Tietoturvapolitiikka

Tietoturvapolitiikka

Sisällys

1. TIETOTURVA

Osekk on dynaaminen, korkeatasoinen ja työelämälähtöinen koulutuksen järjestäjä. Sen oppilaitokset ovat arvostettuja ja kansainvälisiä. Ne muodostavat keskeisen osan Oulun seudun innovaatioympäristöä. Osekk toimii tietoturvatyössään avoimesti, opiskelijoiden ja sidosryhmien parhaaksi sekä yhdessä sovittuja tietoturvan pelisääntöjä noudattaen.

Osekk noudattaa toiminnassaan tietoturvan ja tietosuojan hallintamenettelyä, joka pohjautuu voimassaoleviin lakeihin, asetuksiin ja viranomaismääräyksiin.

Keskeisiä lakeja ovat

- henkilötietolaki
- sähköisen viestinnän tietosuojalaki
- laki yksityisyyden suojasta työelämässä
- rikoslaki.

Tietoturvalla tarkoitetaan tiedon luottamuksellisuuden, eheyden ja käytettävyyden varmistamista. Luottamuksellisuudella tarkoitetaan sitä, että tieto on vain niiden käytettävissä, joilla on sen käyttöön oikeus. Eheydellä varmistetaan, että tieto on suojattu tahattomalta tai tarkoitukselliselta tiedon luotettavuutta uhkaavalta muuttamiselta. Käytettävyys tarkoittaa sitä, että tieto on saatavilla silloin, kun tietoa tarvitaan. Turvattavia tietoja ovat sekä manuaalisessa että sähköisessä muodossa olevat tiedot.

Tietoturvapolitiikalla yhtymähallitus määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot koulutuskuntayhtymässä. Tietoturvapolitiikkaa tarkennetaan erikseen annettavilla tietojen käsittelyn säännöillä ja ohjeilla.

2. TAVOITE

Osekkin tietoturvallisuustyön tavoitteena on mahdollistaa yhtymän ja sen oppilaitosten häiriötön toiminta turvaamalla riittävällä ja tarkoituksenmukaisella tasolla toiminnalle tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, havaita ja estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida niistä mahdollisesti aiheutuvat vahingot.

Tietoturvakäytännöillä luodaan ja ylläpidetään luotettava ja turvallinen ympäristö omien sekä sidosryhmien tietojen käsittelyssä.

3. VASTUUT

Yhtymähallitus hyväksyy tietoturvapolitiikan. Yhtymähallitus voi valvontatehtävässään käyttää tarvittaessa sisäistä tai ulko-puolista arviointia tietoturvariskien hallitsemiseksi.

- Kuntayhtymän johtaja vastaa tietoturvan kokonaisuudesta.
- Toimialojen ja yksiköiden johtajat vastaavat tietoturvan toteutumisesta omissa toimin-

taympäristöissään ja oman toimialansa tai yksikkönsä riittävästä tietoturvaresursoinnista sekä siitä, että henkilöstöllä on riittävä perehdytys tietoturvaan.

- Esimiehet seuraavat vastuualueensa tietoturvallisuuden toteutumista osana tavanomaista sisäistä valvontaa.
- Tietojärjestelmien omistajat huolehtivat tietojen käsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta, pääsynvalvonnasta ja toimintojen jatkuvuudesta. Omistajien tehtävänä on yhdessä tietoturvaryhmän kanssa kartoittaa tietojärjestelmiensä toimintaan liittyvät riskit. Tietoriskien hallinnassa noudatetaan Osekkin riskienhallintapolitiikan linjaa.
- Tietoturvavastaava yhdessä tietoturvaryhmän kanssa vastaa hallinnollisen ja teknisen tietoturvan, laite- ja kytkentätilojen tietoturvan sekä jatkuvuussuunnittelun järjestämisestä, kehittämisestä ja seurannasta.
- Henkilöstön velvollisuus on ilmoittaa havaitsemistaan tietoturvaan liittyvistä puutteista tai väärinkäytöksistä esimiehelleen tai tietoturvavastaavalle.
- Jokaisen tietoja käsittelevän tulee huolehtia omaan tehtäväänsä sisältyvästä tietoturvallisuudesta perehtymällä siitä annettuihin ohjeisiin sekä noudattamalla huolellisuutta tietoja ja asiakirjoja käsiteltäessä.

4. ORGANISOINTI JA TOTEUTUS

Tietoturvan hyvä hallintatapa edellyttää toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua ja riittävää resursointia erilaisten uhkatilanteiden varalta. Tietoturvan toteuttaminen vaatii sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja viestintää. Tietoturvan kehittämistä ja ylläpitoa koordinoi tietoturvavastaava yhdessä tietoturvatyöryhmän kanssa. Tietoturvatyöryhmän tehtävänä on valmistella tietoturvapolitiikka, laatia tietoturvaan liittyvät esitykset, ohjeet ja toimintamallit sekä tiedottaa niistä.

Tietojen käsittelyyn ja tietojärjestelmiin liittyviä riskejä hallitaan tietoturvallisuuden riskien hallinnan periaatteiden mukaisesti. Tietoaineisto luokitellaan tietojen kriittisyyden ja tunnistettujen tietoturvariskien mukaisesti. Riskikartoitusten toteutumista ja ohjeiden noudattamista seurataan systemaattisesti osana sisäistä valvontaa.

Tiedot ja tietojärjestelmät suojataan asianmukaisesti sekä normaali- että poikkeusolojen häiriötilanteisiin hallinnollisin ja teknisin toimenpitein. Toimintaympäristön riskeihin varaudutaan varustamalla laite- ja kytkentätilat tarvittavin kulunvalvonta- ja suojausratkaisuin. Toimintaa varmistetaan ajantasaisilla varautumissuunnitelmilla.
Tietojen turvallisesta käsittelystä solmitaan sopimukset myös Osekkin tietoja käsittelevien organisaatioiden sekä muiden yhteistyökumppaneiden kanssa.
Henkilön käyttö- ja kulkuoikeudet määräytyvät työtehtävien mukaan.

5. SEURANTA JA HÄIRIÖTILANTEET

Tietoturvallisuutta seurataan hyvien valvontaperiaatteiden mukaisesti. Tietoturvapolitiikan ja tietoturvasta annettujen ohjeiden noudattamisen valvonta on osa kuntayhtymän sisäistä valvontaa.

Tietojärjestelmien toimintaa valvotaan systemaattisesti voimassaolevien lakien edellyttämällä tavalla. Valvontaa toteuttavat henkilöt ovat vaitiolovelvollisia työssään käsittelemistä tiedoista.

Tietoturvaloukkauksissa tai tietoturvaan liittyvässä uhkatilanteessa kuntayhtymän johtajalla tai hänen määräämällään henkilöllä on oikeus määrätä suljettavaksi tietty tietoliikenneyhteys, järjestelmä, tunnus tai laite. Tietoturvallisuuden rikkomustilanteisiin liittyvät toimenpiteet on kuntayhtymässä määritelty erikseen.

6. VIESTINTÄ

Kuntayhtymän johtaja vastaa tietoturvaviestinnästä, sen kehittämisestä ja koordinoinnista.

Toimialajohtajat vastaavat tietoturvaviestinnästä omilla toimialoillaan sekä päättävät tietoturvaviestintävastuista toimialoillaan.

Tiedottamisesta erityistilanteissa ja poikkeusoloissa päättää kuntayhtymän johtaja niiltä osin kuin siitä ei ole muutoin säädetty tai määrätty.

7. TIETOSUOJA JA REKISTERIT

Henkilötietoja sisältäviä rekisterejä käsitellään voimassaolevan tietosuojalainsäädännön ja rekisteriselosteiden mukaisesti. Henkilöllä on oikeus tarkastaa, mitä tietoa hänestä on tallennettu, ellei voimassaolevasta lainsäädännöstä muuta johdu. Henkilötietojen käsittelijät vastaavat henkilötietoaineiston lainmukaisesta käsittelystä.

8. TIETOTURVAPOLITIIKAN HYVÄKSYMINEN JA VOIMAANTULO

Yhtymähallitus hyväksyy kuntayhtymän tietoturvapolitiikan ja siihen tehtävät muutokset. Tietoturvapolitiikka tulee voimaan 1.8.2012 lukien.

9. KÄSITTEET

Tietoturvan osa-alueet ovat hallinnollinen-, henkilöstö-, fyysinen-, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

Tietoturva (information security)
"Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Käytettävyys tarkoittaa tietoturvallisuuden yhteydessä sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta."

Tietosuoja (privacy protection)
Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä.

Tietoturvapolitiikka (information security policy)
Johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta.

Tietoturvasuunnittelu (information security planning)
Suunnitteluprosessi, johon kuuluu muun muassa uhka-analyysi, perusturvallisuuden määrittely sekä toipumisvalmiuden ja poikkeusolojen valmissuunnittelu, ja jonka tuloksena on tietoturvasuunnitelmia, -linjauksia ja -ohjeistoja

Eheys (integrity)
Ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Käytettävyys (availability)
Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Luottamuksellisuus (confidential)
Vain tietyn henkilön tai tiettyjen henkilöiden tietoon tarkoitettu.

Fyysinen turvallisuus (physical security)
Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden.

Hallinnollinen tietoturva (administrative and organizational information security)
Tietoturvaan tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.

Henkilöstöturvallisuus (personnel security)
"Henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen sekä työyhdistelmien järjestelyihin liittyvien turvallisuustekijöiden hoitamista"

Valtionhallinnon tietoturvasanasto
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/name.jsp

UUSIKATU 2, PL 213, 90101 OULU, PUHELIN 010 27 21011, FAKSI 010 27 21150, S-POSTI OSEKK@OSEKK.FI www.osekk.fi