Kuvaus järjestelmän vaatimustenmukaisuuden nykytilasta

Tilaajaorganisaation itsearviointi

# Johdanto

Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit on kuvattu tilaajaorganisaation näkökulmasta Traficomin verkkosivuilta löytyvässä ohjeessa[[1]](#footnote-1). Osana näitä prosesseja tilaajaorganisaatiolta edellytetään kuvausta siitä, kuinka tarkastettavassa kohteessa on toteutettu arviointikriteeristössä kuvatut vaatimukset.

# Täyttöohje

Kuvaus pyydetään täyttämään tähän lomakepohjaan. Kuvauksen tulee olla sellaisella tarkkuudella, että sen avulla pystytään suunnittelemaan järjestelmän tarkastuskokonaisuudet ja räätälöimään tarkastuksessa käytetyt työkalut tarkastuskohteen mukaisesti. Kuvauksessa viitatut aineistot pyydetään toimittamaan liitteinä. Soveltuvia aineistoja voivat olla esimerkiksi organisaation turvallisuusjohtamista ohjaavat käytännöt, järjestelmän verkkokuvat, sekä kuvaukset järjestelmän ylläpitokäytännöistä.

Kuvaus [tarkastuskohteen nimi]

vaatimustenmukaisuuden nykytilasta

Tilaajaorganisaation itsearviointi

# Tarkastuksen kohde

|  |  |
| --- | --- |
| **Järjestelmän nimi:** |  |
| **Turvallisuusluokka:** |  |
| **Vaatimusmäärittely:** |  |

# Versiohistoria

|  |  |  |
| --- | --- | --- |
| **Päivämäärä** | **Muutokset** | **Tekijä** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Osa-alue T: Turvallisuusjohtaminen

|  |  |
| --- | --- |
| **T-01 - Hallinnollinen tietoturvallisuus - Johdon tuki, ohjaus ja vastuu - Turvallisuusperiaatteet** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Organisaation johto vastaa, että  a) organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan, | [Tähän kuvataan kuinka vaatimus on täytetty / jätetty täyttämättä arviointikohteessa.] |
| b) turvallisuusperiaatteet ovat turvallisuusluokiteltujen tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset, | [Tähän kuvataan kuinka vaatimus on täytetty / jätetty täyttämättä arviointikohteessa.] |
| c) turvallisuusperiaatteet ohjaavat tietoturvallisuustoimenpiteitä. | [Tähän kuvataan kuinka vaatimus on täytetty / jätetty täyttämättä arviointikohteessa.] |
| d) organisaatiossa on järjestetty riittävä valvonta turvallisuusluokiteltujen tietojen tiedonhallintaan liittyvien velvoitteiden ja ohjeiden noudattamisesta. | [Tähän kuvataan kuinka vaatimus on täytetty / jätetty täyttämättä arviointikohteessa.] |
| **Aineistot** | [Tähän listataan viitatut aineistot ja vastaavat auditointinäyttönä käytetyt tiedot.] |

|  |  |
| --- | --- |
| **T-02 - Hallinnollinen tietoturvallisuus - Turvallisuustyön tehtävien ja vastuiden määrittäminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Organisaatio on määritellyt turvallisuuden hoitamisen tehtävät ja vastuut. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-03 - Hallinnollinen tietoturvallisuus - Tietoturvallisuusriskien hallinta** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Organisaatio on arvioinut olennaiset turvallisuusluokiteltuihin tietoihin kohdistuvat riskit ja mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-04 - Hallinnollinen tietoturvallisuus - Turvallisuusohjeistus** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Organisaatiossa on ajantasaiset ohjeet turvallisuusluokiteltujen tietojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta sekä tietoturvallisuustoimenpiteistä. Ohjeet kattavat turvallisuusluokiteltaviin tietoihin liittyvät prosessit ja käsittely-ympäristöt tietojen koko elinkaaren ajalta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-05 - Hallinnollinen tietoturvallisuus - Turvallisuustyön resurssit** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Organisaatiolla on käytössään riittävä asiantuntemus turvallisuusperiaatteiden varmistamiseksi. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-06 - Hallinnollinen tietoturvallisuus - Toimintahäiriöt ja poikkeustilanteet** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Organisaatiolla on määritetty ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta pienennettäisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset turvallisuusluokiteltujen tietojen käsittelyyn ja säilyttämiseen.  a) Organisaatio on huomioinut turvallisuusluokiteltujen tietojen suojaamisen hätä- tai häiriötilanteissa. |  |
| b) Suojaustoimenpiteet ovat riittävät estämään luvattoman pääsyn turvallisuusluokiteltuihin tietoihin ja tietojen ilmitulon sekä turvaamaan niiden eheyden ja käytettävyyden. |  |
| c) Turvallisuusluokitellut tiedot on suojattu teknisiltä ja fyysisiltä vahingoilta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-07 - Hallinnollinen tietoturvallisuus - Turvallisuuspoikkeamien hallinta** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Tapahtuneesta tai epäillystä kansainvälisen turvallisuusluokitellun tiedon vaarantaneesta poikkeamasta on ilmoitettava välittömästi toimivaltaiselle turvallisuusviranomaiselle. |  |
| 2. Organisaatiolla on menettelytavat tietoturvallisuuspoikkeamien asianmukaiseen käsittelyyn.  a) Organisaatiolla on ohjeistus ja menettely, jolla tapahtuneesta tai epäillystä turvallisuusluokitellun tiedon vaarantaneesta poikkeamasta saadaan välittömästi tieto organisaation sisällä.  b) Organisaatio on määrittänyt, miten ja kenelle poikkeamista tai niiden epäilyistä tulee ilmoittaa.  c) Organisaatio on selvittänyt millaiset tietoturvallisuuspoikkeamat edellyttävät viranomaisyhteydenottoa. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-08 - Hallinnollinen tietoturvallisuus - Tietojen luokittelu** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Tätä vaatimusta sovelletaan vain viranomaisen tietojenhallintaan:  1. Tiedot on luokiteltu lakisääteisten vaatimusten perusteella:  a) Viranomaisella on tietojen luokitteluun ohje.  b) Tietosisällöltään salassa pidettävät turvallisuusluokiteltavat aineistot ja asiakirjat (ml. luonnokset) varustetaan turvallisuusluokkaa kuvaavalla merkinnällä.  c) Asiakirja merkitään asiakirjan osien (esim. liitteet) ylintä turvallisuusluokkaa vastaavalla merkinnällä.  d) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi asiakirjasta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-09 - Henkilöstöturvallisuus - Työsuhteen aikaiset muutokset turvallisuusluokiteltujen tietojen käsittelyssä** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Työsuhteen aikaiset muutokset turvallisuusluokiteltujen tietojen käsittelyssä on huomioitu työsuhteen elinkaaren eri vaiheissa. Erityisesti tulee huomioida toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja työsuhteen päättyessä. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-10 - Henkilöstöturvallisuus - Henkilöstön luotettavuuden arviointi** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Turvallisuusluokiteltuja tietoja käsittelevien henkilöiden luotettavuus selvitetään tarvittaessa hakemalla henkilöistä asianmukaisen laajuinen henkilöturvallisuusselvitys. |  |
| 2. Kansainvälisten tietoturvallisuusvelvoitteiden sitä edellyttäessä, henkilölle voidaan myöntää pääsy kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tai sitä korkeamman turvallisuusluokan kansainvälisiin tietoihin vasta sen jälkeen, kun hänelle on myönnetty asianmukaisen tason henkilöturvallisuusselvitystodistus (PSC). |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-11 - Henkilöstöturvallisuus - Salassapito- ja vaitiolovelvollisuus** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Turvallisuusluokiteltua tietoa käsitteleville henkilöille on selvitetty tietojen suojaamista koskevat tietoturvallisuusperiaatteet ja -toimenpiteet ja henkilö on antanut vakuutuksen tietojen suojaamista koskevasta vastuustaan. Salassapito- tai vaitiolositoumusmenettely on käytössä, kun turvallisuusluokiteltua tietoa käsittelee henkilö, jota virkavastuu ei koske. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-12 - Henkilöstöturvallisuus - Turvallisuuskoulutus** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Johdon on huolehdittava siitä, että organisaatiossa on tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja organisaation lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä tietojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja organisaation ohjeista (vrt. T-04). |  |
| 2. Turvallisuusluokiteltuun tietoon kohdistuvat ja henkilön tehtävien kannalta keskeiset uhat sekä ajantasaiset ohjeet (vrt. T-04) on koulutettu henkilöstölle. |  |
| 3. Turvallisuusluokiteltavien tietojen käsittelyä koskeva koulutus on säännöllistä ja koulutuksiin osallistuneista pidetään kirjaa. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **T-13 - Henkilöstöturvallisuus - Tiedonsaantitarve ja käsittelyoikeudet** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Organisaation on pidettävä ajantasaista luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan II tai III tietoja. |  |
| 2. Luettelossa on mainittava henkilön tehtävä, johon turvallisuusluokitellun tiedon käsittelytarve perustuu. |  |
| 3. Pääsy turvallisuusluokiteltuun tietoon voidaan myöntää vasta, kun henkilön työtehtävistä johtuva tiedonsaantitarve on selvitetty. |  |
| 4. Organisaatiolla on menettely, jolla varmistetaan turvallisuusluokiteltujen tietojen käsittelyoikeuksien poistaminen tiedonsaantitarpeen päätyttyä. |  |
| **Aineistot** |  |

# Osa-alue F: Fyysinen turvallisuus

|  |  |
| --- | --- |
| **F-01 - Yleiset vaatimukset - Fyysisten turvatoimien tavoite** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Fyysisten turvatoimien tavoitteena on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin:  a) varmistamalla, että turvallisuusluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti;  b) mahdollistamalla henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin tiedonsaantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella;  c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet; ja  d) estämällä oikeudetta tapahtuva tunkeutuminen tai viivyttämällä sitä. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-02 - Yleiset vaatimukset - Fyysisten turvatoimien riskien arviointi** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Tietojenkäsittelyyn kohdistuvat olennaiset riskit on selvitettävä ja fyysiset turvatoimet (F-03) on mitoitettava riskien arvioinnin mukaisesti. |  |
| 2. Riskien arvioinnissa on otettava huomioon kaikki asiaan kuuluvat tekijät, erityisesti seuraavat:  a) Turvallisuusluokiteltujen tietojen turvallisuusluokka ja salassapitoperuste;  b) Turvallisuusluokiteltujen tietojen käsittely- ja säilytystapa sekä määrä ottaen huomioon, että tietojen suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista;  c) Turvallisuusluokiteltujen tietojen käsittely- ja säilytysaika;  d) Turvallisuusluokiteltujen tietojen käsittely- ja säilytyspaikan (turvallisuusalue) ympäristö: rakennuksen ympäristö, sijoittuminen rakennuksessa, tilassa tai sen osassa;  e) Hälytystilanteisiin liittyvä vasteaika;  f) Ulkoistetut toiminnot, kuten huolto-, siivous-, kiinteistö- ja turvallisuuspalvelut;  g) Tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu uhka tiedoille. |  |
| 3. Mikäli kyseessä on kansainvälinen turvallisuusluokiteltu tieto, fyysisten turvatoimien valinnan ja riskien arvioinnin on perustuttava Suojelupoliisin tai Pääesikunnan tekemään uhka-arvioon. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-03 - Yleiset vaatimukset - Fyysisten turvatoimien valinta (monitasoinen suojaus)** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. 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. |  |
| 2. Monitasoista suojausperiaatetta soveltaen on arvioitava ja hyväksyttävä asianmukainen ja riskiarvioon nähden riittävä turvatoimien yhdistelmä, joka muodostuu hallinnollisista, toiminnallisista ja fyysisistä keinoista, kuten:  a) rakenteelliset esteet: fyysinen este, jolla turvallisuusalueet ja sitä ympäröivät tilat rajataan ja luvatonta tunkeutumista vaikeutetaan ja hidastetaan; |  |
| b) kulunvalvonta: kulunvalvonnalla rajataan pääsyä turvallisuusalueille ja sitä ympäröiviin tiloihin. Tavoitteena havaita luvattomat pääsy-yritykset, estää asiattomien henkilöiden pääsy ja valvoa alueella liikkuvia. Kulunvalvonta voi kohdistua alueeseen, alueen yhteen tai useampaan rakennukseen tai rakennuksen alueisiin tai huoneisiin. Valvonnassa voidaan hyödyntää mekaanisia, sähköisiä tai sähkömekaanisia teknisiä järjestelmiä tai muunlaisia fyysisiä keinoja. Myös vartiointihenkilöstö, vastaanottovirkailija tai oma henkilöstö voi osallistua valvontaan. |  |
| c) tunkeutumisen ilmaisujärjestelmä: rakenteellisen esteen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisen ilmaisujärjestelmää (murtohälytysjärjestelmä). Järjestelmää voidaan käyttää myös vartiointihenkilöstön tekemän valvonnan asemasta tai tueksi. |  |
| d) vartiointihenkilöstö: koulutettua, valvottua, varustettua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä vartiointihenkilöstöä voidaan käyttää muun muassa kulunvalvonnan tukena sekä turvallisuusalueelle tai sitä ympäröivien tilojen tunkeutumista suunnittelevien henkilöiden aikeiden havaitsemisessa ja toimien estämisessä. |  |
| e) kameravalvonta: kameravalvontaa voidaan käyttää turvallisuusalueella tai sen ympärillä erityisesti laittoman tiedustelun ennalta ehkäisemisessä sekä ilmenevien poikkeamien ennalta ehkäisemisessä, hälytysten todentamisessa ja tapahtuneiden poikkeamien selvittämisessä. Vartiointihenkilöstö voi käyttää kameravalvontaa reaaliaikaisena, aktiivisena kuvan tarkkailuna tai jälkikäteen passiivisena kuvamateriaalin analysointina. |  |
| f) turvallisuutta ylläpitävät menettelyt: vastuiden ja tehtävien määrittäminen, erilaiset prosessit ja toimintamallit, kuten pääsyoikeuksien ja avainten hallinta, henkilöstön ohjeistus ja perehdyttäminen sekä järjestelmien huolto- ja ylläpitotoimet. |  |
| g) valaistus: mahdollinen tunkeutuja voidaan havaita valaistuksen avulla ja vartiointihenkilöstö voi valvoa aluetta tehokkaasti, joko suoraan tai kameravalvontajärjestelmää hyödyntämällä. |  |
| 3. Laitteet on tarkastettava ja huollettava säännöllisin väliajoin. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-04 - Yleiset vaatimukset - Tiedon käsittely ja säilytys** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Kansallisia turvallisuusluokiteltuja tietoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta. |  |
| 2. Kansainvälisiä turvallisuusluokiteltuja tietoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-05.1 - Turvallisuusalueiden vaatimukset - Hallinnollinen alue - Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet)** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Alueella on oltava selkeästi määritelty näkyvä raja. Aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-05.2 - Turvallisuusalueiden vaatimukset - Hallinnollinen alue - Pääsyoikeuksien myöntäminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Ainoastaan asianmukaisesti valtuutetuilla henkilöillä on itsenäinen pääsy alueelle. Organisaation on määriteltävä alueen pääsyoikeuksien ja avainhallinnan menettelyt ja roolit. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-05.3 - Turvallisuusalueiden vaatimukset - Hallinnollinen alue - Vierailijat** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Muilla kuin organisaation asianmukaisesti valtuuttamilla henkilöillä (vierailijoilla) on aina oltava saattaja. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-05.4 - Turvallisuusalueiden vaatimukset - Hallinnollinen alue - Äänieristys** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Alueen äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan turvallisuusluokitelluista tiedoista, joihin kaikilla ei ole tiedonsaantitarvetta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-05.5 - Turvallisuusalueiden vaatimukset - Hallinnollinen alue - Tunkeutumisen ilmaisujärjestelmät** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Ei vaatimuksia. Tarvittaessa tunkeutumisen ilmaisujärjestelmää voidaan käyttää täydentävänä monitasoisen suojauksen riskienhallintakeinona tai F-05.8 2a-kohdan toteutustapana. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-05.6 - Turvallisuusalueiden vaatimukset - Hallinnollinen alue - Salaa katselun estäminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu mukaan lukien, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-05.7 - Turvallisuusalueiden vaatimukset - Hallinnollinen alue - Tila- ja laitetarkastukset (ainoastaan TL II / EU-S)** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Organisaation on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella hallinnollisella alueella, jossa käsitellään turvallisuusluokan II tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. |  |
| 2. Myös alue on tarvittaessa tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin. Tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-05.8 - Turvallisuusalueiden vaatimukset - Hallinnollinen alue - Tiedon käsittely ja säilyttäminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Alueella voi säilyttää turvallisuusluokan IV tietoa. Tiedot tulee säilyttää soveltuvassa lukitussa toimistokalusteessa. Tietoja sisältävä päätelaite tulee säilyttää soveltuvassa lukitussa toimistokalusteessa, mikäli mahdollista. |  |
| 2. Alueella voi säilyttää kansallista turvallisuusluokan III tietoa kyseisen turvallisuusluokan vaatimukset täyttävässä päätelaitteessa, mikäli päätelaitetta säilytetään: a) valvotussa tilassa tai b) soveltuvassa lukitussa toimistokalusteessa turvapussissa tai vastaavalla tavalla. Mahdollinen tilan valvonta tulee toteuttaa F-05.5-vaatimuksen mukaisesti. Poiketen kansallisen turvallisuusluokitellun tiedon säilyttämissäännöistä, kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tietoa ei voi säilyttää hallinnollisella alueella. |  |
| 3. Soveltuvien lukittujen toimistokalusteiden avaimet tai pääsykoodit ovat sellaisten henkilöiden hallussa, joilla on tiedonsaantitarve säilytysyksikössä säilytettävään tietoon. Kyseisten henkilöiden on osattava numeroyhdistelmät ulkoa. Turvallisuusluokiteltuja tietoja sisältävien säilytysyksiköiden numeroyhdistelmät on vaihdettava:  - uuden turvallisen säilytyspaikan vastaanoton yhteydessä  - aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos.  - aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen.  - kun jokin lukoista on huollettu tai korjattu. |  |
| 4. Alueella voi käsitellä turvallisuusluokkien IV-II tietoa, jos pääsy tietoihin on suojattu sivullisilta. Päätelaitteessa olevan turvallisuusluokitellun tiedon käsittelyssä tulee lisäksi huolehtia, että päätelaite ja tietoliikennejärjestelyt täyttävät niihin kohdistuvat vaatimukset. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.1 - Turvallisuusalueiden vaatimukset - Turva-alue - Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet)** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Alueella on oltava selkeästi määritelty näkyvä raja. |  |
| 2. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen säilytyksen edellyttämä turvallisuustaso. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.2 - Turvallisuusalueiden vaatimukset - Turva-alue - Kulunvalvonta** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Alueen rajalla tulee valvoa kaikkea kulkua sisään ja ulos kulkulupien avulla tai tunnistamalla henkilöt henkilökohtaisesti. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.3 - Turvallisuusalueiden vaatimukset - Turva-alue -Pääsyoikeuksien myöntäminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Itsenäinen pääsyoikeus alueelle voidaan myöntää vain organisaation asianmukaisesti valtuuttamalle henkilölle, jonka luotettavuus on varmistettu ja jolla on erityinen lupa tulla alueelle (need to access the area). |  |
| 2. Organisaation on määriteltävä alueen pääsyoikeuksien ja avainten hallinnan menettelyt ja roolit. |  |
| 3. Mikäli turva-alueella käsitellään ja säilytetään kansainvälistä turvallisuusluokiteltua tietoa, itsenäinen pääsyoikeus alueelle voidaan myöntää vain organisaation asianmukaisesti valtuuttamalle henkilölle, jolla on voimassaoleva kansainvälinen henkilöturvallisuusselvitys (PSC) ja erityinen lupa tulla alueelle tiedonsaantitarpeensa perusteella (need-to-know). |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.4 - Turvallisuusalueiden vaatimukset - Turva-alue - Vierailijat** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Muilla kuin niillä henkilöillä, joille on myönnetty itsenäinen pääsyoikeus tilaan (vierailijoilla) on aina oltava saattaja. |  |
| 2. Jos turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin, sovelletaan lisäksi seuraavia vaatimuksia:  - alueella tavanomaisesti säilytettyjen tietojen korkein turvallisuusluokka on ilmoitettava selkeästi;  - 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. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.5 - Turvallisuusalueiden vaatimukset - Turva-alue - Turvallisuusohjeet** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Kullekin turva-alueelle on laadittava turvallisuusmenettelyt, joissa on määräykset seuraavista asioista:  a) Tiedon säilyttäminen ja käsitteleminen alueella (F-06.10): turvallisuusluokka tiedoille, joita alueella voidaan käsitellä ja säilyttää.  b) sovellettavat valvonta- ja suojatoimenpiteet (muun muassa F-06.7 – F-06.9).  c) Pääsyoikeuksien myöntäminen alueelle (F-06.3): henkilöt, joilla on pääsy alueelle ilman saattajaa erityisen luvan ja luotettavuuden varmistamisen perusteella  d) Vierailijat (F-06.4): tarvittaessa menettelyt saattajien käyttämiseksi tai turvallisuusluokiteltujen tietojen suojaamiseksi silloin, kun muille henkilöille myönnetään pääsy alueelle  e) muut asiaan kuuluvat toimenpiteet ja menettelyt "aja. Aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.6 - Turvallisuusalueiden vaatimukset - Turva-alue - Äänieristys** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Alueen äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan turvallisuusluokitelluista tiedoista, joihin kaikilla ei ole tiedonsaantitarvetta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.7 - Turvallisuusalueiden vaatimukset - Turva-alue - Tunkeutumisen ilmaisujärjestelmät** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 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). |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.8 - Turvallisuusalueiden vaatimukset - Turva-alue - Salaa katselun estäminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu mukaan lukien, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.9 - Turvallisuusalueiden vaatimukset - Turva-alue - Tila- ja laitetarkastukset (ainoastaan TL II / EU-S)** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Organisaation on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella turva-alueella, jossa käsitellään turvallisuusluokan II tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. |  |
| 2. Myös alue on tarvittaessa tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-06.10 - Turvallisuusalueiden vaatimukset - Turva-alue - Tiedon käsittely ja säilyttäminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Alueella voi säilyttää riskien arviointiin ja fyysisten turvatoimien valintaan perusten kaikkiin turvallisuusluokkiin kuuluvia tietoja. |  |
| 2. Turvallisuusluokan III ja sitä korkeamman turvallisuusluokan tietoja tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa. Myös päätelaite tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa, mikäli mahdollista. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen säilytyksen edellyttämä turvallisuustaso. |  |
| 3. Säilytysyksikön avaimet tai pääsykoodit ovat sellaisten henkilöiden hallussa, joilla on tiedonsaantitarve säilytysyksikössä säilytettävään tietoon. Kyseisten henkilöiden on osattava numeroyhdistelmät ulkoa. Turvallisuusluokiteltuja tietoja sisältävien säilytysyksiköiden numeroyhdistelmät on vaihdettava:  - uuden turvallisen säilytyspaikan vastaanoton yhteydessä  - aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos.  - aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen.  - kun jokin lukoista on huollettu tai korjattu. |  |
| 4. Alueella voi käsitellä kaikkiin turvallisuusluokkiin kuuluvia tietoja, jos pääsy turvallisuusluokiteltuihin tietoihin estetään sivullisilta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-07 - Teknisesti suojattu turva-alue** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Teknisesti suojattuihin turva-alueisiin sovelletaan turva-alueen vähimmäisvaatimusten (F-06) lisäksi seuraavia vaatimuksia:  a) alueilla on oltava tunkeutumisen ilmaisujärjestelmä (murtohälytysjärjestelmä), alueet on pidettävä lukittuina silloin, kun niitä ei käytetä, ja niitä on vartioitava silloin, kun ne ovat käytössä.  b) kaikkien henkilöiden kulkua ja materiaalien tuontia alueelle on valvottava;  c) alueet on tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin Suojelupoliisin tai Pääesikunnan vaatimusten mukaisesti. Tällaiset tarkastukset on suoritettava myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta; ja  d) Alueella saa olla ainoastaan kyseiselle alueelle hyväksyttyjä tietoliikenneyhteyksiä, puhelimia, muita viestintävälineitä tai elektronisia laitteita. |  |
| 2. Kaikki viestintä-, sähkö- tai elektroniset laitteet on tarkastettava, ennen kuin niitä käytetään alueilla, joilla pidetään EU SECRET / NATO SECRET -turvallisuusluokan tietoihin liittyviä kokouksia tai tehdään tällaisiin tietoihin liittyvää työtä, silloin kun EU:n tai Naton turvallisuusluokiteltuihin tietoihin kohdistuva uhka arvioidaan korkeaksi, ja näin varmistettava, ettei niillä voi tahattomasti eikä laittomasti välittää ymmärrettävässä muodossa olevia tietoja turva-alueen rajojen ulkopuolelle. |  |
| 3. Suojelupoliisi tai Pääesikunta päättää teknisesti suojattuun turva-alueeseen liittyvästä uhka-arvioinnista, riskien hallintatoimenpiteistä ja mahdollisen tilapäisesti perustettavan teknisesti suojatun turva-alueen turvallisuusjärjestelyjen hyväksynnästä tapauskohtaisesti. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-08.1 - Tietoaineistoturvallisuus - Tietojen välitys postilla ja kuriirilla** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Turvallisuusluokitellut tiedot tulee kuljettaa tietojen riittävän suojaamisen huomioivia, organisaation ohjeita noudattaen. |  |
| 2. Turvallisuusluokitellut tiedot on pakattava niin, että ne on suojattu luvattomalta ilmitulolta. |  |
| 3. Turvallisuusluokiteltuja tietoja saa kuljettaa turvallisuusalueiden ulkopuolelle suojaamalla sähköiset tietovälineet viranomaisen hyväksymällä salauksella (ks. I-12). |  |
| 4. Turvallisuusluokan IV salaamattomia tietoja voidaan kuljettaa postipalvelujen välityksellä. |  |
| 5. 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. |  |
| 6. Kansainvälisiä turvallisuusluokiteltuja tietoja koskevat vaatimukset on varmistettava tapauskohtaisesti Suojelupoliisilta tai Pääesikunnasta. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-08.2 - Tietoaineistoturvallisuus - Turvallisuusluokiteltujen tietojen kopioiminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Kopioihin ja käännöksiin sovelletaan alkuperäistä tietoa koskevia turvatoimia. |  |

|  |
| --- |
| *Turvallisuusluokka II* |

|  |  |
| --- | --- |
| Kohdan 1 lisäksi  2. Turvallisuusluokan II tietojen kopiot ja niiden käsittelijät on luetteloitava. |  |
| 3. Turvallisuusluokan II tietojen kopiointia varten on hankittava tiedon laatineen viranomaisen lupa. |  |
| 4. Kansainvälisiä turvallisuusluokiteltuja tietoja saa kopioida ja kääntää, mikäli tiedon luovuttaja ei ole sitä kieltänyt." |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-08.3 - Tietoaineistoturvallisuus - Turvallisuusluokiteltujen tietojen kirjaaminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Kansainvälisiä turvallisuusluokiteltavia tietoja käsittelevien organisaatioiden on määriteltävä vastaava kirjaamo. Kirjaamo on määritettävä turva-alueeksi. |  |
| 2. Kansallisten turvallisuusluokkien II-III ja kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tai sitä korkeamman luokan tiedon vastaanottaminen ja lähettäminen tulee kirjata. |  |
| 3. Turvallisuusluokan III tietojen ja niitä korkeamman tason tietojen käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi). |  |
| 4. Kansainvälisten turvallisuusluokan III (CONFIDENTIAL) tieto ja sitä korkeamman tason tieto tulee kirjata sille tarkoitetussa kirjaamossa. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **F-08.4 - Tietoaineistoturvallisuus - Ei-sähköisten tietojen tuhoaminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |

|  |
| --- |
| *Turvallisuusluokka IV* |

|  |  |
| --- | --- |
| 1. Ei-sähköisten turvallisuusluokiteltujen tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. Sähköisessä muodossa olevien tietojen osalta ks. I-21. |  |

|  |
| --- |
| *Turvallisuusluokka III* |

|  |  |
| --- | --- |
| Kohdan 1 lisäksi  2. Kansainvälisten turvallisuusluokan III (CONFIDENTIAL) tietojen osalta, kirjaajan on allekirjoitettava tuhoamistodistus, joka tallennetaan kirjaamoon/rekisteröintipisteeseen. Kirjaustiedot on päivitettävä vastaavasti. Kirjaamon/rekisteröintipisteen on säilytettävä tuhoamistodistukset vähintään viiden vuoden ajan. (vrt. F-08.3). |  |

|  |
| --- |
| *Turvallisuusluokka II* |

|  |  |
| --- | --- |
| Kohtien 1-2 lisäksi  3. Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle. |  |
| 4. Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö. |  |
| 5. Kansainvälisten turvallisuusluokan II (SECRET) tietojen tuhoaminen on suoritettava todistajan läsnä ollessa. Todistajalla on oltava vähintään tuhottavan tiedon turvallisuusluokkaa vastaava turvallisuusselvitys. |  |
| **Aineistot** |  |

# Osa-alue I: Tekninen tietoturvallisuus

|  |  |
| --- | --- |
| **I-01 - Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen - Verkon rakenteellinen turvallisuus** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| *Turvallisuusluokka IV* | |
| 1) Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä. |  |
| 2) Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä. |  |
| 3) Hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne salataan viranomaisen ko. turvallisuusluokalle hyväksymällä salausratkaisulla (vrt. I-12 ja I-15). |  |
| *Turvallisuusluokat III-II* | |
| Kohtien 1 ja 3 lisäksi:  4) Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää toimivaltaisen viranomaisen ko. turvallisuustasolle hyväksymän yhdyskäytäväratkaisun käyttöä. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-02 - Vähimpien oikeuksien periaate - Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöt ko. turvallisuusluokan sisällä** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-03 - Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan - Suodatus- ja valvontajärjestelmien hallinnointi** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan.  a) Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen, poistaminen ja valvonta (vrt. I-16) on vastuutettu ja organisoitu. |  |
| b) Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia. |  |
| c) Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-04 - Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen - Hallintayhteydet** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Hallintayhteydet on rajattu turvallisuusluokittain, ellei käytössä ole toimivaltaisen viranomaisen ko. turvallisuusluokille hyväksymää yhdyskäytäväratkaisua. |  |
| 2. Hallintaliikenteen sisältäessä turvallisuusluokiteltua tietoa ja kulkiessa matalamman turvallisuusluokan ympäristön kautta, turvallisuusluokitellut tiedot on salattu toimivaltaisen viranomaisen hyväksymällä salaustuotteella. |  |
| 3. Hallintaliikenteen kulkiessa ko. turvallisuusluokan sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen |  |
| 4) Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-05 - Suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - Langaton tiedonsiirto** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Langattomassa tiedonsiirrossa tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä salausratkaisulla (vrt. I-12). |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-06 - Vähimpien oikeuksien periaate - Pääsyoikeuksien hallinnointi** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Tietojärjestelmien käyttöoikeudet on määritelty. |  |
| 2. Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käsittelyoikeuksista (vrt. T-13) on varmistuttu |  |
| 3. Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä. |  |
| 4. Käyttöoikeudet on pidettävä ajantasaisina. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-07 - Monitasoinen suojaaminen - Tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun alueen sisällä** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-08 - Vähimmäistoimintojen ja vähimpien oikeuksien periaate - Järjestelmäkovennus** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut. |  |
| 2. Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. |  |
| 3. Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi. |  |
| 4. Kovennusten voimassaolosta ja vaikuttavuudesta huolehditaan koko tietojärjestelmän elinkaaren ajan. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-09 - Monitasoinen suojaaminen - Haittaohjelmasuojaus** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-10 - Monitasoinen suojaaminen - Turvallisuuteen liittyvien tapahtuminen jäljitettävyys** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen. |  |
| 2. Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. |  |
| 3. Turvallisuusluokan II–III tiedon käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi). |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-11 - Monitasoinen suojaaminen - Poikkeamien havainnointikyky ja toipuminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 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. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-12 - Tietoturvallisuustuotteiden arviointi ja hyväksyntä - Salausratkaisut** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Toimivaltainen viranomainen on hyväksynyt käytetyt salausratkaisut (ja -tuotteet) ko. turvallisuusluokalle ko. käyttöympäristössä turvallisuusluokiteltujen tietojen luvattoman paljastumisen ja muuntelun estämiseksi. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-13 - Monitasoinen suojaaminen koko elinkaaren ajan - Ohjelmistojen suojaaminen verkkohyökkäyksiltä** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Tietojenkäsittely-ympäristön turvallisuus, myös niiden tekniset ja muut kuin tekniset turvatoimet, testataan hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että ne on moitteettomasti toteutettu, integroitu ja konfiguroitu. |  |
| 2. Tietoturvallisuutta vaarantavia verkkohyökkäyksiä vastaan suojaudutaan ja suojauksista sekä niiden toiminnasta huolehditaan tietojenkäsittely-ympäristön elinkaaren ajan." |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-14 - Monitasoinen suojaaminen - Hajasäteily (TEMPEST)** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Turvatoimia toteutetaan turvallisuusluokiteltuihin tietoihin liittyvässä tietojenkäsittely-ympäristössä toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymillä menetelmillä niin, että tahattomat sähkömagneettiset vuodot eivät vaaranna tietoja (TEMPEST-turvatoimet). |  |
| 2. Käsiteltäessä turvallisuusluokan III tai II tietoja sähköisesti, on pidettävä huolta, että elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi. |  |
| 3. Nämä turvatoimet on suhteutettava tiedon hyväksikäytön riskiin ja turvallisuusluokkaan . |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-15 - Turvallisuusluokiteltujen tietojen välitys fyysisesti suojattujen alueiden välillä - Tiedon sähköinen välitys** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella, tieto/tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä turvallisuusluokiteltuja tietoja. |  |
| 2. Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-16 - Turvallisuusluokitellun tiedon käsittelyyn liittyvän tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Muutoshallintamenettelyt** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| 1. Turvallisuuden varmistamista pidetään vaatimuksena koko tietojenkäsittely-ympäristön elinkaaren ajan sen alullepanosta käytöstä poistamiseen. |  |
| 2. Tietoturvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä. |  |
| 3. Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten- ja asetustenhallintaprosessia. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-17 - Turvallisuusluokiteltujen sähköisessä muodossa olevien tietojen käsittely fyysisesti suojattujen alueiden sisällä - Fyysinen turvallisuus** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| *Turvallisuusluokka IV* | |
| 1. Turvallisuusluokiteltuja tietoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta (vrt. F-04 ja I-18). |  |
| 2. Tietojen käsittely on mahdollista toimivaltaisen viranomaisen hyväksymillä turvallisuusalueilla (vrt. F-04) ja toimivaltaisen viranomaisen hyväksymillä menettelyillä turvallisuusalueiden ulkopuolella (vrt. I-18) |  |
| 3. Tietojen säilytys on mahdollista toimivaltaisen viranomaisen hyväksymillä turvallisuusalueilla (vrt. F-04) ja toimivaltaisen viranomaisen hyväksymillä menettelyillä turvallisuusalueiden ulkopuolella (vrt. I-18). |  |
| 4. Turvallisuusluokan IV tietoja sisältävät tietovarannot ja näiden tietojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle (vrt. F-04). |  |
| *Turvallisuusluokka III-II* | |
| *Kohtien 1 ja 2 lisäksi:*  5. Tietojen säilytys on mahdollista toimivaltaisen viranomaisen hyväksymillä turva-alueilla (vrt. F-04). Vrt. vain kansallisia tietoja koskeva poikkeus kohdassa 6 sekä etäkäyttö kohdassa I-18. |  |
| 6. 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 (vrt. I-12), ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle riittävästä luottamuksellisuudesta ja eheydestä on huolehdittu toimivaltaisen viranomaisen hyväksymällä menetelmällä (vrt. F-04). Vrt. etäkäyttö kohdassa I-18." |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-18 - Turvallisuusluokiteltujen tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä - Etäkäyttö ja etähallinta** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| *Turvallisuusluokka IV* | |
| 1. Käyttäjät ja päätelaitteet tunnistetaan riittävän luotettavasti. Tietojen välitys ja käsittely turvallisuusalueiden (vrt. F-04) välillä on mahdollista vain toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymien korvaavien menettelyjen mukaisesti. |  |
| 2. Turvallisuusluokiteltuja tietoja on turvallisuusalueiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta. Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan. |  |
| 3. Elleivät turvallisuusalueiden ulkopuolelle viedyt turvallisuusluokiteltua tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä, tietovälineitä ei jätetä valvomatta. |  |
| 4. Järjestelmien etäkäyttö ja -hallinta edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokan tietojen suojaamiseen hyväksymää liikenteen salausta. |  |
| 5. Päätelaitteessa olevat tiedot tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla, ja päätelaitteen ko. turvallisuusluokalle riittävästä eheydestä tulee huolehtia. |  |
| *Turvallisuusluokka III-II: Kohtien 1-5 lisäksi:* | |
| 6. Turvallisuusluokiteltuja tietoja ei avata matkalla eikä lueta julkisilla paikoilla. |  |
| 7. Järjestelmien etäkäyttö ja -hallinta rajataan toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle (vrt. F-04). Vrt. vain kansallisia tietoja koskeva poikkeus kohdassa 8. |  |
| 8. Vain kansallisten 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, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla, ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle riittävästä luottamuksellisuudesta ja eheydestä on huolehdittu toimivaltaisen viranomaisen hyväksymällä menetelmällä. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-19 - Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Ohjelmistohaavoittuvuuksien hallinta** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-20 - Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Varmuuskopiointi** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| Turvallisuusluokiteltua tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto on suojattu. |  |
| **Aineistot** |  |

|  |  |
| --- | --- |
| **I-21 - Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen** | |
| **Vaatimus** | **Kuinka tämä on toteutettu arviointikohteessa?** |
| *Turvallisuusluokka IV* | |
| 1. Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. Ei-sähköisten tietojen osalta ks. F-08.4. |  |
| *Turvallisuusluokka III:* Kohdan 1 lisäksi | |
| 2. Kansainvälisten turvallisuusluokan III (CONFIDENTIAL) tietojen osalta, kirjaajan on allekirjoitettava tuhoamistodistus, joka tallennetaan kirjaamoon/rekisteröintipisteeseen. Kirjaustiedot on päivitettävä vastaavasti. Kirjaamon/rekisteröintipisteen on säilytettävä tuhoamistodistukset vähintään viiden vuoden ajan. (vrt. F-08.3). |  |
| *Turvallisuusluokka II:* Kohtien 1-2 lisäksi | |
| 3. Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle. |  |
| 4. Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö. |  |
| 5. Kansainvälisten turvallisuusluokan II (SECRET) tietojen tuhoaminen on suoritettava todistajan läsnä ollessa. Todistajalla on oltava vähintään tuhottavan tiedon turvallisuusluokkaa vastaava turvallisuusselvitys. |  |
| **Aineistot** |  |

1. www.ncsa.fi > Asiakirjat > Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset [↑](#footnote-ref-1)