

Elenian tietoturvapolitiikka

Missiomme

Elämää
sähköistämässä

Visiomme

Luotettava kestävän
kasvun rakentaja

Arvomme

Vastuu tulevaisuudesta | Asiakasta lähellä
Avoin ja luotettava yhteistyö | Rohkeus uudistua

Turvaamme yhdessä Suomen tulevaisuuden varmalla sähkönjakelulla ja erinomaisilla palveluilla. Eettiset periaatteemme ja johtamisjärjestelmämme edistävät vastuullisuutta ja kestäväää kehitystä kaikessa toiminnassamme.

Soveltamisalue

ISO 27001 -standardiin pohjautuvaa Tietoturvan hallintajärjestelmää ja -politiikkaa sovelletaan Elenia-konsernin yhtiöissä. Tämä politiikka linjaa Elenian johdon tahtotilan tietoturvan toteutuksessa.

Tietoturvan hallintajärjestelmän soveltamisala on kuvattu dokumentissa ”Elenia ISO/IEC 27001 Tietoturvan hallintajärjestelmän sovellusalue”. Tietoturvan hallintajärjestelmä näkyy strategioissamme, prosesseissamme ja jo-
kapäiväisessä toiminnassamme. Poliitiikan linjauksia noudattavat Elenia-konsernin yhtiöiden henkilöstö ja Elenian yhteistyökumppanit.

Strategiamme mukaan tavoitteenamme on maailmanluokan taso tietoturvallisuudessa. Osana vastuullista ver-
kon kehittämistä sekä uusien tuotteiden ja palveluiden kehitystyötä otamme huomioon turvallisuuden ja ympä-
ristön kaikissa päätöksissämme. Teemme työtä, jotta elenialaiset ja kumppanimme voivat työskennellä päivittäin
turvallisessa, terveellisessä ja motivoivassa työympäristössä.

Sitoumukset

Elenian vastuullisuusjohtamisen periaatteet ja sitoumukset on kuvattu Elenian Vastuullisuuden ja kestävän kehi-
tyksen politiikassa.

Tavoitteet, johtaminen ja vastuut

Varmistamme asiakkaidemme arjen sujuvuuden ja yhteiskunnan huoltovarmuuden sekä toiminnan jatkuvuuden
kaikissa tilanteissa. Varaudumme luonnonresurssien niukkuuteen ja saatavuuden heikentymiseen. Valvomme ja
edistämme sähköverkkomme turvallisuutta jatkuvasti.

Tietoturvallisuuden tavoitteena on Elenian tiedon ja tietojärjestelmien luottamuksellisuuden, eheyden ja saata-
vuuden varmistaminen.

Elenian IT:n ja tietoturvan periaatteet ja perustoiminta ajantasaisine yhteystietoineen on kuvattu Elenian intranet
-sivustolla. Tietoturvaan liittyvät vastuut on kuvattu periaatetasolla myös Elenian kyberstrategiassa (ID 115522).

Toimintamme noudattaa tietosuojalle ja tietoturvalle asetettuja lakeja, asetuksia ja muita säädöksiä.

Tarkoituksenmukaiset menettelyohjeet tukevat tietoturvapolitiikan periaatteita ja tavoitteita. Menettelyohjeissa
kuvataan hallinnolliset ja tekniset toimenpiteet tietojen ja suojaamiseksi sekä toiminnan jatkuvuuden varmistami-
seksi normaaleissa ja poikkeustilanteissa.

Tietoturvallisuustyö sisältyy jokaiseen työtehtävään ja on jatkuva prosessi, johon jokainen sitoutuu niin omas-
sa työssään kuin osana liiketoimintaprosesseja. Jokainen elenialainen noudattaa toiminnassaan tätä politiikkaa
ja menettelyohjeita. Elenian yhteistyökumppanit noudattavat sopimusveloitteitaan ja vastaavat hallittavissaan
olevan tiedon tietoturvallisuudesta omalta osaltaan.

Tietoteknisen järjestelmän vastaava henkilö tai palvelun tuottaja vastaa kyseisen järjestelmän tietoturvallisuus-
desta, tietoturva vaatimuksien noudattamisesta sekä tietoturvallisuuden jatkuvasta seurannasta ja kehittämis-
estä.

Jokaisen tiedonkäsittelijän velvollisuus on viipymättä ilmoittaa havaitsemistaan tietoturvallisuuden puutteista ja
epäilemistään väärinkäytöksistä tai tietoturvarikkomuksista voimassa olevien ohjeiden mukaisesti.

Sitoudumme jatkuvasti parantamaan tietoturvallisuuden hallintajärjestelmää ja arvioimaan sen sopivuutta, riit-
tävyyttä ja vaikuttavuutta.

Tietoturvan käsitteet

Tietoturvallisuus: Tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttäminen.

Tietoturvallisuuden hallintajärjestelmä: Liiketoimintariskien arviointiin perustuva johtamisjärjestelmän osa, jonka
avulla luodaan, toteutetaan, käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan hyvää tietoturval-
lisuutta.

Luottamuksellisuus: tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen saatavilla. Luottamuksellisuus si-
dotaan 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 vastea-
jassa. Tiedot eivät ole tuhoutuneet tai tuhoittavissa vikojen, tapahtumien tai muun toiminnan seurauksena.

Hallintakeinot

Tietoturvallisuuden ylläpito ja kehittäminen on jatkuva prosessi, jossa käytetään apuna hallinnollisia, fyysisiä ja
tietoteknisiä ratkaisuja.

Tietoturvatomiien riittävä ja oikea taso varmistetaan osana yrityksen riskienhallintaa tietoturvan hallintajärjes-
telmän riskienhallintametodologian mukaisesti. Tunnistettujen puutteiden korjaamiseen ja riskien pienentämiseen
tarvittavat toimenpiteet dokumentoidaan riskirekisteriin. Järjestelmistä vastaavat henkilöt ja palvelun tuottajat
suorittavat korjaavat ja ehkäisevät toimenpiteet.

Valvonta ja seuranta

Tietoturvallisuudesta huolehtimiseen liittyy jatkuva seuranta, mittaus sekä turvallisuustason ja poikkeamien ra-
portointi. Seurantaa toteutetaan teknisin ja hallinnollisin keinoin. Tietoturvapäällikkö koordinoi tietoturvallisuuden
seurantaa ja raportoi tietoturvallisuuden tasosta ja poikkeamista johdolle.

Tietoturvallisuuden päämittareita ovat tietoturvapoikkeamien lukumäärä sekä niiden aiheuttamien sähkönjakelun
katkojen määrä vuoden aikana.

Elenian johtamisjärjestelmän mukaisesti liiketoiminta- ja toimintokohtaisesti on mahdollista asettaa myös muita
väliaikaisia tai pysyviä mittareita, mikäli niiden katsotaan tukevan toiminnan johtamista ja kehittämistä.

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

IT-ympäristön ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisen ja ulkoisen auditoinnin avulla
toiminnan lain ja vaatimustenmukaisuuden toteamiseksi, parannettavien kohteiden havaitsemiseksi, sekä kumppa-
neiden tietoturvallisuuden tason ja tietoturvasopimusveloitteiden täyttymisen seuraamiseksi.

Tietoturvallisuudesta viestitään tietoturvan vuosikellon mukaisesti sekä silloin, kun halutaan nostaa jokin ajan-
kohtainen asia esille.

Elenia on Suomen toiseksi suurin sähköverkkoyhtiö ja Suomen suurin energia-alan asiakaspalveluntuottaja. Huolehdimme sähköverkon
ylläpidosta ja uudistamisesta, rakennamme sähköverkkoa ja -liittymiä kumppaniyhtiöidemme kanssa, mittaamme asiakkaidemme
sähkönkulutuksen ja toimitamme energiatiedot sähkönmyyjille. Palveluliiketoimintamme tarjoaa asiakaspalvelua ja sähkömarkkinoihin
liittyviä monipuolisia palveluita energia-alalle ja muille infrayhtiöille.

