Päämäärä ja tavoitteet

Tietoturvapolitiikka määrittelee Seinäjoen koulutuskuntayhtymän (ylläpitäjäorganisaatio) tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot. Tietoturvallisuus on osa ylläpitäjäorganisaation laatujärjestelmää.

Ylläpitäjäorganisaation tietoturvallisuustyön päämäärä on turvata ylläpitäjäorganisaation toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Hallinnollisten, teknisten ja muiden toimenpiteiden avulla ylläpitäjäorganisaation tiedot, tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa.

Ylläpitäjäorganisaation tavoitteena on, että tietoturvajärjestelyt ovat hyvää kansallista ja kansainvälistä tasoa. Lisäksi tavoitteena on, että tietoturvallisuuden perustaso kattaa ylläpitäjäorganisaation kaiken tietojenkäsittelyn ottaen huomioon yksikköjen perusluonteen ja mahdollisen tarpeen tietoturvallisuuden tehostamiseen.

Tietoturvallisuus

Tässä dokumentissa tietoturvallisuudella tarkoitetaan automaattisesti tapahtuvan (atk-pohjaisen) tietojenkäsittelyn turvaamista. Tämän ohella tietoturvallisuustoimet koskevat kaikkea sähköisessä, audiovisuaalisessa, suullisessa ja kirjallisessa muodossa olevaa tiedon käsittelyä, siirtoa ja säilyttämistä.

Tietoturvallisuus rakentuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä soveltuvilta osin pääsynvalvonnasta ja kiistämättömyydestä.

Luottamuksellisuus tarkoittaa, että tiedot ovat sovituilla tavoilla ja sovittuun aikaan vain niiden käyttöön oikeutettujen saatavissa ja ettei tietoja paljasteta tai muutoin saateta sivullisten tietoon.

Eheys tarkoittaa, että tiedot ja tietojärjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ole muuttuneet tai vahingoittuneet laitteisto- tai ohjelmistovikojen, luonnon-tapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena.

Käytettävyys tarkoittaa, että tiedot ja tietojenkäsittelyjärjestelmät ovat toiminnan kannalta hyväksyttävän ajan kuluessa käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille.

Pääsynvalvonta tarkoittaa, että tietoa tai tietojärjestelmää ei voi käyttää ilman asianmukaista lupaa.

Kiistämättömyys tarkoittaa todisteiden luomista sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen.

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Toimintaan kuuluvat tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

Tietoturvallisuus kattaa kaikenlaiset ylläpitäjäorganisaation automaattiset tietojenkäsittelytehtävät sisältäen myös arkistoinnin.

Ylläpitäjäorganisaation tietoturvallisuuden varmentaminen tapahtuu kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten ja suositusten pohjalta sekä valtionhallinnon tietoturvallisuudesta annettuja ohjeita ja suosituksia noudattaen.

Vastuut

Ylin vastuu tietoturvallisuudesta on ylläpitäjäorganisaation hallituksella ja ylläpitäjäorganisaation johtajalla. Tulosyksiköiden johtajat vastaavat tietoturvasta tulosvastuualueidensa osalta.

Tietohallintopäällikkö vastaa yhdessä tietoturva-alan atk-pääsuunnittelijan kanssa tietoturvallisuuden kehittämisestä kokonaisuutena, tietoturvallisuuden toteutuksen valvonnasta sekä tietoturvatietouden edistämisestä ylläpitäjäorganisaatiossa saamiensa resurssien ja toimintavaltuuksien puitteissa.

Tietoturvallisuuden käytännön toteuttamista yksiköissä ja niiden tietojenkäsittelyjärjestelmissä ohjaa ja valvoo kullekin yksikölle nimettävä tietoturvavastaava.

Ylläpitäjäorganisaatiossa on nimetyt tietokonejärjestelmien ylläpitäjät (ylläpidon vastuuhenkilöt). Jokaiselle tietojärjestelmälle tai sen osalle on heistä nimetty vastuuhenkilö.

Jokainen ylläpitäjäorganisaation tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan. Kukin ylläpitäjäorganisaation tietojärjestelmien ja niiden sisältämien tietojen ylläpitäjä tai omistaja vastaa tietojensa ja tietojärjestelmiensä suojaamisesta.

Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely

Tietoturvasta vastaamaan nimetyillä henkilöillä on asianmukainen valtuutus ja velvollisuus tehdä ylläpitäjäorganisaation tietojärjestelmien tietoturvallisuuden kartoituksia ja ryhtyä toimenpiteisiin havaittujen tietoturvallisuuden heikkouksien parantamiseksi.

Jokainen ylläpitäjäorganisaation tietojenkäsittelyjärjestelmien käyttäjä on velvollinen noudattamaan ylläpitäjäorganisaation hyväksymiä käyttösääntöjä ja tietoturvaohjeita.

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista yksikkönsä johdolle, tietoturvavastaavalle sekä tietohallintopäällikölle. Nämä reagoivat niihin erikseen määriteltävällä tavalla.

Vakavien tietoturvarikkomusten varalle ylläpitäjäorganisaatioon nimetään erityinen ryhmä, joka päättää rikkomuksen takia vaadittavista, välittömistä toimenpiteistä.

Vakaviin tietoturvarikkomuksiin liittyvä sisäinen ja julkinen tiedottaminen hoidetaan tapauskohtaisesti ylläpitäjäorganisaation keskustoimiston kautta, joko ylläpitäjäorganisaation johtajan tai tietohallintopäällikön taikka heidän valtuuttamansa henkilön toimesta.

Tietoturvallisuuden toteuttaminen käytännössä

Tietoturvallisuuden tavoitteiden saavuttaminen on jatkuva prosessi, joka sisältää hallinnollisia, fyysisiä ja teknisiä ratkaisuja. Tietoturvapolitiikan pohjalta laaditaan ylläpitäjäorganisaation käyttösäännöstö ja tietoturvaa koskevat suunnitelmat. Myös ylläpitäjäorganisaation toimintayksiköissä ja eri tietojärjestelmiä koskien laaditaan tarkempia tietoturvallisuuden kehityssuunnitelmia ja menettelytapaohjeita.

Ylläpitäjäorganisaation tietoturvallisuuden kehittämistarpeiden ja -tavoitteiden määrittelemiseksi ylläpitäjäorganisaation tietoturvallisuusriskit kartoitetaan. Myös kartoitus on jatkuva prosessi. Kartoituksen tavoitteena on tunnistaa toimintaa vaarantavat uhat, kartoittaa tietojenkäsittelyn haavoittuvat kohdat ja arvioida menetykset uhan toteutuessa sekä arvioida tietoturvallisuuden rakentamisen kustannukset riskien vähentämiseksi. Tietoturvallisuusriskit kartoitetaan ylläpitäjäorganisaation opetuksen, hallinnon sekä muiden järjestelmien ja käyttöympäristöjen tasolla. Lisäksi kartoitetaan yksittäisten laitosten erityiset tietoturvallisuusriskit.

Tietoturvallisuustason määrittämiseksi ylläpitäjäorganisaation tietoaineistot ja tietojärjestelmät luokitellaan: tietoaineistot luottamuksellisuuden mukaan ja tietojärjestelmät tärkeyden mukaan. Kullekin turvallisuusluokalle määritellään tietoturvallisuustaso ja sen mukaiset tietoturvatoimenpiteet.

Henkilökunnan saatavissa on sekä WWW-palvelun kautta, että kirjallisessa muodossa heidän toimissaan tarvitsemansa käyttösäännöt. Opiskelijoille tiedotetaan tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista. Yleensäkin ylläpitäjäorganisaatioyhteisön jäsenten tietoturvallisuustietoisuutta lisätään eri tavoin tiedottamalla. Ylläpitäjäorganisaation tietojenkäsittelyn ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisen tarkastuksen keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvallisuuden puutteet analysoidaan järjestelmien ylläpitäjien ja omistajien kanssa.