**Tunnistuspalveluntarjoajan auditoinnin**

**mallikriteeristö**

Viestintäviraston suositus

211/2019

luonnosversio 28.11.2018

Sisältö

1 Johdanto 3

1.1 Suosituksen versiot 3

1.2 Suosituksen tavoitteet 3

2 Auditointikriteeristö 4

2.1 Palvelun tarjoajan luotettavuus 5

2.2 Toiminnan tietoturva 6

2.2.1 Turvallisuusjohtaminen 6

2.2.2 Turvaorganisaatio ja resurssit 11

2.2.3 Henkilöstöturvallisuus ja omaisuuden hallinta 13

2.2.4 Tietojen luokittelu 17

2.2.5 Riskit ja jatkuvuuden varmistaminen 19

2.2.6 Fyysinen turvallisuus 26

2.2.7 Tekninen turvallisuus 35

2.3 Tunnistusmenetelmän tietoturva 55

3 LIITE A: Mobiilitunnistusratkaisun arviointikriteeristö 58

3.1 Vaatimukset liittyen arkkitehtuuriin, suunnitteluun ja uhkakuvien mallintamiseen 58

3.2 Tiedon tallennukseen ja yksityisyyteen liittyvät vaatimukset 59

3.3 Salausvaatimukset 61

3.4 Tunnistaminen ja istunnonhallinta 62

3.5 Tietoliikenne 64

3.6 Alustaan liittyvät vaatimukset 65

3.7 Koodin laatu ja kehitysympäristön vaatimukset 66

3.8 Resilience vaatimukset 67

# Johdanto

Tässä suosituksessa kuvataan tunnistuspalveluntarjoajille mallikriteeristö tunnistuspalvelun auditoimiseksi. Tässä mallikriteeristössä esitetyt kriteerit tulee arvioida tunnistuspalvelun kannalta. Tunnistuspalveluntarjoajat voivat käyttää tässä suosituksessa olevaa kriteeristöä tai käyttää jotakin toista Viestintäviraston määräyksen Sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (M72) 15 §:n vaatimukset täyttävää kriteeristöä.

## Suosituksen versiot

|  |  |
| --- | --- |
| Suosituksen versio ja päivämäärä | Tehdyt muutokset |
| 211/2016 O 2.11.2016 | 1. julkaistu versio |
| 211/2019 S x.x.2019 | * korjataan asiakirjatyyppi suositukseksi * päivitetään kriteeristö ja tulkintaohjeet * lisätään Liite A kriteeristö sovellusten ja mobiilisovellusten arvioinnille |

## Suosituksen tavoitteet

Suositus koskee vahvan sähköisen tunnistamisen välineiden tarjoajia ja välityspalveluita.

Suosituksen tarkoitus on selkeyttää toimijoille, mitä palveluun liittyvien auditointien tulisi kattaa, jotta auditoinnit kelpaavat niin kansallisen kuin rajat ylittävän tunnistuspalvelun tarjontaan. Esimerkkikriteeristön noudattaminen ei ole pakollista, mutta se on yksi tapa osoittaa määräyksen 72[[1]](#footnote-1) 15 §:n mukaisten vaatimusten täyttäminen. Auditoinnin lopputuloksena toimitetaan Viestintävirastolle tunnistuspalvelun tarkastuskertomus, jonka sisältö on määritelty Viestintäviraston ohjeessa 215/2016 O

Palvelujen vaatimuksista säädetään

* vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista annetussa laissa (617/2009, jäljempänä *tunnistus- ja luottamuspalvelulaki*),
* Euroopan parlamentin ja neuvoston (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta antamassa asetuksessa (jäljempänä *eIDAS-asetus*),
* Komission täytäntöönpanoasetuksessa (EU) 2015/1502 (nk. varmuustasoasetus) ja
* Viestintäviraston määräyksessä 72A/2018 M.

Tunnistus- ja luottamuspalvelulain 42 a §:n mukaan Viestintäviraston tehtävänä on valvoa lain noudattamista.

# Auditointikriteeristö

Tämä arviointikriteeristö on koottu ISO 27001 -standardin vaatimuksista täydennettynä ISO 27002 -vaatimuksilla sekä ETSI EN 319 411-1 -standardilla siltä osin kun ISO 27001 -standardi ei kata määräyksen M72 15 §:n vaatimuksia.

Auditointikriteeristö on luotu kohdennettavaksi organisaatioihin jotka osallistuvat luottamusverkostoon. Tässä kriteeristössä esitetyt vaatimukset tulee tarkastaa kohdentaen ne organisaation luottamusverkostossa tapahtuvaan toimintaan.

Säädösviittaukset:

* LoA: eIDAS asetuksen täytäntöönpanoasetuksen (EU) 2015/1502 mukainen tunnistuksen varmuustaso
* TunnL: Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009
* M72: Viestintäviraston määräys sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 72A/2018 M

Standardit:

* ISO/IEC 27001 – 27002
* ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
* Liite A: OWASP Mobile AppSec Verfication
* Liite A: RFC 2289 / 4226 / 6238

## Palvelun tarjoajan luotettavuus

Auditoinnin ei tarvitse kattaa palveluntarjoajan yleistä luotettavuutta tai käyttäjille ja luottaville osapuolille tarjottavia tietoja palvelusta (tunnistusperiaatteet, sopimusehdot, hinnastot). Näistä riittää toimijan oma selvitys, jonka palveluntarjoaja toimittaa Viestintäviraston arvioitavaksi. Tästä syystä tätä osuutta ei tarkastella esimerkkikriteeristössä. Viestintävirastolle tunnistuspalvelun aloitus-, lopetus- ja muutosilmoitusten yhteydessä toimitettavia tietoja on kuvattu tarkemmin ohjeessa 214/2016 O.

## Toiminnan tietoturva

Viestintäviraston määräyksen M72 15§:n mukaan tunnistuspalvelun auditoinnin täytyy kattaa vaatimukset, jotka kohdistuvat tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen:

1. tietoturvallisuuden hallintaan
2. tietojen säilyttämiseen
3. tiloihin ja henkilökuntaan
4. teknisiin toimenpiteisiin
5. sekä tunnistusmenetelmän luotettavuuteen ja tietoturvaan.

Vaatimusten täyttyminen voidaan todentaa auditoimalla tunnistuspalvelun toimintaan liittyvät turvallisuusjohtamisen, turvaorganisaation ja resurssien, henkilöstöturvallisuuden ja omaisuuden hallinnan, tietojen luokittelun, riskien ja jatkuvuuden varmistamisen, fyysinen turvallisuuden ja teknisen turvallisuuden osa-alueet.

### Turvallisuusjohtaminen

Organisaatiolla tulee olla käytössään turvallisuusjohtamiseen tarkoitetut hallintajärjestelmät.

|  |
| --- |
| *LoA:*  *”tietoturvallisuuden hallintajärjestelmällä” tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvallisuuteen liittyvät riskit hyväksyttävällä tasolla.* |

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Tulee tunnistaa **olennaiset** turvallisuusjohtamiseen vaikuttavat ulkoiset ja sisäiset tekijät | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaation ja sidosryhmien henkilöstön tulee ymmärtää liiketoiminnan ja tietoturvan suhde. Mitä vaikutuksia tietoturvan pettämisellä on liiketoiminnalle ja sen jatkuvuudelle. | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (4.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tunnistettuihin tekijöihin kohdentuvat vaatimukset ja turvallisuusvaatimukset tulee määritellä | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (4.1, 4.2,) | eIDAS 2, eIDAS 3 |  |
| 1. Tulee tunnistaa ja määritellä tarkoituksenmukaisuus, käytettävyys ja kohteet turvallisuusjohtamisen ja hallinnointi järjestelmän käyttöönotossa | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (4.3, 5.1) | eIDAS 2, eIDAS 3 |  |
| 1. Turvallisuusjohtamisen tulee olla organisaation johdon hyväksymä | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.1) | eIDAS 2, eIDAS 3 |  |
| 1. Johdon tulee sitoutua turvallisuusjohtamisen toteuttamiseen organisaatiossa | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 | ISO 27001 (5.1) | eIDAS 2, eIDAS 3 |  |
| 1. Käytössä tulee olla tietoturvapolitiikka | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.2) | eIDAS 2, eIDAS 3 |  |
| 1. Turvallisuusjohtamisen tulee olla jatkuvasti kehittyvä kokonaisuus | TunnL 8.1 § kohta5  LoA 2.4  M72 4 § | ISO 27001 (5.1, 10.2) | eIDAS 2, eIDAS 3 |  |
| 1. Turvallisuusjohtamisen tulee noudattaa ajantasaisia lainsäädäntöjä ja määräyksiä | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.3, 6.1.3 LiiteA 5.1) | eIDAS 2, eIDAS 3 | Sähköisen tunnistuspalvelun tarjontaan liittyvää lainsäädäntöä kuten tunnistus- ja luottamuspalvelulakia ja henkilötietolakia. |
| 1. Käyttöönotettavaa turvallisuusjohtamisen mallia tulee suunnitella, käyttöönottaa, ylläpitää ja parantaa jatkuvasti | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.1, 10.2) | eIDAS 2, eIDAS 3 |  |
| 1. Käytössä olevat turvallisuudenjohtamiseen vaikuttavat tekijät tulee dokumentoida | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (7.5, 6.1.3 LiiteA 6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Turvallisuusperiaatteet ja politiikat kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.2) | eIDAS 2, eIDAS 3 |  |
| 1. Politiikat julkaistaan ja niistä tiedotetaan henkilökuntaa ja tarvittaessa sidosryhmiä | TunnL 8.1 § 5, 13 §, § §  LOA 2.4  M72 4 § | ISO 27001 (5.2, 6.1.3 LiiteA 5.1.1) | eIDAS 2, eIDAS 3 |  |
| 1. Turvadokumentaatio tulee olla kaikkien sähköisen tunnistamisen tehtäviin osallistuvien saatavilla ja tiedossa | TunnL 8.1 § 5, 13 §,  LOA 2.4  M72 4 § | ISO 27001 (7.5.3, 6.1.3 LiiteA 5.1.1) | eIDAS 2, eIDAS 3 |  |
| 1. Turvallisuusperiaatteet ja politiikat ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.2) | eIDAS 2, eIDAS 3 |  |
| 1. Johto vastaa siitä, että tietoturvajohtamisen toteuttamisen resurssit ovat riittävät | TunnL 13 §  LOA (2.4.4 2.4.5  M72 4.2 § kohdat 2 ja 4 | ISO 27001 (5.1) | eIDAS 2, eIDAS 3 |  |
| 1. Määritellyn turvadokumentaation kattavuuden ja ajantasaisuuden seuranta on vastuutettu. Ajantasaisuutta seurataan jatkuvuuden ja tehokkuuden varmistamiseksi. | TunnL 8.1 § kohta 5  LOA 2.4  M72 4 § | ISO 27001 (7.5, 6.1.3 LiiteA 5.1.2) | eIDAS 2, eIDAS 3 |  |
| 1. Turvallisuusperiaatteet ja politiikat ohjaavat turvallisuustoimintaa | TunnL 8.1 § kohta 5  LOA 2.4  M72 4.2 § kohta 2 | ISO 27001 (5.2, 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Turvallisuusperiaatteiden toteutumisesta seurataan ja raportoidaan | TunnL 8.1 § kohta 5  LOA 2.4  M72 4.2 § kohdat 2 ja 6 | ISO 27001 (5.2, 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaation on asetettava turvallisuustavoitteet ja perusteet tavoitteiden asettamiselle | TunnL 8.1 § kohta 5  LOA 2.4  M72 4.2 § kohta 1 (vastaa ympäristön tarpeisiin) | ISO 27001 (6.2, 6.1.3 LiiteA 16.1, 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Palveluiden ja muun toiminnan riskit pitää havainnoida erillisellä prosessilla | TunnL 8.1 § kohta 5  LOA 2.4  M72 4.2 § kohta 5 (toiminta) | ISO 27001 (8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Palveluiden ja muun toiminnan riskien käsittelyyn tulee luoda selkeä toimintaprosessi. | TunnL 8.1 § kohta 5,  LoA 2.4  M72 4 § | ISO 27001 (8.3) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaatiolla tulee olla menetelmä yleisten haavoittuvuuksien seurantaan | TunnL 8.1 § kohta 5  LOA 2.4  M72 5.1 § kohta 2 | ISO 27001 (10.1, 6.1.3 LiiteA 12.6) | eIDAS 2, eIDAS 3 | Poikkeamia tulee seurata. Havaitut poikkeamat tulee analysoida. Tarvittavat korjaavat muutokset tulee päivittää politiikkaan ja periaatteisiin |

### Turvaorganisaatio ja resurssit

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Tulee olla määriteltynä turvallisuudesta vastaava organisaatio | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.3) | eIDAS 2, eIDAS 3 |  | |
| 1. Turvaorganisaation tehtävät, vastuut ja tekijät täytyy olla määriteltynä | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.3) | eIDAS 2, eIDAS 3 |  | |
| 1. Organisaation tulee tunnistaa ja määritellä tarvittavat resurssit tietoturvajohtamisen perustamiseen, käyttöönottoon, ylläpitoon ja jatkuvaan kehittämiseen | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (5.1, 7.1) | eIDAS 2, eIDAS 3 |  | |
| 1. Fyysisen turvallisuuden tehtävät ja vastuu on määritelty niihin tiloihin joissa organisaation tehtäviä suoritetaan, sekä laitteistoja säilytetään | TunnL 8.1 § kohta 4  LoA 2.4  M72 4 §, 15 § | ISO 27001 (4.2 5.36.1.1, 6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 | Organisaation fyysisen turvallisuuden vastuut on määriteltävä  ISO27002 (6.1.1)  KATAKRI v.2015 (T02)  Tunnistuspalveluntarjoaja vastaa myös alihankkijoista ja muista sen lukuun toimivista (TunnL §13.4) | |
| 1. Tietoteknisen turvallisuuden tehtävät ja vastuut on määritelty kaikkiin tarpeellisiin organisaation osa-alueisiin | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 §, 5 §, 15 § | ISO 27001 (4.2, 5.3, 6.1.3 LiiteA 6.1.1) | eIDAS 2, eIDAS 3 |  | |
| 1. Vastuut poikkeamatilateisiin ja sidosryhmäviestintään on määritelty | TunnL 8.1 § kohta 5  LoA 2.4 | (7.4, 5.3, 6.1.3 LiiteA 6.1) | eIDAS 2, eIDAS 3 | Toiminnan kannalta tärkeät viranomaiset ja muut sidosryhmät on tunnistettu  Toiminnan vaatimuksien mukaista viestintää tulee noudattaa. | |
| 1. Organisaatio määrittää tietoturvan hallinnan tehtäväroolit siten, että turvapoikkeamatilanteessa kukin toimija tietää omat tehtävänsä ja vastuunsa | TunnL 8.1 § kohta 5  LoA 2.4 | (5.3, 6.1.3 LiiteA 6.1) | eIDAS 2, eIDAS 3 |  | |
| 1. Tehtävät ja roolit tulee dokumentoida | TunnL 8.1 § kohta 5  LoA 2.4 | (7.5, 6.1.3 LiiteA 6.1) | eIDAS 2, eIDAS 3 |  | |
| 1. Järjestelmät on varmistettava niin, että turvapoikkeamista palautuminen on tehokasta ja saatavuusvaatimukset täyttävää. | TunnL 8.1 § kohta 4  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 17.2) | eIDAS 2, eIDAS 3 | Saatavuusvaatimukset ovat sopimusasia | |
| 1. Henkilöstön tehtävät ja toiminnot on määriteltävä siten, ettei yksi henkilö pysty omalla toiminnallaan aiheuttamaan vakavaa turvallisuuspoikkeamaa | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 6.1) | eIDAS 2, eIDAS 3 |  | |
| 1. Organisaatiolla on käytössään riittävä asiantuntemus tietoturvallisuuden varmistamiseksi | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.1) | eIDAS 2, eIDAS 3 |  | |
| 1. Henkilöstöturvallisuudella varmistutaan osaamisen ja luotettavuuden toteutumisesta | TunnL 8.1 § kohta 5, 13 §  LoA 2.4 | ISO 27001 (7.2, 6.1.3 LiiteA 7.2.2) | eIDAS 2, eIDAS 3 | Tunnistuspalveluntarjoaja vastaa myös alihankkijoista ja muista sen lukuun toimivista. (TunnL §13.4) | |
| 1. Kaikki tietoturvallisuuden vastuualueet on määritelty ja niihin kohdistuva asiantuntemus on tunnistettu | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 6.1) | eIDAS 2, eIDAS 3 |  | |
| 1. Käytössä oleva omaisuus ja järjestelmät on tunnistettu. Kaikkiin omaisuuteen ja järjestelmiin on nimetty turvallisuusvastaava | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.1, 6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  | |
| 1. Kullekin henkilöstön vastuuroolille on nimettävä useampi kuin yksi soveltuva henkilö | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 6.1) | eIDAS 2, eIDAS 3 | Vastuullisella tulee olla määriteltynä varahenkilö | |
| 1. Henkilöturvallisuudella varmistetaan että toiminnassa on organisaation eri tasoilta ne edustettuina, joilla on relevantti rooli, osaaminen ja toimenkuva | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2) | eIDAS 2, eIDAS 3 |  | |
| 1. Resurssien riittävyyttä arvioidaan säännöllisesti | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.1) | eIDAS 2, eIDAS 3 | Asiantuntemuksen riittävyys tulee arvioida säännöllisesti turvallisuustyön toteutumisen varmistamiseksi.  KATAKRI v.2015 (T03) | |
| 1. Henkilöstön koulutusten tilasta pidetään kirjaa ja huolehditaan siitä, että henkilöstön uudelleenkoulutus ja lisäkoulutus on säännöllistä | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2) | eIDAS 2, eIDAS 3 |  | |
| 1. Uudelleenkoulutus on suoritettava, kun organisaation toiminnoissa tai palveluissa tulee merkittäviä muutoksia | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2) | eIDAS 2, eIDAS 3 | Organisaation tulisi noudattaa määriteltyä turvallisuuskoulutusohjelmaa  ISO27002 (7.2.2) | |

### Henkilöstöturvallisuus ja omaisuuden hallinta

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Henkilökunnan tulee tuntea toimintaan kohdentuvat riskit ja lait | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.3) | eIDAS 2, eIDAS 3 | Henkilökunnan tulee tuntea tehtäviensä vaikutus tietoturvallisuuteen.  ISO27002 (7.2.2) |
| 1. Henkilökunnalle on määriteltävä erilliset perehdyttämisohjeet tietojen käsittelylle | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.3, 6.1.3 LiiteA 7.1.2) | eIDAS 2, eIDAS 3 | Erityistä huolenpitoa tulee noudattaa käyttäjien henkilötietojen käsittelyssä  ISO27001 (6.1.3 LiiteA 18.1.4) |
| 1. Organisaatiolla tulee olla käytössään käyttö- ja pääsyoikeuksien hallintaan tehdyt ohjeistukset | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.3) | eIDAS 2, eIDAS 3 | Käyttäjien tulee noudattaa organisaation pääsynhallinta politiikkaa  ISO27001 (6.1.3 LiiteA 9.3.1) |
| 1. Luokitellun tiedon käsittelijöille tulee tehdä turvaselvitykset | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 7.1.1) | eIDAS 2, eIDAS 3 |  |
| 1. Henkilökunnan on tehtävä tarkoituksenmukaiset salassapito- ja vaitiolositoumukset | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7) | eIDAS 2, eIDAS 3 | Salassapito- ja vaitiolositoumukset tulee tehdä kaikille luottamuksellista tietoa käsitteleville henkilöille.  Salapitosopimukset ja niiden sisältö arvioidaan määräajoin  ISO27002 (7.1.2) |
| 1. Organisaatiossa työskenteleville tulee olla määriteltynä selkeät tehtävät, roolit ja vastuut | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 7.1.2) | eIDAS 2, eIDAS 3 |  |
| 1. Henkilökunnan ja sidosryhmien tietoturvallisuuteen liittyvät vastuut tulee olla kuvattuna | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 7.1.2) | eIDAS 2, eIDAS 3 |  |
| 1. Henkilökunnan turvallisuus huomioidaan rekrytoidessa, muutoksissa, sekä päättyessä | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 7) | eIDAS 2, eIDAS 3 |  |
| 1. Työtehtävien vaihtumiseen ja loppumiseen on kuvattu selkeä toimintaprosessi | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 7) | eIDAS 2, eIDAS 3 | Vaihtumisen yhteydessä huomioitava uuden tehtävän vaatima osaaminen ja koulutus.  ISO27002 (7.2.2) |
| 1. Resurssien osaamista on ylläpidettävä koulutuksella ja tarkoituksenmukaisilla turvallisuusohjeistuksilla | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 7.2.2) | eIDAS 2, eIDAS 3 |  |
| 1. Prosesseille ja käsittely-ympäristöille on tehty tarkoituksenmukaiset turvallisuusohjeistukset, jotka huomioivat tiedon koko elinkaaren | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.5, 6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Henkilökunnan tietoisuutta ohjeistuksesta ylläpidetään säännöllisesti | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.5.3) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaation johto vastaa turvallisuuskoulutuksen ja -tietoisuuden ajantasaisuudesta | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2) | eIDAS 2, eIDAS 3 | Turvallisuuskoutuksen ja – tietoisuuden ajantaisaisuus tulee varmentaa säännöllisesti. Johto vastaa vaatimuksen toteutumisesta.  IS27002 (7.2.2) |
| 1. Turvallisuuskoulutus on säännöllistä ja dokumentoitua. Koulutuksen tehokkuutta seurataan | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2) | eIDAS 2, eIDAS 3 |  |
| 1. Henkilökunnan tulee tuntea organisaation politiikat ja ohjeistukset | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.3) | eIDAS 2, eIDAS 3 |  |
| 1. Ohjeiden ja politiikkojen noudattamista valvotaan ja päivitetään säännöllisesti | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2) | eIDAS 2, eIDAS 3 |  |
| 1. Työtehtävien vaikutukset tietoturvajohtamiseen ja tietoturvan toteutumiseen organisaatiossa tulee olla henkilökunnan tiedossa | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2, 6.1.3 LiiteA 7.2.2) | eIDAS 2, eIDAS 3 |  |
| 1. Tietoturvallisuusrikkeistä on selkeät sanktiot | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2, 6.1.3 LiiteA 7.2.3) | eIDAS 2, eIDAS 3 | Organisaatiolla tulee olla sisäiset kurinpidolliset menetelmät henkilöstön aiheuttamien tahallisten vahingontekoja tai laiminlyöntien varalta  Organisaatiolla tulee olla menetelmä havaittujen vahingontekojen raportointiin  ISO27002 (7.2.3) |
| 1. Organisaatiossa työskenteleville annetaan ohjeistukset, sekä koulutusta tietojen luokittelu huomioiden | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7) | eIDAS 2, eIDAS 3 | Turvallisuuskoulutuksessa huomioidaan yksityisyydensuoja ja henkilötietojen käsittely  ISO27001 (6.1.3 LiiteA 18.1.4) |
| 1. Turvallisuuskoulutus suunnitellaan kattamaan kaikki tietoturvallisuuden osa-alueet. | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.2) | eIDAS 2, eIDAS 3 | Koulutuksen on katettava: turvallisuuskäytännöt, tietoturvatietoisuus, tehtäväkohtainen sovellusten ja laitteiden operointi, vastuualuekohtaiset hallinnolliset ja operatiiviset käytännöt, toimintamenettelyt poikkeustilanteissa  KATAKRI v2015 (T11) |
| 1. Käyttäjillä tulee olla oikeudet vain niihin osa-alueisiin joilla on vaikutusta työnteon kannalta | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| 1. Pääsy tietoihin tulee myöntää vain tiedonsaantitarpeen mukaisesti | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 9.1.2) | eIDAS 2, eIDAS 3 | Tiedonsaantitarpeen luettelointi tulee ulottaa kaikkiin sidosryhmiin, joilla on mahdollisesti pääsy tietoihin tai laitteistoihin joilla palvelua ylläpidetään  KATAKRI v.2015 (T12) |
| 1. Organisaation tulee varmistaa henkilöstön taustat ja pätevyys nimettyihin tehtäviin | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 7.1) | eIDAS 2, eIDAS 3 |  |
| 1. Käsittelyoikeudet luokiteltuun tietoon tulee dokumentoida ja päivittää säännöllisesti | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.5, 6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| 1. Erillisiä tarkastuksia pääsyoikeuksiin tulee toteuttaa | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7.5, 6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| 1. Henkilöstön työsuhteet ja tehtävät on kirjattu voimassa oleviin sopimuksiin | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (7, 6.1.3 LiiteA 7.1.2) | eIDAS 2, eIDAS 3 |  |

### Tietojen luokittelu

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Tietosisällöltään luottamukselliset aineistot ja asiakirjat varustetaan luokittelua kuvaavalla merkinnällä | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Asiakirja merkitään asiakirjan osien ylintä luokitusta vastaavalla merkinnällä | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi asiakirjasta | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Luokitellun tiedon käsittely toteutetaan organisaation tietojenluokitteluohjeistuksen mukaisesti | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Luokitellusta järjestelmästä siirrettävä tieto säilyttää saman luokituksen | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Järjestelmien luokittelussa tulee huomioida suojattavan tiedon koko elinkaari | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Luokittelussa tulee huomioida tiedon arvo, juridiset vaatimukset, arkaluonteisuus, sekä kriittisyys | TunnL 8.1 kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Tunnistusjärjestelmään liittyvät laitteet, ohjelmistot ja muu omaisuus tulee luetteloida | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Laitteilla, ohjelmistoilla ja muulla omaisuudella tulee olla määritelty omistaja | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Laitteiden, ohjelmistojen ja muu omaisuuden hyväksytty käyttö tulee olla määriteltynä | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Henkilökunnan ja sidosryhmien tulee palauttaa kaikki laitteet, ohjelmistot ja muu omaisuus organisaatiolle työsuhteen tai sopimuksen päätyttyä | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Ohjelmistojen ja järjestelmien luokittelu tulee pohjautua käsiteltävän tiedon luokitteluun | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Luokiteltua tietoa käsittelevien ohjelmien prosessit tulee analysoida riskien osalta | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |
| 1. Tiedon suojaus tulee käyttöönottaa kaikissa tiedon elinkaaren vaiheissa | TunnL 8.1 § kohta 5  LoA 2.4 |  | eIDAS 2, eIDAS 3 | Ylätason vaatimus sille, että tieto on suojattava kaikissa elinkaaren vaiheissa (C, I, A eli Confidentiality, Integrity, Availability). |
| 1. Kaikella luokitellulla tiedolla tulee olla määritelty käyttöpolitiikka | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.3 LiiteA 8.2) | eIDAS 2, eIDAS 3 |  |

### Riskit ja jatkuvuuden varmistaminen

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Organisaatiolla on käytössä riskienhallintaprosessi | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskienhallinnan on oltava säännöllinen ja jatkuva, dokumentoitu prosessi | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1.2) | eIDAS 2, eIDAS 3 |  |
| 1. Riskien analysoinnissa on käytettävä vakiintunutta, avointa ja ymmärrettävää järjestelmällistä menetelmää | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 | Riskien analysoinnissa tulee huomioida: toteutumisen vaikutukset, todennäköisyys, riskien luokittelu  ISO31000 |
| 1. Riskienhallintaprosessin tulee tunnistaa tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat riskit | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskeillä tulee olla tunnistetut omistajat | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tunnistetut riskit tulee luokitella ja priorisoida | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskien käsittelyssä turvatoimet on mitoitettu huomioiden käsiteltävän tiedon vaatimukset. | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 | Riskein käsittelyssä turvatoimet on mitoitettu ottaen huomioon: tiedon luokitus, tiedon määrä, tiedon muoto, tiedon luokitteluperuste, tiedon sijoitustilat suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan |
| 1. Organisaatio dokumentoi keskeisiltä osin sovellettavat valvonta- ja turvatoimet | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaation tulee tunnistaa sisäiset ja ulkoiset asiat joilla on vaikutusta palvelun toteutumisen ja tietoturvajohtamisen toteuttamiseksi | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaation tulee tunnistaa turvallisuus vaikutukset ja vaatimukset jotka kohdistuvat tunnistettuihin osapuoliin | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskienhallintaan osallistuvat tarvittavat tahot organisaation sisältä ja ulkopuolelta | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskienhallinnan on katettava vähintään turvallisuusjohtamisen, tila- ja tietoturvallisuuden osa-alueet | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tunnistetut riskit on otettava huomioon tarvittavien sidosryhmien osalta | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaation tulee varmistaa, että luottamuksellisia tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation turvallisuustavoitteiden asettamisessa | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation turvatoimien suunnittelussa | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation muutoksenhallinnassa | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation hankintamenettelyissä (soveltuvilta osin) | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tarvittava yhteydenpito viranomaisiin ja kriittisiin sidosryhmiin on säännöllistä ja dokumentoitua | TunnL 8.1 § kohta 5  LoA 2.4 | ISO 27001 (6.1) | eIDAS 2, eIDAS 3 |  |

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa missä estetään luvaton pääsy tietoihin | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 17.1) | eIDAS 2, eIDAS 3 |  |
| 1. Jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa missä estetään luvaton tietojen ilmitulo | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 17.1) | eIDAS 2, eIDAS 3 |  |
| 1. Jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa missä estetään tietojen eheyden menetys | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 17.1) | eIDAS 2, eIDAS 3 |  |
| 1. Jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa missä estetään tietojen saatavuuden menetys | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 17.1) | eIDAS 2, eIDAS 3 |  |
| 1. Toiminnan jatkuvuussuunnitelmiin on sisällytettävä ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset luokiteltujen tietojen käsittelyyn ja säilyttämiseen | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 17.1) | eIDAS 2, eIDAS 3 |  |
| 1. Poikkeamista tehdyt havainnot tuodaan osaksi riskienarviointia | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3, 6.1.3 LiiteA 16.1.6) | eIDAS 2, eIDAS 3 |  |
| 1. Poikkeamista tehtyjen havaintojen pohjalta päivitetään toipumis- ja jatkuvuussuunnitelmia | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 16.1.6) | eIDAS 2, eIDAS 3 |  |
| 1. Kolmansilta osapuolilta liitettävät laitteet tai ohjelmat tulee täyttää organisaation tietoturvallisuudelle asetetut vaatimukset | TunnL 8.1 § kohta 5  LoA 2.4  M72 4-5 § | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 | Henkilökunnan, sekä kaikkien ulkopuolisten henkilöiden tulee vastata henkilökohtaisesti kaikesta organisaaiton resurssien käytöstä.  ISO27002 (8.1.3) |
| 1. Organisaation tulee nimetä ja dokumentoida jokaiseen laitteistoon ja muuhun omaisuuteen vastuulliset | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Laitteistojen, tilojen ja ohjelmistojen oikeudet tulee dokumentoida | TunnL 8.1 § kohta 5  LoA 2.4  M72 5 § | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Laitteet ja ohjelmat tulee olla inventoitu ja niillä tulee olla ajantasaiset huolto- ja ylläpitosopimukset | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Vastuullisten osaamisen taso tulee varmistaa ja ylläpitää | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 8.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietoturvallisuuden varmistamiseksi kaikki sidosryhmät tulee tunnistaa | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 8.1, sekä 17.1) | eIDAS 2, eIDAS 3 | Kaikkien sidosryhmien tunnistaminen on välttämätöntä jatkuvuus-suunnitelman toteutuksessa. |
| 1. Sidosryhmien toimintaa seurataan ja valvotaan säännöllisesti. | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (Liite A 15.2.1) | eIDAS 2, eIDAS 3 |  |
| 1. Sidosryhmiltä hankittuihin palveluihin kohdistuvia muutoksia seurataan ja valvotaan säännöllisesti. | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (Liite A 15.2.2) | eIDAS 2, eIDAS 3 |  |
| 1. Prosessit tulee varmistaa tietoturvallisuuden ja jatkuvuuden varmistamiseksi | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (Liite A 8.1, sekä 17.1) | eIDAS 2, eIDAS 3 | Kaikkien prosessien tunnistaminen on välttämätöntä jatkuvuus-suunnitelman toteutuksessa. |

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Organisaatiolla on menettelytavat turvallisuuspoikkeamien asianmukaiseen käsittelyyn | TunnL 8.1 § kohta 5  LoA 2.4  M72 4-5 § | ISO 27001 (10, 6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 | Viestintäviraston asettamat tarkoituksenmukaiset turvallisuus-poikkeamien menettelytavat on huomioitu. Vaatimuksia asetetaan mm. Määräyksen 72 11 §:ssä. |
| 1. Organisaatiolla on määritelty päätöksenteko ja toimintamalli poikkeamien ilmaantuessa | TunnL 8.1 § kohta 5  LoA 2.4  M72 4-5 § | ISO 27001 (10, 6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaation vastuut ja toimintatavat on määriteltynä poikkeamatilanteissa | TunnL 8.1 § kohta 5  LoA 2.4  M72 4-5 § | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 | Nopean ja tehokkaan reagoinnin varmistamiseksi hallinnolliset vastuut ja prosessit tulisi määritellä.  ISO27002 (16.1.1) |
| 1. Organisaatio on määrittänyt henkilöt ja tahot, joille turvallisuuspoikkeamista tai niiden epäilyistä tulee ilmoittaa | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaatiolla on määritellyt prosessit tietoturvapoikkeamien ja heikkouksien havainnointiin ja raportointiin | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaatiolla on määritelty poikkeamien eskalointi ja tarvittaessa tiedotusmalli sisäisille ja ulkoisille sidosryhmille | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Havaittujen poikkeamien analyysista ja ratkaisuista saatuja tietoja hyödynnetään tulevien tapahtumien toteutumisen estämiseksi ja vähentämiseksi | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 | Huomioitava toiminnan suunnitelmallisuus, prosessien monitorointi, poikkeamien havainnointi, tapahtumien ja poikkeamien analysointi, lokien hallinta, tietomurtojen selvityksen kannalta oleellisten tallenteiden käsittely, sekä koulutukseen ja tiedottamiseen liittyvät vaatimukset |
| 1. Organisaation tulee auditoida ja raportoida suunnitellun tietoturvallisuuden toteutumisesta säännöllisesti. | TunnL 29, 31 §  LoA 2.4.7 | ISO 27001 (9.2) | eIDAS 2, eIDAS 3 | Tunnistuslain 31 §:n mukaan Tarkastuskertomus on voimassa arvioinnissa käytetyn standardin määrittelemän ajan, kuitenkin enintään 2 vuotta. |
| 1. Organisaation johdon tulee säännöllisesti arvioida tietoturvallisuuden toteutuminen jatkuvuuden, riittävyyden, sekä tehokkuuden varmistamiseksi. | TunnL 8.1 § kohta 5  LoA 2.4  M72 4 § | ISO 27001 (9.3) | eIDAS 2, eIDAS 3 |  |

### Fyysinen turvallisuus

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Tiloissa on toteutettu tarkoituksenmukainen pääsynvalvonta jolla varmistutaan siitä, että vain asianomaisilla henkilöillä on pääsy. | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 | Pääsynvalvonta tiloihin on huomioitu kaikissa mahdollisissa sisäänpääsyaukoissa  Tarpeettomat sisäänpääsyaukot hallinnoidaan ja tarvittaessa eriytetään muista toimitiloista  KATAKRI v.2015 (F) |
| 1. Alueet, joissa säilytetään tai käsitellään luottamuksellisena pidettäviä tietoja, on suojattu asianmukaisella lukituksella, kulunvalvonnalla tai muilla toimenpiteillä luvattoman pääsyn estämiseksi tiloihin ja siellä oleviin asiakirjoihin | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 | Tilojen turvallisuudessa tulee varmistua siitä että puhtaanpöydän politiikkaa noudatetaan, näyttöjen salakatselu on huomioitu, luokiteltua tietoa säilytetään aina lukitussa kaapissa. |
| 1. Organisaatiossa käytettävät laitteistot ja niiden käytettävyys tulee olla suojattuna murtoa, ilkivaltaa, paloa, lämpöä, kaasuja, pölyä, tärinää, vettä ja sähkönkäytön katkoksia vastaan | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 | Palvelin- ja laitetiloja ohjaavan LVI-automaatiohallinnan etäkäyttö on estetty  Palvelin- ja laitetilojen olosuhdesensoreja suojataan ja valvotaan  KATAKRI (F08), ISO27002 11.2, VAHTI 2/2013 |
| 1. Luvattoman pääsyn estämiseksi huomioidaan laitteistossa käsiteltävän tiedon luokittelu | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 |  |
| **Tietojen fyysiseksi suojaamiseksi on perustettu tarvittavat fyysisesti suojatut alueet (vyöhykkeistäminen)** | | | | |
| 1. Tilat on jaettu turvavyöhykkeisiin käsiteltävän tiedon luottamuksellisuus, arkaluonteisuus, sekä kriittisyys huomioiden | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 | Erityisesti tulee huomioida henkilötietojen ja muiden yksilösuojaa vaativien tietojen käsittelyn vaatimukset.  Toimitilojen turvallisuudessa on huomioitava toimitilojen käyttötarkoitus.  Hallinnollisista tiloista ei ole suoraa ylläpidollista yhteyttä luottamuksellista tietoa käsittelevään laitetilaan.  Teknisellä toimitila-alueena tunnistetaan ne alueet, joissa ylläpidetään ja hallinnoidaan luokiteltua tietoa käsitteleviä laitteistoja.  ISO27002 (11), KATAKRI v.2015 (F) |
| 1. Luottamuksellista tietoa sekä luottamuksellista tietoa sisältäviä laitteita ei siirretä turvavyöhykkeestä ilman perusteluita | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 |  |
| 1. Turvavyöhykkeissä käytettävän suojauksen vahvuuden tulee perustua käsiteltävän tiedon luokitteluun sekä toteutettuun riskianalyysiin | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 |  |
| 1. Alueelle on pääsy ilman saattajaa vain henkilöillä, joilla on lupa tulla alueelle | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS2 | Tiloihin joissa käsitellään luottamuksellista tietoa tulee olla pääsy vain hyväksytyillä henkilöillä.  KATAKRI v.2015 (F02) |
| 1. Prosessit ja ohjeistukset työskentelylle turvavyöhykkeillä on määriteltynä | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietojen fyysiseen suojaamiseen tarkoitetut turvallisuusjärjestelmät ja laitteet ovat hyväksyttyjen teknisten standardien tai vähimmäisvaatimusten mukaisia | TunnL 8.1 § 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2.2) | eIDAS 2, eIDAS 3 | Turvajärjestelmät ja laitteet (kuten turvakaapit, kassakaapit, kulunvalvonta-järjestelmät, tunkeutumisen-havaitsemis-järjestelmät, hälytysjärjestelmät ja valvonta-järjestelmät).  KATAKRI v.2015 (F03) |
| 1. Fyysisen turvallisuuden järjestelmiä ja laitteita tulee testata ja pitää käyttökuntoisina | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1 / 6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 |  |
| 1. Turvavyöhykkeitä pidetään lukittuna silloin, kun ne ei ole käytössä ja vartioituna silloin, kun ne on käytössä | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1 / 6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 |  |
| 1. Avaimia turvavyöhykkeille valvotaan | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 |  |
| 1. Turvavyöhykkeille on laadittu turvallisuusmenettelyt, joissa on määräykset sovellettavista valvonta- ja suojatoimenpiteistä | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 | Mikäli toimitiloissa ei ole asennettu murtohälytysjärjestelmää ja alueella ei ole henkilöstöä palveluksessa ympäri vuorokauden, se on tarvittaessa tarkistettava normaalin työajan päätteeksi ja satunnaisin ajankohdin sen ulkopuolella.  Laitetiloissa jossa käsitellään luokiteltua tietoa on oltava murtohälytys-järjestelmä, jonka on katettava turva-alueen suojatun rajan.  Laitetiloissa jossa käsitellään luokiteltua tietoa on oltava rikosilmoitin-järjestelmä ja ilmoituksensiirto, joka testataan kerran kuukaudessa. Rikosilmoitinjärjestelmän hallinta on organisaatiosta nimetyn vastuuhenkilön hallinnassa  ISO27002 (11), KATAKRI v.2015 (F) |
| 1. Turvavyöhykkeillä ei tule säilyttää avoimesti asiakirjoja eikä muuta luokiteltua materiaalia | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 |  |
| 1. Tyhjän pöydän ja tyhjän näytön politiikat ovat käytössä | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 |  |
| 1. Mikäli alueella säilytetään luokiteltuja tietoja, alueella on kyseisen tiedon säilyttämiseen hyväksytty tila tai säilytysratkaisu.   Käytetyn säilytysratkaisun turvallisuuden tulee perustua tehtyyn riskianalyysiin. | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 | Mikäli tiloissa säilytetään luottamuksellisia tietoja, tulee siellä olla kyseisen tiedon säilyttämiseen hyväksytty tila tai säilytysratkaisu.  Mikäli luokitellun tietoaineiston säilytysyksikkönä käytetään lukittavaa kaappia, on varmistuttava siitä, että tunkeutumisesta jää jälki  Mikäli tiloissa säilytetään luottamukselliseksi luokiteltua tietoa (esimerkiksi henkilötietoja) on ne säilytettävä SFS-EN 14450 luokan S2 turvakaappissa tai vastaavassa  Mikäli suojattavaa tietoa säilytetään tilassa hyväksytyssä säilytysyksikössä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden antaa sellainen rakenteellinen suoja, että niiden kautta alueelle tunkeutuminen on hidasta ja vaikeaa  ISO27002 (11), KATAKRI v.2015 (F) |
| 1. Kaapeloinnin turvallisuus tulee varmentaa keskeytyksiä, häiriötä tai vahinkoja vastaan | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 |  |
| 1. Turvavyöhykkeet tarkastetaan säännöllisesti mahdollisten luvattomien tietoliikenneyhteyksien ja viestintävälineiden sekä muiden elektronisten laitteiden löytämiseksi | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1 / 6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 | Laitetiloissa, sekä teknisissä toimitiloissa ei ole luvattomia tietoliikenneyhteyksiä tai laitteita  Laitetilat, sekä tekniset toimitilat tarkastetaan säännöllisesti mahdollisten luvattomien tietoliikenneyhteyksien ja viestintävälineiden sekä muiden elektronisten laitteiden löytämiseksi  ISO27002 (11), KATAKRI v.2015 (F) |
| 1. Liikuteltavat (mobiili) laitteistot tulee suojata ja niitä varten tulee määritellä erillinen politiikka | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 8.3) | eIDAS 2, eIDAS 3 | Luokiteltua tietoa ei tule käyttää niille tarkoitetun ympäristön ulkopuolella (off-site)  ISO27001 (11.2.5) |
| 1. Liikuteltavat (mobiili) laitteistot tulee suojata.   Operatiivisen verkon hallintaan tulee käyttää vain organisaation tietoturvaperiaatteiden mukaan suojattua laitteistoa.  Operatiivisen verkon hallinta tulee toteuttaa *korotetulla varmuustasolla* siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on erityisesti arvioitu ja minimoitu. | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2 | *Korotetulla varmuustasolla* on tehtävä dokumentoitu riskiarvio, jos tunnistuspalvelun tuotannon hallintaverkkoon on pääsy organisaation yleisesti käytössä olevalla päätelaitteella, jolla on pääsy myös muihin organisaation palveluihin kuten sähköpostiin |
| 1. Liikuteltavat (mobiili) laitteistot tulee suojata.   Operatiivisen verkon hallinta tulee toteuttaa k*orkealla varmuustasolla* siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on kokonaisuutena arvioiden estetty. | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 3 | *Korkealla varmuustasolla* vaatimuksen voi täyttää käyttämällä tunnistuspalvelun tuotannon hallintaverkkoon pääsyssä sellaista organisaation päätelaitetta, jossa on estetty pääsy muihin organisaation palveluihin ja jossa ei ole käytettävissä muita kuin hallintaverkon käytön kannalta välttämättömiä toimintoja. Myös jokin toteutus, jossa päätelaitteen yhteys toimistoverkkoon olisi toteutettu terminoidusti virtualisointiin tai kvm-periaatteeseen (etätyöpöytä) perustuvalla ratkaisulla, voisi olla kokonaisuutena arvioiden riittävän turvallinen. |
| 1. Tiedon saatavuus ja eheys tulee varmentaa suositusten mukaisella laitteiston ylläpidolla | TunnL 8.1 § 5 kohta  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 |  |
| 1. Laitteistoja tai muuta omaisuutta ei voi poistaa ilman tarkoituksenmukaista auktorisointia | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 8.3) | eIDAS 2, eIDAS 3 |  |
| 1. Laitteiston hävittämiseen tai uudelleen käyttöön toteutetaan turvallista menetelmää | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 8.3) | eIDAS 2, eIDAS 3 |  |
| 1. Laitteita ei saa jättää valvomatta ilman tarkoituksenmukaista suojausta | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 8.3) | eIDAS 2, eIDAS 3 |  |
| 1. Luokitellun tiedon käsittely tilassa on huolto-, asennus- ja siivoustoimien aikana kielletty | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tiedon salakatselua ja salakuuntelua vastaan on suojauduttu | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 11.1) | eIDAS 2, eIDAS 3 | Tiedon esiintymismuodosta riippumatta luokiteltua tietoa käsitellään siten, ettei tieto näy asiattomille. Erityistä huomiota kiinnitetään henkilötietoihin ja tunnistetietoihin  Hallintaan käytetyn tilan ikkunat on varustettu näköestesuojalla tai laitteisto on sijoitettu siten, ettei ikkunasta ole näköyhteyttä.  Luottamuksellisista tiedoista käytävä keskustelu ei saa välittyä viereisiin tiloihin niille, joilla ei ole tietoon oikeutta.  Kannettavissa tietokoneissa on sivusta katselun estävä näyttösuoja.  ISO27001 (18.1.4)  KATAKRI v.2015 (F04) |
| 1. Loogiset ja fyysiset jatkuvuussuunnitelmat on varmistettu yhteneväisiksi ja toisiaan tukeviksi | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 17.1) | eIDAS 2, eIDAS 3 | Hallinnolliset ja ylläpidolliset laitteistot on tunnistettu ja varmennettu organisaation jatkuvuussuunnitelman mukaisesti  Palvelimet ja laitteet on tunnistettu ja varmennettu toimintavaatimusten mukaisesti |
| 1. Organisaation tulee tarkastaa käyttöönotettujen jatkuvuuden varmistavien menetelmien toiminnallisuus säännöllisesti | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 17.1) | eIDAS 2, eIDAS 3 |  |

### Tekninen turvallisuus

| **Kriteeri** | | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- | --- |
| 1. Operatiivinen ympäristö ja prosessit tulee olla dokumentoituna ja saatavilla | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 12.1) | eIDAS 2, eIDAS 3 | Tietojenkäsittely-ympäristön loogisen turvallisuuden tulee olla kuvattuna ja dokumentoituna.  ISO27002 (12.1.1) |
| 1. Muutosten hallintaan tulee olla määriteltynä selkeät prosessit | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 12.1.2) | eIDAS 2, eIDAS 3 |  |
| 1. Resurssien riittävyys tulee olla tunnistettuna ja sitä tulee tarkkailla | | TunnL 8.1 § kohta5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 7.1) | eIDAS 2, eIDAS 3 |  |
| 1. Resurssien riittävyydessä tulee huomioida mahdolliset tulevaisuuden lisätarpeet | | TunnL 8.1 § kohta 5  LoA 2.4.5  M72 4 § | ISO 27001 (6.1.3 LiiteA 7.1) | eIDAS 2, eIDAS 3 |  |
| 1. Ohjelmistojen ja järjestelmien asentaminen ja käyttöönotto operatiiviseen ympäristöön tulee suorittaa valtuutetun henkilön toimesta | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.5) | eIDAS 2, eIDAS 3 |  |
| 1. Operatiivisten ohjelmistojen ja järjestelmien tietoturvallisuus tulee varmistaa säännöllisillä tarkastuksilla | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.5) | eIDAS 2, eIDAS 3 |  |
| 1. Hallintaan käytettävä tietojenkäsittely-ympäristö on erotettu muista ympäristöistä | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Palvelinsalin tietojenkäsittely-ympäristö on erotettu muista ympäristöistä | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 | Mikäli erottaminen ei ole mahdollista, niin muun ympäristön pitää myös täyttää tunnistuspalvelun tarjonnalle asetetut vaatimukset. On myös varmistettava, että auditoijalla on pääsy tunnistuspalvelun tietojenkäsittely-ympäristöön kokonaisuudessaan muun tietojenkäsittely-ympäristön sitä estämättä. Muun tietojenkäsittely-ympäristön auditoijat eivät saa päästä käsiksi missään tilanteissa tunnistuspalveluntarjonnan tietojenkäsittely-ympäristöön. Lisäksi tunnistuspalveluntarjonnan tietojenkäsittely-ympäristöön on pääsy ainoastaan siihen nimetyillä henkilöillä. |
| 1. Tietojenkäsittely-ympäristön kytkeminen muiden suojaustasojen ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne salataan määritellyn politiikan mukaisesti. | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 10.1) | eIDAS 2, eIDAS 3 | Hyödynnetään kansallisesti ja kansainvälisesti hyväksyttyjä salausratkaisuja  ISO27002 10.1 KATAKRI (I04)  x |
| **Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöt ko. suojaustason sisällä** | | | | | |
| 1. Organisaation tulee noudattaa vähimpien oikeuksien periaatetta | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 | Ylläpidon hallintaliikenne toimiston hallintaverkossa tulee noudattaa vahempien oikeuksien periaatetta.  KATAKRI v.2015 (I04) |
| 1. Dokumentaatioon tulee selkeästi kuvata eri turvatason verkkoalueet, sekä niiden välissä toimivat suodatus- ja valvontajärjestelmät | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| 1. Operatiivinen verkko tulee olla loogisesti eriytettynä ylläpito- ja hallinnointiverkosta | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 | Operatiiviseen palvelunympäristöön tulee olla hallinnallinen pääsy ainoastaan hallinnointiverkosta salattuja yhteyksiä hyödyntäen |
| 1. Ylläpito- ja hallinnointiverkon tulee olla loogisesti eriytettynä muusta toimistoverkosta | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Operatiivisen verkon yhteyksien julkiseen verkkoon tulee olla riskiperusteisia, vain palvelun toiminnallisuudet mahdollistavia yhteyksiä | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 | Palvelimien yhteydet julkiseen verkkoon tulee rajata vain välttämättömien palvelun tarjoamien rajapintojen käyttöön  Kaikki tarpeettomat palvelut ja protokolla tulee poistaa käytöstä, sekä käytössä olevat protokollat määritellä sallituksi vain toiminnallisuuden kannalta välttämättömin menetelmin  KATAKRI v.2015 (I02) |
| 1. Kaikki muut kuin toiminnalle tarpeelliset yhteydet on nimenomaisesti kielletty tai suljettu | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Kaikesta hallinnallisesta toiminnasta on luotava audit-trail | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 12.4) | eIDAS 2, eIDAS 3 |  |
| 1. Audit-trail tiedon käsittelyoikeudet on eriytetty (segregation of duties) hallinnollisista oikeuksista | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.4) | eIDAS 2, eIDAS 3 |  |
| 1. Verkkojen eristyksen säännöt ja ohjeet tarkastetaan säännöllisin väliajoin | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 18.2) | eIDAS 2, eIDAS 3 |  |
| 1. Liikennettä tulee valvoa ja poikkeamiin reagoida välittömästi | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Saman vyöhykkeen sisällä olevia tietojärjestelmiä hallinnoidaan samojen turvallisuusmenettelytapojen mukaisesti | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Vyöhykkeiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain erikseen hyväksytty, toiminnalle välttämätön liikenne sallitaan (default-deny). | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietojenkäsittely-ympäristössä on varauduttu yleisiin verkkohyökkäyksiin | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.6) | eIDAS 2, eIDAS 3 |  |
| 1. Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen ja poistaminen on vastuutettu ja organisoitu | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietojenkäsittely-ympäristön asetuksien ja toiminnan tarkastukset ovat säännöllisiä. | | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | ISO 27001 (6.1.3 LiiteA 12.7) | eIDAS 3 | Tarkistetaan myös huollon aikana ja poikkeuksellisten tilanteiden jälkeen.  Tietoliikenneympäristön suodattavien ja valvovien järjestelmien asetukset suositellaan tarkastettavaksi 6kk välein. |
| **Luottamuksellisten tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - Langattomat verkot** | | | | | |
| 1. Langattomien verkkojen kautta kulkeva tietoliikenne salataan kansainvälisesti hyväksytyllä menetelmillä | | TunnL 8.1 § kohdat 4-5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 | Langattomien verkkojen radiorajapintaa käsitellään kuin julkista verkkoa. Yleistä Radiorajapinnan käyttöä langattomissa verkkoyhteyksissä tulkitaan poistumiseksi fyysisesti suojatun alueen ulkopuolelle |
| 1. Operatiivisessa verkossa ei tule olla langattomia verkkoja aktivoituna | | TunnL 8.1 § kohdat 4-5  LoA 2.4.3  M72 5 § | ISO 27001 (6.1.3 LiiteA 11.2) | eIDAS 2, eIDAS 3 | Palvelinsalin laitteistoissa tulee hyödyntää fyysistä turvalliseksi suunniteltua kaapelointia.  ISO27002 (11.2.3) |
| **Pääsyoikeuksien hallinnointi** | | | | | |
| 1. Organisaation pääsyoikeuksien hallinnoinnin avulla rajoitetaan pääsy tietoon ja tiedonkäsittely-ympäristöihin suunnitelmallisesti ja dokumentoidusti | TunnL 8.1 § kohta  LoA 2.4.6  M72 5 § | | ISO 27001 (6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| 1. Pääsy järjestelmiin ja ohjelmiin rajataan organisaation pääsynvalvonnan politiikan mukaisesti | TunnL 8.1 § kohta 5  LoA 2.4.6  M72 5 § | | ISO 27001 (6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä | TunnL 8.1 § kohta 5  LoA 2.4.6  M72 5 § | | ISO 27001 (6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| 1. Luottamuksellisten tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan ja tietojärjestelmien asianmukaisilla turvallisuusjärjestelyillä ja muilla toimenpiteillä | TunnL 8.1 § kohta 5  LoA 2.4.6  M72 5 § | | ISO 27001 (6.1.3 LiiteA 9.4) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaation pääsynvalvontapolitiikassa kuvataan erikseen käytetyt pääsynvalvontamenetelmät | TunnL 8.1 § kohta 5  LoA 2.4.6  M72 5 § | | ISO 27001 (6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| **Tietojenkäsittely- ympäristön toimijoiden tunnistaminen fyysisesti suojatun alueen sisällä** | | | | | |
| 1. Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät tietojenkäsittely-ympäristön toimijoiden tunnistamiseen | TunnL 8.1 § kohta 5  LoA 2.4.6  M72 5 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Käytetyt menetelmät valitaan tietojenkäsittely-ympäristön tietoturvatason, sekä riskianalyysin perusteella | TunnL 8.1 § kohta 5  LoA 2.4.3 ja 2.4.6  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Käyttäjien rekisteröinti ja rekisteröinnin purkamisen prosessi on määritelty, käyttöönotettu ja dokumentoitu | TunnL 8.1 § kohta 5  LoA 2.4.3 ja 2.4.6  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaatiossa on käyttöönotettu provisiointiprosessi joka mahdollistaa käyttäjän oikeuksien poistamisen kaikista tunnistetuista järjestelmistä | TunnL 8.1 § kohta 5  LoA 2.4.3 ja 2.4.6  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Käyttäjäoikeuksien myöntämistä ja käyttöä rajoitetaan ja hallinnoidaan | TunnL 8.1 § kohta 5  LoA 2.4.3 ja 2.4.6  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Tunnistetietojen myöntäminen ja välittäminen toteutetaan turvallisen prosessin mukaisesti | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Tiedon omistajat tarkastavat myönnetyt ja käytössä olevat käyttäjäoikeudet säännöllisesti | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Käyttäjien tulee noudattaa organisaation ohjeistuksia tunnistetiedon käsittelyssä | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4 § | | ISO 27001 (6.1.3 LiiteA 9.3) | eIDAS 2, eIDAS 3 |  |
| 1. Käyttäjäoikeudet poistetaan välittömästi työsuhteen, alihankintasopimuksen tai vastaavan päättymisen yhteydessä | TunnL 8.1 § kohta 5  LoA 2.4.3 ja 2.4.6  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 | Käyttäjätunnusten lukitseminen riittää, kunhan on määritelty menettelyt, milloin lukitut tunnukset poistetaan. |
| 1. Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti | TunnL 8.1 § kohta 5  LoA 2.4.3 ja 2.4.6  M72 4 § | | ISO 27001 (6.1.3 LiiteA 9.4) | eIDAS 2, eIDAS 3 | Mikäli käytetään salasanatodennusta: käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä  Mikäli käytetään salasanatodennusta: käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin  Ylläpidollisissa ja hallinnallisissa -yhteyksissä edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta  KATAKRI v.2015 (I07) |
| 1. Ohjelmiston koodiin pääsyä rajoitetaan suunnitellusti | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | | ISO 27001 (6.1.3 LiiteA 9.4) | eIDAS 2, eIDAS 3 |  |
| 1. Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.2) | eIDAS 2, eIDAS 3 |  |
| 1. Kaikki käyttäjät tunnistetaan ja todennetaan | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.4) | eIDAS 2, eIDAS 3 |  |
| 1. Päätelaitteet tunnistetaan teknisesti ennen pääsyn sallimista verkkoon tai palveluun, ellei verkkoon kytkeytymistä ole fyysisen turvallisuuden menetelmin rajattu suppeaksi | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 9.1) | eIDAS 2, eIDAS 3 | Toimistoverkossa laitteiden tunnistaminen organisaation politiikan mukaisesti.  Ylläpito- ja hallintaverkossa tulee kontrolloida verkkoon liitettäviä laitteita fyysisellä tai teknisellä kontrollilla.  Operatiivisessa verkossa suojaus voidaan toteuttaa fyysisesti estämällä luvattomat laitteiden liittämiset verkkoon.  KATAKRI v.2015 (I07) |
| **Vähimmäis- toimintojen ja vähimpien oikeuksien periaate - Järjestelmäkovennus** | | | | | |
| 1. Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 4-5 § | | ISO 27001 (6.1.3 LiiteA 12.5) | eIDAS 2, eIDAS 3 |  |
| 1. Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus | TunnL 8.1 § kohta 5  LoA 2.4.3  M72 5 § | | ISO 27001 (6.1.3 LiiteA 12.5 / 6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 |  |
| 1. Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | | ISO 27001 (6.1.3 LiiteA 12.5 / 6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 |  |
| **Haittaohjelmasuojaus** | | | | | |
| 1. Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 12.2) | eIDAS 2, eIDAS 3 | Suositellaan käytettävien palvelimien turvapäivityksien hakeminen erillisestä verkkoon kytketyltä päivityslaitteistolta  ISO27002 (12.2.1), |
| 1. Teknisten toteutusten lisäksi käyttäjiä opastetaan oikeanlaiseen toimintaan | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 12.2) | eIDAS 2, eIDAS 3 |  |
| 1. Kriittisten palvelimien yhteydet julkiseen verkkoon tulee rajata ainoastaan palvelun välttämättömien toiminnallisuuksien mahdollistamiseksi | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| **Turvallisuuteen liittyvien tapahtumien jäljitettävyys** | | | | | |
| 1. Organisaation tulee tallentaa ja monitoroida järjestelmien tapahtumia varmistamalla, että ainakin työasemien, palvelinten, verkkolaitteiden ja vastaavien lokien keräys on päällä | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 12.4) | eIDAS 2, eIDAS 3 |  |
| 1. Verkkolaitteiden ja operatiivisen verkon palvelimien lokeista tulee pystyä jälkikäteen selvittämään mitä hallintatoimenpiteitä laitteille on tehty, milloin ja kenen toimesta | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 12.4) | eIDAS 2, eIDAS 3 |  |
| 1. Tapahtumalokeja tulee kerätä järjestelmän toiminnasta, käyttäjän toimista, turvaan liittyvistä tapahtumista ja poikkeuksista | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 12.4) | eIDAS 2, eIDAS 3 |  |
| 1. Tapahtumia tulee seurata ja tarkastaa säännöllisesti | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 12.4) | eIDAS 2, eIDAS 3 |  |
| 1. Operatiivisen verkon kaikkien laitteiden kellot tulee synkronoida yhteisen hyväksytyn NTP -palvelun kautta | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 12.4) | eIDAS 2, eIDAS 3 |  |
| 1. Laitteiden ja ohjelmistojen lokien kirjaaminen tulee määritellä ja dokumentoida | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 12.4) | eIDAS 2, eIDAS 3 |  |
| 1. Lokien tallentaminen ja säilöminen jälkikäteen tapahtuvaa tutkintaa varten on suunniteltua ja toteutettava turvallisesti | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § ja 7.5 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 | Eräs suositeltu tapa lokien turvaamiseksi on ohjata keskeiset lokitiedot keskitetylle ja vahvasti suojatulle lokipal­velimelle, jonka tiedot varmuuskopioidaan säännöllisesti. |
| 1. Lokeille pitää määritellä säilöntään riittävän pitkä aika jälkikäteen tapahtuvaa selvitystä varten | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| **Poikkeamien havainnointikyky ja toipuminen** | | | | | |
| 1. Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään estämään muut vahingot | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 13.1) | eIDAS 2, eIDAS 3 |  |
| 1. Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään palauttamaan tietojenkäsittely-ympäristön suojattu tilanne | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 17.1) | eIDAS 2, eIDAS 3 |  |
| 1. Kaikkien verkkojen rajojen poikkeamia tulee havainnoida ja poikkeamista tulee raportoida | TunnL 8.1 § kohta 5  LoA 2.4.3 ja  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Organisaatiolla tulee olla selkeät toimintaprosessit poikkeamien hallintaa, sekä niistä tiedottamiseen | TunnL 8.1 § 5kohta  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Poikkeamien hallinnan hallinnolliset vastuut ja menetelmät tulee määritellä ja prosessi tulee dokumentoida | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 | Palveluntarjoaja nimeää henkilöt, joiden vastuulla on poikkeamien seuranta, säännön mukainen hoitaminen ja niistä raportointi  ISO27002 (16.1.1) |
| 1. Poikkeamat tulee raportoida sovittuja kanavia hyödyntäen mahdollisimman nopeasti | TunnL 8.1 § kohta 5 ja 16 §  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 | Eri tahoille ilmoittamisessa sisäisesti ja ulkoisesti voi olla eri kynnykset raportoinnille. |
| 1. Työntekijöiltä ja muilla osapuolilta, jotka käyttävät operatiivista verkkoa, tulee vaatia havaintojen kirjaamista sekä raportointia | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Kaikki havainnot käsitellään ja niiden vaikuttavuus luokitellaan sovittujen menetelmien mukaan | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Poikkeamista annetaan hälytys organisaation ennalta määrittelemien rajojen mukaan. | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| 1. Poikkeamien korjauksesta ja analysoinnista saatua tietoa hyödynnetään tulevien tapahtumien estämiseksi | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 16.1) | eIDAS 2, eIDAS 3 |  |
| **Tietoturvallisuus-tuotteiden arviointi ja hyväksyntä – Salausratkaisut** | | | | | |
| 1. Salausratkaisujen käytöstä on määritelty ja käyttöönotettu politiikka | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 10.1) | eIDAS 2, eIDAS 3 | Vaatimus voidaan täyttää siten, että hankitut salaisratkaisut noudattavat kansainvälisiä suosituksia  ISO27002 (10.1.1), KATAKRI v.2015 (I12) |
| 1. Politiikassa huomioidaan salausavaimien suojaus koko niiden elinkaaren ajalla | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 10.1) | eIDAS 2, eIDAS 3 | Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä  Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja  Prosessit edellyttävät vähintään kryptografisesti vahvojen avaimien käyttöä, turvallista avaintenjakelua, turvallista avainten säilytystä, säännöllisiä avaintenvaihtoja, vanhojen tai paljastuneiden avainten vaihdon, sekä valtuuttamattomien avaintenvaihtojen estämisen  ISO27002 (10.1.2), KATAKRI v.2015 (I12) |
| **Ohjelmistojen turvallisuus ja ohjelmistoilla toteutettavat pääsynhallinta-toteutukset** | | | | | |
| 1. Tietojenkäsittely-ympäristön turvallisuus, tekniset ja muut kuin tekniset turvatoimet, testataan hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan ja ne on moitteettomasti toteutettu, integroitu ja konfiguroitu | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 14.1) | eIDAS 2, eIDAS 3 |  |
| 1. Operatiiviseen verkkoon liitettävien ohjelmistojen tulee noudattaa turvallisen ohjelmoinnin periaatteita | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | | ISO 27001 (6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 | Sovelletaan organisaation sisällä toteutettaviin kehitysprojekteihin sekä ulkoistettuihin järjestelmän kehitystoimintoihin.  Rajapintojen määrittelyt tulee erikseen säilyttää dokumentoituna |
| **Luokitellun tiedon käsittelyyn liittyvän tietojenkäsittely-ympäristön suojaus: muutos-hallintamenettelyt** | | | | | |
| 1. Turvallisuuden varmistamista pidetään vaatimuksena koko tietojenkäsittely-ympäristön elinkaaren ajan sen alullepanosta käytöstä poistamiseen | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 |  |
| 1. Ohjelmistoihin tehdään vain välttämättömät muutokset. Muutoksia kontrolloidaan ja seurataan säännöllisesti. | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4-5 § | ISO 27001 (6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 |  |
| 1. Muutoksille toteutetaan tietoturvallisuus, sekä hyväksyntä testit ennen niiden käyttöönottoa. | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4-5 § | ISO 27001 (6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 | Testauksessa huomioitava tunnistusprotokollan erityispiirteet. |
| 1. Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 |  |
| 1. Käytössä on tuotannosta eriytetty kehitysympäristö. | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4-5 § | ISO 27001 (6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 | Kehitysympäristössä ei tule hyödyntää todellisia henkilötietoja. Jos todellisten henkilötietojen käyttäminen on välttämätöntä tulee ympäristöä kohdella kuten tuotantoympäristöä. |
| 1. Ulkoistettua kehitystä valvotaan ja hallinnoidaan kuin sisäistä. | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 14.2) | eIDAS 2, eIDAS 3 |  |
| **Luokiteltujen tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä: etäkäyttö ja etähallinta** | | | | | |
| 1. Tiedon välittämiseen ja käsittelyyn tulee olla politiikat määriteltynä. Politiikoissa tulee huomioida tiedon käsittely kaikissa mahdollisissa tietovälineissä | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 13.2) | eIDAS 2, eIDAS 3 |  |
| 1. Tiedon välittämiseen eri osapuolien välillä tulee olla sopimukset määriteltynä | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 13.2) | eIDAS 2, eIDAS 3 |  |
| 1. Tiedon välittämisessä huomioidaan tiedon luottamuksellisuus.   Tarvittaessa osapuolien välille määritellään vaadittavat luottamuksellisuuden, sekä non-disclosure sopimukset.  Sopimusten tarpeellisuutta arvioidaan säännöllisesti. | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 13.2) | eIDAS 2, eIDAS 3 |  |
| 1. Sähköinen tiedonvälitys tulee olla luokittelun mukaisesti suojattua | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 13.2) | eIDAS 2, eIDAS 3 |  |
| 1. Luokitellun tiedon etäkäyttö ja hallinta tulee toteuttaa organisaation turvallisia menetelmiä hyödyntäen. | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 6.2) | eIDAS 2, eIDAS 3 | Ks. myös kriteerit 148-149. |
| 1. Järjestelmien etäkäyttö-/-hallintaratkaisu edellyttää vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 6.2) | eIDAS 2, eIDAS 3 |  |
| 1. Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 6.2) | eIDAS 2, eIDAS 3 |  |
| 1. Salaamattomia tietoja sisältäviä tietovälineitä ei tule käyttää | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 6.2) | eIDAS 2, eIDAS 3 |  |
| 1. Järjestelmien etäkäyttö-/-hallintaratkaisu edellyttää kansainvälisesti hyväksyttyä liikenteen salausta | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 6.2) | eIDAS 2, eIDAS 3 |  |
| 1. Luokiteltua tietoa ei avata matkalla eikä lueta julkisilla paikoilla | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4 § | ISO 27001 (6.1.3 LiiteA 6.2) | eIDAS 2, eIDAS 3 |  |
| **Ohjelmisto-haavoittuvuuksien hallinta** | | | | | |
| 1. Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.6) | eIDAS 2, eIDAS 3 |  |
| 1. Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 4-5 § | ISO 27001 (6.1.3 LiiteA 12.6) | eIDAS 2, eIDAS 3 |  |
| 1. Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat tarkastetaan vähintään puolivuosittain korjauskohteiden löytämiseksi | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.7) | eIDAS 2, eIDAS 3 |  |
| 1. Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat tarkastetaan merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.7) | eIDAS 2, eIDAS 3 |  |
| 1. Tarkastellaan säännöllisesti keskitetyistä päivityksenjakopalveluista päivitysten asennuksen onnistumista | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.6) | eIDAS 2, eIDAS 3 |  |
| **Varmuuskopiointi** | | | | | |
| 1. Luottamuksellista ja luokiteltua tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto on | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.3) | eIDAS 2, eIDAS 3 | Toteutettava varmuuskopiointi tulee pohjautua tehtyyn riskiarvioon  Varmuuskopioon tulee olla pääsy vain nimetyillä ja tunnistetuilla henkilöillä  Tietojen siirtäminen ja tallentaminen tulee toteuttaa viranomaisten hyväksymää salausratkaisua hyödyntäen  Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden  ISO27002 (12.3.1), KATAKRI v.2015 (I24) |
| 1. Varmuuskopioita tulee ottaa ja testata säännöllisesti hyväksytyn politiikan mukaisesti | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.3) | eIDAS 2, eIDAS 3 |  |
| 1. Erityisesti henkilötietojen ja tunnistetietojen varmuuskopioinnin suojaamisessa tulee huomioida tiedon kriittisyyden aiheuttamat erityisvaatimukset | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.3 / 6.1.3 LiiteA 18.1) | eIDAS 2, eIDAS 3 |  |
| 1. Varmuuskopiointi on mitoitettava toimintavaatimuksiin | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.1) | eIDAS 2, eIDAS 3 | Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden  ISO27002 (12.3.1), KATAKRI v.2015 (I24) |
| 1. Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.3) | eIDAS 2, eIDAS 3 |  |
| 1. Palautusprosessin dokumentointi on riittävällä tasolla | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.3) | eIDAS 2, eIDAS 3 |  |
| 1. Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12k.3) | eIDAS 2, eIDAS 3 |  |
| 1. Varmuuskopiot tulee suojata fyysisen ja loogisen pääsynhallinnan menetelmin vähintään tiedon ja mahdollisesti kasautumisvaikutuksen nostaman luokittelun mukaisesti | | TunnL 8.1 § kohta 5  LoA 2.4.3,  M72 5 § | ISO 27001 (6.1.3 LiiteA 12.3) | eIDAS 2, eIDAS 3 |  |

## 

## Tunnistusmenetelmän tietoturva

Tässä osiossa käsitellään LoA:n kohtien 2.1-2.3 vaatimuksia.

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. LoA 2.1 Hakemus ja rekisteröinti vaatimukset | TunnL 15 §, 17 §, (17 § a), 18 §, (20 §) ja 24 §.  LoA 2.1.1, 2.1.2, (2.1.3, 2.1.4) | ETSI 309 411: 6.2.2, 6.2.3, 6.2.4, 6.3.4 |  | Sähköisen tunnistamisen menetelmien käyttöön liittyvät ehdot ja edellytykset eivät kuulu arvioinnin piiriin, vaan tunnistuspalveluntarjoajan on ilmoitettava ne Viestintävirastolle M72 16 §:n 1) mukaisesti selvityksenä muiden vaatimusten täyttymisestä.  ETSI 319 411 kohta 6.2.2 tulee soveltaa Komission täytäntöönpanoasetuksen 2015/1502 tarkennettujen vaatimusten mukaan  VTJ-kyselyä voidaan pitää luotettavana lähteenä henkilöllisyyden olemassaolon tarkistamiseksi.  LoA 2.1.3 ja 2.1.4 Vaatimukset tulee käydä läpi vain jos tunnistuspalveluntarjoaja tarjoaa oikeushenkilöille tunnistusvälinettä. |
| 1. LoA 2.2 Sähköisen tunnistamisen menetelmien hallinnan vaatimukset | TunnL 8 §, 8 a §, 21 §, 22 §, 25 §,  LoA 2.2.1, 2.2.2, 2.2.3, 2.2.4 | ETSI 309 411: 6.2.3, 6.3.3, 6.3.4, 6.3.6, 6.3.9, 6.5.4 |  |  |
| 1. LoA 2.3 Todentamismekanismin vaatimukset | TunnL 8 §, 8 a§  LoA 2.3.1 |  |  |  |

# LIITE A: Mobiilitunnistusratkaisun arviointikriteeristö

Tässä liitteessä listataan niitä kriteereitä, joiden avulla pystytään osoittamaan **tunnistussovelluksen** tai **tunnistusta tekevän mobiilisovelluksen** osan tietoturvallisuus. Kriteeristö on sovellettu OWASP Mobile AppSec Verfication standardista, josta julkaistiin ensimmäinen versio vuonna 2018. Tässä kriteeristössä myös on otettu käyttöön OWASP:n ehdottama kaksitasoinen arviointi. Lisäksi OWASP standardista on hyödynnetty kriteerejä, joilla pyritään huomioimaan mahdolliset murtamisyritykset itse mobiilisovelluksessa. Tämä kriteeristö laajentaa OWASP standardin kohtaa 4, jossa käsitellään tarkemmin tunnistukseen liittyviä seikkoja.

+ RFC 2289 / 4226 / 6238

## Vaatimukset liittyen arkkitehtuuriin, suunnitteluun ja uhkakuvien mallintamiseen

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Kaikki sovelluksen komponentit on tunnistettu ja ne ovat tarpeellisia | VIITTAUS | OWASP Mobile AppSec Verification Standard, Chapter 1 | L1+L2 | Tarvittaessa |
| 1. Turvakontrollit on toteutettu sekä älypuhelinsovellukseen että (remote endpoint) |  |  | L1+L2 |  |
| 1. Korkean tason arkkitehtuuri on määritelty itse sovellukselle ja siihen liittyville (ulkoisille) palveluille ja tietoturva on arkkitehtuurissa huomioitu |  |  | L1+L2 |  |
| 1. Sovelluksessa käsiteltävä arkaluontoiset tiedot on selvästi tunnistettu |  |  | L1+L2 |  |
| 1. Kaikki sovelluksen komponentit on selkeästi tunnistettu ja jokaisen komponentit kohdalla on olemassa tieto onko kyseessä toiminnallinen (business) vai tietoturvafunktio |  |  | L2 |  |
| 1. Sovellukseen ja sen käyttämiin palveluihin liittyvät uhkakuvat ja mahdolliset vastatoimet on tunnistettu |  |  | L2 |  |
| 1. Kaikilla turvakontrolleilla on keskitetty toteutus |  |  | L2 |  |
| 1. Salausavainten hallintaan on tarkkaan määritelty menetelmätapa, joka pohjautuu kansainvälisesti hyväksyttyyn ajantasaiseen standardiin |  |  | L2 |  |
| 1. Sovelluksesta löytyy mekanismi, jonka avulla se voidaan päivittää pakotetusti |  |  | L2 |  |
| 1. Tietoturvallisia käytäntöjä noudatetaan koko sovelluksen elinkaaren ajan |  |  | L2 |  |

## Tiedon tallennukseen ja yksityisyyteen liittyvät vaatimukset

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Alustan tarjoamia palveluita / ominaisuuksia hyödynnetään täysimittaisesti sovelluksen tallentaessa salausavaimia ja / tai tunnistetietoja (credentials) | VIITTAUS | OWASP Mobile AppSec Verification Standard, Chapter 2 | L1+L2 | Tarvittaessa |
| 1. Mitään luottamuksellista tietoa ei tallenneta sovellusympäristön tai alustan tarjoaman salaisuuksien tallennusta varten tarkoitetun ominaisuuden ulkopuolelle |  |  |  |  |
| 1. Mitään arkaluonteista tietoa ei kirjoiteta sovelluksen lokeihin |  |  | L1+L2 |  |
| 1. Mitään arkaluonteista tietoa ei jaeta ulkoisten tahojen kanssa, ellei se ole ennalta määritelty arkkitehtuurissa |  |  | L1+L2 |  |
| 1. Näppäimistön välimuistia ei käytetä tekstinsyöttökentissä, jotka saattavat sisältää arkaluonteista tietoa |  |  | L1+L2 |  |
| 1. Arkaluontaista tietoa tai salaisuuksia (salasana, PIN -koodi) ei missään vaiheessa paljasteta käyttöliittymän kautta |  |  |  |  |
| 1. Leikepöytää ei käytetä tietoelementtien kohdalla, jotka saattavat sisältää arkaluonteista tietoa |  |  | L1+L2 |  |
| 1. Arkaluonteista tietoa ei jaeta käytettäessä IPC -mekanismeja |  |  | L1+L2 |  |
| 1. Käyttöliittymän kautta ei paljasteta arkaluonteista tietoa |  |  | L1+L2 |  |
| 1. Varmuuskopioissa ei tallenneta arkaluoneista tietoa |  |  | L2 |  |
| 1. Sovelluksen siirtyessä taustalle, arkaluonteinen tieto poistetaan käyttöliittymäkomponenteista |  |  | L2 |  |
| 1. Sovellus ei pidä arkaluonteista tietoa muistissa tarpeettoman pitkään, ja kun tietoa ei enää tarvita, poistetaan se muistista välittömästi |  |  | L2 |  |
| 1. Sovellus pakottaa käyttöön minimitason laiteturvallisuuden (esim vaatii laitteen avauskoodin asettamisen) |  |  | L2 |  |
| 1. Käyttäjälle kerrotaan parhaista käytännöistä, joita käyttäjän tulisi noudattaa liittyen henkilökohtaiseen tietoon ja sen käsittelyyn |  |  | L2 |  |

## Salausvaatimukset

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Sovellus ei luota pelkästään symmetrisiin salausmenetelmiin ja kovakoodattuihin avaimiin ainoana salauskeinona | VIITTAUS | OWASP Mobile AppSec Verification Standard, Chapter 3 | L1+L2 | Tarvittaessa |
| 1. Sovellus käyttää hyväksi havaittuja salausmenetelmiä |  |  | L1+L2 | Tähän listaa |
| 1. Käyttötapauksiin soveltuvat ja hyväksi havaitut salausmenetelmät ovat käytössä |  |  | L1+L2 |  |
| 1. Sovellus ei käytä vanhentuneita tai huonoiksi todettuja salauskäytäntöjä tai algoritmeja |  |  | L1+L2 |  |
| 1. Salausavaimia ei uudelleenkäytetä |  |  | L1+L2 |  |
| 1. Käytetty satunnaislukugeneraattori on tarpeeksi turvallinen ja laadukas |  |  | L1+L2 |  |

## Tunnistaminen ja istunnonhallinta

Tässä kappaleessa käytetään soveltuvin osin OWASP:n standardia ja kappaletta 4. Lisäksi kriteerejä on listattu nimenomaan tunnistusspesifisiin asioihin.

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Sovellus ei tallenna tunnistetietoja / kredentiaaleja selväkielisinä missään vaiheessa | VIITTAUS |  |  | Tarvittaessa |
| 1. Jos sovellus lähettää palvelimelle viestejä, joiden palvelinpäässä tapahtuva validointi johtaa tunnistukseen, tulee kyseiset viestit lähettää turvallisesti käyttäen ajantasaisia ja hyväksyttyjä salauskäytäntöjä (esim. TLS 1.2 tai uudempi ja sanomatason salaus) |  |  |  |  |
| 1. Jos sovellus perustuu, tai sen osana on kertakäyttösalasanoihin perustuva menetelmä, tulee kertakäyttösalasanan (OTP) luonnissa käyttää standardeihin perustuvia ratkaisuja (RFC 2289 / 4226 / 6238) |  |  |  |  |
| 1. Tunnistukseen käytetyn salaisuuden tallennukseen käytetään mahdollisuuksien mukaan alustan tarjoamia palveluita / laitteisto-ominaisuuksia, kuten laitteistotason turvaosiota tai käyttöjärjestelmän tarjoamia palveluita arkaluonteisen tiedon tallennukseen (esim. keychain) [Korotettu = softa / OS –taso, korkea = sertifioitu laitteistokomponentti???] |  |  |  |  |
| 1. Tieto virheellisestä syötteestä lähetetään jokaisen kerran jälkeen palvelimelle. Palvelin seuraa virheellisten syötteiden määrää ja sovellus lukittuu automaattisesti X virheellisen syötteen jälkeen. [entä avaus? Tai OS –tasolle tallennetut tunnisteet kuten sormenjälki?]. Jos verkkoyhteyttä ei ole, eikä viestejä saada lähetettyä palvelimelle turvallisesti, sovellus itse noudattaa samaa logiikkaa. |  |  |  |  |
| 1. Jos käytössä on istuntotunnisteet, käytetään satunnaisia istuntotunnisteita |  |  |  |  |
| 1. Token-pohjaisessa ratkaisussa varmistetaan että token on allekirjoitettu hyväksyttävällä ja turvallisella algoritmilla |  |  |  |  |
| 1. Istunnon tai tokenin voimassaoloaika määritellään palvelinpäässä |  |  |  |  |
| 1. Valtuutuspolitiikat, joiden perusteella myönnetään pääsy sovellukseen, määritellään (tunnistus)palvelinpäässä |  |  |  |  |
| 1. Jos alustan ominaisuuksista johtuen tunnistuksessa ei pystytä yhdellä tekijällä yksilöimään käyttäjää (Apple iOS, sormenjälki), on käytössä yhdistelmä, millä käyttäjä pystytään yksilöimään luotettavasti (Esim. päätelaite = hallinta, salaisuuteen liittyvä PIN-koodi = tieto ja sormenjälki = ominaisuus) |  |  |  |  |
| 1. Useamman tekijän tunnistuksessa (multi-factor, strong authentication), käytetään käyttäjän tietoon (salasana, PIN-koodi) tai ominaisuuteen (sormenjälki, kasvot, iris) perustuvaa tekijää avaamaan salaisuus, jolla itse tunnistuspyyntö allekirjoitetaan asymetrisellä menetelmällä. |  |  |  |  |
| 1. 1 tai useampi laite, mutta yksi identiteetti |  |  |  |  |
| 1. Käyttäjällä tulee olla mahdollisuus deaktivoida / poistaa käytöstä tunnistussovellus a) yhdestä laitteesta b) kaikista c) kaikista laitteista ja revokoida sähköinen identiteetti (tai revokointi johtaa kaikkien instanssien deaktivoitumiseen) |  |  |  |  |
| 1. Korotetulla tasolla sovelluksen / sovelluksen osan tulee tarjota turvallinen palautusmekanismi. Korkealla tasolla tunnistusmenetelmän uusimiseen tulee käyttää eIDAS asetuksen mukaisesti vahvaa prosessia (pääsääntöisesti tarkoittaa käyntiä rekisteröintipisteessä) |  |  |  |  |
| 1. Ja sitten tähän lisää… |  |  |  |  |

## Tietoliikenne

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Verkkoliikenne on suojattu viestintäviraston suosittelemalla yhteyskäytännöllä [LINKKI] ja suojatut kanavat ovat yhdenmukaisesti käytössä sovelluksessa | VIITTAUS | OWASP Mobile AppSec Verification Standard, Chapter 5 | L1+L2 | Tarvittaessa |
| 1. Sovellus tarkistaa TLS (tai vastaava) salausmenetelmän asetukset ja varmistaa että ne noudattavat hyväksi havaittuja käytäntöjä |  |  |  |  |
| 1. Sovellus tarkistaa muiden palveluiden / palvelinpään varmenteen statuksen ja vain luotetut varmentajat ovat sallittuja |  |  | L1+L2 |  |
| 1. Sovellus käyttää omaa varmennevarastoaan tai sitoo (pinning) palvelinvarmenteen / julkisen avaimen ja luottaa ainoastaan tähän sidottuun tunnisteeseen |  |  | L2 |  |
| 1. Kriittisissä toiminnoissa, kuten tietojen palauttamisessa tai rekisteröinnissä sovellus ei luota yksittäiseen turvattomaan kommunikointikanavaan (sähköposti, SMS) |  |  | L2 |  |
| 1. Sovellus käyttää vain ajantasaisia ohjelmistokirjastoja yhteyksien ja tietoturvan toteuttamisessa |  |  | L2 |  |

## Alustaan liittyvät vaatimukset

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Sovellus pyytää alustalta vain minimioikeudet | VIITTAUS | OWASP Mobile AppSec Verification Standard, Chapter 6 | L1+L2 | Tarvittaessa |
| 1. Kaikki sovelluksen ulkopuolelta / ulkopuolisista lähteistä tuleva tieto tarkistetaan ja (sanitize?). |  |  | L1+L2 |  |
| 1. Omaa URL skeemaa tai IPC mekanismeja käytettäessä ei tietoja viedä sovelluksen ulkopuolelle, ellei sitä toteuteta turvallisesti |  |  | L1+L2 |  |
| 1. WebView -komponenteissa käytetään vain tarpeellisia yhteyskäytäntöjä, ja muut suljetaan / varmistetaan että ne eivät ole käytössä |  |  | L1+L2 |  |
| 1. JavaScript on oletusarvoisesti deaktivoitu WebView komponenteissa |  |  | L1+L2 |  |
| 1. Jos sovelluksen natiivimetodit ovat avoimia WebView –komponenteille, varmistetaan että ajetaan vain sovelluspakettiin kuuluvaa JavaScriptiä |  |  | L1+L2 |  |
| 1. Käytössä on turvalliset API:t jos käytetään objektien serialisointia |  |  | L1+L2 |  |

## Koodin laatu ja kehitysympäristön vaatimukset

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Sovellus on allekirjoitettu ja provisioitu voimassaolevalla ja luotetulla varmenteella | VIITTAUS | OWASP Mobile AppSec Verification Standard, Chapter 7 | L1+L2 | Tarvittaessa |
| 1. Sovellus on luotu release mode:ssa, eli esim. moodissa, jossa virheenkorjaus on tehty vaikeammaksi |  |  | L1+L2 |  |
| 1. virheenkorjaussymbolit on poistettu binääreistä |  |  | L1+L2 |  |
| 1. Virheenkorjauskoodi ja –viestit on poistettu |  |  | L1+L2 |  |
| 1. Kaikki kolmannen osapuolen käytetyt komponentit on tunnistettu ja tunnetut haavoittuvuudet selvitetty ja analysoitu |  |  | L1+L2 |  |
| 1. Sovellus huomaa ja käsittelee asianmukaisesti poikkeukset |  |  | L1+L2 |  |
| 1. Turvakontrollien virheenkäsittely oletusarvoisesti evää pääsyn virhetilanteessa |  |  | L1+L2 |  |
| 1. Muistia varataan, käytetään ja vapautetaan turvallisesti |  |  | L1+L2 |  |
| 1. Alustan / kehitysympäristön tarjoamat tietoturvaominaisuudet ovat käytössä |  |  | L1+L2 |  |

## Resilience vaatimukset

| **Kriteeri** | **Säädös-viittaus** | **Standardi** | **LOA -taso** | **Tulkinnat** |
| --- | --- | --- | --- | --- |
| 1. Sovellus huomaa rootatun tai jailbreakatun laitteen ja joko lopettaa toimintansa välittömästi, tai kertomalla asiasta käyttäjälle TAI | VIITTAUS | OWASP Mobile AppSec Verification Standard, Chapter 8 | R | Tarvittaessa |
| 1. Sovellus lähettää viestin palvelinpään toteutukselle huomatessaan ajoympäristöksi rootatun tai jailbreakatun laitealustan. |  |  | R |  |
| 1. Sovellus estää virheenkorjaukseen pyrkivät yritykset ja reagoi jos huomaa virheenkorjaukseen käytetyn ratkaisun liittyneen sovellukseen. Kaikki tunnetut virheenkorjausyhteyskäytännöt tulee olla katettuna. |  |  | R |  |
| 1. Sovellus huomaa ja reagoi jos sovelluksen ajoympäristössä (sandbox) ajonaikaiset tiedostot tai kriittiset tiedot / tiedostot muuttuvat |  |  | R |  |
| 1. Sovellus huomaa ja reagoi yleisesti käytettyihin työkaluihin, joilla pyritään selvittämään sovelluksen lähdekoodia (reverse engineering) |  |  | R |  |
| 1. Sovellus huomaa ja reagoi jos sitä ajetaan emulaattorissa |  |  | R |  |
| 1. Sovellus tarkkailee ja huomatessaan muistiavaruuden muutoksia / manipulointia ja reagoi asianmukaisesti |  |  | R |  |
| 1. Sovellus käyttää useampaa eri puolustusmekanismia tässä kappaleessa esitettyjen kriteerien kohdalla |  |  | R |  |
| 1. Käytössä on tekniikoita, joilla pyritään tekemään sovelluskoodin ymmärtäminen vaikeammaksi (obfuscation) |  |  | R |  |
| 1. Sovellus sitoo itsensä laitealustaan soveliain keinoin (device binding) |  |  | R |  |
| 1. Sovellukselle tärkeät / olennaiset osiot on soveltuvilta osin salattuja tietojärjestelmätasolla. Analysoimalla ei saada selville sovellukselle tärkeitä / olennaisia osioita |  |  | R |  |
| 1. Sovelluskoodin suojaaminen obfuscation tekniikkaa käyttäen tulisi noudattaa ajantasaista tutkimusta / tutkimustuloksia toimivasta obfuskoinnista. |  |  | R |  |

1. Viestintäviraston määräys sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 72A/2018 M. [↑](#footnote-ref-1)