Tiedonhallintalautakunta
Informationshanteringsnämnden

Tietoturvallisuusjaoston uudet suositukset

8.9.2021

Mika Tuikkanen
Tietoturvallisuussuositusten valmistelujaosto

Tiedonhallintalautakunta
Informationshanteringsnämnden

1. Tiedonhallintalautakunnan suosituksista yleisesti
2. TiHL 12§ - Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen
2. TiHL 13§ - Tietoaineistojen ja tietojärjestelmien tietoturvallisuus
3. TiHL 14§ - Tietojen siirtäminen tietoverkoissa
4. TiHL 15§ - Tietoaineistojen turvallisuuden varmistaminen
5. TiHL 16§ - Tietojärjestelmien käyttöoikeuksien hallinta

Tiedonhallintalautakunnan suosituksista yleisesti

- Tiedonhallintalautakunnan tehtävänä on edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista. Tiedonhallintalautakunta ei ole tiedonhallinnan yleisviranomainen, vaan sen tehtävät liittyvät tiedonhallintalakiin.
- Suosituksissa lähtökohtana tiedonhallintalain (906/2019) vaatimusten avaaminen
- Suosituksia - ei määräyksiä
- Suositukset osoitteessa https://vm.fi/tiedonhallintalautakunta
  - Tietoturvasuositukset; **Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta**

TiHL 12§ - Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen

- *Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014). Työnantajan oikeudesta selvittää työntekijän luotettavuuden arvioimiseksi häntä koskevat luottotiedot ja käsitellä huumausainetestejä koskevia tietoja säädetään yksityisyyden suojasta työelämässä annetussa laissa (759/2004)*
- Erityistä luotettavuutta edellyttäviä tehtäviä voidaan tunnistaa esimerkiksi määrittämällä tilanteet, joissa henkilö käsittelee turvallisuusluokiteltavia tai salassa pidettäviä tietoja. Henkilön työskentely tiloissa, joissa henkilön tietoon voi tulla turvallisuusluokiteltavia tai salassa pidettäviä tietoja voi myös edellyttää erityistä luotettavuutta.

TiHL 12§ - Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen

- Tiedonhallintalaki ohjaa osaltaan tilanteita, jotka edellyttävät luotettavuuden varmistamista. Selvityksistä ja prosessista säädetään erikseen.
  - *Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014).*
  - *Työnantajan oikeudesta selvittää työntekijän luotettavuuden arvioimiseksi häntä koskevat luottotiedot ja käsitellä huumausainetestejä koskevia tietoja säädetään yksityisyyden suojasta työelämässä annetussa laissa (759/2004)*
- Erityissäännöksissä on saatettu täsmentää tiedonhallintalain 12 §:n velvoitetta luotettavuuden varmistamisesta
- Selvitykset laaditaan sekä omista että palvelutoimittajien henkilöistä tarpeen mukaan.
- Tiedonhallintayksikkö laatii kuvauksen sellaisista tietoaineistojen käsittelyyn liittyvistä tehtävistä, jotka edellyttävät erityistä luotettavuutta. Näihin tehtäviin nimettävistä henkilöistä haetaan turvallisuusselvitys, mikäli tähän on turvallisuusselvityslain mukaan peruste. Lisäksi tiedonhallintayksikkö ylläpitää luetteloa näistä tehtävistä.

TiHL 13§ - Tietoaineistojen ja tietojärjestelmien tietoturvallisuus

- Aikaisemmin julkaistut suositukset
  - Riskienhallinta
  - Elinkaaren huomioiminen tietojen käsittelyssä
  - Elinkaaren huomioiminen tietojärjestelmissä
  - Tietoturvallisuus tietojärjestelmähankinnoissa

TiHL 13§ - Vikasietoisuus ja toiminnallinen käytettävyys

- *Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti*

TiHL 13§ - Vikasietoisuus ja toiminnallinen käytettävyys

- Varmistamisessa voidaan käyttää
  - testaus ennen käyttöönottoa sekä merkittävien ylläpitotoimien yhteydessä,
    - testauksen laajuus ja toteutustapa valitaan järjestelmän riski-/kriittisyysluokituksen mukaisesti,
    - testataan, että tietoturvallisuus on toteutettu ennalta määritettyjen vaatimusten mukaisesti,
  - Järjestelmätestaus ja hyväksymistestaus; tietoturvallisuuteen liittyvät käyttötapaukset,
  - kuormitustestaus,
  - koodikatselmoinnit,
  - haavoittuvuusskannaukset tai automatisoidut tietoturvatestaukset.
- vikatilanteesta toipumisen suunnittelu
- Testauksista pitää syntyä raportteja, joista selviää mitä on testattu ja millaisia tuloksia testauksessa on saatu. Testaustulokset huomioidaan järjestelmäkehityksessä.
- Määritettäessä haavoittuvuustestauksen löydösten kriittisyyttä on syytä käyttää standardoitua menetelmää kuten CVSS:ää (Common Vulnerability Scoring System) ja määritellä palvelutoimittajien sopimuksiin tiukemmat vaatimukset sen perusteella onko kyseessä matalan, keskitason vai korkean luokan haavoittuvuus.
  - Vian kriittisyys tulee vaikuttaa myös korjauksen prioriteettiin

TiHL 13§ - Toiminnallinen käytettävyys

- Toiminnallisen käytettävyyden turvaamiseksi on varmistettava, että
  - tietojärjestelmä on helposti opittava
  - sen toimintalogiikka on helposti muistettava
  - sen toiminta tukee niitä työtehtäviä, joita käyttäjän pitää tehdä tietojärjestelmällä ja
  - tietojärjestelmä edistää sen käytön virheettömyyttä
- Miten?
  - räätälöidyissä järjestelmissä käytettävyyden määrittely ja suunnittelu hyväksytyn menetelmän mukaan. Toteutuksen käytettävyyttä on testataan jatkuvasti kehittämisen aikana.
  - valmisohjelmistoissa toteutetaan käytettävyystestaus hyväksymistestauksen yhteydessä
  - testaus toteutetaan eri käyttäjäryhmien näkökulmasta
  - käytettävyystestausta voidaan tehdä jo hankintavaiheessa, jolloin voidaan varmistaa hankittavan järjestelmän soveltuvuus käyttötarpeeseen

TiHL 14§ - Tietojen siirtäminen tietoverkossa

- *Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä.*
- Yleinen tietoverkko tarkoittaa tiedonhallintalaissa hallintovaliokunnan mietinnön mukaan internetiä,
  - On kuitenkin suositeltavaa käsitellä yleisenä tietoverkkona myös muita oman hallinnan ulkopuolisia verkkoalueita (esim. operaattorien yritysverkot).
- Salausratkaisujen tulee perustua salassa pidettävän tiedon luokitteluun ja riskiarvioon. Salaus tulee toteuttaa kulloinkin voimassa olevien viranomaisvaatimusten ja suositusten mukaisesti.
- Laki puhuu salassa pidettävästä tiedosta ja yleisestä tietoverkosta. Lähtökohtaisesti kannattaa kuitenkin käsitellä kaikkea tietoa niin kuin se olisi salassa pidettävää ja salata tietoliikenneyhteydet aina oletusarvoisesti. Organisaatioiden omia verkkoja kannattaa käsitellä turvattomina verkkoina ja salata liikenne myös siellä samojen periaatteiden mukaan.
- Mikäli tietoliikennettä ei kyetä salaamaan, tietojen salaus voidaan toteuttaa siirrettävien tietojen tai tiedostojen tasolla.
  - Mikäli salasana pitää toimittaa vastaanottajalle tulee sen suojaukseen kiinnittää yhtälailla huomiota. Salasanaa ei siksi tulisi esimerkiksi toimittaa samaa kanavaa kuin viesti.

TiHL 14§ - Vastaanottajan tunnistaminen

- *Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.*
- Vastaanottajan tunnistaminen riittävän tietoturvallisella tavalla tulee määritellä käyttötapauskohtaisesti tiedon arvon ja riskiarvioinnin perusteella. Erityisesti, kun käsitellään turvallisuusluokiteltuja tietoja, tulee huomioida tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä
- Lähtökohtaisesti tiedon vastaanottaja (ja pääsääntöisesti myös lähettäjä) tulisi tunnistaa vahvasti. Mikäli kyseessä on tietojärjestelmien välinen tietojensiirto, voidaan hyödyntää varmenteita (sertifikaatteja).

TiHL 15§ - Tietoaineistojen turvallisuuden varmistaminen

- *Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:*
- *1) tietoaineistojen muuttumattomuus on riittävästi varmistettu;*
- *2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;*
- *3) tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu;*
- *4) tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu;*
- *5) tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu;*
- *6) tietoaineistot voidaan tarvittavilta osin arkistoida.*

- *Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.*

TiHL 15§ - Vahingoilta suojaaminen

- Viranomaisella tulee olla varmuus siitä, että käsiteltävä tieto tai järjestelmä on suojattu fyysisiltä vahingoilta kuten tulipalot, vesivahingot tai ilkivalta sekä sähköisiä menetelmiä käyttäen aiheutetuilta fyysisiltä vahingoilta kuten laitteiden rikkoutuminen.
  - Suojaus riskiarvioinnin perusteella
- Kullekin tietoaineistolle tulisi määritellä hyväksytyt sijainnit, joissa sähköisessä ja paperisina olevia aineistoja ja tietovarantoja voidaan käsitellä ja myös säilyttää. Sijaintien määrittelemisessä pitää huomioida palvelujen toteuttamistapa, kuten palveluntuottajat, pilvipalvelut ja tiedon käsittelyn fyysinen sijainti.
- Kriittiset järjestelmät tulisi kahdentaa, niin että toimintaa voidaan jatkaa toisesta konesalista tai sijainnista käsin silloin, kun toiminta ensisijaisessa ylläpitosijainnissa on estynyt.

TiHL 16§ - Käyttöoikeuksien hallinta

- *Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina.*
- *Ainoastaan oikeutetuille käyttäjille sekä järjestelmille myönnetään pääsy- ja käyttöoikeus tietoihin ja tietojärjestelmiin. Käyttöoikeuksien hallinnan tulee noudattaa vähimpien oikeuksien periaatetta ja sen on katettava järjestelmien koko elinkaari*
- *Käyttäjätilien hallintaa ja käyttöä seurataan ja valvotaan poikkeamien ja uhkien havaitsemiseksi sekä niihin reagoimiseksi.*

TiHL 16§ - Käyttöoikeuksien hallinta

- On suositeltavaa dokumentoida ja ottaa käyttöön riskienarviointiin perustuva käyttövaltuuksien hallintapolitiikka. Politiikka sisältää käyttöoikeuksien ja -valtuuksien määrittelemisen, myöntämisen ja hallinnoinnin periaatteet ja toimintatavat.

TiHL 16§ - Käyttöoikeuksien hallinta

- Käyttöoikeuksien hallinnan edellytykset

1. Käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).
2. Käyttäjätilien luontiin, hyväksymiseen, ylläpitoon ja poistamiseen tulee olla kuvattu menettely ja käyttöoikeuden tulee perustua tunnuksen saajan kanssa tehtyyn sopimukseen (esim. työsopimus, ostopalvelusopimus).
3. Käyttöoikeuksien käsittely ja myöntäminen tulee ohjeistaa.
4. Järjestelmien käyttäjille annetaan vain ne tiedot, oikeudet tai valtuudet, jotka ovat työtehtävien kannalta tarpeellisia. Käyttöoikeudet on määriteltävä kullekin tietojärjestelmän käyttäjälle työtehtävien perusteella ja vähimpien oikeuksien periaatteella
5. Jokaiselle käyttäjätunnukselle tulee olla nimetty vastuuhenkilö eli omistaja. Tunnuksen omistajuus on määriteltävä erikseen, jos myönnetään tunnuksia kone- tai palvelutileille, kuten esim. ohjelmistorobotiikan käyttöön.
6. Yhteiskäyttötunnuksia tulee käyttää vain erikseen hyväksytyissä poikkeustapauksissa.
7. Järjestelmään myönnetyistä käyttöoikeuksista tulee olla saatavilla ajantasainen tieto. Jokaisesta myönnetystä käyttöoikeudesta ja siihen tehdyistä muutoksista tulee jäädä merkintä (paperi tai sähköinen).
8. Käyttöoikeuden myöntämisen yhteydessä tulee tarkistaa, että henkilöllä on oikeutus käyttöoikeuden saamiselle sekä riittävä koulutus kyseisen järjestelmän käyttöön.
9. Organisaation ulkoiset ja sisäiset käyttäjät tulee olla eroteltavissa käyttäjätunnuksen perusteella.
10. Tarpeettomat käyttäjätilit ja käyttöoikeudet tulee poistaa, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta, vaihtaessa työtehtäviään tai, kun käyttäjätiliä ei ole käytetty ennalta määritellyn ajanjakson aikana).
11. Organisaatiolla on oltava selkeät ja toimivat menettelyt käyttäjien tehtävien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä niistä aiheutuvien toimenpiteiden tekemiseen.
12. Käyttöoikeudet tulee katselmoida säännöllisesti. Katselmointi tulee dokumentoida.
13. Vaaralliset käyttöoikeusyhdistelmät on tunnistettava, dokumentoitava ja eriytettävä mahdollisuuksien mukaan. Mikäli tehtäviä ei voida eriyttää, tulee niistä syntyviä riskejä hallita riskienhallinnan keinoin..
14. Käyttöoikeuksien hallinnassa erityishuomio korkeamman riskiprofiilin rooleihin (pääkäyttäjät, ylläpitäjät ja muut erityistä luotettavuutta edellyttävät työtehtävät) ja niihin liitettyihin käyttöoikeuksiin. Erityisrooleille erillinen haku- ja päätösprosessi.

Tiedonhallintalautakunta
Informationshanteringsnämnden

Kiitos

Mika Tuikkanen
Mika.tuikkanen@vm.fi

+358 295 530 036