CINIA OY:N TIETOTURVAPOLITIIKKA

Cinian liiketoiminnan perustana on asiakkaiden, kumppaneiden ja oman henkilöstön luottamus yhtiön kykyyn huolehtia tietoaineiston turvallisesta käytöstä ja hallinnasta sekä yhtiön tuottamien palveluiden tietoturvallisuudesta. Cinian tietoturvapolitiikassa määritellään, kuinka Cinia toiminnoissaan varmistaa vaatimusten mukaisen tietoaineiston luottamuksellisuuden, muuttumattomuuden, saatavuuden, kiistämättömyyden ja paikkansapitävyyden.

Tietoturvapolitiikkaa täydentää ja täsmentää Cinian aiemmin julkaisemaa Turvallisuuspolitiikkaa ja Tietosuojapolitiikkaa.

Tätä tietoturvapolitiikkaa sovelletaan Cinia Oy:ssä ja sen tytäryhtiöissä (”Cinia”). Kaikki Cinian työntekijät ja vuokratyöntekijät ovat velvollisia perehtymään tähän asiakirjaan ja toimimaan sen mukaisesti työpaikalla ja sen ulkopuolella työtehtäviin liittyvissä asioissa.

Tietoturvapolitiikan päämäärä

Tietoturvapolitiikan päämääränä on suojata Cinian hallussa oleva tietoaineisto siihen kohdistuvilta sellaisilta tahallisilta ja tahattomilta uhkilta, jotka voivat vahingoittaa liiketoimintaa tai muutoin luottamusta yhtiön toimintaan. Tietoturvapolitiikassaan yhtiö määrittää ne periaatteet, toimintatavat ja vastuut, joita noudatetaan Cinian tietoturvan ylläpidossa ja kehittämisessä. Tietoturvapolitiikka antaa perusteet tietoturvasta julkaistaville alemman tasoisille määräyksille ja ohjeille.

Tietoturvapolitiikka täsmentää Cinian turvallisuuspolitiikassa määritettyjä yritysturvallisuuden perusteita ja liittyy kiinteästi henkilötietojen käsittelystä julkaistuun Cinian tietosuojapolitiikkaan. Tietoturvariskit arvioidaan ja niiden hyväksyttävälle tasolle saattamiseksi tarvittavat toimenpiteet määritetään riskienhallinnan vuosikellon mukaisesti.

Tietoturvapolitiikan perusteet

Cinia tuottaa palvelunsa digitaalisessa ympäristössä (”kyberympäristössä”), minkä vuoksi tietoturvallisuudesta huolehtimisessa korostuvat digitaalisen turvallisuuden ylläpitoon liittyvät toimenpiteet. Teknologian jatkuvan kehittymisen ja sen myötä myös jatkuvasti muuttuvien digitaalisten uhkien muutosten seuranta on keskeinen osa yhtiön tietoturvakäytäntöjä.

Cinia on lainsäädännössä määritetty teleyritys, jota koskevat teleyritysten tietoturvalle ja varautumiselle säädetyt velvoitteet ja näiden nojalla annetut viranomaismääräykset. Tietoturvaa koskevia velvoitteita on säädetty myös tietosuojalainsäädännössä.

Cinia on palvelusopimuksissaan sitoutunut asiakkaidensa kanssa erikseen sovittujen tietoturvavaatimusten täyttämiseen. Merkittävä osa asiakkaista on yhteiskunnan kriittistä infrastruktuuria ylläpitäviä ja palveluita tuottavia yhtiöitä ja virastoja, minkä vuoksi Cinian tietoturvan ylläpidossa korostuu myös laaja yhteiskuntavastuu.

Ciniassa sen omaa tai asiakkaiden tietoaineistoa käsittelevät vain ne henkilöt, jotka tätä tietoa työssään tarvitsevat ja joille on myönnetty käyttöoikeus tähän tietoon. Tiedon käyttöä valvotaan muun muassa pääsynhallinnalla ja lokituksella.

Cinia soveltaa tietoturvallisuutensa ylläpidossa ISO/IEC 27001 -standardin mukaisia omaan toimintaympäristöönsä soveltamiaan ja dokumentoimiaan toimintamalleja.

Tietoturvallisuuden ylläpito

Palvelutuotannon ja yhtiön muun toiminnan tietoturvallisuuden varmistamiseksi keskeiset vastuut ja prosessit on määritetty. Tavoitteiden mukaisen tietoturvan ylläpitämiseksi:

- emoyhtiön johtoryhmä vahvistaa yhtiötasoiset vastuut, tehtävät ja resurssoinnin
- turvallisuudesta vastaava johtaja valmistelee yhtiötasoiset päätökset yrityksen johtoryhmän käsiteltäväksi
- turvallisuuspäällikkö seuraa riskiympäristön kehitystä, ylläpitää yrityksen tietoturvallisuuden hallintajärjestelmää, johtaa ja sovittaa yhteen päivittäiset tietoturvan ylläpitotehtävät sekä tekee esityksiä tarvittavista lisätoimenpiteistä
- kyberturvallisuusvalvomo vastaa tuotanto- ja toimistoverkkojen sekä -palvelujen teknisestä valvonnasta ympärivuorokautisesti sekä johtaa ja koordinoi kyberpoikkeamien teknistä selvitystä
- liiketoimintajohtajat vastaavat tuottamiensa tai alihankkimiensa palveluiden vaatimustenmukaisesta tietoturvasta sekä jatkuvuuden hallinnasta
- esimiehet vastaavat yksiköissään ja tiimeissään niitä koskevien tietoturvakäytäntöjen noudattamisesta
- jokainen cinialainen perehtyy ja noudattaa työntekijöitä koskevia tietoturvaohjeita.

Tietojärjestelmien omistajat vastaavat järjestelmiensä tietoturvasta tekemällä ja dokumentoimalla ohjelmistopäivitykset sekä konfiguraatiomuutokset, huolehtimalla tarvittavasta pääsynhallinnasta sekä ylläpitämällä integroidun tuotantoympäristön varmenteet ajan tasalla. Järjestelmä- ja integraatiomuutokset suunnitellaan ja toteutetaan tietoturvallisesti muutoshallintaprosessin mukaisesti.

Cinian kyberturvallisuusvalvomo valvoo ja ylläpitää yhtiön omien sekä asiakkaiden järjestelmäympäristöjen kyberturvallisuutta ympärivuorokautisesti keräämällä loki- ja tapahtumadataa sekä havainnoimalla poikkeamia kerätyn datan perusteella. Teknisessä selvitystyössä ja liiketoiminnan jatkuvuuden varmistamisessa operointikeskusta tukevat yhtiön muut resurssit.

Cinian tietoturvakäytännöt on dokumentoitu. Palveluita koskevaa tietoturvadokumentaatiota ylläpidetään palvelukuvausten yhteydessä ja muita tietoturvadokumentteja yhtiön intranetissä. Dokumentaation ylläpitovastuut on määritetty ja julkaistu.

Tietoturvallisuuden johtamisessa ylläpidetään Ciniassa sisäistä dokumentaatiota vähintään seuraavista asioista:

- tietoturvariskien arvioinnista ja hallinnasta
- käyttövaltuushallinnasta ja myönnetyistä käyttöoikeuksista
- järjestelmärekisteristä ja järjestelmistä
- järjestelmien etäkäytöstä
- tietoaineiston luokittelusta ja salauskäytännöistä
- päätelaitteiden turvallisesta käytöstä sekä
- palveluiden jatkuvuudenhallinnasta.

Kaikille cinialaisille järjestetään säännöllistä tietoturvakoulutusta, joka dokumentoidaan. Uudet cinialaiset perehdytetään yhtiön tietoturvakäytäntöihin ja –ohjeistukseen osana henkilöstöhallinnon ja esimiehen järjestämää perehdytysohjelmaa.

Kaikki tietoturvatapahtumat, hyökkäykset ja haavoittuvuudet sekä näitä koskevat epäilyt raportoidaan käytössä olevilla raportointityökaluilla tai –menetelmillä. Henkilötietoihin kohdistuvista tietoturvaloukkauksista tai näiden epäilyistä raportoidaan tietosuojaohjeistuksen mukaisesti. Kyberturvallisuusvalvomo seuraa tietoturvallisuustilannetta ja raportoi siitä johtoryhmälle säännöllisesti.

Emoyhtiön johtoryhmä ja turvallisuudesta vastaava johtaja järjestävät vuosittain seurantatarkastuksia turvallisuuden ja tietoturvan ylläpidosta.

Tietoturvapolitiikan vahvistaminen

Cinian johtoryhmä on vahvistanut tämän tietoturvapolitiikan 20.8.2018 sekä päivitetyn tietoturvapolitiikan 18.11.2019 ja 7.5.2020.

Cinia-konsernin emoyhtiön hallitus on hyväksynyt tämän päivitetyn tietoturvapolitiikan 28.5.2020.