Tietoturvakuvaus

SMS Gateway

1 Hallinnollinen tietoturva

1.1 Henkilöstö

Toimittajan on määriteltävä henkilöstönsä tietoturvaan liittyvät velvollisuudet ja vastuut sekä varmistettava henkilöstönsä soveltuvuus tietoturvaan liittyviin tehtäviin tämän sopimuksen kattamien tehtävien ja tietojen käsittelyn osalta.

Toimittajan on vältettävä työtehtävien ja vastuiden yhdistämistä, jos yhdistämisestä syntyy tietoturvariskejä tämän sopimuksen soveltamisen osalta.

Toimittajan on toteutettava sopimuksen kohde siten, että käyttöoikeudet tilaajan aineistoon sekä siihen liittyviin loki-, hallinta- ja konfiguraatiotietoihin annetaan vain henkilöille, jotka tarvitsevat näitä oikeuksia sopimuksen mukaisten työtehtäviensä suorittamiseen. Oikeudet myönnetään pienimmän oikeuden periaatteen mukaisesti.

Toimittaja pitää kirjaa järjestelmäkohtaisesti siitä, keillä on pääsy sopimuksen kohteen toteuttavaan järjestelmään, mitkä oikeudet henkilöllä ovat ja millä perusteella oikeus on annettu. Toimittaja poistaa käyttöoikeudet välittömästi tilanteen mukaan (esimerkiksi työntekijän poistuessa toimittajan tai alihankkijan palveluksesta) ja tarkistaa aktiiviset käyttöoikeudet vähintään kerran vuodessa.

1.2 Tietoturvan hallinta

Toimittaja varmistaa sopimuksen kohteen toimittamiseen käyttämiensä tietojärjestelmien ja tietoliikennejärjestelmien tietoturvan. Toimittaja käyttää sopimuksen kohteen toimittamiseen vain sellaisia tietojärjestelmiä ja tietoliikenneratkaisuja, joiden tietoturvariskejä toimittaja pystyy valvomaan ja hallitsemaan, ja joiden tietoturva myös tilaajan on mahdollista auditoida.

1.3 Tilaajan aineisto

Toimittaja määrittelee henkilöstönsä pääsyn tilaajan aineistoon käyttäjäkohtaisesti. Toimittaja saa käsitellä tilaajan aineistoa vain sopimuksen kohteen toteuttamiseksi. Tilaajan aineiston käyttäminen toimittajan omaan liiketoimintaan on kiellettyä.

Tilaajan aineistoa käsitellessään toimittaja noudattaa voimassaolevaa Suomen ja Euroopan Unionin lainsäädäntöä. Toimittajan on muistutettava henkilöstään siitä, että tietosuojaa koskevan lainsäädännön rikkominen saattaa johtaa rikosoikeudelliseen vastuuseen.

Käsitellessään henkilötietoja ulkomailla toimittaja noudattaa Suomen lakia ja viranomaismääräyksiä. Toimittaja takaa saman tietoturvan ja tietosuojan tason riippumatta tiedon käsittelymaasta.

Sopimuksen kohteen sisältämät tiedot sekä niiden varmuuskopiot voidaan tallentaa Euroopan talousalueella. Tietoja ei saa siirtää muihin maihin.

1.4 Tietojen hävittäminen

Sopimuksen tai tietyn palvelukokonaisuuden päättyessä tai purkautuessa toimittaja palauttaa tilaajalle tilaajan luovuttaman, ajan tasalla olevan aineiston tai muutoin tilaajan palvelua koskevan aineiston sekä hävittää omilta taltioiltaan tilaajan tietoaineiston, ellei muuta ole sovittu.

Tilaaja palauttaa osaltaan toimittajan aineiston takaisin toimittajalle ja hävittää mahdolliset jäljennökset aineistosta ja sen osista ellei muuta ole sovittu. Ohjelmaa tai aineistoa ei kuitenkaan saa hävittää, mikäli laki tai viranomaisten määräykset edellyttävät sen säilyttämistä.

Tilaajan aineiston toimittamisesta tämän kappaleen mukaisesti ei toimittajalla ole oikeutta erillisveloitukseen.

1.5 Tiedon antaminen ei-julkisista asiakirjoista

Toimittaja ei saa antaa tilaajan tietoja kolmansille osapuolille, kuten muille toimittajan asiakkaille tai viranomaisille. Toimittaja ohjaa tilaajan ei-julkisia tietoja koskevat tietopyynnöt välittömästi tilaajalle.

Toimittaja ei saa yhdistää tilaajan antamia ei-julkisia tietoja muihin tietoihin muussa tarkoituksessa kuin sopimuksen kohteen toteuttamiseksi tai tilaajan erikseen antamaa toimeksiantoa suorittaakseen.

1.6 Muutoksenhallinta

Toimittaja ei saa tehdä sopimuksen kohteeseen tietoturvan tasoa heikentävää muutosta, ellei siitä ole kirjallisesti etukäteen sovittu sopijapuolten kesken.

1.7 Tietoturvasitoumukset ja tunnushakemukset

Toimittajan vastuulla on varmistaa, että kaikki sopimuksen kohteen kanssa työskentelevät henkilöt tuntevat tämän sopimuksen vaatimukset ja ovat sitoutuneet sopimuksen noudattamiseen. Toimittaja valvoo toiminnan sopimuksenmukaisuutta.

Jos toimittajan tai tämän alihankkijan palveluksessa oleva henkilö tarvitsee tunnukset tilaajan tietojärjestelmiin, tulee hänen esimiehensä täyttää ja allekirjoittaa tilaajan tunnushakemuslomake sekä toimittaa se sopimuksen yhdyshenkilölle.

Tilaajan tiloissa liikkuessaan toimittajan henkilöstön on käytettävä voimassa olevaa kuvallista henkilökorttia.

1.8 Pääsy tilaajan laitetiloihin

Toimittajan palveluksessa olevat henkilöt voivat päästä tilaajan toimitiloihin sekä käyttää tilaajan laitteita ja ohjelmistoja erikseen sovittavalla tavalla, jos se on välttämätöntä sopimuksen kohteen toteuttamiseksi. Toimittajan palveluksessa olevien henkilöiden tulee tällöin noudattaa tilaajan osoittaman vastuuhenkilön antamia ja muita tiloissa yleisesti noudatettavia ohjeita sekä käyttää henkilökorttia.

2 Tietoturva-auditoinnit

Tilaajalla on oikeus tehdä itse tai teettää riippumattomalla kolmannella osapuolella toimittajan tietoturvakäytäntöjen tai toimituksen kohteen tietoturva-auditointi kerran vuodessa.

Mikäli auditointi toteutetaan tilaajan valitseman kolmannen osapuolen toimesta, tilaaja maksaa kolmannelle osapuolelle suoritettavat korvaukset. Toimittaja on kuitenkin velvollinen osallistumaan auditointiin siten, että toimittaja toimittaa auditoinnin tekevälle taholle auditoinnissa tarvittavan dokumentaation ja muut auditoinnin kannalta välttämättömät tiedot kohtuullisessa ajassa ilman erillistä veloitusta.

Mikäli auditoinnissa paljastuu merkittäviä tietoturvapuutteita, toimittaja sitoutuu korjaamaan puutteet viipymättä ilman erillistä veloitusta.

Tarkastus on suoritettava siten, että toimittajan turvallisuusjärjestelyt eivät vaarannu.

3 Toimittajan raportointivelvollisuudet

3.1 Ilmoitusvelvollisuus

Sopijapuolen on ilman aiheetonta viivytystä ilmoitettava toiselle sopijapuolelle sellaisista sopijapuolen tietoon tulleista seikoista, jotka voivat vaikuttaa sopimuksen kohteen toteuttamisen tietoturvallisuuteen. Velvollisuus koskee muun ohella tietoturvariskejä ja muutoksia turvajärjestelyissä.

Toimittajan on ilmoitettava tilaajalle tiedossaan olevat sopimuksen kohteen tai sen toteutusteknologian tai komponenttien haavoittuvuudet sekä niiden korjausmahdollisuudet ja toimenpiteet, joilla tietoturvan heikentyminen voidaan minimoida.

Toimittajan tulee viipymättä ilmoittaa tilaajalle havaitsemansa tietoturvaloukkaukset tai tietoturvaa uhkaavat tekijät, jotka koskevat sopimuksen kohdetta tai tilaajaa, sekä kyseisten uhkien tai loukkausten aiheuttamat toimenpiteet.

Uhkaavia tekijoitä ovat esimerkiksi:

1. vanhentuneet salausmenetelmät

2. vanhentuneet ohjelmistoversiot ja puuttuvat päivitykset
3. palvelunestohyökkäykset
4. toimittajan joutuminen tietomurron kohteeksi

Lisäksi toimittajan tulee ilmoittaa viipymättä sopimuksen kohteen poikkeavaan käyttöön liittyvät seuraavat tilanteet:

1. vakiintuneesta normaalitasosta äkillisesti kohonnut tai muuttunut käyttövolyymi, resurssien käyttö tai virheilmoitusten määrä
2. järjestelmän tai sovelluksen verkkoliikenteen äkillinen muuttuminen.

Toimittajan tulee ilmoittaa tilaajalle tietoturvaan liittyvässä dokumentaatiossa tapahtuneet muutokset ja toimittaa viipymättä tilaajalle ajan tasalla oleva dokumentaatio.

3.2 Määräajoin suoritettava raportointi

Toimittajan on raportoitava tilaajale tilaajan pyynnöstä sekä mahdollisen tietoturvaloukkauksen selvityksen yhteydessä seuraavat seikat:

1. Ylläpitotunnuksien luettelo (henkilöiden nimet) ja tunnusten tila.
2. Käyttäjätunnuksien lukumäärä ja tila.
3. Asennettujen tietoturvapäivityksien suhde julkaistuihin.
4. Ylläpitomenettelyjen ajantasaisuus: ylläpitomenettelyissä tapahtuneet muutokset tai se, että muutoksia ei ole tapahtunut.
5. Asennettujen ohjelmistojen ajantasaisuus ja muuttumattomuus.
6. Palautumissuunnitelman ajantasaisuus ja arvio palautuksen toteutuksen kestosta.
7. Varmenteiden ajantasaisuus.
8. Laitteiston ajantasaisuus. Toimittajan on pidettävä yllä laitteista, niiden kokoonpanosta ja ohjelmistoasennuksista ajantasaista muutoshallintadokumentaatiota, joka on oltava saatavilla ja siirrettävissä tilaajalle viivytyksettä.

4 Varautuminen yleisesti tunnettuihin tietoturvauhkiin

Toimittajan tulee tilaajan pyynnöstä antaa tilaajalle vuosittain vapaamuotoinen selvitys sopimuksen kohteeseen liittyvistä yleisistä tietoturvauhkista sekä siitä, miten tarjoaja on ratkaisussaan varautunut yleisiin tietoturvauhkiin.

5 Koventaminen

Tuotantokäyttöön siirryttäessä ratkaisusta on passivoitava testaus- ja asennuskäyttöön perustetut käyttäjätunnukset ja palvelut sekä palvelut ja ominaisuudet, joita tilaaja ei aio ottaa käyttöön. Lisäksi tuotantokäytön alkaessa ratkaisusta on passivoitava asennusta ja testausta varten käytössä olleet tietoliikenneportit sekä ohjelmistopalvelut ja -komponentit.

Toimittaja vastaa, että sopimuksen kohteen toteuttamisen kannalta turhia palveluita ei asenneta (esimerkiksi ftp, smtp).

6 Haittaohjelmasuojaus

Jokaisessa sopimuksen kohteen toteuttamisessa käytettävässä tietoverkkoon liitettävissä olevassa laitteessa on oltava ajantasainen haittaohjelmasuojaus (”virustorjunta”). Toimittaja vastaa siitä, että järjestelmän haittaohjelmasuojaus on ajan tasalla ja raportoi tilaajalle haittaohjelmasuojauksen tilasta säännöllisesti.

7 Pääsyn- ja käyttövaltuuksien hallinta

7.1 Yleiset vaatimukset

Käyttövaltuuksien hallinta perustuu roolipohjaiseen käyttövaltuuksien hallintaan. Sopimuksen kohteen ylläpidon ja käytön tulee tapahtua yksilöidyillä henkilökohtaisilla käyttäjätunnuksilla, joiden käyttö voidaan tarvittaessa jäljittää. Kaikkien tunnusten on oltava dokumentoituja. Sopimuksen kohteessa ei saa olla pysyvästi koodattuja tunnuksia ja salasanoja. Tilaajan on pystyttävä vaihtamaan tarvittaessa kaikki salasanat.

Sopimuksen kohteen toteutuksessa tulee olla pääsynvalvontamekanismi, joka estää muita kuin käyttäjiä, joille on annettu käyttövaltuudet, käyttämästä järjestelmää. Jos pääsynvalvontamekanismi on käyttäjätunnus/salasana-autentikaatio, toteutuksen on oltava sellainen, että järjestelmä ei säilytä salasanoja selväkielisinä.

Sopimuksen kohteen tavanomaisen käytön ei tule edellyttää ylläpitotunnuksia. Ylläpitotunnuksia käytetään ainoastaan asentamisessa ja ylläpidossa.

Toimittajan henkilökunta saa käyttöoikeudet tilaajan järjestelmiin tilaajan käyttövaltuuksien hallintamenettelyn mukaisesti.

Tilaajalla on oikeus rajoittaa käyttäjän käyttöoikeuksia tai sulkea käyttäjätunnus, jos tilaajalla on esimerkiksi syytä epäillä, että käyttäjätunnus on kaapattu tai sitä käytetään vahingollisella tavalla. Sopimuksen kohde on toteutettava niin, että edellä mainitut ylläpitotoimet voidaan tehdä ohjeistetusti ja tarvittaessa välittömästi joko tilaajan pääkäyttäjän toimesta tai tilaajan palvelupyynnön perusteella.

8 Tietoliikenne

8.1 Yleiset tietoliikennevaatimukset

Toimittajan on ilmoitettava tarkat tiedot ratkaisun tietoliikenneyhteyksistä, mukaan lukien tietoliikenneprotokollat, palveluportit ja yhteydenmuodostussuunnat.

Langatonta ja langallista verkkoa käyttävien palvelujen tulee riittävän käytettävyyden takaamiseksi olla teknisesti toteutettu niin, että palvelut toipuvat tilapäisistä tietoliikennekatkoista.

9 Yhteyksien suojaus

Sopimuksen kohteen toteutuksessa tietoliikenneyhteyksien tulee olla salattuja. Toimittajan konesalin sisäiset lähiverkkoyhteydet voivat kuitenkin olla salaamattomia. Käytetyt salausratkaisut pitää pystyä tarvittaessa vaihtamaan.

10 Kryptografiset vaatimukset

Sopimuksen kohteessa käytettävien salausmenetelmien on täytettävä viimeisimmän Viestintäviraston ohjeen "Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot" vaatimukset tasolle ST IV.

10.1 Tietoturvaprotokollat

Sopimuksen kohteeseen liittyvät tietoliikenne suojataan salauksella. Suojaamisen käytetään lähtökohtaisista uusinta vakaata protokolla- ja algoritmiversiota. Tällä hetkellä vaatimustasona ovat seuraavat:

- Sovellusliikenteen salauksessa käytetään TLS-versiota 1.2 tai uudempaa
- Toimipisteiden väliseen liikenteeseen käytetään jotain seuraavista:
    - IPsec-tunnelointia (IKEv2)
    - TLS-protokollaa.

10.2 Varmenteet

Salauksen toteuttamiseen voidaan käyttää mm. seuraavia, tilaajan kautta saatavia varmenteita:

1. Tilaajan AD-domainin varmennepalvelussa tuotetut varmenteet, joihin tilaajan hallinnassa olevat laitteet luottavat. Tilaaja vastaa näiden varmenteiden sulkulistan julkaisemisest säännönmukaisesti.
2. Kaupallisista varmenteista käytetään tällä hetkellä VRK:n, Geotrustin, Entrustin ja Verisignin varmenteita.