Kysely- ja välityspalvelun tekniset tietoturvavaatimukset terveydenhuollon ulkopuolisille toimijoille

Tietoturvavaatimukset

16.2.2026

Versio 1.0.0

Kanta-palvelut

Julkinen

Kela
Kanta-palvelut
PL 450, 00056 Kela

FPA
Kanta tjänsterma
PB 450, 00056 FPA

www.kanta.fi
kanta@kanta.fi

Kanta-palvelut 16.2.2026

Muutoshistoria

Versio	Muutos	Tekijä	PVM
1.0.0	Ensimmäinen versio erillisestä Kysely- ja välitys-palveluun liittyvien terveydenhuollon ulkoisten toimijoiden tietoturvavaatimuksista	Kanta-palvelut	16.02.2026

Kanta

Kysely- ja välityspalvelun terveydenhuollon ulkoisten toimijoiden tietoturvavaatimukset

Kanta-palvelut 16.2.2026

Sisällys

1 Johdanto

Kysely-ja välityspalvelu on Kanta-palveluihin kuuluva tietojärjestelmäpalvelu, jonka avulla asiakastietoja välitetään sosiaali-ja terveydenhuollon ulkopuolisille toimijoille. Palvelun avulla voidaan välittää vain Kanta-palveluihin tallennettuja todistuksia ja lausuntoja. Kysely- ja välityspalvelua käytetään tällä hetkellä terveydenhuollon lomakeasiakirjoihin kuuluvien todistusten ja lausuntojen välitykseen. Nämä välitettävät määrämuotoiset asiakirjat ovat ensisijaisesti tarkoitettu sosiaali- ja terveydenhuollon ulkopuolisille tahoille, lähinnä muille viranomaisille, jotka käyttävät niitä esimerkiksi rekisteröintitarkoituksiin tai lupien tai etuuksien myöntämisprosesseissa.

Kysely- ja välityspalveluun liitytään DVV:n toteuttaman Palveluväylän kautta (Suomi.fi-palveluväylä - Suomi.fi kehittäjille). Palvelun käyttöä varten tulee Kysely- ja välityspalvelua käyttävän järjestelmän liittyä Palveluväylän käyttäjäksi.

1.1 Dokumentin rakenne

Tässä ohjeessa kuvataan Kysely- ja välityspalveluun liittyvälle terveydenhuollon ulkopuolisen toimijalle kohdistuvat tekniset tietoturvavaatimukset. Vaatimusten pohjana on käytetty JulKri - Henkilötietot ja Erityinen henkilötietoryhmä -kriteeristöä. Toteutusesimerkit on toteutettu terveydenhuollon ulkopuolisen toimijan liittymismallille Kanta-palveluiden Kysely- ja välityspalveluun.

Luvussa 1 kuvataan lyhyesti Kysely- ja välityspalvelu, dokumentinrakenne sekä viittaukset lainsäädäntöön sekä THL:n ohejeisiin. Informatiivisissa viittauksissa on listattu yleisiä tietoturvaan ja turvalliseen ohjelmistokehitykseen ohjeita ja malleja.

Luku 2 käsittelee laki- ja määräysperusteita tälle ohjeistukselle.

Tarkemmat tietoturvavavaatimukset ovat liitteenä 1 olevassa taulukossa.

1.2 Viittaukset

Viittaukset lähteisiin ovat joko erityisiä (julkaisupäivän ja/tai painoksen tai versionumeron perusteella) tai epäspesifisiä. Tiettyihin viittauksiin sovelletaan vain lainattua versiota. Epäspesifisiin viittauksiin sovelletaan viitatun asiakirjan viimeisintä versiota (mukaan lukien mahdolliset muutokset).

1.2.1 Normatiiviset viittaukset

Tietosuojalaki 1050/2018

Asiakastietolaki 703/2023

Määräykset - Tiedonhallinta sosiaali- ja terveysalalla - THL

- THL määräys 2/2024 Määräys valtakunnallisten tietojärjestelmäpalveluiden avulla terveydenhuollon ulkopuolelle välitettävistä asiakirjoista
- THL määräys 5/2024 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista
- Määräys 5/2024 liite 1: olennaisten vaatimusten soveltamisohjeet
- Liite 3f, Profiilit: Todistusten profiilit (.xlsx)

TLS cipher suitet suojaustasoille IV-III (Traficom)

Liite 1 Kysely- ja välityspalvelun tietoturvavaatimukset.xlsx

1.2.2 Informatiiviset viittaukset

Mikä on Palveluväylä? - Suomi.fi-palveluväylä - Suomi.fi kehittäjille

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) : Suositus ja kriteeristö - Valto

https://github.com/OWASP/ASVS/raw/v5.0.0/5.0/OWASP_Application_Security_Verification_Standard_5.0.0_en.pdf

CWE - CWE Top 25 Most Dangerous Software Weaknesses

Building Security Maturity Model (BSIMM) Consulting Services | Black Duck

OWASP SAMM | OWASP Foundation

Turvallinen tuotekehitys - kohti hyväksyntää | Kyberturvallisuuskeskus

2 Lainsäädäntöperusta

Terveydenhuollon todistusten ja lausuntojen arkistointi Kanta-palveluihin ja niiden välitys Kysely- ja välitys -palvelulla perustuu lakiin sosiaali- ja terveydenhuollon asiakastietojen käsittelystä.

Kanta-palvelun välittämät todistukset ja lausunnot koskevat pääsääntöisesti Tietosuojalain 1050/2018 6§ mukaisia henkilön erityisiä henkilötietoryhmiä (terveystietoja). Asiakastietolaki 702/2023 4 § asettaa Sosiaali- ja terveydenhuollon asiakastiedot pysyvästi salassa pidettäväksi.

2.1 Asiakastietolaki 703/2023, 66 §

Valtakunnallisten tietojärjestelmäpalvelujen ja sinne tallennettujen tietojen on oltava aina käytettävissä. Tietojärjestelmäpalveluilla on oltava tarpeelliset varajärjestelmät toimintahäiriöiden ja poikkeusolojen varalle. Seuraavan listauksen tummennetut kohdat koskevat Kysely- ja välityspalvelua.

Kansaneläkelaitoksen vastaa:

1) valtakunnallisten tietojärjestelmäpalvelujen edellyttämistä teknisistä määrittelyistä ja teknisistä ohjeista;
2) valtakunnallisiin tietojärjestelmäpalveluihin tallennettujen tietojen turvallisuuden varmistamisesta sekä tietojen hävittämisestä säilytysajan päättymisen jälkeen;
3) vastuullaan olevien valtakunnallisten tietojärjestelmäpalvelujen toteuttamisesta siten, että asiakas- tai hyvinvointietoja ja muita valtakunnallisiin tietojärjestelmäpalveluihin tallennettuja tietoja luovutetaan vain tämän lain ja sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019) mukaisesti;
4) asiakas- ja hyvinvointitiedon käytön ja luovutuksen tallentumisesta lokirekisteriin;
5) koodistopalvelun tietoteknisestä toteuttamisesta;
6) valtakunnallisiin tietojärjestelmäpalveluihin liittyvästä tiedottamisesta väestölle; sekä
7) valtakunnallisiin tietojärjestelmäpalveluihin liitettävien tietojärjestelmien ja hyvinvointisovellusten yhteentoimivuuden testaamisesta.

Kansaneläkelaitoksella on oikeus:

1) saada Sosiaali- ja terveydenhuollon lupa- ja valvontavirastolta valtakunnallisiin tietojärjestelmäpalveluihin liittyvien lakisääteisten tehtävien hoitamiseksi tarvittavat tiedot sosiaali- ja terveydenhuollon ammattihenkilöistä;
2) käsitellä asiakas- ja hyvinvointitietoja siltä osin kuin valtakunnallisten tietojärjestelmänpalvelujen ylläpitoon kuuluvat tehtävät välttämättä edellyttävät;
3) päättää järjestelmän tietotekniseen toimintaan liittyvistä asioista, jollei tästä laista tai sen nojalla annetuista säännöksistä muuta johdu;
4) antaa tahdonilmaisupalvelussa olevia luovutusten hallintaan liittyviä asiakirjoja ja niiden lokitietoja sosiaali- ja terveydenhuollon palvelunantajille asiakastietojen käytön ja luovutuksen seurantaa ja valvontaa varten, jos on ilmeistä, ettei siten vaaranneta turvajärjestelyjen toteutumista;
5) suorittaa palveluidensa ja palveluissa säilytettävien tietojen käyttöön sekä tietoliikenteeseen ja tietoliikenteen lokitietoihin kohdentuvaa valvontaa tietoturvan lisäämiseksi; sekä
6) salassapitovelvoitteiden estämättä saada Digi- ja väestötietovirastolta valtakunnallisia tietojärjestelmäpalveluita koskevien tehtävien hoitamiseksi tarvittavat välttämättömät tiedot.

Tietoturvallisuuden varmistamiseksi Kansaneläkelaitos ylläpitää valvontakeskusta sekä ryhtyy tarvittaviin toimenpiteisiin yhteistyössä palvelunantajien kanssa poikkeavaa toimintaa havaitessaan. Kansaneläkelaitoksen on viipymättä ilmoitettava Liikenne- ja viestintäviraston kyberturvallisuuskeskukselle havaitsemistaan tietoturvallisuusloukkauksista ja tietoturvallisuuden häiriöistä ja salassapitosäännösten estämättä annettava sille välttämättömät tiedot.

Kansaneläkelaitos voi laatia ja luovuttaa valtakunnallisten tietojärjestelmäpalveluiden ohjaamisesta, valvonnasta ja kehittämisestä vastaaville viranomaisille valtakunnallisissa tietojärjestelmäpalveluissa olevista tiedoista ja asiakirjojen kuvailutiedoista ja lokitiedoista yhteenvetoja, joilla on merkitystä valtakunnallisten palvelujen kehittämisessä, seurannassa tai raportoinnissa. Kansaneläkelaitos voi laatia ja luovuttaa palvelunantajalle sen omassa rekisterissä oleviin, valtakunnallisiin tietojärjestelmäpalveluihin tallennettuihin asiakastietoihin ja lokitietoihin perustuvia yhteenvetoja, joilla on merkitystä palvelunantajan toiminnan kehittämisessä, seurannassa, raportoinnissa ja valvonnassa. Yhteenvedot eivät saa sisältää henkilötietoja.

Valtakunnallisten tietojärjestelmäpalvelujen suojaamisessa noudatetaan sitä, mitä valtion viranomaisten ja kuntien tietoturvallisuutta koskevista velvoitteista erikseen säädetään. Kansaneläkelaitos ei saa antaa valtakunnallisten tietojärjestelmäpalvelujen järjestämiseen liittyvien tässä laissa tarkoitettujen rekisterien eikä niihin liittyvien lokirekistereiden käsittelyä tai säilyttämistä ulkopuolisten tehtäväksi.

2.2 Asiakastietolaki 703/2023, 76§

Valtakunnallisten tietojärjestelmäpalvelujen avulla saadaan välittää todistuksia, lausuntoja ja muita asiakastietoja sisältäviä asiakirjoja sosiaali- ja terveydenhuollon ulkopuoliselle toimijalle. Asiakirjoja saadaan salassapitosäännösten estämättä välittää asiakkaan pyynnön tai vastaanottajan lakiin perustuvan pyynnön taikka tiedon luovuttajan lakiin perustuvan tiedonantovelvollisuuden perusteella. Asiakirjojen välittäminen toteutetaan valtakunnalliseen tietojärjestelmäpalveluun kuuluvan Kysely- ja välityspalvelun avulla.

Terveyden ja hyvinvoinnin laitos antaa määräykset siitä, minkä tyyppisiä asiakirjoja saa välittää Kysely- ja välityspalvelun avulla.

2.3 THL määräys 2/2024

Asiakirjoja saa salassapitosäännösten estämättä välittää asiakkaan pyynnön tai vastaanottajan lakiin perustuvan pyynnön taikka tiedon luovuttajan lakiin perustuvan tiedonantovelvollisuuden perusteella.
Tämän määräyksen nojalla voidaan välittää ammattihenkilön tuottamia seuraavan tyyppisiä asiakirjoja sekä niiden tietosisältöjä sosiaali- ja terveydenhuollon ulkopuolisille tahoille:

- Lääkintölaillisia todistuksia ja lausuntoja sekä muita todistuksia, jotka vahvistetaan terveydenhuollon ammattihenkilöistä annetun lain 23 §:n mukaisesti.
- Muita lääkärintodistuksia ja lausuntoja, joissa selvitetään potilaan terveydentilaa ja jotka ovat välttämättömiä lausunnon vastaanottavan tahon tehtävien suorittamiseksi.

- Kuolemansyyn selvittämisestä annetussa asetuksessa (948/1973) tarkoitettuja, THL:n hyväksymiä ja vahvistamia kuolintodistuksiin liittyviä asiakirjoja.
- Muita terveydenhuollon asiakirjoja tai niiden määrättyjä tietosisältöjä, jotka ovat välttämättömiä vastaanottavan organisaation lakisääteisen tehtävän hoitamiseksi.
- Kysely- ja välityspalvelun kautta voidaan luovuttaa myös todistukseen ja lausuntoon tietoisesti liitetty muu yksilöity asiakirja.

Välitettävät tietosisällöt noudattavat THL:n eri tietorakenteiden jakelualustoilla julkaistuja kansallisia rakenteita.

Edellä luetellut todistukset, lausunnot ja asiakirjat tai niiden erikseen rajatut tietosisällöt saa välittää Kelan Kanta-palveluiden Kysely- ja välityspalvelun avulla niille tahoille, joilla on lainsäädännön perusteella oikeus kyseisiin asiakirjoihin ja asiakirjojen tietosisältöihin.

THL laatii todistusten, lausuntojen ja asiakirjojen tai niiden erikseen rajattujen tietosisältöjen välittämiseen liittyvät erilliset kansalliset toimintamallit sekä ohjeet todistuksia, lausuntoja ja asiakirjoja laativille ja vastaanottaville toimijoille. Lisäksi THL voi antaa ohjeita välitysperusteista ja siitä mitä todistuksia, lausuntoja ja asiakirjoja tai niiden erikseen rajattuja tietosisältöjä tai niihin tietoisesti liitettyjä muita yksilöityjä asiakirjoja voi Kysely- ja välityspalvelun avulla välittää terveydenhuollon ulkopuolelle.

Todistuksia vastaanottavan palvelun, joka on yhteydessä Kanta-palveluihin kuuluvaan Kysely- ja välityspalveluun hakeakseen sen kautta todistuksia, on noudatettava:

- Myöhemmin annettavaa sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisia vaatimuksia koskevaa THL:n määräystä 5/2024 ja sen liitteitä 3b ja 3f soveltuvin osin, lukuunottamatta liitteen 3f sisältämää Kanta-palveluihin todistuksia tai lausuntoja tuottavan palvelun profiilia.
- THL:n myöhemmin antamaa ohjetta Kysely- ja välityspalveluun liittyvien terveydenhuollon ulkopuolisten organisaatioiden liittymisen edellytyksistä.
- Voimassa olevia Kysely - ja välityspalvelun toiminnallisia määrittelyjä.

2.4 THL määräys 5/2024

Liite 3f, Profiilit: Todistusten profiilit

- 3f1: Kanta-arkistosta todistuksia tai lausuntoja kyselevä palvelu
- 3f2: Kanta-arkistosta todistuksia tai lausuntoja vastaanottava palvelu

3 Tietoturvavaatimukset

Kysely- ja välityspalvelun Tietoturvavaatimukset perustuvat JulKri-suosituksen arviointikriteereistä. Vaatimuksiin on nostettu henkilötietoja ja erityisiä henkilötietoryhmiä käsitteleville tietojärjestelmille annetut tietoliikenneturvallisuuden, tietojarjestelmäturvallisuuden sekä käyttöturvallisuuden vaatimukset.

Alla on kuvattu lyhyesti tietoturvavaatimukset. Vaatimukset on kuvattu tarkemmin liitteessä 1.

Taulukko 1 Tietoturvavaatimukset

Tunniste	Nimi	Vaatimus
TEK-01	**Verkon rakenteellinen turvallisuus**	Tietojenkäsittely-ympäristö on erotettu julkisista tietoverkoista riittävän turvallisella tavalla.
TEK-01.1	**Verkon rakenteellinen turvallisuus - salaus yleisissä tietoverkoissa**	Yleisessä tietoverkossa salassa pidettävää tietoa sisältävä tietoliikenne salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia tai vaihtoisesti siirto toteutetaan muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä.
TEK-01.2	**Verkon rakenteellinen turvallisuus - palomuuri**	Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuustasojen ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä.
TEK-02	**Tietoliikenne-verkon vyöhykkeistäminen**	Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava monitasoisen suojaamisen periaatteen mukaisesti.
TEK-03	**Suodatus- ja valvontajärjestelmien hallinnointi**	Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan.
TEK-03.1	**Suodatus- ja valvontajärjestelmien hallinnointi - vastuutus ja organisointi**	Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen, poistaminen ja valvonta on vastuutettu ja organisoitu.
TEK-03.2	**Suodatus- ja valvontajärjestelmien hallinnointi - dokumentointi**	Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.
TEK-03.3	**Suodatus- ja valvontajärjestelmien hallinnointi - tarkastukset**	Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.
TEK-04	**Hallintayhteydet**	Hallintapääsy tapahtuu rajattujen, hallittujen ja valvottujen pisteiden kautta.
TEK-04.1	**Hallintayhteydet - vahva tunnistaminen julkisessa verkossa**	Hallintapääsyn julkisesta verkosta tai muun käytettävän etähallintaratkaisun tulee edellyttää vahvaa, vähintään kahteen todennustekijään pohjautuvaa käyttäjätunnistusta.
TEK-04.2	**Hallintayhteydet - hallintayhteyksen salaaminen**	Hallintaliikenne julkisessa verkossa on salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia.
TEK-04.3	**Hallintayhteydet - vähimmät oikeudet**	Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti.
TEK-04.4	**Hallintayhteydet - henkilökohtaiset tunnukset**	Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia.
TEK-05	**Langaton tiedonsiirto**	Langattomassa tiedonsiirrossa tietoliikenne salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat

		valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia.
TEK-06	**Kasautumisvaikutus**	Kasautumisvaikutus on huomioitu tietojenkäsittely-ympäristön suojaamisessa.
TEK-07	**Pääsyoikeuksien hallinnointi**	Tietojärjestelmien käyttöoikeudet on määritelty.
TEK-07.1	**Pääsyoikeuksien hallinnointi - pääsyoikeuksien myöntäminen**	Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käyttötarpeesta on varmistuttu.
TEK-07.2	**Pääsyoikeuksien hallinnointi - pääsyoikeuksien rajaaminen**	Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.
TEK-07.3	**Pääsyoikeuksien hallinnointi - pääsyoikeuksien ajantasaisuus**	Käyttöoikeudet on pidettävä ajantasaisina.
TEK-08	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen**	Tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti.
TEK-08.1	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen**	Kaikki käyttäjät tunnistetaan ja todennetaan yksilöllisillä henkilökohtaisilla käyttäjätunnisteilla.
TEK-08.2	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen**	Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti.
TEK-08.3	**Tietojenkäsittely-ympäristön toimijoiden tunnistaminen**	Käyttäjätunnukset lukittuvat tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin.
TEK-09	**Tietojärjestelmien fyysinen turvallisuus**	Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.
TEK-10	**Järjestelmäkovennus**	Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.
TEK-10.1	**Järjestelmäkovennus - käytössä olevien palveluiden minimointi**	Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut.
TEK-10.2	**Järjestelmäkovennus - kovennusten varmistaminen koko elinkaaren ajan**	Kovennusten voimassaolosta ja vaikuttavuudesta huolehditaan koko tietojärjestelmän elinkaaren ajan.
TEK-11	**Haittaohjelmilta suojautuminen**	Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.
TEK-12	**Turvallisuuteen liittyvien tapahtumien jäljitettävyys**	Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyden varmistamiseksi.
TEK-12.1	**Turvallisuuteen liittyvien tapahtumien jäljitettävyys - tietojen luovutukset**	Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.
TEK-13	**Poikkeamien havainnointikyky ja toipuminen**	Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely-ympäristön suojattu tilanne viipymättä.

TEK-13.1	**Poikkeamien havainnointikyky ja toipuminen - poikkeamien havainnointi lokitiedoista**	Alikriteeri tarkentaa pääkriteerin vaatimusta.
TEK-14	**Ohjelmistojen turvallisuuden varmistaminen**	Sovellukset ja ohjelmointirajapinnat (API:t) suunnitellaan, kehitetään, testataan ja otetaan käyttöön alan hyvien turvallisuuskäytäntöjen mukaisesti. Sovellusten ja rajapintojen on kestettävä niitä vastaan käytettävissä olevat yleiset hyökkäysmenetelmät ilman, että käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus vaarantuu.
TEK-16	**Tiedon salaaminen**	Kun salassa pidettävää tietoa siirretään yleisissä tietoverkoissa, tieto salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee valmistajalta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.
TEK-16.1	**Tiedon salaaminen - salaaminen turvallisuusalueen sisällä**	Kun salassa pidettävää tietoa siirretään sisäisessä verkossa, voidaan käyttää alemman tason salausta tai salaamatonta tiedonsiirtoa riskinhallintaprosessin tulosten perusteella.
TEK-17	**Muutoshallintamenettelyt**	Tietojenkäsittely-ympäristöön tehtäviin muutoksiin on käytössä turvallisuuden huomioiva muutostenhallintamenettely.
TEK-17.1	**Muutoshallintamenettelyt - uudelleenarviointi**	Tietoturvallisuutta koskevat tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.
TEK-17.2	**Muutoshallintamenettelyt - dokumentointi**	Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten- ja asetustenhallintaprosessia.
TEK-18	**Etäkäyttö**	Etäkäytössä käyttäjät ohjeistettu ja tunnistetaan riittävän luotettavasti.
TEK-18.1	**Etäkäyttö - tietojen ja tietoliikenteen salaaminen**	Turvallisuusalueen ulkopuolella etäkäytössä käytettävät päätelaitteet, muistivälineet ja tietoliikenneyhteydet ovat suojattu käyttäen sellaisia salausratkaisuja, joissa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat valmistajilta saatujen tietojen mukaan moderneja salausvahvuuksia ja -asetuksia.
TEK-19	**Ohjelmistohaavoittuvuuksien hallinta**	Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.
TEK-20	**Varmuuskopiointi**	Varmistus- ja palautusprosessit on suunniteltu, toteutettu, testattu ja kuvattu siten, että ne vastaavat lainsäädännön ja toiminnan vaatimuksia.
TEK-21	**Sähköisessä muodossa olevien tietojen tuhoaminen**	Sähköisessä muodossa olevien tietojen tuhoaminen on järjestetty luotettavasti. Salassa pidettävien tietojen tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.
TEK-21.1	**Sähköisessä muodossa olevien tietojen tuhoaminen - arkistointi**	Tietojen arkistointivelvollisuus on huomioitu tiedon elinkaaren hallinnassa.
TEK-21.2	**Sähköisessä muodossa olevien tietojen tuhoaminen - pilvipalveluissa olevan tiedon tuhoaminen**	Alikriteeri tarkentaa pääkriteerin vaatimusta.