KUVAUS TIETOTURVASTA JA TIETOJEN SUOJAUKSESTA

1. Yleistä

Tämä Kiinteistövaihdannan palvelun (KVP) rajapintojen käyttöä koskeva tietoturvakuvaus tulee täytettynä ja Maanmittauslaitoksen hyväksymänä muodostamaan viitteessä mainitun sopimuksen tietoturvaliitteen.

Tämän kyselyn määritelmät on kuvattu sopimuksessa.

2. Asiakkaan tietojärjestelmän yleiskuvaus

Asiakkaan tulee laatia kuvaus tietoturvan toteuttamisesta ja tietosuojan varmistamisesta organisaatiossaan.

Kuvauksen tulee sisältää seuraavat tietokokonaisuudet:

2.1. Yleiskuvaus järjestelmästä

Tähän kohtaan kirjoitetaan suppea yleiskuvaus, josta selviää (KVP) tietojen käsittelyyn liittyvät asiat, prosessit ja käyttäjät asiakkaan ympäristössä. Kuvauksessa tulee huomioida tietoturvallisuus Maanmittauslaitoksen, asiakkaan ja loppuasiakkaan välillä.

2.2. Kuvaus tietoliikenneratkaisusta

Tähän kohtaan kuvataan, miten loppuasiakas hoitaa tietojen käsittelyn loppukäyttäjään päin. Käytännössä kuvaus on helpointa toteuttaa kuvana, josta käyvät ilmi myös tietoliikenneyhteyttä koskevat tietoturvaratkaisut. Tietoliikenneratkaisujen kuvaamisen lisäksi tulee olla myös kuvaus lokitietojen käsittelystä, käsittelyoikeuksista ja säilyttämisestä säilytysaikoineen. Sopimuksen mukaan lokitietojen säilytysaika määräytyy Tunnistusrajapinnan käyttöhetken mukaisesti, ja se voi vaihdella käytännössä 11 vuodesta 12 vuoteen.

3. Tarkentavat kysymykset

Yleiskuvausta täydennetään seuraavilla KVP-tietojen käsittelyä (mukaan lukien tietojen katselu) tarkentavilla kysymyksillä.

3.1. Hallinnollinen ja henkilöstöturvallisuus

3.1.1. Kenellä Asiakkaan henkilökuntaan kuuluvalla on pääsy asiakkaan järjestelmän lokitietoihin, jotka koskevat tämän sopimuksen mukaisia lokitietoja? Pääsyoikeudet kuvataan rooli-tasolla.

3.1.2. Kuinka lokitietojen käsittelyä seurataan ja valvotaan asiakkaan organisaatiossa?

3.1.3. Sitoutuuko asiakkaan henkilöstö kirjallisesti lokitietojen salassapitoon ja asianmukaiseenkäsittelyyn? Missä ja kuinka kauan mahdollisia salassapitosopimuksia säilytetään?

3.1.4.	Kuinka käyttöoikeuksien hallinta (käyttöoikeuksien myöntäminen, muuttaminen, tarkistaminen, poistaminen ja hyväksyminen) hoidetaan? Kysymys koskee sekä Asiakkaan omaa henkilöstöä että loppuasiakkaita.
3.1.5.	Kuinka usein Asiakkaan henkilöstön käyttöoikeudet tarkistetaan?
3.2.	**Tietojen turvaaminen**
3.2.1.	Kuinka poistettavaksi sovitut tai vanhentuneet lokitiedot hävitetään asiakkaan tietojärjestelmistä?
3.2.2.	Otetaanko lokitietiedoista varmuuskopioita? Miten, missä ja kuinka kauan niitä säilytetään?
3.2.3.	Miten lokitietojen suojaus asiattomalta, vahingossa tai laittomasti tapahtuvalta tietojenmuuttamiselta, on järjestetty?
3.2.4.	Kuinka lokit hävitetään?
3.3.	**Fyysinen turvallisuus**

3.3.1.	Missä organisaation laitteissa ja tiloissa lokitietoja säilytetään?
3.4.	**Käyttäjien tunnistaminen**
3.4.1.	Kuinka loppuasiakas varmistaa KVP-tietojen käsittelyn edellyttämän vahvan tunnistautumisen kaikkien niiden henkilöiden osalta, joilla on mahdollisuus päästä KVP-tietoihin?
3.5.	**Käyttö- ja laitteisto, ohjelmisto- ja tietoliikenneturvallisuus**
3.5.1.	Kuka (rooli) vastaa organisaation käyttö- ja laitteisto-, ohjelmisto- ja tietoliikenneturvallisuudesta?
3.5.2.	Miten estetään ulkopuolisten pääsy asiakasorganisaation tietoverkkoon?
3.5.3.	Kuinka asiakas varmistaa, että salassa pidettävää lokitietoa ei joudu asiattomille tietovälineiden huollon tai poiston yhteydessä?
3.6.	**Poikkeamatilanteet ja raportointi**

3.6.1. Kuinka mahdollisia poikkeamatilanteita seurataan organisaatiossa?
3.6.2. Kuinka mahdollisista tietoturvapoikkeamista tai niiden uhasta raportoidaan Maanmittauslaitokselle?