ELENIAN **TIETOTURVA-POLITIIKKA**

Tietoturvapolitiikka perustuu Elenian strategioihin, arvoihin, eettisiin periaatteisiin ja ISO/IEC 27001 -standardiin. Politiikan tarkoituksena on linjata tietoturvallisuuden tavoitteet, vastuut ja toimintatavat.

Tätä politiikkaa sovelletaan tietoturvallisuuden hallintajärjestelmään, jonka laajuus on määritelty tietoturvan hallintajärjestelmän sovellusalueen lausunnossa. Politiikan linjauksia noudattavat Elenia-konsernin yhtiöiden henkilöstö ja Elenian yhteistyökumppanit.

1. Tavoitteet, johtaminen ja vastuut

Tietoturvallisuuden tavoitteena on Elenian tiedon ja tietojärjestelmien luottamuksellisuuden, eheyden ja saatavuuden varmistaminen.

Elenian IT-periaatteet, perustoiminta, jatkuvuus sekä tietoturvan periaatteet on kuvattu Elenian IT-politiikassa. Vastuut ja hallintomalli on kuvattu Elenian kyberstrategiassa. Toimintamme noudattaa tietosuojalle ja tietoturvalle asetettuja lakeja, asetuksia ja muita säädöksiä.

Tietoturvapolitiikan periaatteita ja tavoitteita tukemaan julkaistaan tarvittavat menettelyohjeet. Menettelyohjeissa kuvataan hallinnolliset ja tekniset toimenpiteet tietojen ja suojaamiseksi sekä toiminnan jatkuvuuden varmistamiseksi normaaleissa ja poikkeustilanteissa.

Tietoturvallisuustyö sisältyy jokaiseen työtehtävään ja on jatkuva prosessi, johon jokainen sitoutuu niin omassa työssään kuin osana liiketoimintaprosesseja. Jokainen elenialainen ja Elenian yhteistyökumppani noudattaa toiminnassaan tätä politiikkaa, menettelyohjeita sekä sopimusvelvoitteita ja vastaa hallittavissaan olevan tiedon tietoturvallisuudesta omalta osaltaan. Päävastuu tietyn tiedon tai palvelun tietoturvallisuudesta on sen omistajalla.

Tietoteknisen järjestelmän tai palvelun tuottaja vastaa kyseisen palvelun tietoturvallisuudesta, tietoturvavaatimuksien noudattamisesta sekä tietoturvallisuuden jatkuvasta seurannasta ja kehittämisestä. Jokaisen tiedonkäsittelijän velvollisuus on viipymättä ilmoittaa havaitsemistaan tietoturvallisuuden puutteista ja epäilemistään väärinkäytöksistä tai tietoturvarikkomuksista voimassaolevien ohjeiden mukaisesti.

Elenia sitoutuu jatkuvasti parantamaan tietoturvallisuuden hallintajärjestelmää ja arvioimaan sen sopivuutta, riittävyyttä ja vaikuttavuutta.

2. Tietoturvan käsitteet

Tietoturvallisuus Tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttäminen.

Tietoturvallisuuden hallintajärjestelmä (ISMS): Liiketoimintariskien arviointiin perustuva johtamisjärjestelmän osa, jonka avulla luodaan, toteutetaan, käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan hyvää tietoturvallisuutta.

Luottamuksellisuus: Tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen saatavilla. Luottamuksellisuus sidotaan henkilöiden luotettavaan tunnistamiseen (autentikointi) sekä tiedon käytön juridiseen kiistämättömyyteen.

Eheys: Tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena.

Saatavuus: Järjestelmien tiedot ja palvelut ovat niihin oikeutettujen käytettävissä etukäteen määritellyssä vasteajassa. Tiedot eivät ole tuhoutuneet tai tuhottavissa vikojen, tapahtumien tai muun toiminnan seurauksena.

3. Hallintakeinot

Tietoturvallisuuden ylläpito ja kehittäminen on jatkuva prosessi, jossa käytetään apuna hallinnollisia, fyysisiä ja teknisiä ratkaisuja. Otamme tietoturvallisuuden huomioon kaikissa päätöksissämme.

Tietoturvatoimien riittävä ja oikea taso varmistetaan osana yrityksen riskienhallintaa tietoturvan hallintajärjestelmän riskienhallintametodologian mukaisesti. Tunnistettujen puutteiden korjaamiseen ja riskien pienentämiseen tarvittavat toimenpiteet dokumentoidaan riskirekisteriin. Korjaavien ja ehkäisevien toimenpiteiden suorittamisesta vastaavat tietojen ja järjestelmien omistajat.

4. Mittarit, seuranta ja viestintä

Tietoturvallisuudesta huolehtiminen perustuu jatkuvaan seurantaan, mittareihin sekä turvallisuustason ja poikkeamien raportointiin. Seurantaa toteutetaan teknisin ja hallinnollisin keinoin. Tietoturvapäällikkö koordinoi tietoturvallisuuden seurantaa ja raportoi tietoturvallisuuden tasosta ja poikkeamista johdolle osana kvartaaliraportointia.

Tietoturvallisuuden mittarit ovat:

1. Tietoturvakoulutuksen kattavuus
2. Tietoturvasopimusvelvoitteiden täyttyminen
3. Tietojärjestelmien tietoturvallisuuden tilannekuva

Tietoturvakoulutus on pakollinen kaikille elenialaisille ja kaikille kumppaneille, jotka käyttävät Elenian tietojärjestelmiä. Tietojärjestelmien käyttöoikeudet voi saada vasta tietoturva- ja tietosuojaperehdytyksen hyväksytyn suorituksen ja tietoturvasitoumuksen allekirjoittamisen jälkeen.

Tietoturvasopimusvelvoitteiden täyttymistä ja kumppanien tietoturvallisuuden tasoa seurataan omavalvonnan avulla sekä ulkoista arviointia ja auditointia käyttäen.

Lain ja toiminnan vaatimustenmukaisuuden toteamiseksi sekä parannettavien kohteiden havaitsemiseksi IT-ympäristön ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan omavalvonnan avulla ja ulkoista arviointia ja auditointia käyttäen.

Tietoturvallisuudesta viestitään tietoturvan vuosikellon mukaisesti.

25.6.2019
Tapani Liuhala
toimitusjohtaja

ELENIA