

Sovelto Oyj:n tietoturvapoliittika

Vastuu Sovelto Oyj:n toiminnasta on sen ylimmällä johdolla. Yrityksen toiminta ja palvelut ovat suuresti riippuvaisia tietotekniikkapalveluiden saatavuudesta ja niiden turvallisesta toiminnasta. Tietotekniikan hyödyntäminen ja tietoturvallisuuden panostaminen ovat johdon strategisia päätöksiä, joilla vaikutetaan Sovelto Oyj:n toimintakykyyn merkittäväällä tavalla.

Sovelto Oyj:n toiminnan ydin perustuu tietoon. Tiedon turvaaminen on oleellinen osa Sovelto Oyj:n toiminnan ja palveluiden laatua, kokonaisturvallisuutta ja yrityksessä tapahtuvaa päivittäistä tietojen käsittelyä. Tietoturvallisuuden hyvä hallinta edellyttää kaiken toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua, varautumista erilaisiin uhkatilanteisiin, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää.

Sovelto Oyj:n tavoitteena on luoda ja ylläpitää luotettava ja turvallinen ympäristö henkilökunnan, asiakkaiden ja ulkoisten sidosryhmien tietojen käsittelyyn.

Tietoturvapoliittika on Sovelto Oyj:n johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot yrityksessä.

Tietoturvapoliittika on julkinen asiakirja ja se voidaan antaa kaikille siitä kiinnostuneille tiedoksi.

Tavoitteet

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Tietojen turvaamisessa huomioidaan omina osa-alueinaan valtionhallinnon käytännön mukaan hallinnollinen, henkilöstö-, fyysinen, tietoaaineisto-, tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuus. Tietojen turvallisuudesta on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan.

Sovelto Oyj:n tavoitteena on turvata riittäväällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen.

Tietoturvatyö on tietojen turvaamiseksi tehtävää jatkuvaa kehittämistä, suunnittelua, toteuttamista ja seurantaa koko Sovelto Oyj:n henkilöstön osalta. Tietoturvatyöllä pyritään ennaltaehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhista aiheutuvat vahingot tai rajoittamaan ne hyväksyttävälle tasolle sekä varautumaan poikkeamatilanteista toipumiseen.

Sovelto Oyj varautuu tietoturvallisuuden osalta häiriö- ja poikkeusoloihin siten, että yrityksen toimintaa voidaan jatkaa mahdollisimman häiriöttömästi kaikissa olosuhteissa.

Sovelto Oyj:n tietoturvallisuudesta huolehditaan kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti sekä noudattaen myös valtionhallinnon tietoturvallisuudesta antamia ohjeita ja suosituksia.

Sovelto Oyj:n tavoitteena on, että tietoturvajärjestelyt ovat hyvää kansallista ja kansainvälistä tasoa.

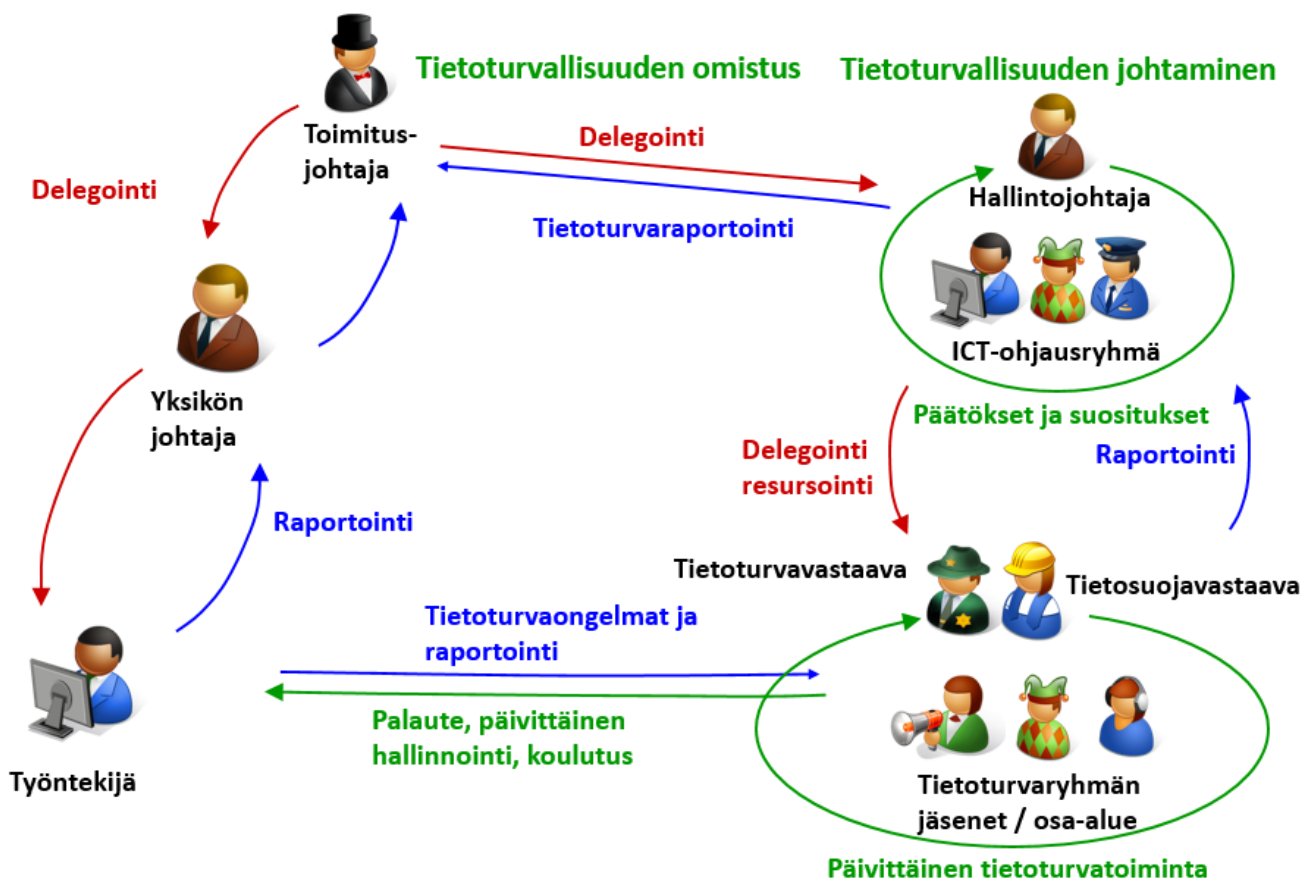
Sovelto Oyj:n eri toimipisteiden perusluonne ja mahdolliset tarpeet turvallisuuden tehostamiseen tulee ottaa huomioon tietoturvallisuuden toimintoja suunniteltaessa.

Vastuut ja organisointi

Tietoturvallisuuden toteuttaminen on jatkuvaa laaja-alaista toimintaa, jota ei voida asettaa vain muutaman vastuuhenkilön kannettavaksi, vaan johon tarvitaan tiivistä ja rakentavaa yhteistyötä kaikkien Sovelto Oyj:n työyhteisöön kuuluvien henkilöiden ja ryhmien kesken. Tietoturvallisuus toimii tehokkaimmillaan silloin, kun kaikki tiedon käsittelijät huolehtivat oman tehtäväkenttensä tietoturvallisuudesta parhaalla mahdollisella tavalla.

Vastuu Sovelto Oyj:n toiminnasta on sen ylimmällä johdolla.

Vastuu tietoturvallisuuden toteuttamisesta ja valvonnasta kuuluu jokaiselle yrityksessä jollain tavalla toimivalle henkilölle.



KUVA 1. Sovelto Oyj:n tietoturvallisuuden hallinnointi

Tietoturvallisuus on osa Sovelto Oyj:n kokonaisturvallisuutta ja tietohallintoa.

Sovelto Oyj:n johtoryhmä vastaa tietoturvallisuuden päälinjauksista, strategisesta ohjauksesta, seurannasta sekä riittävästä resursoinnista.

Sovelto Oyj:n johtoryhmä nimeää yrityksen omistamien tietojen ja tietojärjestelmien omistajat, jotka toimivat näiden omien osa-alueidensa vastuuhenkilöinä.

Tietojen ja tietojärjestelmien omistajat vastaavat tietoturvallisuuden toteutumisesta.

Vastuu tietoturvallisuuden kokonaisvaltaisesta kehittämisestä on **hallintojohtajalla**, joka raportoi tietoturvallisuuden tilasta toimitusjohtajalle. Hallintojohtajan tukena käytännön toteutuksissa ovat ICT-ohjausryhmän jäsenet sekä eri toimialueista vastaavat asiantuntijat. ICT-ohjausryhmän keskeisinä tehtävinä tietoturvallisuuden osalta ovat:

- suunnitella, kehittää, toteuttaa ja valvoa Sovelto Oyj:n tietoturvallisuutta
- hallita tietojärjestelmiin ja tietotekniikkapalveluihin liittyviä tietoturvallisuuden riskejä, ja sekä huolehtia, että yrityksellä on poikkeusolojen jatkuvuussuunnitelmat infrastruktuurin, keskeisten järjestelmien ja palveluiden osalta
- vastata Sovelto Oyj:n tietoliikenneverkon turvallisuudesta, keskeisten tietoturvallisuutta parantavien ohjelmistojen ja laitteistojen hankinnasta sekä näihin liittyvistä palveluista
- ylläpitää ja tuottaa ajantasaista koko yritystä koskevaa tietoturvaohjeistusta sekä tiedottaa ajankohtaisista tietoturvallisuuden aiheista
- huolehtia henkilöstön tietoturvatietoisuuden lisäämisestä ja tietoturvakoulutuksen suunnittelusta

Tietoturvavastaava toimii yhteistyössä Sovelto Oyj:n ICT-ohjausryhmän ja Sovelton tietoturvaryhmän kanssa. Tietoturvavastaavan tehtävänä on:

- vastata tietoturvallisuuden kehittämisestä kokonaisuutena osana Sovelto Oyj:n tietohallintoa ja osana Sovelto Oyj:n kokonaisturvallisuutta
- organisoida ja koordinoida tietoturvallisuuden toimintojen ja ryhmien toimintaa yrityksessä
- vastata tietoturvaluuskoulutuksen järjestämisestä sekä tiedottaa tietoturvaluusasioista ja -ongelmista
- valvoa ja puuttua havaitsemiinsa tietoturvapoikkeamiin sekä johtaa tietoturvapoikkeamatilanteiden sisäistä tutkintaa
- kehittää yhdessä Sovelton omien asiantuntijoiden sekä muiden tietoturvatyöntekijöiden kanssa kansallista tietoturvayhteistyötä
- raportoida hallintojohtajalle Sovelto Oyj:n tietoturvallisuuden tilanteesta

Tietoturvavastaavan tukena toimivat nimetyt tietoturvaryhmän jäsenet ja muut Sovelton asiantuntijat, joiden erityisenä tehtävänä on tukea käytännön tietoturvatyötä ja auttaa yrityksen tietoturvatavoitteiden toteuttamisessa.

Sovelto Oyj:n työyhteisöön kuuluvien henkilöiden ja ryhmien vastuut ja velvollisuudet on määritelty henkilöstön tietoturvaohjeessa.

Pääsääntö on se, että jokainen Sovelto Oyj:n tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on viime kädessä itse vastuussa tietoturvallisuuden toteuttamisesta.

Toteutuskeinot

Tietojen käsittelyyn ja tietojärjestelmiin liittyviä riskejä hallitaan tietoturvallisuuden riskien hallinnan periaatteiden mukaisesti. Tunnistettujen riskien ja haluttujen kehittämistoimien pohjalta tietoturvavastaava laatii Sovelto Oyj:n tietoturvan kehittämissuunnitelman. Tietoturvaryhmä apunaan muut asiantuntijat avustavat riskien hallinnoinnissa yritystä luomalla sääntöjä ja menettelyohjeita, sekä rakentamalla teknisiä työkaluja, joilla tietoturvariskejä voidaan tunnistaa ja ehkäistä.

Tietoturvallisuuden ylläpito ja kehittäminen on jatkuva prosessi, joka tapahtuu hallinnollisten, fyysisten ja tietoteknisten ratkaisujen avulla.

Tietojen ja tietojärjestelmien omistajat toteuttavat tietoturvallisuuden käytännön riskien hallintaa tietoturvakartoituksin ja tunnistettuja riskejä ehkäisemällä. Kartoituksia toistetaan määräajoin sekä merkittävien muutosten yhteydessä. Yksittäiset tietoturvatoteutukset kuvataan tarvittaessa erillisissä suunnitelmissa. Tietoturvallisuuden puutteet analysoidaan ja korjataan tietojen omistajien ja järjestelmien ylläpitäjien toimesta.

Tietoturvallisuus sisältyy Sovelto Oyj:n toimintaprosessien kehittämiseen sekä yksiköiden vuosisuunnitteluun.

Henkilökunnalle tiedotetaan tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista sekä järjestetään koulutustilaisuuksia.

Käyttäjien toiminnan tietoturvallisuutta ohjataan ohjeilla ja säännöillä sekä tietojen turvallisen käsittelyn koulutuksella ja tiedotuksella.

Tietojen turvallisesta käsittelystä solmitaan sopimukset myös Sovelto Oyj:n tietoja käsittelevien organisaatioiden sekä muiden yhteistyökumppaneiden kanssa.

Sovelto Oyj:n tietoturvallisuutta koskevat asiat eivät ole aktiivisen ulkoisen tiedottamisen aihe. Tietoturvallisuuteen liittyvästä tiedottamisesta vastaa tietoturvavastaava.

Seuranta ja ongelmatilanteiden käsittely

Tietoturvallisuudesta huolehtiminen edellyttää jatkuvaa tietoturvallisuuden seurantaan sekä sen tason ja poikkeamien raportointia. Seuranta toteutetaan sekä teknisin että hallinnollisin keinoin. Tietoturvavastaava koordinoi tietoturvallisuuden seurantaan ja raportoi tietoturvallisuuden tasosta ja sen poikkeamista hallintojohtajalle. Lisäksi tietoturvavastaava raportoi ICT-ohjausryhmälle.

Tietoturvavastaava voi tarvittaessa käynnistää Sovelto Oyj:n tietojen käsittelyn turvallisuuteen liittyviä kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi. Tietoturvavastaava voi puuttua myös tiedon turvattomaan manuaaliseen käsittelyyn.

Jos tiedon hallintatavasta tai tietojärjestelmästä on uhkaa Sovelto Oyj:n tietoturvallisuudelle, tietoturvavastaavalla on oikeus määrätä sille säännösten pohjalta hallinnollisia tai teknisiä rajoituksia.

Yksiköissä tietoturvallisuuden seurantaan koordinoivat yksikön johtaja ja tietojärjestelmien vastuuhenkilöt. Seuranta on kattavaa ja jatkuvaa, puutteista raportoidaan kampuksen tietoturvakoordinaattorille. Tietoturvavastaava johtaa poikkeamien sisäistä tutkintaa ja huolehtii rikostapauksissa yhteydenpidosta viranomaisiin.

Tietoturvarikkomusten tutkinnan aikana tietoturvavastaavalla on mahdollisuus rajoittaa käyttöoikeuksia tietojärjestelmiin.

Jokaisen tiedon käsittelijän velvollisuutena on ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista tiedon tai tietojärjestelmän omistajalle.

Sovelto Oyj

21.3.2018

JULKINEN

Tietoturvavastaava vastaa tietoturvapoikkeamien jatkotoimenpiteistä säännösten ja kuvattujen prosessien pohjalta.

Ohjeet ja säännöt

Tietoturvapoliittikkaa tukevat ICT-ohjausryhmän ja tietoturvaryhmän ylläpitämät asianmukaiset tietoturvallisuuteen ja tietojärjestelmiin liittyvät ohjeistukset ja säännöt.

Tietoturvallisuuden ja tietojärjestelmien käyttöön liittyvistä säännöistä ja niiden ajantasaistamisesta päättää hallintojohtaja.

Tietoturvallisen toiminnan tueksi henkilöstölle on luotu toimintaohjeita ja prosesseja, jotka on julkaistu erillisessä sisäisessä dokumentissa. Lisäksi henkilöstölle on tehty useita ohjevideoita aiheeseen liittyen.

Liitteet

Tietoturvaan liittyvät liitteet ovat pääosin luottamuksellisia asiakirjoja. Dokumentaatio ja sen ylläpito on jatkuva prosessi, jolla pyritään pitämään ohjeistus ajantasaisena ja kaikkien tiedossa. Dokumentaatioon kuuluvat mm. seuraavat tätä tietoturvapoliittikkaa tukevat asiakirjat:

1. Tietoturvan kehittämissuunnitelma
2. Tietoturvaan liittyvien toimintojen prosessikuvaukset
3. Tietoturvan ohjeistus henkilöstölle
4. Asiakirjojen luokittelu ja käsittelyohje
5. Roolien määrittely, vastuut ja kontrollit