Granon Tietoturvapolitiikka

Sisällysluettelo

Muutoshistoria

versio	pvm	kuka ja selite
0.9	8.2.2021	PH, ensi versio kommentoitavaksi
0.9.1	8.3.2021	PH, AL. Muokattu kommenttien mukaan
0.9.2	18.3.2021	Ulkopuolisen asiantuntijan muokattu versio
0.9.3	18.3.2021	PH muokattu versio
0.9.4	22.3.2021	PH muokattu versio, muutoksia kommenttien mukaan
1.0	25.3.2021	Hallitus, Ensimmäinen hyväksytty ja julkaistu versio
1.0.1	7.5.2021	PH Korjauksia käännöstä varten

Tietoturvapolitiikka

Johdanto

Tämä tietoturvapolitiikka on Grano Oy:n johdon hyväksymä strateginen linjaus, jossa määritetään Granon keskeiset tietoturvallisuuden tavoitteet ja toteuttamiskeinot, sekä tietoturvallisuuden organisointi ja siihen liittyvät vastuut. Tässä politiikassa tietoturvalla tarkoitetaan tiedon luottamuksellisuuden, eheyden ja käytettävyyden varmistamista tiedon kaikissa eri muodoissa. Tietoturva tarkoittaa myös sitä, miten vastataan soveltuvin osin lain, asetusten ja yhteistyökumppanien asettamiin tietoturvallisuusvaatimuksiin. Tällä politiikalla haluamme viestiä, että pidämme tietoturva-asioita tärkeinä.

Tietoturvallisuutta toteutetaan ja kehitetään riskilähtöisesti käyttäen tarkoituksenmukaisia sekä kustannustehokkaita ratkaisuja. Tietoturvapolitiikan tarkoituksenmukaisuutta arvioidaan Granon johtoryhmässä vuosittain.

Tietoturvapolitiikka yhdessä Granon arvojen, riskienhallinta-, turvallisuus- ja tietosuojapolitiikkojen kanssa ovat keskeinen osa Granossa ja Panostajassa noudatettavaa hyvää hallinnointitapaa (Corporate Governance).

Tietoturvapolitiikka ja siihen liittyvät tarkentavat ohjeet julkaistaan Granon Intranetissä ja ne koskevat koko Granon henkilökuntaa kaikilla toimialueilla, sekä muita henkilöitä, joille on myönnetty pääsy Granon tietoihin.

Tämä politiikka voidaan antaa myös tiedoksi sidosryhmille turvallisuusasioista viestimiseksi palveluiden hankinnan ja toimittamisen yhteydessä.

Päämäärä

Tämä politiikka määrittelee tietoturvan perusvaatimukset ja luo pohjan politiikan mukaisen toiminnan suunnittelulle sekä jalkauttamiselle. Politiikan käytännön toteutumiseksi yrityksessä ylläpidetään myös tarkempaa ohjeistusta tietoturvan eri osa-alueille.

Tietoturvapolitiiikka ilmaisee Granon tahtotilan, jota tarkennetaan politiikan liitteiden ja käytännön tietoturvaohjeiden avulla. Ulkoisten osapuolten, kuten alihankkijoiden ja palveluntoimittajien osalta tämän politiikan vaatimukset sisällytetään soveltuvilta osin hankintasopimuksiin.

Tietoturvan ensisijaisena päämääränä on Granon vastuulla olevien toimintojen jatkuvuuden turvaaminen kaikissa olosuhteissa. Tarkoituksenmukainen ja suunnitelmallinen tietoturva mahdollistaa Granon toimintoihin liittyvien ICT-ratkaisujen käytettävyyden, tietojen eheyden ja luottamuksellisuuden. Tämän tulee toteutua joka olosuhteissa ja kaikissa prosesseissa, rekistereissä ja palveluissa. Tietoturvapolitiikka luo perustan Granon tietojärjestelmien toiminnan häiriöttömyyden ja tietojenkäsittelyn turvallisuuden varmistamiselle.

Granossa asiakastietojen, asiakkaiden toimittamien materiaalien ja muiden Granon toimintojen tuottaman ja käsittelemän datan turvaaminen on olennainen osa vastuullista toimintaa.

Tietoturvan ohjausmalli ja vastuut

Kaikki Granolla työskentelevät henkilöt vastaavat tietoturvallisuusasioista osana muita työtehtäviään oman toimenkuvansa ja vastuualueidensa mukaisesti. Tämä tarkoittaa sitä, että henkilökohtaista vastuuta tietoturvasta huolehtimisesta ei voida siirtää muille, eikä ulkoistaa.

Henkilökunnan vastuulla on tuntea tietoturvallisuudesta annetut ohjeet ja säädökset, sekä noudattaa niitä. Jokaisen vastuulla on lisäksi osallistua hänelle osoitettuun koulutukseen sekä raportoida havaitsemistaan tietoturvallisuuspoikkeamista, ongelmista, uhista ja ohjeiden vastaisesta toiminnasta viivyttelemättä tietoturvavastaavalle.

Tietoturvavastaava kehittää ja koordioi tietoturvallisuustyötä Granolla ja toimii yhteyshenkilönä tietoturvallisuusasioissa sidosryhmien suuntaan. Tietoturvavastaava huolehtii tietoturvallisuuden toteutumisesta tämän politiikan ja siihen liittyvien ohjeistusten mukaisesti. Tietoturvavastaava raportoi tietoturvallisuuden tilasta kerran vuodessa kirjallisesti.

Tietohallinto koordinoi tietoturvaprosessia ja vastaa alueen raportoinnista. Tietohallinto toteuttaa yhdessä liiketoimintojen ja tukitoimintojen kanssa tietoturvariskien tunnistamista sekä hallintatoimenpiteiden määrittämistä.

Granon hallituksen tehtäviin kuuluu sisäisen valvonnan ja riskienhallintajärjestelmien tehokkuuden arviointi. Tässä roolissa hallitus vahvistaa konsernin tietoturvapolitiikan sekä käsittelee kokouksissaan Granon keskeiset tietoturvariskit ja niiden hallinnan, sekä antaa tarvittaessa niitä koskevia ohjeita.

Toimitusjohtaja vastaa siitä, että Granossa tietoturvallisuuteen liittyvät prosessit ja politiikat hallinnoidaan suunnitelmallisesti osana riskienhallintajärjestelmää. Tietoturvan toteuttamisessa toimitusjohtajalla on apunaan tietohallinto- ja riskienhallintatoiminnot.

Granon ulkopuolisten toimijoiden vastuulla on tuntea heille osoitetut tietoturvallisuudesta annetut säädökset, määräykset ja ohjeet, sekä noudattaa niitä, ja informoida yhteyshenkilöään havaitsemistaan Granoon liittyvistä tietoturvallisuuspoikkeamista, ongelmista, uhista ja ohjeiden vastaisesta toiminnasta viivyttelemättä.

Tietoturvan toteuttaminen

Granon tietoturvallisuustyötä ohjaavat (1) Suomen ja EU:n tietoturvallisuutta ja tietosuojaa koskeva lainsäädäntö; (2) Tietoturvajohtamisen ja riskienhallinnan kautta tunnistetut keskeisimmät riskit. Tietoturvan ohjausmalli on osa Granon riskien- ja jatkuvuudenhallinnan ohjausmallia.

Riskien arviointi
Riskienarviointi tehdään Granon hallituksen linjausten mukaisesti. Riskiarviointeja toteutetaan ja niistä aiheutuvia toimenpiteitä seurataan säännöllisesti tietoturvavastaavan toimesta ja niistä raportoidaan vähintään kerran vuodessa.

Tietojen luokittelu ja käsittely
Granolla on käytössä tietojen luokittelumenetelmä, jossa ohjeistetaan, miten tiedot tulee luokitella ja määritellään tietoturvakontrollit eri luokkiin kuuluvan tiedon käsittelylle.

Henkilötietojen käsittely
Tietosuojapolitiikassa ja – ohjeistuksissa määritellään, kuinka asiakas- ja henkilötietoja käsitellään Granossa.

Tietoturvavaatimukset
Granossa tietoturvavaatimukset määrittävät sopimuskumppaneilta vaadittavan minimitason tietoturvan osalta.

Tietoturvakoulutus
Koko Granon henkilökunnan on suoritettava vuosittain tietoturvallisuuden verkkokoulutus. Koulutuksen suoritusta seurataan. Lisäksi valituille kohderyhmille järjestetään tehtäväkohtaista tietoturvakoulutusta.

Tietojärjestelmien valvonta ja seuranta
Tietoturvatason parantaminen ja ylläpitäminen edellyttävät tietojärjestelmien toiminnan systemaattista ja jatkuvaa 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
Tietoturvapoikkeamilla tarkoitetaan tapahtumia, jotka vaarantavat jonkin kolmesta tietoturvan peruselementistä (luottamuksellisuus, eheys ja saatavuus). Granolla on menettelytavat ja palvelut tietoturvapoikkeamien havaitsemiseksi. Mahdollisten tietoturvaloukkauksien käsittelyyn on määritellyt toimintamallit ja niistä raportoidaan johdolle. Jokainen, jolle on myönnetty pääsy Granon tietoihin, on velvoitettu ilmoittamaan havaitsemistaan tietoturvapoikkeamista välittömästi tietoturvavastaavalle tai omalle yhteyshenkilölleen.

Tietoturvarikkomukset
Tietoturvarikkomukseksi lasketaan tietoturvapolitiikan ja -ohjeistuksen vastainen toiminta. Grano on määritellyt menettelytavat rikkomustilanteille.

Tiedottaminen
Granon tietoturvapolitiikka on julkinen. Tarkemmat tietoturvavastuut määritellään politiikan liitteissä, jotka ovat Granon sisäisiä.

Granon henkilöstölle tiedotetaan tietoturvallisuudesta ja sitä koskevista määräyksistä ja ohjeista sekä niiden muutoksista sisäisissä koulutuksissa ja Intranetissä. Sisäisestä tiedottamisesta vastaa Granon tietoturvavastaava.

Noudattaminen

Tietoturvapolitiikan ja -ohjeistuksen noudattaminen on jokaisen Granon tietoja käsittelevän tehtävä. Tietoturvapolitiikan ja -ohjeistuksen noudattaminen on pakollista ja niiden vastainen toiminta tai noudattamatta jättäminen voi olla peruste varoitukselle, työsuhteen irtisanomiselle tai rikosoikeudellisille seuraamuksille.