

Tietoturvapoliittikka

Tässä politiikassa kuvataan Würth Oy:n, Ferrometal Oy:n ja Würth Elektronik Oy:n (jäljempänä Yritykset) tietoturvapoliittikan 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 tämän politiikan mukaisen toiminnan suunnittelulle ja toimeenpanolle. Poliittikan organisaation kattavan toteutuksen tukemiseksi laaditaan lisäksi tarkempia ohjeistuksia tietoturvan eri osa-alueille.

Tietoturvallisuutta toteutetaan ja kehitetään riskilähtöisesti käyttäen tarkoituksenmukaisia ja kustannustehokkaita ratkaisuja. Tietoturvapoliittikan tarkoituksenmukaisuutta arvioidaan Yritysten johdonkatselmuksessa vuosittain.

Tietoturvapoliittikka yhdessä Yritysten arvojen, Code of Conduct, riskienhallinta-, turvallisuus- ja tietosuojapolitiikkojen kanssa ovat keskeinen osa Yrityksissä noudatettavaa hyvää hallintoa. Muutokset Tietoturvapoliittikassa vahvistetaan aina Yritysten ylimmässä johdossa.

Tietoturvapoliittikan päämäärä

Tietoturvan ensisijaisena päämääränä on yrityksen vastuulla olevien toimintojen jatkuvuuden turvaaminen kaikissa olosuhteissa. Tarkoituksenmukainen ja tehokas tietoturva mahdollistaa yrityksen toimintoihin liittyvien ICT-ratkaisujen käytettävyyden, prosesseissa ja palveluissa käytettävien tietojen eheyden sekä luottamuksellisuuden kaikissa olosuhteissa kaikissa Würth konsernin Suomen yrityksissä. Tämä politiikka luo perustan Würth Oy:n, Würth Elektronik Oy:n ja Ferrometal Oy:n tietojärjestelmien ja tietojenkäsittelyn turvallisuuden varmistamiselle.

Yrityksessä asiakastietojen ja muiden digitaalisten toimintojen tuottaman ja käsittelemän datan turvaaminen on olennainen osa vastuullista toimintaa, jota sekä asiakkaamme että yhteistyökumppanimme edellyttävät yrityksiltä. Digitaalisuuden kasvu merkitsee sitä, että tietoturvallisuutta säännellään enenevässä määrin myös lainsäädännöllä.

Yritykset ovat sitoutuneet vaatimusten mukaiseen toimintaan ja tietoturvan jatkuvaan kehittämiseen vuosittaisen tietoturvan kehityssuunnitelman mukaisesti. Würth on sitoutunut toimimaan henkilötietoja käsitellessään EU:n tietosuoja-asetuksen sekä kansallisen lainsäädännön mukaisesti.

Tämä Tietoturvapoliittikka on nähtävillä Yritysten intranetissä henkilöstölle ja Yrityksissä työskenteleville. Jokaisen työntekijän ja Yrityksissä työskentelevän on noudatettava tietoturvapoliittikkaa, sitä täydentäviä periaatteita ja ohjeita sekä soveltuvaa lainsäädäntöä.

Vastuut ja organisointi

Tietoturvapoliittikka kattaa Yritysten kaikki toiminnot Suomessa. Henkilöstön on noudatettava poliittikkaa.

Yritysten hallituksen puheenjohtaja vastaa siitä, että kussakin yrityksessä on toimiva tietoturva osana riskienhallintajärjestelmää. Tietoturvan toteuttamisessa hallituksen puheenjohtajalla on apunaan yrityksen tietohallinto-, laatu- ja riskienhallintatoiminnot. Riskienhallinnan ohjausryhmä, jossa on eri osastojen ja/tai Yritysten edustajat, käsittelee ja seuraa tietoturvariskejä sekä riskienhallintatoimenpiteiden toteutumista.

Vastuu tietoturvan toteuttamisesta on Yritysten johdolla. Tietohallinto koordinoi ja kehittää tietoturvaprosesseja, vastaa käytännön toteutuksesta yhdessä palveluntarjoajien kanssa, raportoinnista sekä toteuttaa yhdessä liiketoimintojen ja yhteisten toimintojen kanssa tietoturvariskien tunnistamista ja hallintatoimenpiteiden määrittämistä. Yritysten henkilöstön pitää tunnistaa tietoturvaan liittyvät riskit ja reagoida niihin.

Tietoturvan hallinta/ohjausmalli

Würth Oy:n tietohallinto johtaa tietoturvan kehittämistä ja ylläpitoa sekä vastaa tietoteknisestä toiminnan jatkuvuudesta kaikissa Yrityksissä. Yrityksiä tiedotetaan tietotekniikan, tietoturvan ja jatkuvuuden hallinnan muutoksista ja kehittämisestä.

Würth Oy:n tietohallinto vastaa tavoitteiden saavuttamisesta ja myös ICT/tietoturvan kehittämisestä ja jatkuvuudesta.

Tietoturvaa koskevat päätökset tekee hyväksymisvaltuuksiensa puitteissa Würth Oy:n tietohallintopäällikkö ja Würth Oy:n toimitusjohtaja / Yritysten hallituksen puheenjohtaja.

Yrityksellä on menettelytavat ja palvelut tietoturvapoikkeamien havaitsemiseksi. Mahdollisten tietoturvaloukkauksien käsittelyyn ja raportointiin on määritelty hallintaprosessin avulla, jota johtaa tietohallintopäällikkö.

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

Tietoturvan hallintajärjestelmän mukainen toiminta varmistetaan sisäisen valvonnan sekä sisäisten ja ulkoisten tarkastusten ja auditointien avulla. Teknistä tietoturvaa valvotaan jatkuvasti ja tärkeimpiin ympäristöihin tehdään erillisiä tietoturvatarkastuksia.

Tietoturvakoulutus

Yrityksellä on käytössä erilaisia, säännöllisesti toteutettavia toimenpiteitä työntekijöiden tietoturvallisuustietoisuuden parantamiseksi. Näitä ovat muun muassa verkkokoulutukset, huijausviestisimulaatiot sekä uutisointi/viesti intraneteissa ja ilmoitustauluilla. Lisäksi valituille kohderyhmille järjestetään kohdennettua tietoturvakoulutusta.

Riskien arviointi

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

Tietoturvarikkomukset

Tietoturvarikkomukseksi lasketaan tietoturvapoliitikan ja -ohjeistuksen vastainen toiminta. Yritykset ovat määritelleet menettelytavat rikkomustilanteille.

Riihimäellä 22.2.2024

Mika Rantanen
Yritysten hallituksen puheenjohtaja