Yritys Oy
Tietoturvapolitiikka

Julkinen

Muutoshistoria

Versio	Päivämäärä	Muutoksen kuvaus	Hyväksytty
1.0	1.1.2020	Tietoturvapolitiikan malli	

Sisällys

Yritys Oy:n tietoturvapolitiikka

1 Johdanto

Liiketoiminnan tuloksellisuus on suoraan riippuvainen sidosryhmien osoittamasta luottamuksesta. Luottamus on liiketoiminnan edellytys ja menestystekijä.

Tietoturvallisuus on turvallisuuskulttuurin keskeinen osatekijä. Turvallisuuskulttuurilla tarkoitetaan johdon ja henkilöstön yhtenäistä vakiintunutta tapaa ottaa huomioon turvallisuusnäkökohdat päätöksiä tehtäessä, asioita ratkaistaessa ja prosesseja toteutettaessa.

Yhtenäisen ja vakiintuneen turvallisuuskulttuurin avulla pyritään saamaan kohtuullinen varmuus liiketoimintaprosessien luotettavuudesta, häiriöttömyydestä ja jatkuvuudesta.

Turvallisuuskulttuurin keskeisenä tavoitteena on varmistaa tiedon saatavuuden, eheyden ja luottamuksellisuuden toteutuminen kaikissa liiketoimintaprosesseissa. Nämä tavoitteet saavutetaan yhtenäisellä turvallisuuskulttuurilla, jonka olennainen osa on hyvä tietohallintatapa.

Hyvään tietohallintatapaan sisältyy velvollisuus huolehtia tiedonkäsittelyn asianmukaisesta suunnittelusta, tietoturvaratkaisuista ja testauksista, riskien hallinnasta, vahinkojen ja väärinkäytösten ennaltaehkäisystä sekä poikkeamaraportoinnista.

Tässä ohjausasiakirjassa linjataan Yritys Oy:ssä noudatettavat tietoturvakäytänteet. Käytänteet ovat toimintoja ja henkilöstöä sitovia sekä linjaavat kahdenvälisissä sopimuksissa noudatettavat sopimusosapuolten kohtuulliset huolellisuusvaatimukset (due diligence).

2 Soveltamislaajuus

Tietoturvapolitiikka velvoittaa henkilöstöä, toimintoja ja sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Yritys Oy:n omistamia tai hallinnoimia tietoja.

Tietoturvapolitiikka kattaa Yritys Oy:n omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

3 Tietoturvapolitiikasta poikkeaminen

Tietoturvapolitiikan käytänteistä voidaan poiketa toimitusjohtajan päätöksellä

4 Lainsäädännön velvoitteet

Yritys Oy noudattaa toiminnoissaan lakeja, asetuksia, johdon hyväksymiä toimintalinjauksia, työjärjestystä sekä yhteistyökumppaneiden välillä solmittuja sopimuksia.

Yhteistyökumppaneiden kokeman luottamuksen ylläpito ja parantaminen edellyttää tietoturvakäytänteiden läpinäkyvyyttä ja eräin osin tarkastettavuutta. Yritys Oy on sitoutunut huolehtimaan liikesalaisuuslain (595/2018) piiriin ja kahdenvälisiin sopimuksiin liittyvistä salassapitovelvollisuuksista.

5 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan menettelyitä, jotka koostuvat Yritys Oy:n antamista työnjohdollisista määräyksistä, hallinnollisista ohjeista, prosesseista, ratkaisuista ja teoista, jotka edistävät tavoitteeksi asetetun tietoturvallisuustason muodostumista.

Tietoturvallisuuden hallinta perustuu lakien ja säädösten sekä Yritys Oy:n liiketoimintaprosessien asettamiin vaatimuksiin. Yritys Oy on sitoutunut tietoturvallisuuden jatkuvaan ylläpitoon ja kehittämiseen prosessimaisella toiminnalla.

6 Tietoturvallisuuden organisointi

Tietoturvallisuutta johdetaan ja kehitetään osana operatiivista riskienhallintaa. Tietoturvallisuuden hallintajärjestelmä on Yritys Oy:n riskienhallintajärjestelmän osa.

Vastuu tietoturvallisuuden hallintajärjestelmän toimivuudesta on hallituksella ja toimitusjohtajalla. Vastuisiin liittyviä tehtäviä on delegoitu edelleen työjärjestyksen mukaisesti toimintojen johdolle ja tapauskohtaisesti periytetty sopimusperusteisesti sopimuskumppanille.

Tietohallinnosta vastaava johtaja vastaa tietoturva-arkkitehtuurista, teknisten tietoturvaratkaisujen implementoinnista ja tietojärjestelmien riittävästä redundanssista.

Toimintojen johtajat vastaavat omien liiketoimintaprosessien asianmukaisesta tietoturvallisuudesta. Kukin toiminto nimeää tietoturvallisuuden vastuuhenkilön, jonka tehtävänä on koordinoida toiminnon tietoturvakäytänteitä.

Tietoturvapäällikkö vastaa tietoturvaratkaisujen koordinoinnista yhdessä tietohallinnosta vastaavan johtajan sekä toimintojen nimeämien vastuuhenkilöiden kesken.

Tietoturvapäällikkö osallistuu uusien tietoturvaratkaisuiden valmisteluun. Tietoturvapäällikön vastuulla on myös seurata alan kehitystä ja ehdottaa toimintojen nimeämille vastuuhenkilöille liiketoimintaprosesseihin tarvittavia muutoksia sekä edistää asianmukaisin toimenpitein turvallisuuskulttuurin ylläpitoa ja kehittymistä.

Projektipäälliköt vastaavat omien projektiensa osalta asianmukaisten ja riittävien tietoturvakäytänteiden toteuttamisesta. Tietoturvapäällikkö osallistuu projektien tietoturvasuunnitelmien laadintaan. Tietoturvasuunnitelman hyväksyy projektin ohjausryhmä.

Lähiesimiesten tehtävänä on soveltaa tietoturvapolitiikan käytänteitä arkipäivän työtilanteissa ja edistää hyvää tiedonkäsittelytapaa.

7 Raportointivastuut

Sisäinen tarkastus arvioi mm. tietoturvan hallintajärjestelmän toimivuutta kohdassa 10 mainittujen tietoturvaperiaatteiden mukaisesti. Sisäinen tarkastus raportoi hallituksen puheenjohtajalle.

Tietohallintojohtaja vastaa tietojärjestelmiin liittyvien poikkeamien raportoinnista johtoryhmälle.

Tietoturvapäällikkö raportoi keskitetysti toimintojen operatiiviset tietoturvapoikkeamat johtoryhmälle.

Käyttäjät ja ylläpitäjät ilmoittavat havaitsemistaan tietoturvapuutteista, tietoihin liittyvistä väärinkäytösepäilyistä ja epäilemistään tietoturvarikkomuksista tietoturvapäällikölle ja lähiesimiehilleen.

8 Kriisiviestintä

Tietoturvaloukkauksiin liittyvä kriisiviestintä tapahtuu ennalta laaditun viestintäsuunnitelman mukaisesti.

9 Sidosryhmät

Yhteistyökumppaneiden kesken solmitaan asianmukaiset salassapitosopimukset (NDA). Salassapitosopimuksen liiteasiakirjaksi voidaan liittää Yritys Oy:n tietoturvapolitiikka.

10 Tietoturvaperiaatteet

10.1 Henkilöstöturvallisuus

Henkilöstö on sitoutunut työsopimusten yhteydessä luottamuksellisten tietojen salassapitoon.

Ulkopuolisten yritysten palveluksessa olevat henkilöt ovat sitoutuneet kahden välisissä sopimuksissa edustamansa yrityksen laajuiseen tai henkilökohtaiseen tietojen salassapitoon.

Rekrytointien yhteydessä suoritetaan tapauskohtaiseen harkintaan perustuen lakien ja säädösten tarjoamissa puitteissa tarpeelliset taustatarkistukset.

10.2 Tietoturvakoulutus ja perehdyttäminen

Henkilöstö on perehdytetty tietoturvakäytänteitä koskeviin periaatteisiin. Henkilön osallistumisesta perehdytykseen on tehty kirjaus henkilöstöhallintajärjestelmään.

Lähiesimies vastaa, että työntekijä saa työtehtävien edellyttämän tietoturvaperehdytyksen.

Tietoturvaohjeistus on osa henkilöstön perehdyttämismateriaalia. Henkilöstöllä on velvollisuus tutustua tietoturvaohjeistukseen.

Yhteistyökumppaneilta edellytetään tietoturvakäytänteisiin perehtymistä ennen yhteistyön aloittamista, mikäli he käsittelevät Yritys Oy:n omistamia tai hallinnoimia tietoja.

10.3 Kulunvalvonta

Henkilöstölle on jaettu kulkuoikeuksin varustetut kuvalliset henkilökortit, joita henkilöstö pitää toimitiloissa liikkuessa näkyvillä.

Sidosryhmien edustajille luovutetaan tarvittaessa kuvaton henkilökortti rajoitetuin kulkuoikeuksin.

Vierailijoille luovutetaan vierailijakortti, ilman kulkuoikeuksia. Vierailijoiden liikkuminen toimitiloissa tapahtuu valvotusti isännän ohjauksessa.

10.4 Käyttövaltuudet ja käyttäjän tunnistaminen

Tietojärjestelmien ja tietojen käyttö on sallittua työtehtävien hoitamiseksi. Muu käyttö on luvatonta käyttöä.

Tietojärjestelmään kirjautuminen tapahtuu henkilökohtaisen käyttäjätunnuksen avulla.

Yhteiskäyttöiset käyttäjätunnukset ovat poikkeamia tietoturvapolitiikasta.

Yhteiskäyttöisiä käyttäjätunnuksia ei myönnetä operatiivisiin tietojärjestelmiin.

Henkilön käyttövaltuudet yksilöidään työtehtävien mukaisesti, joko roolipohjaisesti tai yksilöidysti.

Käyttövaltuuden myöntämisen peruste on työtehtävä. Henkilön asemaan perustuvia käyttövaltuuksia ei myönnetä.

Työtehtävien muuttuessa käyttövaltuudet tarkistetaan.

Työsuhteen päättyessä käyttövaltuudet poistetaan.

Todettuihin väärinkäytöksiin ja väärinkäytösten yrityksiin puututaan lakien ja säädösten mukaisilla prosesseilla.

10.5 Tietoaineiston käsittely

Yritys Oy:n tietojärjestelmiin tallennettu tieto on yrityksen omaisuutta, jota ei saa kopioida tai julkaista yrityksen intressien vastaisesti.

Liikesalaisuuden piiriin kuuluva tieto on salassa pidettävää tietoa, vaikka tiedosta, tallennustavasta tai asiakirjasta ei suoraan ilmenisi turvaluokitusta. Työntekijällä on epäselvissä tapauksissa selonottovelvollisuus.

Yhteistyökumppanin tiedot kuuluvat liikesalaisuuden piiriin. Tietoja on mahdollista käyttää siinä tarkoituksessa ja laajuudessa kuin tietojen käytöstä on kahdenväliseen sopimukseen kirjattu.

Tietoaineistoa käsitellään sen elinkaaren vaiheissa siten, ettei tiedon saatavuus, eheys tai luottamuksellisuus vaarannu.

10.6 Henkilötietojen käsittely

Henkilötietojen käsittelyä säätelee EU:n tietosuoja-asetus (GDPR), kansalliset säädökset ja tietosuojavaltuutetun toimiston antamat soveltamisohjeet. Henkilötietojen käsittely on sallittua edellä mainituissa puitteissa.

10.7 Järjestelmäkehitys

Tietohallinnon tehtävänä on varmistaa liiketoimintaprosesseja tukevien tietojärjestelmien käytettävyys sekä hyvän tietohallintotavan toteutuminen tietojärjestelmien suunnittelussa, testauksessa ja ylläpidossa.

Tietohallinto ylläpitää tietoturva-arkkitehtuuria, joka mahdollistaa toiminnoille luotettavien tietoturvaratkaisujen käyttöönoton ja tukee liiketoimintaprosessien kehittämistä.

Laitteistot ja ohjelmistot on hankittu keskitetysti ja koordinoidusti luotettavilta toimittajilta asianmukaisin käyttölisenssein.

10.8 Sähköpostin käyttö

Yrityksen sähköposti on tarkoitettu työtehtävien hoitoon.

Asiakkaiden yhteydenottoja ja asiakaspalvelua varten on luotu omat sähköpostiosoitteet.

Yrityksen luottamuksellisia tietoja ei välitetä salaamattoman sähköpostiyhteyden kautta.

Henkilötietojen välittäminen salaamattoman sähköpostin kautta edellyttää kyseisen henkilön nimenomaista jälkeenpäin todennettavissa olevaa lupaa.

10.9 Julkisten verkkopalveluiden käyttö

Sosiaalisen median ja yksityisten sähköpostitilien varomaton käyttö voi vaarantaa tietojärjestelmän eheyden ja luottamuksellisuuden.

Tietohallinto voi rajoittaa yksityiskäyttöön liittyvien verkkopalveluiden käyttöä ilman ennakkoilmoitusta, mikäli tietojärjestelmien eheys tai luottamuksellisuus vaarantuvat.

10.10 Etätyö ja työnteko vakituisen työpaikan ulkopuolella

Etätyö on luvanvaraista. Esimies voi tapauskohtaisesti harkintansa perusteella sallia henkilölle satunnaisen etätyömahdollisuuden. Pysyväisluonteinen etätyömahdollisuus edellyttää henkilöltä kirjallista sitoutumista etätyöohjeen noudattamiseen.

Etätyönä suoritettaviin työtehtäviin sovelletaan samoja tietoturvaperiaatteita kuin toimitilakiinteistössä suoritettaviin työtehtäviin.

Työtehtävien suorittamiseen käytetään työnantajan hallinnoimia laitteita ja etäyhteyksiä.

10.11 Tietojen lokitus

Tietojärjestelmien käytöstä kirjataan tapahtumatietoja, joita tarvitaan tietojärjestelmän käytettävyyden, eheyden ja luottamuksellisuuden turvaamiseksi sekä väärinkäytösten selvittämiseksi.

Lokitietoja tallennetaan yrityksen kaikista tietojärjestelmistä esimerkiksi tietokannoista, sovelluksista ja palomuureista.

Lokitietojen avulla ylläpitohenkilöstö valvoo järjestelmien, tietoliikenteen ja sovellusten toimintaa sekä käyttöä osana normaalia ylläpitotoimintaa.

Lokitiedot arkistoidaan. Lokitietojen säilytysajat on määritelty tapauskohtaisesti lakeja ja säädöksiä noudattaen.

10.12 Tietojen varmistaminen

Tietohallinto huolehtii keskitetysti tietojen varmistamisesta. Tiedot varmuuskopioidaan hyvää tietohallintatapaa noudattaen ja johdon hyväksymien varmuuskopiointirutiinien mukaisesti.

Varmuuskopiointirutiinit on testattu siten, että on saatu riittävä varmuus operatiivisten järjestelmien palauttamisesta kohtuullisessa ajassa.

Ulkoistettujen käyttöpalveluiden osalta varmuuskopiointi on määritelty käyttöpalvelua tarjoavan osapuolen ja Yritys Oy:n tietohallinnon välillä solmitussa palvelusopimuksessa.

10.13 Haittaohjelmien torjunta

Tietojen saatavuus, eheys ja luottamuksellisuus on turvattu hyvän tietohallintatavan mukaisin teknisin, ohjelmallisin ja hallinnollisin ratkaisuin.

10.14 Verkkopalvelut

Sidosryhmille tarjottavien verkkopalveluiden tietoturvallisuus on huomioitu rakentamisen aikana tapahtuvissa suunnittelu- ja testausvaiheissa.

Ennen tuotantoon siirtoa verkkopalvelu on auditoitu ulkopuolisen luotettavan tahon toimesta ja palvelulle on suoritettu asianmukaiset testit.

Verkkopalvelu otetaan tuotantoon, mikäli se on todettu ulkopuolisen tahon toimesta kaikilta osin turvalliseksi.

Käyttöympäristössä tai sovelluksessa tapahtuvien muutosten yhteydessä verkkopalvelu auditoidaan uudelleen.

Verkkopalvelun ylikuormitustilanteisiin on varauduttu asianmukaisin toimenpitein siten, ettei palvelun käytettävyys vaarannu.

11 Tietoturvapolitiikan voimaantulo

Tietoturvapolitiikka on toimitusjohtajan ja johtoryhmän vahvistama ja annettu hallitukselle tiedoksi.

Tietoturvapolitiikka on toimitusjohtajan ja johtoryhmän päätöksillä hyväksytty XX.XX.XXXX.

Tietoturvapolitiikka on annettu tiedoksi hallitukselle XX.XX.XXXX