdentamalla.<br>Organisaatiossa otetaan järjestelmistä varmistusten lisäksi suojakopioita, joita säilytetään vähintään eri palotilassa kun varsinaisia tietoja.<br>Tietoaineistot on riskiarviointiin perustuen hajautettu maantieteellisesti vähintään kahteen eri paikkaan ja riittävän etäälle toisistaan Suomen rajojen sisäpuolella.<br>Julkisen hallinnon kriittisimmät palvelut ja niiden tiedonsiirto toteutetaan mahdollisuuksien mukaan turvallisuusverkon vaatimusten mukaisesti. |
| **Lainsäädäntö** | TiHL 13 § 1 ja 2 mom, 15 § |
| **Muita lisätietoja** | Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6 |
| **Tunniste** | **VAR-08.1, L:, E:, S:Kriittinen, TS:** |
| **Nimi** | **Vikasietoisuus - riippuvuudet** |
| **Vaatimus** | Palvelujen riippuvuus muista palveluista ja toisista toimijoista on otettu huomioon koko tietojenkäsittely-ympäristön ja sen vikasietoisuuden suunnittelussa. |
| **Toteutusesimerkki** | Organisaatio on tunnistanut kriittiset palvelut sekä niiden koko palveluketjun.<br>Koko palveluketju on toteutettu hyödyntäen riittävän vikasietoisia palveluita.<br>Vikasietoisuuden toteutuksessa hyödynnetään vikasietoisia alustaratkaisuja kuten esimerkiksi turvallisuusverkkoa. |
| **Lainsäädäntö** | TiHL 13 § 1 ja 2 mom, 15 § |
| **Muita lisätietoja** | Yhteiskunnan turvallisuusstrategia 2017 |
| **Tunniste** | **VAR-09, L:, E:, S:Tärkeä, TS:** |
| **Nimi** | **Tietojärjestelmien toipumissuunnitelmat** |
| **Vaatimus** | Tietojärjestelmien toipumissuunnitelmien tulee olla laadittu, otettu käyttöön ja yhteensovitettu keskenään. |
| **Yleiskuvaus** | Toipumissuunnitelmat on määritetty organisaation toiminnan kannalta tärkeiden tietojärjestelmien häiriötilanteista palautumiseen. |

| | |
|---|---|
| **Toteutusesimerkki** | ICT-palveluiden tarvitsemat minimitasot voidaan määritellä palvelusta laaditussa SLA-sopimuksessa sekä toipumissuunnitelmassa. Minimitasot voidaan asettaa aikavaatimuksina, laitteistoalustana tai tietoliikennekapasiteettina, joka vähintään tarvitaan.<br><br>Toipumissuunnitelmien olemassaolosta vastaa aina palvelun tilaaja. Ulkoistetussa palvelussa järjestelmäkohtaisten toipumissuunnitelmien valmistelusta vastaa palveluntarjoaja. Tilaaja varmistaa, että palveluntarjoaja on testaa toipumissuunnitelmia säännöllisesti. |
| **Lainsäädäntö** | TiHL 4 § 2 mom 2 k, 13 § 1 ja 2 mom, 15 § 1 mom |
| **Viitteet** | VAR-02, |

VNK TÄYTTÄÄ, MINISTERIÖN JULKAISUSARJAN NIMI JA JULKAISUN VUOSI : SARJANUMERO.