STERA TIETOTURVAPOLITIIKKA

Tässä politiikassa kuvataan Stera-konsernin (”Stera”) tietoturvapolitiikan päämäärä ja linjaukset sekä vastuut ja organisointi.

Tässä politiikassa tietoturvalla tarkoitetaan tiedon luottamuksellisuuden, eheyden ja käytettävyyden varmistamista sen esitystavasta riippumatta. Tämä politiikka määrittelee tietoturvan perusvaatimukset ja luo pohjan politiikan mukaisen toiminnan suunnittelulle ja jalkauttamiselle. Politiikan läpiviennin tukemiseksi laaditaan lisäksi tarkempaa ohjeistusta tietoturvan eri osa-alueille.

Tietoturvallisuutta toteutetaan ja kehitetään riskilähtöisesti käyttäen tarkoituksenmukaisia ja kustannustehokkaita ratkaisuja. Tietoturvapolitiikan tarkoituksenmukaisuutta arvioidaan Stera-konsernin tietohallinnon ohjaustiimissä vuosittain.

Tietoturvapolitiikka yhdessä Steran arvojen, riskienhallinta-, turvallisuus- ja tietosuojapolitiikkojen kanssa ovat keskeinen osa Sterassa noudatettavaa hyvää hallinnointia.

Tietoturvapolitiikan päämäärä

Tietoturvan ensisijaisena päämääränä on Stera-konsernin vastuulla olevien toimintojen jatkuvuuden turvaaminen kaikissa olosuhteissa. Tarkoituksenmukainen ja tehokas tietoturva mahdollistaa Steran toimintoihin liittyvien ICT-ratkaisujen käytettävyyden, prosesseissa ja palveluissa käytettävien tietojen eheyden sekä luottamuksellisuuden kaikissa olosuhteissa kaikissa toimintamaissa. Tämä politiikka luo perustan Stera-konsernin tietojärjestelmien ja tietojenkäsittelyn turvallisuuden varmistamiselle.

Sterassa asiakastietojen ja muiden digitaalisten toimintojen tuottaman ja käsittelemän datan turvaaminen on olennainen osa vastuullista toimintaa, jota sekä asiakkaamme että yhteistyökumppanimme edellyttävät Steralta. Digitaalisuuden kasvu merkitsee sitä, että tietoturvallisuutta säännellään enenevässä määrin myös lainsäädännöillä. Jokaisen Stera-konsernin työntekijän kaikissa toimintamaissa on noudatettava tietoturvapolitiikkaa, sitä täydentäviä periaatteita ja ohjeita sekä soveltuvaa lainsäädäntöä.

Tietoturvan toteuttaminen

Riskien arviointi

Tietoturvariskejä arvioidaan ja analysoidaan säännöllisesti niiden liiketoimintavaikutusten perusteella. Riskiarviointi tulee laatia myös uusien järjestelmien määrittelyvaiheessa ja merkittävien toiminnan kriittisyyteen vaikuttavien muutosten yhteydessä.

Tiedonhallintaluokitus

Steralla on tiedonhallintaluokitus, jossa määritellään tiedon luokitus ja datan kriittisyys liiketoiminnalle sekä huomioidaan käyttöoikeudet.

Henkilötietojen käsittely

Tietosuojapolitiikassa ja -ohjeistuksissa määritellään, miten henkilötietoja käsitellään Sterassa.

Tietoturvavaatimukset

Steran tietoturvavaatimukset määrittävät sopimuskumppaneilta vaadittavan minimitason tietoturvan osalta. Vaatimustenmukainen tietoturvan taso voidaan tarvittaessa todentaa auditoinnein.

Tietoturvakoulutus

Steralla on käytössä erilaisia, säännöllisesti toteutettavia toimenpiteitä työntekijöiden tietoturvallisuustietoisuuden parantamiseksi. Näitä ovat muun muassa verkkokoulutukset, huijausviestisimulaatiot sekä uutisointi intranetissä. Lisäksi valituille kohderyhmille järjestetään kohdennettua tietoturvakoulutusta. Koulutuksien suunnittelu toteutetaan osittain yhteistyössä HR-tiimin kanssa. Työntekijöiden osaamismatriisien täydennys tarvittavilta osin sekä tietoturva huomioidaan tulevissa koulutussuunnitelmissa.

Valvonta ja seuranta

Tietoturvatason parantaminen ja ylläpitäminen edellyttävät tietojärjestelmien toiminnan systemaattista ja jatkuvaa automaattista valvontaa. Valvontaa toteuttavat henkilöt ovat lain mukaan vaitiolovelvollisia työssään käsittelemistä tiedoista.

Tietoturvatilanteesta raportoidaan normaalin sisäisen valvonnan sekä sisäisten ja ulkoisten tarkastusten yhteydessä. Teknistä tietoturvaa arvioidaan jatkuvasti ja tärkeimpiin ympäristöihin tehdään erillisiä tietoturvatarkastuksia.

Tietoturvapoikkeamien käsittely

Steralla on menettelytavat ja palvelut tietoturvapoikkeamien havaitsemiseksi. Mahdollisten tietoturvaloukkauksien osalta niiden käsittely tapahtuu Tietohallinnossa ja raportointi konsernin johtoryhmälle.

Tietoturvarikkomukset

Tietoturvarikkomukseksi lasketaan tietoturvapolitiikan ja -ohjeistuksen vastainen toiminta.

Vastuut ja organisointi

Tietoturvapolitiikan hyväksyy Stera konsernin johtoryhmä.

Tietoturvapolitiikka kattaa Steran yhtiöiden toiminnot kaikissa Steran toimintamaissa. Steran henkilöstön on noudatettava politiikkaa. Steran yhtiöt ja yksiköt huolehtivat politiikan toteutuksesta ja tarvittavasta resursoinnista omassa toiminnassaan.

Toimitusjohtaja vastaa siitä, että Sterassa on toimiva tietoturva osana riskienhallintajärjestelmää. Tietoturvan toteuttamisessa toimitusjohtajalla on apunaan konsernin tietohallinto. Tietohallinto, käsittelee ja seuraa konsernin tietoturvariskejä sekä riskienhallintatoimenpiteiden toteutumista sekä raportoi näistä konserninjohtoryhmälle.

Vastuu tietoturvan toteuttamisesta on konsernin johtoryhmän jäsenillä. Tietohallinto koordinoi ja kehittää tietoturvaprosesseja, vastaa käytännön toteutuksesta yhdessä palveluntarjoajien kanssa, vastaa raportoinnista sekä

toteuttaa yhdessä liiketoimintojen ja yhteisten toimintojen kanssa tietoturvariskien tunnistamista ja hallintatoimenpiteiden määrittämistä. Jokaisen Steralaisen pitää tunnistaa omaan tehtäväänsä tai yleisesti konserniin vaikuttavat tietoturvaan liittyvät riskit ja reagoida niihin. Koulutusten kattavuutta ja kohdentamista seurataan yhteistyössä Steran oman HR-tiimin kanssa.

Tietoturvan ohjaus

Tietoturvan ohjausmekanismina toimii BCP-toimintamalli, jossa tietoturva omana osanaan. Työjärjestyksensä mukaisesti Stera konsernin johtoryhmä muun muassa seuraa ja arvioi Steran sisäisen valvonnan, sisäisen tarkastuksen ja BCP-toimintamallin tehokkuutta. Konsernin johtoryhmä yhdessä IT-tiimin kanssa käsittelee konsernin merkittävimmät tietoturvariskit.

Voimaantulo

Hyväksytty Stera konsernin johtoryhmässä, Turku 12.12.2022.