OPR-Finance

Tietoturvapolitiikka

1. Tietoturvapolitiikan tarkoitus

Tämä tietoturvapolitiikka määrittelee tietoturvallisuustyön tavoitteet, vastuut ja keinot koko organisaation (OPR-Finance) toiminnassa. Politiikkaa täydennetään erillisillä ohjeilla ja prosessikuvauksilla.

2. Tietoturvapolitiikan tavoitteet

Tietoturvallisuudella varmistetaan, että kaikki organisaation suojausta vaativat tiedot tunnistetaan, luokitellaan ja suojataan asianmukaisella tavalla. Tavoitteena on, että tietoja ei käytetä luvattomasti, että tiedot eivät muutu tai tuhoudu hallitsemattomasti ja että tiedot ovat tarvittaessa käytettävissä.

3. Vastuu tietoturvallisuudesta

Tietoturvallisuuden kokonaisvastuu on organisaation johdolla ja tarkemmin vastuut on määritetty seuraavasti:

- **Tietoturvavastaava:** Tietoturvavastaava vastaa tietoturvallisuuden organisoinnista ja ylläpidossa koko organisaatiossa. Tietoturvavastaavan vastuulla on laatia esityksiä tietoturvan parantamiseksi, kerätä ja välittää tietoa tietoturvallisuuteen liittyvistä asioista sekä tarkistaa tietoturvatilanne säännöllisesti. Tietoturvavastaava raportoi organisaation johdolle tietoturvapoikkeamista ja tietoturvan tilasta.
- **Prosessin omistaja:** Prosessin omistaja vastaa prosessissa käytetyistä järjestelmistä sekä niiden tietoaineistoista ja tietoturvasta.
- **Järjestelmävastaava:** Järjestelmävastaava vastaa järjestelmän operatiivisesta toteutuksesta sekä ylläpidosta, yhteistyössä prosessin omistajan kanssa.
- **Esimiesten** vastuulla on huolehtia siitä, että omat alaiset ovat tietoisia annetuista tietoturvaohjeista ja noudattavat niitä.
- **Koko henkilöstö** on vastuussa heidän käyttäjätunnuksillaan tehdyistä toimenpiteistä. Lisäksi he vastaavat tietoturvapolitiikan, tietoturvaperiaatteiden ja tietoturvaohjeistuksien noudattamisesta omassa työssään, ja ovat velvollisia ilmoittamaan havaitsemistaan tietoturvapoikkeamista esimiehelleen ja/tai tietoturvavastaavalle.

4. Tietoturvan hallinnan keinot

Riskienhallinta

Tietoturvariskit kartoitetaan osana organisaation operatiivista riskienhallintaa. Tunnistetuille riskeille pyritään laatimaan hallintasuunnitelma, tarvittavat toimenpiteet aikataulutetaan ja vastuutetaan.

Tietojen luokittelu ja suojaus

Kaikki tiedot ja järjestelmät pyritään luokittelemaan niiden suojaustarpeen mukaan. Tietojen ja tietojärjestelmien luokittelu on tiedon omistajan vastuulla. Mikäli järjestelmä sisältää useaan suojausluokkaan kuuluvaa tietoa, käsitellään tätä järjestelmää korkeimman sen sisältämän tiedon suojausluokan mukaan.

Valvonta ja seuranta

Kokonaisuuden hallinnan ja koordinoinnin vastuu on Tietoturvavastaavalla. Näihin toimiin kuuluu myös annettujen ohjeistusten noudattamisen valvonta ja teknisten valvontamenettelyjen tilanteen seuranta.

Tietoturvapoikkeamien hallinta

Tietoturvapoikkeamien hallintaprosessissa määritellään, miten toimitaan tietoturvaloukkaus- tai epäillyissä tietoturvaloukkaustilanteissa. Selvät tietoturvapoikkeamat käsitellään johdon katselmoinnissa.

Jatkuvuus- ja toipumissuunnittelu

Keskeiset järjestelmät on tunnistettu ja niiden suojaamiseksi ja jatkuvuuden varmistamiseksi on tehty riittävät toimenpiteet.

Ulkoistuskumppanien osalta riittävän tietoturvallisuuden taso ja jatkuvuussuunnittelu pyritään varmistamaan sopimusteitse ja auditointioikeuden avulla.

Koulutus ja perehdytys

Uusille työntekijöille kerrotaan, miksi tietoturvallisuus on toiminnassa tärkeää ja esitellään noudatettavat tietoturvaohjeet. Tietoturvatietoisuutta tarjotaan organisaation työntekijöille koulutussuunnitelman mukaisesti. Esimiehet ovat vastuussa alaistensa tietoturvatietoisuuden ylläpidosta ja seurannasta.

5. Politiikan voimassaolo ja katselmointi

Tämä tietoturvapolitiikka on voimassa hyväksymispäivästä alkaen. Politiikka katselmoidaan johdon toimesta säännöllisesti, jolloin siihen tehdään tarvittavat päivitykset.