Ohje erillistyöasemien tietoturvallisuuden varmistamisesta

Muutoshistoria

Päivämäärä	Kuvaus
25.10.2023	Julkaisuversio.

Sisältö

1 Johdanto

Liikenne- ja viestintävirasto Traficomin tehtäviin kuuluvista tietojärjestelmien arvioinneista ja hyväksynnistä säädetään laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004, kv-titulaki), turvallisuusselvityslaissa (706/2014) ja laissa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista (1406/2011, arviointilaki). Laissa tietoturvallisuuden arviointilaitoksista (1405/2011, arviointilaitoslaki) säädetään arviointilaitosten ja niiden pätevyysalueiden hyväksymisestä.

Kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti esimerkiksi EU:n ja Naton turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien tulee läpikäydä hyväksyntäprosessi (akkreditointi). Traficomin myöntämää hyväksyntää on mahdollista hakea tietojärjestelmissä käsiteltävien kansainvälisten turvallisuusluokiteltujen tietojen suojaamiseen. Kansallista turvallisuusluokiteltua tietoa käsitteleviin viranomaisten tietojärjestelmiin ei kohdistu lainsäädännöstä yleistä velvoitetta tietojärjestelmän hyväksynnälle (akkreditoinnille). Viranomaisilla on kuitenkin mahdollisuus hakea Traficomin arviointia tietojärjestelmissä käsiteltävien kansallisten turvallisuusluokiteltujen tietojen suojaamisen tasosta. Arviointi- ja hyväksyntäprosesseja on kuvattu kattavammin Traficomin ohjeessa tietojärjestelmien arviointi- ja hyväksyntäprosesseista[1].

Turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien suunnittelussa tulee huomioida sekä toiminnalliset että turvallisuuteen liittyvät tarpeet. Pysyvästi tietoverkoista erotettujen erillistyöasemien käyttö on yleinen tapa toteuttaa turvallisuusluokitellun tiedon sähköinen käsittely siten, että yleiset turvallisuusluokiteltuihin tietoihin kohdistuvat riskit saadaan hallittua nopeasti ja kustannustehokkaasti.

2 Ohjeen tarkoitus

Ohjeessa kuvataan erillistyöasemien keskeiset suojaukset, jotka toteuttamalla sekä kansallisen että kansainvälisen turvallisuusluokitellun tiedon käsittelyyn liittyvät yleiset riskit saadaan pidettyä hyväksyttävällä tasolla. Erillistyöaseman suojaamisessa tulee huomioida sen koko elinkaari, toisin sanoen ajanjakso, joka alkaa erillistyöaseman käyttöönoton suunnittelusta ja kattaa muun muassa turvallisen asennuksen, käyttöönoton, käytön sekä käytöstä poiston.

> Erillistyöasemalla tarkoitetaan ohjeessa kaikista tietoverkoista pysyvästi erotettua tietokonetta sekä tarvittaessa myös erillistyöasemaan kiinteästi kytkettävää langallista hiirtä.

Ohje on tarkoitettu erillistyöasemia käyttäville viranomaisille ja yrityksille sekä niitä arvioiville tahoille. Arvioija voi olla Traficom tai pätevyysalueensa rajoissa[2] Traficomin hyväksymä tietoturvallisuuden arviointilaitos. Arvioija voi olla myös suojelupoliisi tai Pääesikunta, jos Traficom ja toinen viranomainen ovat niin nimenomaisesti sopineet kv-titulain 5 § tai turvallisuusselvityslain 9 §:n mukaisesti.

Ohje on laadittu tukemaan turvallisuusluokiteltua tietoa käsittelevien viranomaisten ja yritysten sisäistä riskienhallintatyötä. Ohje tukee myös tietojärjestelmien

[1] Liikenne- ja viestintävirasto. 2023. Liikenne- ja viestintävirasto Traficomin ohje tietojärjestelmien arviointi- ja hyväksyntäprosesseista. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-tietojarjestelmien-arviointi-ja-hyvaksyntaprosesseista.pdf.
[2] Lisätietoa: Traficomin hyväksymät tietoturvallisuuden arviointilaitokset. 2023. URL: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset.

hyväksyntäprosessin tehokasta läpikäyntiä tilanteissa, joissa kansainvälinen tietoturvallisuusvelvoite edellyttää erillistyöasemien hyväksyntää (akkreditointia).

Ohje kattaa kansalliset turvallisuusluokat KÄYTTÖ RAJOITETTU (TL IV), LUOTTAMUKSELLINEN (TL III) ja SALAINEN (TL II) sekä niiden kansainväliset vastineet RESTRICTED, CONFIDENTIAL ja SECRET. Suojausten yhteydessä kuvataan myös esimerkkejä suojausten täyttymisen vaatimustenmukaisuuden osoittamisesta. Fyysisen turvallisuuden osalta on huomioitava, että tiedon käsittely edellyttää yleensä toimivaltaisen turvallisuusviranomaisen (Supo DSA tai PE DSA) lausuntoa erillistyöaseman ja siihen liittyvien tallennemedioiden fyysisestä suojaamisesta (tilaturvallisuudesta).

3 Tietoturvallisuuden varmistamiseen liittyvät vaatimukset

Viranomaisten velvollisuus suojata kansallista turvallisuusluokiteltua tietoa perustuu erityisesti lakiin julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) ja valtioneuvoston asetukseen asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019, turvallisuusluokitteluasetus). Kansainvälisten turvallisuusluokiteltujen tietojen suojaamiselle asetetut vaatimukset ovat valtaosin yhteneviä kansallisten vastineiden kanssa. Kansainvälisten turvallisuusluokiteltujen tietojen suojaamisessa on kuitenkin huomioitava kyseiseen tietoon liittyvät erityisvaatimukset. Esimerkiksi EU:n ja Naton turvallisuusluokitellun tiedon suojaaminen perustuu kyseisten yhteisöjen turvallisuussääntöihin[3]. Kansallisten ja kansainvälisten turvallisuusluokiteltujen tietojen suojaamista ja arviointitoiminnan eroavaisuuksia on käsitelty yksityiskohtaisemmin Traficomin ohjeessa kansainvälistä turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien arviointi- ja hyväksyntätoiminnasta[4].

Sekä kansalliseen että kansainväliseen sääntelyyn pohjautuvat suojausvaatimukset on koottu Katakri 2020 -työkaluun[5] ja sen Nato-liitteeseen[6]. Erillistyöaseman suojaamisessa tulee huomioida keskeiset erillistyöaseman elinkaaren vaiheet. Erillistyöaseman tekniseen suojaamiseen soveltuvat erityisesti seuraavat:

- Pääsyoikeuksien hallinta (Katakri 2020 / I-06)
- Tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä (Katakri 2020 / I-07)
- Järjestelmäkovennus (Katakri 2020 / I-08)
- Haittaohjelmasuojaus (Katakri 2020 / I-09)
- Turvallisuuteen liittyvien tapahtumien jäljitettävyys (Katakri 2020 / I-10)
- Poikkeamien havainnointikyky ja toipuminen (Katakri 2020 / I-11)
- Hajasäteily (TEMPEST) ja elektroninen tiedustelu (Katakri 2020 / I-14)
- Tiedon sähköinen välitys (Katakri 2020 / I-15)
- Muutoshallintamenettelyt (Katakri 2020 / I-16)
- Fyysinen turvallisuus (Katakri 2020 / I-17)
- Ohjelmistohaavoittuvuuksien hallinta (Katakri 2020 / I-19)
- Varmuuskopiointi (Katakri 2020 / I-20)

[3] Neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU). Naton turvallisuussäännöstö (C-M(2002)49-REV1) tarkentavine direktiiveineen, teknisen tietoturvallisuuden osalta erityisesti AC/322-D/0048-REV3.
[4] Liikenne- ja viestintävirasto. 2021. Ohje kansainvälistä turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien arviointi- ja hyväksyntätoiminnasta. 2021. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Ohje_kansainvalista_turvallisuusluokiteltua_tietoa_kasittelevien_tietojarjestelmien_arviointi-_ja_hyvaksyntatoiminnasta.pdf.
[5] Kansallinen turvallisuusviranomainen. 2020. Katakri 2020 – Tietoturvallisuuden auditointityökalu viranomaisille. URL: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf.
[6] Kansallinen turvallisuusviranomainen. 2023. Katakri 2020 – Tietoturvallisuuden auditointityökalu viranomaisille. Liite IV: Naton turvallisuusluokitellun tiedon suojaaminen. URL: https://um.fi/documents/35732/0/Katakri-2020-Liite-IV-2023-05-10+%282%29.pdf.

- Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen (Katakri 2020 / I-21)

Lisäksi tulee huomioida erillistyöaseman suojaamisen näkökulmasta erityisesti seuraavat:

- Turvallisuustyön tehtävien ja vastuiden määrittäminen (Katakri 2020 / T-02)
- Tietoturvallisuusriskien hallinta (Katakri 2020 / T-03)
- Turvallisuusohjeistus (Katakri 2020 / T-04)
- Turvallisuuspoikkeamien hallinta (Katakri 2020 / T-07)
- Henkilöstön luotettavuuden arviointi (Katakri 2020 / T-10)
- Turvallisuuskoulutus (Katakri 2020 / T-12)
- Tiedonsaantitarve ja käsittelyoikeudet (Katakri 2020 / T-13)

4 Erillistyöasemien keskeiset suojaukset

Tässä luvussa kuvataan erillistyöasemien keskeiset suojaukset. Suojausten jaottelussa on käytetty näkökulmana erillistyöaseman suojausten arviointia sekä käsiteltävien tietojen turvallisuusluokkaa. Turvallisuusluokan kuvauksissa käytetään kansallisia merkintöjä TL IV-II, jotka kattavat tässä ohjeessa myös kansainväliset vastineet RESTRICTED-SECRET, ellei kyseisen suojauksen kohdalla toisin mainita. Suojausten kuvaukset on laadittu siten, että matalamman luokan suojaukset periytyvät ylemmille luokille. Esimerkiksi turvallisuusluokan IV suojaukset tulee huomioida myös turvallisuusluokkien III-II tietoa käsittelevissä erillistyöasemissa. Suojausten yhteydessä kuvataan myös esimerkkejä suojausten täyttymisen vaatimustenmukaisuuden osoittamiseen.

Kuvaus on laadittu Windows-käyttöjärjestelmällä varustetun erillistyöaseman suojaamiseen, mutta sitä voidaan hyödyntää soveltuvin osin myös muilla käyttöjärjestelmillä varustettuihin erillistyöasemiin. Kuvauksessa viitataan joidenkin kokonaisuuksien osalta ulkoisiin lähteisiin. Esimerkiksi järjestelmäkovennuksessa huomioitavat tekijät vaihtelevat käyttöjärjestelmästä ja sen versiosta riippuen, ja siten myös järjestelmäkovennusten arvioinnissa on syytä huomioida kyseiseen käyttöjärjestelmään liittyvät ajantasaiset vertailulähteet[7].

Kuvauksen hyödyntämisessä tulee huomioida koko erillistyöaseman elinkaari, aina suunnittelusta tietoturvalliseen käytöstä poistoon asti. Erillistyöaseman arvioinnissa tulee aina varmistua myös siitä, että erillistyöaseman turvallisen käytön jalkauttamiseen on käytössä riittävät menettelyt (muun muassa selkeät vastuut, ohjeistukset, koulutukset). Joitain sähköiseen käsittelyyn liittyviä riskejä voi olla mahdollista pienentää hyväksyttävälle tasolle myös muilla suojauksilla. Esimerkiksi erillistyöaseman fyysisellä pääsynhallinnalla voi olla mahdollista pienentää useita tietoteknisiin heikkouksiin liittyviä riskejä. Toisaalta esimerkiksi hajasäteilysuojaus voidaan toteuttaa erillistyöaseman sijoittamisella hajasäteilysuojattuun fyysiseen tilaan tai esimerkiksi hajasäteilysuojattua erillistyöasemalaitetta käyttäen[8].

[7] Esimerkkejä vertailulähteistä:
- National Institute of Standards and Technology (NIST) - Checklist Repository. URL: https://ncp.nist.gov/repository.
- Center for Internet Security (CIS). URL: https://www.cisecurity.org/cis-benchmarks.
- Bundesamt für Sicherheit in der Informationstechnik (BSI) - Configuration Recommendations for Hardening of Windows 10 Using Built-in Functionalities. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Cyber-Security/SiSyPHuS/AP11/Hardening_Guideline.pdf.
- Australian Cyber Security Centre (ACSC) - Hardening Microsoft Windows 10 version 21H1 Workstations. URL: https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-21h1-workstations.

[8] Lisätietoa: Liikenne- ja viestintävirasto. 2022. Kansallinen TEMPEST-ohje. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Kansallinen_TEMPEST-ohje_20220705.pdf.

Erillistyöasemassa tapahtuvan tietojenkäsittelyn riskien arviointi on aina kokonaisuus, jossa korostuu arvioijan tekemä kokonaisvaltainen tarkastelu.

4.1 Tietoturvallisuusriskien hallinta

4.1.1 Toteutusesimerkki / TL IV-II

- Organisaatio on arvioinut erillistyöasemaan ja siinä käsiteltäviin turvallisuusluokiteltuihin tietoihin kohdistuvat olennaiset riskit ja mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

4.1.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Erillistyöasemaan ja siinä käsiteltäviin tietoihin liittyvä kirjallinen riskienarviointi, sisältäen tunnistetut riskit ja niitä pienentävät suojaukset.

4.2 Erillistyöaseman suojaaminen fyysisen turvallisuuden menetelmillä

4.2.1 Toteutusesimerkki / TL IV

- Erillistyöasemaa ja siihen liittyviä tallennemedioita käsitellään siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta.
- Erillistyöaseman ja siihen liittyvien tallennemedioiden (esimerkiksi mahdolliset USB-mediat tai/ja varmuuskopiot) käyttöympäristön fyysinen suojaus (ml. siihen liittyvät hallinnolliset käytännöt) täyttää hallinnollisen alueen tai turva-alueen vaatimukset.

4.2.2 Toteutusesimerkki / TL III-II

- Erillistyöaseman ja siihen liittyvien tallennemedioiden (esimerkiksi mahdolliset USB-mediat tai/ja varmuuskopiot) käyttöympäristön fyysinen suojaus (ml. siihen liittyvät hallinnolliset käytännöt) täyttää turva-alueen vaatimukset.

4.2.3 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje erillistyöaseman ja siihen liittyvien tallennemedioiden turvallisesta käytöstä.
- Fyysisen turvallisuuden toimivaltaisen turvallisuusviranomaisen (Supo DSA tai PE DSA) lausunto erillistyöaseman ja siihen liittyvien tallennemedioiden käyttöympäristön fyysisestä suojaamisesta (tilaturvallisuudesta).

4.2.4 Huomioitavaa

- Tässä ohjeessa keskitytään tyypilliseen, nopeasti käyttöönotettavaan toimintamalliin, jossa erillistyöaseman ja siihen liittyvien tallennemedioiden käyttöympäristö rajataan fyysisille turvallisuusalueille siten, että fyysinen käyttöympäristö mahdollistaa kansallisen, EU:n ja Naton turvallisuusluokitellun tiedon käsittelyn ja säilyttämisen.
- Eroavien toimintamallien[9] periaatteita on kuvattu esimerkiksi Katakri 2020 -arviointityökalun kohdissa I-17 ja I-18.
- Vertaa TEMPEST-suojaus luvussa 4.14.

[9] Esimerkiksi toimintamalli, jossa kansallisen tai EU:n turvallisuusluokitellun tiedon käsittely ja säilyttäminen hajautetaan eroaviin fyysisiin käyttöympäristöihin.

4.3 Erillistyöaseman turvallinen ensiasennus

4.3.1 Toteutusesimerkki / TL IV

- Käyttöjärjestelmä valitaan siten, että se on tuen piirissä erillistyöaseman ennakoidun elinkaaren ajan.
- Kaikki asennustoimet toteutetaan siten, että erillistyöasema on ilman verkkokytkentäisyyttä (vrt. luku 4.4).
- Käyttöjärjestelmä asennetaan uudelle tai vastaavassa käytössä olleelle ylikirjoitetulle levylle.
- Käyttöjärjestelmä asennetaan eheältä, luotettavalta asennusmedialta.
- Varmistetaan, että käyttöjärjestelmä asennetaan erillistyöaseman tallennusmedialle (yleensä kiintolevy) käyttäen tiedostojärjestelmää[10], joka tukee nykyaikaisia turvallisuusominaisuuksia.
- Käyttöjärjestelmäohjelmistoon asennetaan turvallisuuspäivitykset (vrt. luku 4.13).
- Erillistyöasemaan asennetaan toiminnalle välttämättömät sovellusohjelmistot siten, että sovellusohjelmistojen eheydestä (vrt. luku 4.13) ja turvallisuudesta pyritään varmistumaan.

4.3.2 Toteutusesimerkki / TL III-II

- Erillistyöasemalaitteiston hankinnassa on tunnistettu ja huomioitu toimitusketjuihin liittyvät riskit.

4.3.3 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus erillistyöasemalaitteiston toimitusketjuihin liittyvien riskien huomioimisesta (toteutus usein osana erillistyöasemaan kohdistuvien riskien arviointia, vrt. luku 4.1).
- Kuvaus erillistyöaseman perustiedoista
  - Erillistyöaseman käyttötarkoitus.
  - Erillistyöaseman merkki ja malli.
- Kuvaukset/ohjeet asennusprosessista.
- Kuva tiedostojärjestelmävalinnasta[11].
- Laitteisto- ja ohjelmistokirjanpito, sisältäen myös perustelun kullekin asennetulle ohjelmistolle/sovellukselle.
- Asennuspöytäkirjat.

4.3.4 Huomioitavaa

- Tässä ohjeessa keskitytään toimintamalliin, jossa yksittäisiä erillistyöasemia asennetaan ilman, että asennusprosessia merkittävästi automatisoitaisiin. Ohjeessa ei käsitellä erillistyöasemien eroaviin tuotantotapoihin[12] liittyviä riskejä tai niitä pienentäviä suojauksia. Ohjetta voi kuitenkin soveltaen hyödyntää myös eroavien tuotantotapojen suojausten suunnittelussa.

[10] Esimerkiksi Windows-käyttöjärjestelmässä tiedostojärjestelmä NTFS.
[11] Esimerkiksi Windows-käyttöjärjestelmässä nähtävissä muun muassa resurssienhallinnan kautta tallennusmedian ominaisuuksista.
[12] Esimerkiksi tuotantotapa, jossa erillistyöasemien asennuksissa hyödynnetään muista verkosta pysyvästi erotettua asennusjärjestelmää.

4.4 Verkkokytkentäisyyden estäminen

4.4.1 Toteutusesimerkki / TL IV

- Tarpeettomat verkkokytkentäisyysrajapinnat on poistettu käytöstä BIOS-/UEFI-tasolla.
    - Käytöstä poistettavat rajapinnat: WLAN, LAN, 3-5G, Bluetooth, sarjaportit, Firewire, Thunderbolt ja vastaavat.
    - Huomioi myös muut BIOS-/UEFI-kovennukset (vrt. luku 4.5.1).

4.4.2 Toteutusesimerkki / TL III

- Tarpeettomat verkkokytkentäisyysrajapinnat (vrt. luku 4.4.1) on poistettu käytöstä (disabled) käyttöjärjestelmästä ohjelmallisesti[13].
- Tarpeettomien ajurien asennukset on poistettu[14] (uninstalled) ja ajurien automaattinen asentuminen[15] on poistettu käytöstä.
- Ohjelmistopalomuuri estää kaiken liikennöinnin.
    - Ohjelmistopalomuuri on päällä ja toiminnassa.
    - Kaikki liikennöinti työasemasta ulos (outbound) tai sinne sisään (inbound) on palomuurin säännöstössä kielletty.
    - Huomioitavaa: Esimerkiksi Windows-käyttöjärjestelmän omassa palomuurissa on suodatus mahdollista asettaa eri verkoille eroavasti. Varmistettava, että estävät säännöt kohdistuvat kaikkeen sisään tulevaan ja kaikkeen ulos lähtevään liikenteeseen. Lisäksi tulee varmistaa, että oletusarvoiset liikennöinnin sallivat sääntöavaukset on poistettu käytöstä.

4.4.3 Toteutusesimerkki / TL II

- Tarpeettomat fyysiset komponentit on poistettu tai fyysisesti tuhottu.
    - Langalliset ja langattomat verkkokortit ja vastaavat komponentit on poistettu. (Vaihtoehtona langallisen verkkokortin osalta sen portin fyysinen tuhoaminen.)

4.4.4 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje prosesseista.
- Kuvat käyttöjärjestelmän laitehallinnan asetuksista.
- Kuvat ohjelmistopalomuurin asetuksista ja säännöstöstä.
- Kuvat BIOS-/UEFI-asetuksista.
- Irrotettujen fyysisten komponenttien kuvaus.
- Ennen/jälkeen kuvat poistetuista/tuhotuista komponenteista.

4.5 Kovennus - BIOS/UEFI

4.5.1 Toteutusesimerkki / TL IV-II

- BIOS-/UEFI-version ajantasaisuuden tarkistaminen ja tarvittaessa turvallisuuspäivitysten asentaminen (vrt. luku 4.13).
- Estetään käynnistäminen muulta kuin ensisijaiseksi määritellyltä laitteelta.
- Suojattu käynnistys (secure boot) asetetaan päälle.
- Estetään pääsy tai/ja asetusten muuttaminen valtuuttamattomalta käyttäjältä. Esimerkkejä:

[13] Toteutettavissa esimerkiksi Windows-käyttöjärjestelmän laitehallinnan (Device Manager) kautta.
[14] Toteutettavissa esimerkiksi Windows-käyttöjärjestelmän laitehallinnan (Device Manager) kautta.
[15] Toteutettavissa esimerkiksi Windows-käyttöjärjestelmän ohjelman SystemPropertiesHardware.exe kautta (Device installation settings).

- Asetetaan riittävän vahva[16] BIOS-/UEFI salasana.
- Salasanan ohitus[17] poistettu käytöstä.
- Salasanan vaihto muilta kuin ylläpitäjiltä[18] estetään.

- Tarpeettomat rajapinnat ja laitteet poistetaan käytöstä.
  - Verkkokytkentäisyys: WLAN, LAN, 3-5G, Bluetooth, sarjaportit, Firewire, Thunderbolt ja vastaavat (vrt. 4.5.1).
  - Muut: Kamera, mikrofoni, telakkaliitäntä ja vastaavat.
- Tarpeettomat toiminnallisuudet[19] poistetaan käytöstä.

4.5.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaukset/ohjeet prosesseista.
- Kuvat BIOS-/UEFI-asetuksista.
- Sisäisen katselmoinnin pöytäkirja/raportti.

4.6 Kovennus - Käyttöjärjestelmä

4.6.1 Toteutusesimerkki / TL IV-II

- Erillistyöaseman käyttöjärjestelmä kovennetaan pohjautuen luotettavaan kovennusviitekehykseen[20].
- Mahdolliset eroavaisuudet kovennusviitekehykseen ovat perusteltuja ja kuvattuja.
- Tarpeettomat käyttöjärjestelmän ominaisuudet[21] poistetaan.
- Käyttöjärjestelmäasennukseen sisältyneet tarpeettomat sovellukset poistetaan.
- Tarpeettomat palvelut (services) poistetaan käytöstä (disable).
- Käytössä ei ole palveluita, joiden polku (service path) sisältää välilyöntejä ilman lainausmerkkejä[22].
- Kovennukset on suhteutettu erillistyöaseman fyysiseen käyttöympäristöön liittyviin riskeihin (vrt. riskienhallinta luvussa 4.1). Esimerkiksi salasanasuojattu näytön lukitus 5-15 minuutin käyttämättömyyden jälkeen.

4.6.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaukset/ohjeet prosesseista.
- Kuvaus käyttöjärjestelmän perustiedoista.
  - Käyttöjärjestelmäversio (tarkka versiotieto).
  - Käytössä oleva kovennusviitekehys ja sen taso.
  - Toteutetut kovennukset verrattuna kovennusviitekehykseen. Eroavaisuuksien perustelut.
- Kuvaus, tuloste (export), kuvakaappaus tai vastaava, josta käy ilmi käytössä olevat palvelut perusteluineen, oikeuksineen ja polkuineen.
- Kovennusasetukset/-politiikat (paikalliset ryhmäkäytännöt).
- Teknisten työkalujen[23] tuottamat vertailutiedot käytössä olevien kovennusasetusten ja kovennusviitekehyksen suositusasetusten välillä.

[16] Yleensä suosituksena vähintään 12 merkkiä siten, että salasanan kompleksisuus on huomioituna.
[17] Joidenkin valmistajien käyttämä termistö: Password bypass: disabled.
[18] Joidenkin valmistajien käyttämä termistö: allow non-admin password changes: disabled
[19] Valmistajakohtaisia esimerkkejä: Miscellaneous devices, Unobtrusive mode, USB configuration, USB Wake Support, AMT, Absolute, OS recovery, BIOS/UEFI recovery, anti-theft, UEFI update via OS.
[20] Esimerkiksi CIS tai DISA STIG.
[21] Engl. Windows Features. Esimerkkejä useisiin erilliskoneiden käyttötapauksiin tarpeettomista ominaisuuksista: Windows Fax and Scan, Remote Differential Compression API Support, Internet Printing Client, Windows Process Activation Service, Work Folders Client, Internet Explorer 11, Legacy Components – DirectPlay, Media Features – Windows Media Player, Windows PowerShell 2.0, XPS Services and XPS Viewer.
[22] Esimerkki kovennuksen ja arvioinnin tueksi: wmic service get name,displayname,pathname,startmode |findstr /i "Auto" |findstr /i /v "C:\Windows\\" |findstr /i /v """
[23] Esimerkiksi Policy Analyzer -työkalu Microsoft-pohjaisten ympäristöjen kovennusasetusten vertailuun.

- Laitteisto- ja ohjelmistokirjanpito, sisältäen myös perustelun kullekin asennetulle ohjelmistolle/sovellukselle.
- Sisäisen katselmoinnin pöytäkirja/raportti.

4.7 Käyttöoikeuksien ja käyttäjätunnusten hallinta

4.7.1 Toteutusesimerkki / TL IV

- Käyttöoikeudet ja käyttäjätunnukset perustuvat tiedonsaantitarpeeseen ja vähimpien oikeuksien periaatteeseen.
- Erillistyöasemassa on vain välttämättömät käyttäjätunnukset. Tarpeettomat käyttäjätunnukset (tilit) on poistettu tai poistettu käytöstä (disabled), esimerkiksi Vieras-tili (guest).
- Käytössä on henkilökohtaiset, käyttäjän yksilöinnin mahdollistavat käyttäjätunnukset.
- Työaseman käyttö tapahtuu peruskäyttäjätason (user) tunnuksilla.
- Ylläpito-oikeudet (administrator) on myönnetty vain välttämättömiin ylläpitotehtäviin ja vain välttämättömille henkilöille. Ylläpitotunnusten käyttö on rajattu vain ylläpitotehtäviin.
- Ylläpitotunnukset säilytetään tietoturvallisella tavalla siten, että salasanat ovat suojattuna sekä saatavilla.
- Käyttäjätunnukset pidetään ajan tasalla. Organisaatiolla on menettely, jolla varmistetaan käyttöoikeuksien poistaminen tiedonsaantitarpeen päätyttyä.
- Käyttäjät todennetaan fyysisen turvallisuusalueen sisällä vähintään salasanaa käyttäen tai kahteen todennustekijään (esim. toimikortti + PIN) nojautuen.
    - Salasanat: Lähtökohtaisesti vähintään 12 merkkiä sisältäen merkkejä ryhmistä iso kirjain, pieni kirjain, erikoismerkki/numero. Vaihtoehtoisesti pidempi salalause.
    - Muiden tunnusta (tiliä) suojaavien tekijöiden huomiointi asetuksissa. Erityisesti:
        - Salasanahistoria (password history), esimerkiksi 10.
        - Lukitusaika (lockout duration), esimerkiksi 30 minuuttia.
        - Lukituksen laskurin asetukset, esimerkiksi tunnuksen lukittuminen viiden epäonnistuneen kirjautumisyrityksen jälkeen.
        - Salasanan vanhentuminen.
    - Käytössä on teknisesti edellä mainitut turvallisuusominaisuudet päälle pakottava politiikka (policy).

4.7.2 Toteutusesimerkki / TL III

- Käyttäjät todennetaan fyysisen turvallisuusalueen sisällä vähintään kahteen todennustekijään (esimerkiksi toimikortti + PIN) nojautuen. Joissain erillistyöaseman käyttöympäristöissä toinen todennustekijä saattaa riskiperustaisesti olla toteutettavissa myös fyysisen turvallisuuden menettelyin.

4.7.3 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje käyttöoikeuksien ja käyttäjätunnusten hallinnasta.
- Kuvakaappaukset/tulosteet käyttöoikeuksien hallintaprosessin toimivuudesta (esimerkiksi tiketit) sekä käyttöoikeuksien ajantasaisuudesta varmistumisesta (esimerkiksi pöytäkirjat käyttöoikeuksien määräaikaistarkastuksista, kuvakaappaukset erilliskoneen käyttöoikeuksista).
- Kuvat, tulosteet tai vastaavat asetuksista ja teknisistä politiikoista (policy).

4.8 Haittaohjelmilta suojautuminen

4.8.1 Toteutusesimerkki / TL IV

- Ohjelmistojen/sovellusten suorittamista rajataan/suojataan ottamalla käyttöön käyttöjärjestelmän tarjoamia suojausominaisuuksia.
    - Windows Defender Application Control (WDAC) ja/tai AppLocker käytössä[24].
- Haittaohjelmantorjuntaohjelmisto on asennettu, käynnissä ja toimintakykyinen.
    - Haittaohjelmantorjuntaohjelmisto on asennettu ja käynnissä.
    - Haittaohjelmien tunnistamiseen käytettävien tietojen (esimerkiksi tunnistetiedot ja havainnointisäännöstöt) päivittäminen toteutetaan erillisellä verkkoon kytketyllä laitteella ja toimitetaan turvallisella tavalla (esimerkiksi optisella medialla) erillistyöasemaan. Vrt. luku 4.13.
    - Haittaohjelmien tunnistamiseen käytettävien tietojen päivityssykli on erillistyöaseman käyttötapaan liittyviin riskeihin nähden riittävän tiheä (esimerkiksi vuosineljänneksittäin tai aina ennen kuin työasemaan kytketään siirrettävää tallennusmediaa).
    - Haittaohjelman tunnistus toteutetaan myös muilla tavoin kuin tunnisteista (esimerkiksi heuristiikka, käyttäytymisen analysointi).
    - Mahdollisille siirrettäville tallennusvälineille tehdään haittaohjelmatarkistus automatisoidusti.
    - Haittaohjelmahavaintojen käsittelyyn on olemassa selkeä toimintamalli, joka on ohjeistettu ja koulutettu erillistyöaseman käyttäjille ja ylläpidolle.
- Ajettavan koodin (javascript, makrot, PowerShell-komentojonot) suorittamisen rajaaminen/estäminen oletuksena erityisesti seuraavista:
    - Selain.
    - Toimisto-ohjelmisto[25].
    - PDF-lukija.
    - PowerShell[26]
- Rajataan Windows Script Host (WSH) -toiminnallisuuden käyttöä haitallisten ohjelmistojen suorittamiseen. Esimerkkejä:
    - WSH otetaan pois käytöstä (disable)[27].
    - Pääsy ohjelmiin wscript.exe ja cscript.exe estetään.
    - Yleinen VBScript- tai Jscript-tuki poistetaan käytöstä poistamalla ActiveX-komponenttien rekisteröinti[28].

4.8.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje ohjelmistojen/sovellusten suorittamista rajaavista/suojaavista menettelyistä.
- Kuvaus/ohje haittaohjelmilta suojautumisen menettelyistä ja prosesseista.
- Kuvat, tulosteet tai vastaavat asetuksista ja teknisistä politiikoista (policy).

[24] Microsoft - Windows Defender Application Control and AppLocker feature availability. URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/feature-availability.
[25] Esimerkki (Office-tuote): Disable all macros without notification / with notification
[26] Useissa windows-ympäristöissä tilan pystyy tarkistamaan esimerkiksi komennolla Get-ExecutionPolicy ja asettamaan komennolla Set-ExecutionPolicy allekirjoittamattomien skriptien ajamisen eston päälle.
[27] Bundesamt für Sicherheit in der Informationstechnik (BSI) - Configuration Recommendations for Hardening of Windows 10 Using Built-in Functionalities. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Cyber-Security/SiSyPHuS/AP11/Hardening_Guideline.pdf - 5.5.2.2 (HD) Disabling the Windows Script Host.
[28] Esimerkki: regsvr32.exe /u vbscript.dll

4.9 Jäljitettävyys

4.9.1 Toteutusesimerkki / TL IV

- Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi on suunniteltu ja toteutettu luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen.
- Käyttöön otettu lokitus kattaa keskeiset turvallisuuteen liittyvät tapahtumat[29].
- Lokien tallennustila ja ylikirjoittuminen on asetettu siten, että lokitiedot säilyvät edellytetyn ajan[30].
- Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä. (Vrt. luku 4.7.)

4.9.2 Toteutusesimerkki / TL III-II

- Lokitiedot varmuuskopioidaan kuukausittain vain tähän tarkoitukseen varatulle USB-tallennusmedialle, jota säilytetään kyseisen turvallisuusluokan mukaisesti kassakaapissa.
- Lokitiedostoista lasketaan tarkistussummat, jotka kirjoitetaan luvattomalta pääsyltä suojattuihin tiedostoihin.

4.9.3 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje menettelyistä riittävän jäljitettävyyden toteuttamiseksi (esimerkiksi lokipolitiikka), kattaen muun muassa kerättävien lokitietojen määrittelyn, teknisen toteutustavan, lokien varmuuskopiointimenettelyt ja vastuuhenkilöt.
- Kuvat, tulosteet tai vastaavat asetuksista ja teknisistä politiikoista (policy).

4.10 Havainnointikyky

4.10.1 Toteutusesimerkki / TL IV

- Poikkeamien havainnointiin on suunnitelma.
- On käytössä menettely räikeimpien poikkeamien, esimerkiksi tunnistetut haittaohjelmat, havainnointiin.

4.10.2 Toteutusesimerkki / TL III-II

- On käytössä uskottava menettely poikkeamien havaitsemiseen lokitiedoista.
- Valvontatehtävät on selkeästi vastuutettuja ja aikataulutettuja.

4.10.3 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje menettelyistä riittävän havainnointikyvyn toteuttamiseksi.

4.11 Levynsalaus

4.11.1 Toteutusesimerkki / TL IV-II

- Levynsalaus on otettu käyttöön.
- Salausasetukset ovat riittävän turvalliset.

[29] Yleensä huomioitava erityisesti lokiryhmät Turvallisuus (security), Järjestelmä (system) ja Sovellus (application), AppLocker , Windows Defender sekä PowerShell-lokit.
[30] Tyypillisenä toteutustapana varmistaa, että lokitiedoille on varattu riittävästi tallennustilaa ja että uudet lokitiedot eivät ylikirjoita vanhempia lokitietoja.

  - Mikäli erillistyöasemaa säilytetään elinkaarensa ajan ko. turvallisuusluokan tietojen säilyttämiseen hyväksytyn fyysisen tilan (vrt. luku 4.2) sisällä, ei edellytetä niin sanottua hyväksyttyä salausta. Tällöin salausasetuksissa voidaan nojautua esimerkiksi valmistajan suosituksiin.
  - Mikäli erillistyöasemaa säilytetään elinkaarensa aikana hyväksytyn fyysisen tilan (vrt. luku 4.2) ulkopuolella ja tarve niin sanotulle hyväksytylle salaukselle, ole yhteydessä Traficomin NCSA-toimintoon.
- Salausavainten hallintakäytännöt on suunniteltu.
- Palautusavain (recovery key) on saatavilla tarvittaessa, säilytys turvallisessa paikassa.

4.11.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje menettelyistä levysalauksen toteuttamista ja salausavainten hallintakäytännöistä.
- Kuvat, tulosteet tai vastaavat asetuksista ja teknisistä politiikoista (policy).

4.12 Tiedon tuonti ja vienti, USB-tallennusmediat ja -laitteet, merkinnät

4.12.1 Toteutusesimerkki / TL IV

- Turvallisuusluokitellun tiedon mahdollinen tuonti/vienti (import/export) työasemaan/työasemasta on toteutettu suunnitellusti.
- Turvallisuusluokitellun tiedon välitys on toteutettu suunnitellusti. Välitystapana
  - kuriirimenettelyt, tai/ja
  - sähköiset menettelyt[31].
- Erillistyöasemaan kytkettävien USB-tallennusmedioiden ja -laitteiden käyttö on suunniteltua.
- Erillistyöasemassa käytetään vain erikseen nimettyjä/sallittuja USB-tallennusmedioita (esimerkiksi USB-tikut).
- Muiden USB-laitteiden (hiiri, CD-asema) käyttö on rajattu vain erikseen nimettyihin/sallittuihin hallinnollisesti tai/ja teknisesti.
- Käsiteltäessä EU:n tai Nato turvallisuusluokiteltua tietoa, erillistyöasemaan ja mahdollisiin siirrettäviin tallennusmedioihin merkitään selkeästi korkeimman niillä käsiteltävän tiedon luokitus ja omistaja.

4.12.2 Toteutusesimerkki / TL III-II

- Erillistyöasemassa käytettävien USB-tallennemedioiden ja -laitteiden käyttö on teknisesti rajattu vain erikseen nimettyihin/sallittuihin.
- Kaikki tallennusmediat on kirjattu laitekirjanpitoon.
- Kaikki erillistyöasemaan sen elinkaaren aikaan liitettävät laitteet (esimerkiksi USB-porttiin kytkettävä CD-asema) ovat vain kyseiseen erillistyöasemakäyttöön varattuja (dedikoituja) ja merkittyjä.

4.12.3 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje turvallisuusluokitellun tiedon tuonnista/viennistä.
- Kuvaus/ohje turvallisuusluokitellun tiedon välittämisestä.
- Kuvaus/ohje USB-tallennemedioiden käytöstä.
- Kuvat, tulosteet tai vastaavat asetuksista ja teknisistä politiikoista (policy).
- Käytännön toteumaa kuvaavien USB-medioiden käyttöä kuvaavien lokitietojen koosteet

[31] Hyväksyttyjen salausratkaisujen ja niihin liittyvien käyttöpolitiikkojen osalta ole tarvittaessa yhteydessä Traficomin NCSA-toimintoon.

- Laitteistokirjanpito.

4.13 Ohjelmistojen turvallisuuspäivitykset

4.13.1 Toteutusesimerkki / TL IV-II

- Käytössä on menettely turvallisuuspäivitysten säännölliseen asentamiseen.
- Päivitysprosessissa pyritään huomioimaan yleiset haittaohjelmiin ja toimitusketjuihin liittyvät riskit. Esimerkkejä:
  - Valmistajan verkkosivuilta löytyvän päivityspaketin lataaminen ja sen eheyden tarkistaminen toisella, turvalliseksi arvioidulla työasemalla.
  - Päivityspaketin siirtäminen erillistyöasemalle optisella medialla tai puhtaalla USB-medialla.
- Menettely on riittävän kattava sisältäen turvallisuuden näkökulmasta oleelliset ohjelmistot. Menettelyn tulee kattaa ainakin käyttöjärjestelmän, sovellusohjelmistot ja laitteisto-ohjelmiston kuten BIOS/UEFI.
- Päivitysmenettelyn sykli on erillistyöaseman käyttötapaan liittyviin riskeihin nähden riittävän tiheä (esimerkiksi vuosineljänneksittäin).
- Käyttöön otetaan menettely sen varmistamiseksi, että kovennukset eivät muutu/poistu päivitysten yhteydessä, ja että mahdolliset päivitysten yhteydessä mukaan tulevat uudet ominaisuudet ovat kovennusten piirissä.

4.13.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje menettelyistä erillistyöaseman ohjelmistojen (käyttöjärjestelmä, sovellusohjelmistot, laiteohjelmisto) turvallisuuspäivityksistä huolehtimiseen.

4.14 TEMPEST

4.14.1 Toteutusesimerkki / TL III-II

- Käsitellyn tiedon turvallisuusluokan mukaiset TEMPEST-suojaukset toteutettu.
  - Työaseman käyttöpiste TEMPEST-suojattu, tai
  - Käytössä TEMPEST-suojattu erillistyöasemalaite, tai
  - Käytössä TEMPEST-kotelointiratkaisu.

4.14.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus TEMPEST-suojauksista.
- TEMPEST-mittausraportti tai/ja -lausunto.

4.15 Eroavien tiedonsaantitarpeiden ja teknisen tarkastusoikeuden huomiointi

4.15.1 Toteutusesimerkki / TL IV

- On otettu käyttöön toimintamalli, jolla pystytään luotettavasti toteuttamaan erillistyöasemien luvallisten käyttäjien pääsy vain tiedonsaantitarpeen mukaisiin tietoihin.
  - Mikäli samalla erillistyöasemalla käsitellään turvallisuusluokiteltuja tietoja, joihin kaikilla erillistyöaseman käyttäjillä ei ole tiedonsaantitarvetta, tulee turvallisuusluokitellut tiedot erotella esimerkiksi käyttöoikeuksin rajattuihin kansioihin. Vrt. luku 4.7.

- On otettu käyttöön toimintamalli, jolla pystytään luotettavasti estämään teknisen tarkastusoikeuden varaavien eri tiedon omistajien pääsy toistensa turvallisuusluokiteltuihin tietoihin. Esimerkkejä:
    - Kullakin erillistyöasemalla käsitellään vain yhden tiedon omistajan tietoja erillistyöaseman elinkaaren aikana.
    - Vaihtoehtoisesti eri omistajien tiedot on eroteltu kyseisille turvallisuusluokitelluille tiedoille hyväksyttyä salausratkaisua hyödyntäen tai/ja käyttöoikeuksin rajattuihin kansioihin siten, että vain kyseisiin tietoihin oikeutetuilla käyttäjätunnuksilla on pääsy kyseisiin tietoihin. Huomioitava, että tämä toteutusmalli ei sovellu tilanteisiin, joissa yksikin tiedon omistaja edellyttää kaikkien omistamaansa tietoa käsitelleiden tallennemedioiden luovuttamista käytön (esimerkiksi hankkeen) päätyttyä ja jossa tiedon luotettava tuhoaminen (esimerkiksi riittävän luotettava ylikirjoitus) ei ole mahdollinen.

4.15.2 Toteutusesimerkki / TL III-II

- On otettu käyttöön toimintamalli, jolla pystytään luotettavasti estämään teknisen tarkastusoikeuden varaavien eri tiedon omistajien pääsy toistensa turvallisuusluokiteltuihin tietoihin. Esimerkkejä:
    - Kullakin erillistyöasemalla käsitellään vain yhden tiedon omistajan tietoja erillistyöaseman elinkaaren aikana.
    - Erillistyöasemalla käsitellään vain sellaisia turvallisuusluokiteltuja tietoja, joiden omistaja ei varaa teknistä tarkastusoikeutta eikä muidenkaan menettelyjen (esimerkiksi tallennemedioiden luovutus takaisin tiedon omistajalle) kautta pysty saamaan pääsyä toisten tiedon omistajien tietoihin.

4.15.3 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus erillistyöaseman käyttäjien tiedonsaantitarpeista ja niiden mahdollisista eroavaisuuksista.
- Kuvaus tunnistetuista tarkastusoikeuden tai vastaavan pääsyn edellyttämistä velvoitteista.
- Kuvaus toimintamallista, jolla hallitaan mahdollisten eroavien tiedonsaantitarpeiden ja tarkastusoikeuksien aiheuttamat riskit.
- Tiedon omistajien kanssa tehdyt sopimukset niiltä osin, kun niillä on vaikutusta mahdolliseen pääsyyn muiden omistajien turvallisuusluokiteltuun tietoon.

4.16 Muutostenhallinta, elinkaari, huolto ja varmuuskopiointi

4.16.1 Toteutusesimerkki / TL IV-II

- Erillistyöaseman muutostenhallinnasta on käytössä suunniteltu menettely.
- Laiterikosta toipumiseen on menettelyt, jotka estävät turvallisuusluokitellun tiedon kulkeutumisen ulkopuolisille.
- Huoltotarpeille on menettelyt, jotka estävät turvallisuusluokitellun tiedon kulkeutumisen ulkopuolisille (erillistyöasema ei lähtökohtaisesti koskaan huoltoon, ei edes ilman tallennusmediaa).
- Erillistyöaseman ja muiden tallennemedioiden turvalliseen tuhoamiseen elinkaaren päättyessä on menettely, joka estää tiedon palauttamisen osin tai kokonaan (esimerkiksi organisaation itsensä valvomana erillistyöaseman sulattaminen, huomioiden myös tuhoamistodistukset ja vastaavat).
- Varmuuskopioiden suojaamisessa noudatetaan vastaavia menettelyjä kuin erillistyöaseman ja sen tallennusmedioiden suojaamisessa.

4.16.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje erillistyöaseman muutostenhallintamenettelyistä.
- Kuvaus/ohje erillistyöaseman huoltotoimenpiteistä.
- Kuvaus/ohje erillistyöaseman varmuuskopiointimenettelyistä.
- Kuvaus/ohje erillistyöaseman tuhoamiskäytännöistä.
- Tuhoamispöytäkirjat.
- Laitteisto- ja ohjelmistokirjanpito.

4.17 Turvallisuustyön tehtävien ja vastuiden määrittäminen

4.17.1 Toteutusesimerkki / TL IV-II

- Organisaatio on nimennyt henkilön, joka on vastuussa erillistyöaseman turvallisuudesta.
- Organisaatiossa on käytössä selkeä toimintamalli erillistyöaseman suojaamiselle hallinnollisen turvallisuuden, henkilöstöturvallisuuden, fyysisen turvallisuuden ja teknisen tietoturvallisuuden menettelyin.

4.17.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Organisaation työjärjestys, tehtäväkuvaukset ja vastaavat kuvaukset vastuista ja tehtävistä.

4.18 Turvallisuusohjeistus ja -koulutus

4.18.1 Toteutusesimerkki / TL IV-II

- Erillistyöaseman turvalliseen käyttöön ja ylläpitoon on ajantasainen ohje.
- Ohje on jalkautettu erillistyöaseman käyttäjille ja ylläpitäjille.
- Ennen EU:n ja Naton turvallisuusluokiteltujen tietojen käsittelyä, käyttäjät ja ylläpitäjät antavat tietojen suojaamista koskevan vakuutuksen.
- Erillistyöaseman turvallista käyttöä koskeva koulutus on säännöllistä ja koulutuksiin osallistuneista pidetään kirjaa.

4.18.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Erillistyöaseman turvallisen käytön ohje.
- Kuvaus ohjeen jalkauttamisesta.
- Erillistyöaseman käyttäjien ja ylläpitäjien antamat kirjalliset vakuutukset.
- Koulutusaineistot.
- Kirjanpito koulutukseen osallistuneista henkilöistä.
- Henkilöiden kuittaukset koulutukseen osallistumisesta.

4.19 Turvallisuuspoikkeamien hallinta

4.19.1 Toteutusesimerkki / TL IV-II

- Organisaatiolla on menettelytavat erillistyöasemaan ja siinä käsiteltävien tietojen tietoturvallisuuspoikkeamien asianmukaiseen käsittelyyn.
    - Ohjeistus ja menettely, jolla tapahtuneesta tai epäillystä turvallisuusluokitellun tiedon vaarantaneesta poikkeamasta saadaan välittömästi tieto organisaation sisällä.

- On määritetty, miten ja kenelle poikkeamista tai niiden epäilyistä tulee ilmoittaa.
- Organisaatio on selvittänyt millaiset tietoturvallisuuspoikkeamat edellyttävät viranomaisyhteydenottoa.
- Menettelytavat huomioivat sen, että tapahtuneesta tai epäillystä kansainvälisen turvallisuusluokitellun tiedon vaarantaneesta poikkeamasta on ilmoitettava välittömästi toimivaltaiselle turvallisuusviranomaiselle.

4.19.2 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Ohje ja kuvaus ohjeen jalkauttamisesta (vrt. 4.18).

4.20 Henkilöstön luotettavuuden arviointi

4.20.1 Toteutusesimerkki / TL IV

- Turvallisuusluokiteltuja tietoja käsittelevien henkilöiden luotettavuus selvitetään tarvittaessa hakemalla henkilöistä asianmukaisen laajuinen henkilöturvallisuusselvitys.
- On huomioitu, että EU:n tai Naton turvallisuusluokitellun tiedon käsittelyyn käytettävän erillistyöaseman ylläpitotehtäviin osallistuville voidaan edellyttää korkeamman luokan PSC:tä kuin mitä erillistyöasemassa käsiteltävät tiedot ovat.

4.20.2 Toteutusesimerkki / TL III-II

- Kansainvälisten tietoturvallisuusvelvoitteiden sitä edellyttäessä, esimerkiksi käsiteltäessä EU:n tai Naton turvallisuusluokiteltua tietoa, 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).

4.20.3 Esimerkki vaatimustenmukaisuuden osoittamisesta

- Kuvaus/ohje henkilöstön luotettavuuden arvioinnista
- Listaukset käyttäjistä ja henkilöturvallisuusselvitystodistusten tasoista.

5 Ohjeen voimassaolo ja jatkokehitys

Ohje on voimassa toistaiseksi ja sitä päivitetään tarvittaessa. Kehitysehdotukset ja lisätietokyselyt pyydetään lähettämään osoitteeseen ncsa (at) traficom (piste) fi.