Senaatin turvallisuusyksikkö 23.6.2020 SEN/327/2018

Toimittajan hallinnollinen tietoturvallisuus, tilaturvallisuus ja tietojenkäsittely-ympäristön turvallisuus (korotettu taso)

Tässä asiakirjassa kuvataan Senaatin Toimittajalle asetettavat hallinnollisen ja fyysisen tietoturvallisuuden sekä tietojärjestelmäturvallisuuden vaatimukset, mikäli Toimittaja käsittelee omissa tiloissaan tai omissa tietojärjestelmissään Senaatin tai sen Asiakkaan Salassa pidettävää tietoaineistoa (korkeintaan TL IV) tai henkilötietoa tai saa pääsyoikeuden Senaatin tai Senaatin asiakkaan tietojärjestelmiin tai toimitiloihin.

Toimittajan tulee noudattaa asiakirjan kohtia 1-6 toiminnassaan ja käsitellessään salassa pidettäviä tai turvallisuusluokiteltua TL IV -tietoja.

Turvallisuusluokiteltua TL III tai korkeamman tietoaineiston käsittely Toimittajan perustasolle hyväksytyissä tietojärjestelmissä ei ole missään tilanteessa sallittua.

TL III -tiedot tulee käsitellä suojaustason vaatimusten mukaisessa tilassa, joka on kuvattu asiakirjan kohdassa 8.

TL III -tietoaineistojen käsittelyä varten edellytetään aina vähintään erillinen verkosta eriytetty työasema. Työaseman vaatimukset on kuvattu asiakirjassa kohdassa 0.

Paperilla olevaa TL III -asiakirjaa voi yksittäistapauksissa käsitellä tilapäisesti Senaatin erillisellä luvalla Toimittajan perustason turvallisuusvaatimukset täyttävässä tilassa.

TL II tai korkeamman tietoaineiston käsittely ohjeistetaan ja sovitaan aina erikseen kirjallisesti.

1. TOIMITTAJAN HENKILÖSTÖ

Hallinnolliset turvallisuusvaatimukset (perustaso) koskevat Toimittajan hallinnollisen turvallisuuden menettelytapoja ja niiden toteutumista.

1. Palvelun toteuttamiseen osallistuvista henkilöistä tulee voida tehdä turvallisuusselvitykset ja edellyttää vaitiolositoumusta.

2. Toimittajan tulee ylläpitää ajantasaista listaa Senaatti-kiinteistöjen toimeksiannoissa työskentelevistä henkilöistä.

2. RISKIENHALLINTA

Toimittajan ja sen alihankkijan tulee täyttää alla esitetyt perustason vaatimukset TL IV-tietojen käsittelyyn, mikäli Toimittajan toimitiloissa käsitellään salassa pidettävää tai turvallisuusluokiteltua tietoaineistoa (TL IV).

1. Toimittajaorganisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit. Riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.

2. Riskienarviointi kattaa turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu tarvittavien sidosryhmien osalta.

3. Mikäli tarpeen; organisaation turvallisuuden hallinta kattaa turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty ja koulutettu ja tehtävä on osa henkilön toimenkuvausta.

3. TIETOTURVAKÄYTÄNNÖT

Salassa pidettävää tietoja tulee käsitellä niin, ettei niiden luottamuksellisuus ja eheys vaarannu missään vaiheessa tiedon elinkaarta.

1. Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella. Tietosisällöltään salassa pidettävät (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa/turvallisuusluokitusta kuvaavalla merkinnällä. Tiedot luokitellaan Senaatin tai sen asiakkaan tekemän luokittelupäätöksen mukaisesti. Toimeksiantoon liittyvän aineiston osalta käytettävän suojaustason toimittajalle vahvistaa aina Senaatti.

2. Pääsy salassa pidettävään tietoon tulee rajata vain tiedon käsittelyyn oikeutetuille ja tietoa työtehtävissään tarvitseville henkilöille.

   2.1. Pääsyoikeuden haltijat tulee olla selvitettävissä.

   2.2. Pääsyoikeuksien myöntö, muutto ja poisto tulee olla ohjeistettu ja dokumentoitu ajantasaisesti.

3. Tiedon käsittelyyn liittyvät käytännöt (ohjeet, säännöt ja prosessit) on määritelty Senaatti-kiinteistöjen salassa pidettävän ja henkilötietoja sisältävän tietoaineiston käsittelyohjeessa palveluntuottajille. Ohjeessa kuvatut toimintatavat on tiedotettu ja koulutettu käsittelijöille.

3.1. Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä.

3.2. Huolehditaan siitä, ettei neuvottelutiloihin jää salassa pidettävää tietoa sisältäviä asiakirjoja tai muita muistiinpanoja kokousten jälkeen.

3.3. Salassa pidettävää tietoa sisältävät laitteet on salattu ja suojattu vahvalla salasanalla.

3.4. Organisaatiolla on ohjeistukset ja käytännöt turvalliselle sekä matka- että etätyön tekemiselle.

4. Tarpeettomat tiedostot tulee tuhota ja tulosteet palauttaa suojaustasoluokituksen edellyttämällä tavalla Senaatin tietoaineiston käsittelyohjeen mukaisesti. Tietojärjestelmien käytön yhteydessä syntyvät suojattavaa tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti.

4.1. Salassa pidettävän ja turvallisuusluokittelun sähköisten aineistojen hävittäminen tapahtuu luotettavasti (ylikirjoitus tai tallenteen fyysinen tuhoaminen) Senaatin tietoaineiston luokittelu- ja käsittelyohjeessa tarkemmin kuvatulla tavalla,

4.2. Ei-sähköisten salassa pidettävien ja turvallisuusluokiteltujen aineistojen tuhoaminen on järjestetty luotettavasti Senaatin tietoaineiston luokittelu- ja käsittelyohjeessa (turvallisuussopimuksen liite 2) kuvatulla tavalla.

4. KOULUTUS

1. Palveluntuotantoon nimettävien henkilöiden hyväksyntä edellyttää, että Senaatin sähköinen turvallisuus- ja tietoturvakoulutus on suoritettu.

2. Toimittajaorganisaatiolla on menettely ja ohjeistus, jolla varmistetaan tarvittava tietoturvaosaaminen tietojen käsittelyä ja säilytystä varten.

3. Toimittajaorganisaatiolla on dokumentoitu menettelytapa ja ohjeistus poikkeamanhallintaan, muutoksenhallintaan sekä kouluttamiseen ja koulutuksen seurantaan.

5. YHTEISTOIMINTA

1. Toimittaja ja Senaatti-kiinteistöt määrittelevät yhteistyön viestintämallin yhteyshenkilöineen.

1.1. Määritetään kontaktihenkilöt ja heidän varahenkilöt / taho.

1.2. Osapuolet ylläpitävät ajantasaista listaa projektiorganisaatiosta ja tiedottavat muutoksista ennalta määriteltyjen periaatteiden mukaan.

1.3. Vastuut voidaan tarvittaessa määrittää tai täsmentää tarkemmin erilliseen liitteeseen. Turvallisuussopimuksen laadinnan yhteydessä nimetään vastuuhenkilöt (turvallisuussopimuksen liite 1 ja 6)

1.4. Toimittajalla on prosessit muutoksen- ja poikkeamanhallintaan. Muutoksista, poikkeamista ja tietoturvan nykytilasta raportoidaan ennalta määriteltyjen periaatteiden mukaan esimerkiksi seurantakokouksissa.

1.5. Toimittajan turvallisuussopimuksen yhteyshenkilö raportoi tietoturva-asioista Senaatin tietoturvallisuuden vastuuhenkilölle ongelmatilanteiden ilmetessä.

1.6. Toimittaja reagoi palvelun/hankinnan kohteeseen liittyviin tietoturvapoikkeamiin viivytyksettä, pitää niistä kirjaa ja raportoi ne Senaatti-kiinteistöjen edustajille sovittujen vastuiden mukaisesti.

2. Toimittaja on Senaatin pyynnöstä velvollinen hyväksyttämään Senaatilla Turvallisuussopimuksessa tarkoitettujen henkilöiden lisäksi sellaiset Toimittajan henkilöt, jotka voivat pääsyoikeuksiensa perusteella keskeyttää tai vaarantaa Senaatin tietojärjestelmien toiminnan taikka vaarantaa tietojärjestelmän tietoturvallisuuden. Senaatti voi hakea tällaisista henkilöistä tarvittaessa henkilöturvallisuusselvityksen.

3. Toimittajan henkilölle myönnetyt Senaatin avaimet/kulkutunnisteet, henkilökortit ja kulkuluvat palautetaan Senaatille sekä käyttäjätunnukset ja pääsyoikeudet poistetaan ilman viivytystä, kun henkilö ei enää osallistu Palvelun tuottamiseen ja;

4. Sopimuksen päätyttyä Toimittaja palauttaa ilman viivytystä Senaatille tämän avaimet/kulkutunnisteet, henkilökortit, kulkuluvat, salausavaimet, lisenssit, kulkukoodit, käyttäjätunnukset, salasanat, muut tunnistautumisvälineet sekä muun Senaatin luovuttaman omaisuuden ja sulkee sopimuksen nojalla avaamansa tietoliikenne-, tietojärjestelmä-, tiedonsiirto- sekä etäkäyttöyhteydet.

6. FYYSINEN TURVALLISUUS (TOIMITTAJAN TOIMITILAT)

Toimittajan ja sen alihankkijan tulee täyttää alla esitetyt perustason vaatimukset salassa pidettävien ja TL IV-tietojen käsittelyyn tarkoitettujen tilojen osalta, mikäli Toimittajan toimitiloissa käsitellään salassa pidettävää tai turvallisuusluokiteltua tietoaineistoa (TL IV).

Ellei ko. tietoja käsitellä toimittajan toimitiloissa, alla olevat kohdat voi poistaa.

Turvallisuuden osa-alue	Vähimmäisvaatimus
1. Ympäröivät rakenteet	Normaalit seinä, katto-, välipohja- ja lattiarakenteet. Ei erityisiä vaatimuksia.
2. Ovi- ja ikkunarakenteet	Normaalit ovi- ja ikkunarakenteet. Ei erityisiä vaatimuksia.
3. Äänieristys	Äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena salassa pidettävään tai TL IV tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan salassa pidettävästä tai TL IV tiedoista, joihin kaikilla ei ole tiedonsaantioikeutta. Äänieristysvaatimus kohdistuu alueen niihin tiloihin, joissa keskustellaan salassa pidettävästä tai TL IV tiedoista. Esimerkki ääneneristävyydestä: a) seinärakenteille 44dB b) oville 42dB c) ilmaääneneristävyys viereisiin tiloihin 40dB.
4. Salaa katselun estäminen	Salassa pidettävän tai turvallisuusluokitellun aineiston salaa katselu, vahingossa tapahtuva mukaan lukien, käsittelyn aikana on estettävä. Tilan lasipinnat voidaan suojata sälekaihtimilla, verhoilla tai kiinteillä kalvoilla. Salaa katselun riskiä voidaan pienentää myös esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä tietokoneen näytönsuojia.
5. Pääsy tilaan	Itsenäinen pääsy käsittely- ja säilytystiloihin tulee olla vain asianmukaisesti tunnistetuilla ja valtuutetuilla henkilöillä
6. Pääsynhallinta	Pääsyn hallinta alueelle voidaan toteuttaa joko mekaanisesti (lukitus), elektronisesti (sähköinen kulunvalvonta) tai henkilökohtaiseen tunnistamiseen perustuen.
7. Vastuuhenkilö	Tiloille on nimetty vastuuhenkilö ja tälle varahenkilö, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta.
8. Avainhallinta / Pääsyoikeuksien hallinta	Toimittaja on määritellyt ja ottanut käyttöön ainakin seuraavat menettelyt ja roolit: 1. pääsyoikeuksien ja avainten hallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu. 2. pääsyoikeuksien ja avainten haltijoista on lista. 3. pääsyoikeudet tarkastetaan säännöllisesti ja ne pidetään ajan tasalla. 4. avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet ovat vastuutettu. • Avainkortteja, jakamattomia avaimia ja kulkutunnisteita säilytetään asianmukaisesti.
9. Aineiston säilytys	Salassa pidettävä tai TL IV aineisto (ml. paperit, muistivälineet ja vastaavat) tulee säilyttää vaatimukset täyttävässä kassakaapissa (SFS-EN 1143-1 Euro II tai vastaava). Alle 1000 kg:n painoinen kassakaappi tulee kiinnittää lattiaan pulttaamalla TAI

	Soveltuvassa lukitussa toimistokalusteessa ja tila tulee valvoa rikosilmoitinjärjestelmällä (vähintään FA taso 2 ja riittävä vartioinnin vasteaika).
10. Turvallisuustekniset järjestelmät	Tilan läheisyyttä ja sitä ympäröivää aluetta valvotaan tallentavalla kameravalvonnalla.
11. Turvallisuusteknisten järjestelmien ylläpito	Käytettävät turvallisuusjärjestelmät pidetään toimintakuntoisina huolehtimalla tarvittavista korjaus- ja huoltotoimenpiteistä, toiminnan testauksista sekä dokumentaation ajantasaisuudesta laitevalmistajan ohjeiden ja suositusten mukaisesti.

7. TEKNINEN TIETOTURVA

Tilaajaan erikseen ilmoittaessa salassa pidettävä tai TL IV tietoaineisto tulee käsitellä erilliskoneella:

- Erilliskone tulee koventaa kohdassa 9 kuvatun mukaisesti, mutta se ei saa olla sama turvakone jolla käsitellään TL III tietoaineistoa.
- Verkosta eriytettyä TL IV erilliskonetta, voi käyttää yrityksen TL IV käsittelyyn hyväksytyissä tiloissa.
- TL IV erilliskonetta voi säilyttää yrityksen TL IV käsittelyyn hyväksytyissä tiloissa.

Mikäli erikseen ei ole ilmoitettu salassa pidettävää tai TL IV tietoaineistoa voidaan käsitellä Toimittajan verkkoympäristössä. Tällöin Toimittajan tietojenkäsittely-ympäristössä käytettävien tietokoneiden ja muiden päätelaitteiden on täytettävä seuraavat tekniset perustason tietoturvallisuusvaatimukset silloin kun ne ovat liitetty julkiseen Internet-verkkoon tai toimittajan sisäiseen tietoverkkoon ja niillä käsitellään salassa pidettävää tai turvallisuusluokiteltua tietoaineistoa (TL IV).

Ellei ko. tietoja käsitellä toimittajan tietojärjestelmissä, alla mainitut vaatimukset voi poistaa.

1. Salassa pidettävä tai turvallisuusluokiteltu tieto tulee käsitellä kaikissa vaiheissa vain Suomessa sijaitsevissa tietojärjestelmissä.

2. Toimittajan lähiverkko tulee olla eriytetty internetistä palomuurilla. Toimittajan tulee laatia verkkokuva, jossa on kuvattuna verkon rakenne ja olennaiset tietoturvallisuuteen vaikuttavat tekniset ratkaisut.

3. Toimittajan tulee arvioida ja hallita käyttämiinsä laitteisiin ja laiteympäristöihin kohdistuvia riskejä.
   3.1. Riskienarvioinnin tulee olla säännöllistä.
   3.2. Riskienhallinnassa tulee tarkastella salassa pidettävän ja turvallisuusluokitellun tiedon luottamukseen, eheyteen ja saavutettavuuteen vaikuttavia tekijöitä. Tiedon luottamuksellisuuteen ja saavutettavuuteen liittyen tulee erityisesti tarkastella jäljitettävyyttä, autentikaatiota ja auktorisaatiota.

4. Salassa pidettävää ja turvallisuusluokiteltua tietoa käsittelevien järjestelmien tulee täyttää vähintään seuraavat minimivaatimukset:
   4.1. Pääsyä salassa pidettävää ja turvallisuusluokiteltua tietoa sisältäviin järjestelmiin tulee rajata pienimpien tarvittavien oikeuksien mukaisesti.
   4.2. Järjestelmän käyttö tai hallinta ei tule olla mahdollista ilman käyttäjän tunnistamista ja todentamista.
   4.3. Käyttäjät tunnistetaan käyttäjätunnus-salasana –parilla, luotettavalla biometrisellä tunnisteella (sormenjälki) tai toimikortilla (”älykortti”) henkilökohtaisen PIN-koodin kera.
   4.4. Ylläpito ja pääkäyttäjätunnukset sekä normaalit käyttäjätunnukset ovat henkilökohtaisia. Mikäli ylläpitotunnukset eivät voi olla henkilökohtaisia, tulee ylläpitotoimet ja tunnuksien käyttö voidaan kohdentaa yksittäiseen henkilöön.
   4.5. Monivaiheista tunnistusta käytetään, mikäli järjestelmä tukee sitä.
   4.6. Usean virheellisen kirjautumisyrityksen jälkeen tulee tunnus lukittua.
   4.7. Järjestelmän kirjautumisista jää merkintä lokeihin.

5. Laitteen tai median jossa salassa pidettävää tai turvallisuusluokiteltua tietoa käsitellään, tai siirretään, tulee olla vahvasti salattu.

6. Laitteen tulee lukittua automaattisesti, mikäli laite on käyttämättä esimerkiksi 15 minuuttia.

7. Laitteessa tulee olla ajantasainen virus- ja haittaohjelmasuojaus, kovalevyn salaus sekä palomuuri kytkettynä käyttöön.

8. Tiedosta tulee ottaa varmuuskopioita. Varmuuskopioita tulee käsitellä vastaavasti kuin itse salassa pidettävää tai turvallisuusluokiteltua tietoa (salaus, huolellinen säilytys). Salassa pidettävää tai turvallisuusluokiteltua tietoaineistoa ei saa tallentaa Suomen rajojen ulkopuolelle (ml. tietojen varmistusratkaisut).

9. Laitetta käytettäessä tulee huolehtia, ettei tiedon luottamuksellisuus vaarannu (esim. työskentely julkisella paikalla).

10. Organisaatiossa on olemassa uusien järjestelmien, järjestelmäpäivitysten ja vastaavien hyväksymiskriteerit. Vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä käytetään.

11. Salassa pidettävän ja turvallisuusluokitellun TL IV käsittelyyn käytetään vain Senaatti-kiinteistöjen hyväksymiä verkkoja ja järjestelmiä. Hyväksyntä voidaan tehdä turvallisuusauditoinnilla tai toimittajan hyväksynnän yhteydessä turvallisuuden hallinnan kuvauksen katselmoinnilla.

12. Aina, kun liikenne kulkee julkisen verkon (Internet, puhelinverkko, GSM-verkko, tai muu verkko, mikä ei ole vaatimusten mukainen) kautta, on liikenne (tai aineisto) salattava luotettavasti siirrettäessä salassa pidettävää tai turvallisuusluokiteltuja (max. TL IV) mukaisia tietoaineistoja.

12.1. Työasemalla tulee olla Senaatti-kiinteistöjen hyväksytty tiedostojen salausohjelma

13. Käytössä on selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpitäjille).

TL III -TIETOJEN JA TIETOAINEISTOJEN KÄSITTELYN VAATIMUKSET

8. FYYSINEN TURVALLISUUS (KOROTETUN TURVALLISUUSTASON TILA)

TL III -tietojen käsittelyn ja säilytyksen osalta vaaditaan erillinen korotetun turvallisuustason tila, jonka tulee täyttää seuraavat vaatimukset:

Turvallisuuden osa-alue	**Vähimmäisvaatimus**
1. Ympäröivät rakenteet	Tilan seinät, katto ja lattia on oltava betonia, terästä, tiiltä tai vahvaa puuta. Puutteelliset rakenteet on vahvennettava Senaatin erillisohjeen mukaisesti. Erillisohjeen saa pyytämällä osoitteesta turvallisuus@senaatti.fi, kun osoittaa mihin Senaatin toimeksiantoon tilaa ollaan rakentamassa. Seinäelementtejä ei saa voida irrottaa kokonaisina tilan ulkopuolelta. Tilan kuoressa ei saa olla muita aukkoja, kuin rikosilmoitinjärjestelmällä valvottuja ovia, ikkunoita tai savunpoisto- ja ilmanottoaukkoja. Aukot voidaan sulkea kalteroinnilla tai vahvoilla terässäleiköillä. Tilaan ei saa olla näköyhteyttä ulkopuolelta.
2. Ovi- ja ikkunarakenteet	Tilan ovien on täytettävä SFS-EN1627 -standardin 3. murronkestoluokan vaatimukset. Ovien rakenteita tarkastettaessa on lisäksi kiinnitettävä huomiota karmin rakenteeseen. Oven ja karmin välykseen, sekä karmien kiinnitykseen seinärakenteeseen. Karmirakenteen on estettävä kiinnitysruuvien sahaaminen ulkoapäin. Välys oven ja karmin välillä max. 2 mm.
3. Ikkunarakenne	Maatason (alle 4 m) ikkunat on suojattava turvalasilla (SFS-EN 356 / P6B), tai sitä turvallisemmalla järjestelyllä. Lisäksi huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne. Kattoikkunat (tai kattotasanteiden tasolla olevat ikkunat) on suojattava turvalasilla (SFS-EN 356 / P6B), tai sitä turvallisemmalla järjestelyllä. Lisäksi huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne.
4. Äänieristys	Äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena TL III tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan TL III tiedoista, joihin kaikilla ei ole tiedonsaantioikeutta. Äänieristysvaatimus kohdistuu alueen niihin tiloihin, joissa keskustellaan TL III tiedoista. Kaapelikouruja tai -hyllyjä ei saa mennä suoraan tilasta toiseen. Kaapelikouruihin äänieristemateriaalin lisääminen tarvittaessa, ilmastointikanaviin vastaavan tasoiset ääniloukut.

	Esimerkki ääneneristävyydestä: a) seinärakenteille 44dB b) ovelle 42dB c) ilmaääneneristävyys viereisiin tiloihin 40dB.
5. Salaa katselun estäminen	Salassa pidettävän tai turvallisuusluokitellun aineiston salaa katselu, vahingossa tapahtuva mukaan lukien, käsittelyn aikana on estettävä. Tilan lasipinnat on suojattava sälekaihtimilla, verhoilla tai kiinteillä kalvoilla ja ikkunat eivät saa olla avattavissa. Salaa katselun riskiä voidaan pienentää myös esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä tietokoneen näytönsuojia.
6. Pääsy tilaan	Itsenäinen pääsy tilaan tulee olla vain asianmukaisesti tunnistetuilla ja valtuutetuilla henkilöillä.
7. Pääsynhallinta	Tila on valvottava sähköisellä kulunvalvonnalla siten, että vain hankkeeseen tai projektiin oikeutetuilla henkilöillä on pääsy tilaan Tilaan kulku voidaan myöhemmin todentaa.
8. Vastuuhenkilö	Tilalle on nimetty vastuuhenkilö ja tälle varahenkilö, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta.
9. Lukitus	Tila on lukittava aina, kun se ei ole miehitetty. Käyttölukko vyöhykkeen rajalla FA:n varmuusluokka 1. Vyöhykkeen rajalla varmuuslukko, varmuusluokka 3. Vyöhykkeen sisällä käyttölukko Tilaan ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. Tilan yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos tiloista on kielletty.
10. Avainhallinta / Pääsyoikeuksien hallinta	Toimittaja on määritellyt ja ottanut käyttöön ainakin seuraavat menettelyt ja roolit: pääsyoikeuksien ja avainten hallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu. a) pääsyoikeuksien ja avainten haltijoista on lista. b) pääsyoikeudet tarkastetaan säännöllisesti ja ne pidetään ajan tasalla. c) avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet on vastuutettu. d) avainkortteja, jakamattomia avaimia ja kulkutunnisteita säilytetään asianmukaisesti.
11. Aineiston säilytys	Tilassa on oltava kassakaappi (vähintään Euro II SFS-EN 1143-1) tai holvi (vähintään Euro IV), jossa TL III tietoaineisto tulee säilyttää. Alle 1000 kg:n painoinen kassakaappi tulee kiinnittää lattiaan pulttaamalla
12. Turvallisuustekniset järjestelmät, kameravalvonta	Tilaa tai sitä ympäröivää aluetta valvotaan tallentavalla ja tunnistettavan tallennekuvan tuottavalla kameravalvonnalla. Tallennusaika tulee olla riittävä,

	vähintään 30 vuorokautta. Huomioitava mahdollisen alueen kameravalvontajärjestelmän vaatima riittävä valaistus myös pimeällä.
13. Turvallisuustekniset järjestelmät, rikosilmoitinjärjestelmä	Tilassa on oltava rikosilmoitinjärjestelmä (vähintään 3-luokka). Ovet, aukot, ikkunat ja tilat on valvottava.
14. Turvallisuustekniset järjestelmät, ilmoituksensiirto	Rikosilmoitinjärjestelmä ja ilmoituksensiirto testataan kerran kuukaudessa. Vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä ja vasteajan testaus tulee tehdä kerran vuodessa. Testaukset tulee dokumentoida.
15. Turvallisuusteknisten järjestelmien ylläpito	Käytettävät turvallisuusjärjestelmät pidetään toimintakuntoisina huolehtimalla tarvittavista korjaus- ja huoltotoimenpiteistä, toiminnan testauksista sekä dokumentaation ajantasaisuudesta laitevalmistajan ohjeiden ja suositusten mukaisesti. Turvajärjestelmien oikeuksienhallinnassa noudatetaan vähimpien oikeuksien periaatetta.
16. Tilaan kohdistuvat ylläpitotoimet	Tilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat valvottuna vain tilaan hyväksytyn henkilön toimesta. Turvallisuusluokkaan III kuuluvan aineiston käsittely tilassa huoltotöiden aikana kielletty.

9. TL III TIEDON KÄSITTELYYN HYVÄKSYTTÄVÄN TIETOKONEEN/PÄÄTELAITTEEN TEKNISET TIETOTURVALLISUUSVAATIMUKSET

TL III -tietojen käsittelyn osalta vaaditaan erillinen turvatyöasema, jonka tulee täyttää seuraavat vaatimukset:

	Vähimmäisvaatimus
1. Yleiset vaatimukset	- Alla olevissa asiakohdissa kuvataan, miten käyttöön otettavien TL III-päätelaitteita hallitaan ja miten työasemat määritellään ja mitä kovennuksia niihin tulee tehdä. - Mikäli toimittajalle on luovutettu käyttöön valtion omistamia laitteita, tulee niitä säilyttää ja käsitellä tässä kuvatun mukaisesti. - Ensisijaisesti laitteet ovat toimittajan verkosta irrallaan olevia eriytettyjä päätelaitteita, joita tulee säilyttää ja joita voidaan käyttää ainoastaan edellä todetussa korotetun tason vaatimukset täyttävässä tilassa. - Mikäli toimittajalla on käytössä turvatilaan toteutettu fyysisesti eriytetty, suljettu verkko, se voidaan tapauskohtaisesti katselmoida ja hyväksyä auditoinnin yhteydessä. Eriytetystä verkosta ei saa olla yhteyksiä internetiin.
2. Omaisuudenhallinta	- Turvatyöasemat ovat toimittajan omaisuutta. Toimittajalla tai sen alihankkijalla tulee olla laitteista erillinen laiterekisteri. - Laiterekisterin ylläpito on vastuutettu toimittajan tai sen alihankkijan nimeämille turvaselvitetyille henkilöille. - Laiterekisteristä tulee käydä ilmi työaseman hankintapäivä, asennuspäivä, sarjanumero, laitetiedot (suoritin, muisti, kiintolevyt) sekä työaseman yksilöivä tunniste. Laiterekisteriä päivitetään, kun laitteita uusitaan tai niitä poistuu palvelusta sekä kaksi kertaa vuodessa tehtävän turvatyöasemien päivityksen yhteydessä. Laiterekisteri tulee esittää pyydettäessä Senaatille.
3. Turvatyöasemien käyttöönotto ja käytöstä poisto	-Turvatyöasemien asennuksesta on laadittava asennuspöytäkirjaa, joka tehdään jokaisesta työasemasta. Pöytäkirjasta käy ilmi asennuksen tekijä ja päivämäärä sekä siinä on asentajan allekirjoitus. - Kun työasema poistetaan käytöstä joko vanhentuneena tai rikkoutuneena suoritetaan kiintolevyn turvallinen tyhjennys ja muut tarvittavat poistoon liittyvät toimenpiteet ja se kirjataan laiterekisteriin käytöstä poistetuksi.
4. Käyttöympäristö	- Turvatyöasemien käyttö on rajattu siten, että niitä saa käyttää vain Senaatin toimeksiannoissa.
5. Käyttöoikeudet	- Turvatyöasemilla on käytössä paikallisesti määritellyt käyttöoikeudet. Jokaisella työasemalla on käyttäjän henkilökohtaisen tunnuksen lisäksi ”Järjestelmänvalvoja”-tunnus ylläpitotoimia varten. Näille tunnuksille asetetaan käyttöönoton yhteydessä vahvat salasanat. ”Järjestelmänvalvoja”-tunnuksen salasanaa ei saa luovuttaa peruskäyttäjälle. - Loppukäyttäjän tunnuksella pystyy käyttämään työasemaa ja siihen asennettuja ohjelmistoja tämän ohjeen kuvaamalla tavalla. Käyttöoikeuksilla ei saa olla mahdollista tehdä mitään ylläpidollisia toimia.

	- Salasanan vähimmäispituus tulla olla määritetty (suositus 10 – 14 merkkiä), salasanassa pitää olla merkkejä vähintään kolmesta luokasta (pienet kirjaimet, isot kirjaimet, numerot ja erikoismerkit), salasanan enimmäisikä on 90 päivää, salasanan vähimmäisikä on yksi päivä, salasana ei saa olla sama kuin viisi edellistä salasanaa, salasana lukitaan esim. viiden virheellisen yrityksen jälkeen ja vapautetaan vasta ylläpidon toimesta. - Kaikissa järjestelmissä teknisistä syistä ei ole mahdollista noudattaa kaikkia tässä kuvatun mukaisia salasanavaatimuksia. Tällöin tästä kuvatusta menettelystä poikkeava toteutustapa ja mahdolliset korvaavat menettelyt tulee dokumentoida.
6. Pääsynhallinta	-Turvatyöasemilla lokitetaan onnistuneet ja epäonnistuneet kirjautumisyritykset käyttöjärjestelmän tapahtumalokeihin. Lokeja voi lukea tavallisilla käyttäjätunnuksilla, mutta niiden tyhjentämiseen tulee edellyttää ”Järjestelmänvalvoja” -tunnuksen oikeuksia. -Mikäli työasemaan yritetään kirjautua väärällä salasanalla riittävän monta kertaa, tunnus lukkiutuu.
7. Päätelaite	-Turvatyöasemissa käytettävä laitemalli on hyvä vakioida mahdollisuuksien mukaan useammaksi vuodeksi kerrallaan. Tällä taataan ympäristön vakaus, varaosien saatavuus ja sovellusten yhteensopivuus. - Eriytetyssä ympäristöissä voidaan käyttää toimittajan omaan käyttöönsä vakiomaa laitemallia. Työasemat on merkittävä yksilöivän tunnisteen lisäksi tarralla, joka kertoo työaseman olevan hyväksytty Senaatin käyttöön.
8. Kovennetun turvatyöaseman tekniset määritykset	- BIOS on salasanasuojattu vahvalla salasanalla - TPM laite on kytketty päälle - TPM laitetta hallitaan käyttöjärjestelmätasolta - TPM laitteen saa resetoitua käyttöjärjestelmästä - TPM laite ei resetoituessaan palaudu tehdasasetuksiin - Käynnistäminen on sallittu vain ensisijaiselta kiintolevyltä (BIOS-asetus) - 3G/4G/5G, WLAN, LAN ja Bluetooth adapterit on kytketty pois käytöstä (BIOS-asetus) - Käyttöjärjestelmätaso (vähintään Windows 10, 64 bit, versio 1809. Huom. Windows 10 Home-versio ei ole sallittu, koska BitLocker ei ole käytettävissä) - Työaseman massamuisti on salattu käyttöjärjestelmään integroidulla salaussovelluksella - Tietoturvapäivitykset on asennettu asennushetkellä vallitsevan hyväksytyn tason mukaisesti - Tarpeettomat palvelut on kytketty pois käytöstä - Windows palomuuri on konfiguroitu estämään kaikki tietoliikenne niin sisään kuin ulospäin -Koneella tulee olla Senaatin hyväksymä tiedostojen salausohjelma -Koneissa voidaan käyttää toimittajan tai sen alihankkijan ympäristössä hyväksyttyä virustorjuntaohjelmistoa. Ohjelmiston tulee mahdollisuuksien mukaan tarkistaa kaikki työasemalle siirrettävät tiedostot automaattisesti sekä suorittaa ajastetun skannauksen kerran päivässä. Ohjelmiston tietoturvakuvaukset ovat siltä hetkeltä, kun työasema on asennettu.
9. Työaseman asentaminen	-Työasemien asentamiseen on hyvä käyttää esimerkiksi levykuvaa tai jotakin muuta automatisoitua asennustapaa. Koneiden asennukseen liittyvät käytänteet toimittaja voi laatia

	oman organisaationsa hyväksymien asennustapojen mukaisesti. Työasemat voidaan asentaa myös ns. käsin suoritetulla asennuksella. -Laiterekisterin yhteyteen tulee laatia tarkka kuvaus ja asennusohje, työasemaan asennettavista ohjelmistoista sekä niiden asetuksista. - Asennuksen jälkeen työasemaa ei saa kytkeä Internet-verkkoon.
10. Oheislaitteet	-Työasemissa saa käyttää vain erikseen hyväksyttyjä oheislaitteita. - Hyväksytyt laitteet (ml. tulostimet ja massamuistit) tulee kirjata laiterekisteriin. - Muistit tulee salata.
11. Päätelaitteella käsiteltävä tieto	- Turvatyöasemat on hyväksytty TL III tasoisen tiedon käsittelyyn Senaatin tietojenkäsittelyohjeen mukaisesti. - TLIII luokiteltua tietoa saa tallentaa muistivälineille (kiintolevyt, siirrettävät muistit) mikäli se on salattuna Senaatin hyväksymällä salausohjelmistolla. Muistivälineitä tulee säilyttää turvatilassa olevassa kassakaapissa.
12. Päätelaitteiden päivittäminen	- Koska turvatyöasemia ei ole mahdollista liittää Internet-verkkoon päivitykset tulee järjestää manuaalisesti esimerkiksi asennusimagen kautta. Työasemat voidaan päivittää myös ns. käsin suoritetulla asennuksella. - Ympäristöön tehtävistä päivityksistä tulee laatia laiterekisterin yhteyteen tarkka kuvaus, päivitetyistä ohjelmistoista sekä niiden asetuksista. - Mahdollinen asennusimage on syytä päivittää vähintään kerran vuodessa ja useammin mikäli palvelua kohtaan syntyy uhka, joka riskianalyysin avulla vahvistetaan niin korkeaksi, että päätetään suorittaa kiireellinen päivitys. Päivitystarpeen analysointi ja päätöksenteko on tietokoneen omistajan tai haltijan vastuulla.
13. Varmuuskopiointi	- Turvatyöasemat eivät ole minkään varmistuspalvelun piirissä. Tästä johtuen toimittajan on suunniteltava ja dokumentoitava menettelytapa tietojen varmistuskopiointia varten. Varmistukset voidaan tehdä erilliselle salatulle kovalevylle. Kovalevyä tulee säilyttää turvatilan kassakaapissa. - Toimittajan ja työaseman käyttäjän vastuulla on se, että tärkeää aineistoa ei säilytetä työasemien kiinteillä massamuisteilla.

TARKISTUSLISTA TYÖASEMIEN ASENNUKSEEN

#	**Toimenpide**	**Suoritettu**
1	KÄYTTÖJÄRJESTELMÄ: Asennetaan ja määritellään virus- ja haittaohjelmantorjunta	
2	KÄYTTÖJÄRJESTELMÄ: Asennetaan viimeisimmät hyväksytyt tietoturvapäivitykset	
3	KÄYTTÖJÄRJESTELMÄ: Poistetaan käytöstä tarpeettomat palvelut (TCP/IP yms.)	
4	KÄYTTÖJÄRJESTELMÄ: Salataan kiintolevy	
5	KÄYTTÖJÄRJESTELMÄ: Määrittele peruskäyttäjän tunnus	
6	KÄYTTÖJÄRJESTELMÄ: Määrittele ”Järjestelmänvalvoja”-tunnus sekä estä ylimääräisten tunnusten käyttö	
7	KÄYTTÖJÄRJESTELMÄ: Asenna hyväksyttyjen lisälaitteiden laiteajurit	
8	BIOS: Asetetaan vahva salasana	
9	BIOS: Asetuksen määritellään TPM –laite	
10	BIOS: Sallitaan työaseman käynnistäminen vain ensisijaiselta kiintolevyltä	
11	BIOS: Poistetaan käytöstä kaikki verkkosovittimet (esim. 3G/4G/5G, WLAN, LAN)	
12	Liimaa turvaluokitus tarra työasemaan	
13	Päivitä tarvittavat tiedot laiterekisteriin	

Esimerkki TL III-turvatyöaseman merkitsemisestä

Senaatti

EI SAA LIITTÄÄ TIETOVERKKOON.

LAITTEEN KÄYTTÖ ON HYVÄKSYTTY VAIN ERIKSEEN NIMETTYIHIN HANKKEISIIN