



# Tehden Oy tietoturvapoliittika

Hyväksytty 13.11.2023

## 1. Johdanto

Tietoturvallisuus on Tehden Oy:n kriittinen menestystekijä ja toiminnan mahdollistaja. Yhtiön hallitus on sitoutunut tietoturvallisuuden kehittämiseen. Tämä yhtiön hallituksen vahvistama tietoturvapoliittika kattaa yrityksen kaikkien toimintaan liittyvät tietojen käsittelyn tehtävät. Tietoturvapoliittika määrittelee ne periaatteet, vastuut, toimintatavat, sekä seurannan ja valvonnan, joita yhtiössä noudatetaan tietoturvan toteuttamisessa ja kehittämisessä.

**Tietoturvallisuudella** tarkoitetaan kaikkien tietojen, missä tahansa muodossa ne esiintyvätään, turvallista käsittelyä. Tietoturvallisuus on tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamista. Tietoturvaan kuuluvat tietoturvaorganisaatio, tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit, sekä välineistön ja tilojen tietoturvaominaisuudet.

Yhtiön **tietoturvaperiaatteet** perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaan, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon yrityksen tietoturvan kehittämisessä.

**Jokaisen yhtiön työntekijän** on tunnettava tämä tietoturvapoliittika ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä. Tietoturvapoliittika koskee kaikkia Tehden Oy:ssä työskenteleviä ja se ulotetaan soveltuvin osin myös toimittajiin ja muihin sidosryhmiin. Tietoturvapoliittika sisältää tietoturvaan liittyvien vastuualueiden jaon yhtiön organisaatiossa.

## 2. Tietoturvatyö ja sen päämäärä

**Tietoturvatyö** on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. **Tietoturvaryhmän puheenjohtaja** vastaa yrityksen tietoturvatyön kokonaisuudesta johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa.

Tietoturvatyö on erityisen tärkeää Tehden Oy:lle, koska yhtiö käsittelee asiakasyritysten ja näiden loppuasiakkaiden tietoja, jotka sisältävät henkilötietoja ja liiketoimintaa koskevia tietoja. Tietoturvatyöllä varmistetaan, että asiakas- ja muita henkilötietoja käytetään vain sopimusten ja lainsäädännön sallimiin tarkoituksiin ja ne ovat vain niitä työhönsä tarvitsevien käytössä.

Tietoturvatyön päämäärä on myös turvata Tehden Oy:n toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai tahallisten, tuottamuksellisten ja tapaturmaisten inhimillisten tekojen aiheuttamilta uhilta ja vahingoilta. Tällaisia voivat olla esim. yhtiötä vastaan kohdistettu vakoilu tai muu rikollinen toiminta, tahattomat tietovuodot, sekä huolimattomuus tai osaamattomuus tietoja käsiteltäessä. Tällaiset tilanteet voisivat aiheuttaa yhtiölle merkittäviä taloudellisia menetyksiä, tuotannollisia tai toiminnallisia vahinkoja.

Tietoturvallisuutta toteutetaan ja kehitetään käyttäen riskien kannalta tarkoituksenmukaisia ja kustannustehokkaita ratkaisuja. Tietoturvallisuutta seurataan aktiivisesti ja poikkeamiin puututaan ennalta määriteltyjen menetelmien mukaisesti. Toiminnassa huomioidaan työntekijöiden, asiakkaiden ja yhteistyökumppanien sopimukset, yksityisyyden suoja sekä muut lakien vaatimukset. **Tietoturvatyötoimenpiteillä** hallitaan uusien toimintatapojen ja teknologioiden käyttöönottoon liittyvät riskit.

Hyväksytyt tietoturvapoliittikan mukainen tietoturvatyö sisällytetään luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa Tehden Oy:n yleistä turvallisuustoimintaa, riskienhallintaa ja sisäistä valvontaa.

### 3. Organisointi ja vastuut

Yhtiön tietoturvaan ja tietosuojaan liittyen **yhtiön hallitus** käyttää ylintä päätäntävaltaa. Hallitus päättää kulloinkin tietoturva- ja tietosuojatyöhön käytettävissä olevista riittäviksi katsomistaan resursseista. Hallitus valvoo tietoturvaryhmän toimintaa. Hallitus päättää yrityksen kokonaisturvallisuuden yleisistä tavoitteista.

**Toimitusjohtaja** päättää yrityksen kokonaisturvallisuuden organisoinnista, resursseista ja toimintavaltuuksista, sekä nimeää tietoturvaryhmän puheenjohtajan ja tietosuojavastaavan.

Yrityksen tietoturvanäkemyksiä edustaa **tietoturvaryhmä**, jonka asettaa toimitusjohtaja. Tietoturvaryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään toimitusjohtajalle hyväksyttäväksi. Tietoturvaryhmä päättää kulloisetkin painotukset eri kokonaisturvallisuuden osa-alueisiin saamansa resurssien ja yleisten tavoitteiden puitteissa. Tietoturvaryhmä hoitaa tehtäviään yhdessä ja vastaa tietoturvaan ja tietosuojaan liittyvistä asioista yhdessä. Tietoturvaryhmä valvoo yhtiön tietoturvaa ja tietosuojaa.

**Esihenkilöt** vastaavat tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omille alaisilleen ja omassa yksikössään tietoturvaryhmän ohjeiden mukaisesti. Tietoturvaryhmä toimii esihenkilöiden tukena tietoturvaan ja tietosuojaan liittyvien kysymysten käsittelyssä.

Lisäksi käytössä olevilla ohjelmistoilla on omat **pääkäyttäjät**, joita tietoturvaryhmä ohjeistaa ja voi kuulla kokouksissa. Kokouksissa voi olla läsnä myös toimitusjohtaja. Ohjelmistojen pääkäyttäjät vastaavat ohjelmien käytön ja ominaisuuksien tarkkailusta tietoturvan kannalta, ja ovat velvollisia ilmoittamaan tietoturvaryhmälle havaitsemistaan mahdollisista riskeistä ja uhista. Tietoturvaryhmä antaa pääkäyttäjille ohjeistuksia käytännön työhön.

**Jokainen Tehden Oy:n työntekijä** on omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä tietoturvaohjeiden noudattamisesta. Työntekijät ovat velvollisia raportoimaan havaitsemistaan tietoturvaan liittyvistä uhista ja poikkeamista tietoturvaryhmälle, tietoturvaryhmän yksittäiselle jäsenelle tai esihenkilölle. Tietoturvaryhmän jäsenten sekä esihenkilöiden tehtävänä on viivytyksettä tuoda raportoitu asia tietoturvaryhmälle tiedoksi. Tietoturvaryhmän vastuulla on ottaa asia käsittelyyn.

## 4. Tietoturvaryhmän roolit

### Tietoturvaryhmän puheenjohtaja

- Järjestää tietoturvaryhmän säännölliset palaverit
- Ehdottaa toimitusjohtajalle uudet jäsenet vaihdosten tapahtuessa
- Varmistaa, että ryhmän sisäiset kokoukset tulevat asianmukaisesti dokumentoitua.
- Johtaa tietoturvaan ja tietosuojaan liittyvää tiedottamista sisäisesti ja yrityksen ulkopuolelle
- Vastaa ryhmän toiminnan kokonaisuudesta toimitusjohtajalta saamiensa resurssien ja toimivaltuuksien puitteissa
- Vastaa tietoturvasuunnitelman päivittämisestä ja esittelemisestä vuosittain toimitusjohtajalle ja hallitukselle

### Tietoturvavastaava

- Vastaa tietoturva-asioiden tiedottamisen asiasisällöstä
- Vastaa tietoturvaosaamisen edistämisestä yhtiössä
- Vastaa tietoturvasuunnitelman toteutuksen valvonnasta tietoturvan osalta

### Tietosuojavastaava

- Vastaa yrityksen henkilötietoja sisältävien henkilörekistereiden suojaamisesta ja valvonnasta
- Vastaa tietosuoja-asioiden tiedottamisen asiasisällöstä
- Vastaa tietosuojaosaamisen edistämisestä yhtiössä
- Vastaa tietoturvasuunnitelman toteutuksen valvonnasta tietosuojan osalta

### Henkilöstövastaava

- Vastaa tietoturvaan ja tietosuojaan liittyvien asioiden huomioimisesta henkilöstöprosesseissa koko työsuhteen elinkaaren ajan

### Henkilökunnan laitteiden tietoturvasta vastaava

- Vastaa työntekijöiden henkilökohtaisessa käytössä olevien työnantajan omistamien laitteiden osalta laitteiden tietoturvan huomioimisesta ja työntekijöiden ohjeistamisesta
- Vastaa yleisestä tietoturvaan liittyvästä ohjeistamisesta koko henkilökunnalle kaikista laitteista, joita työntekijät käyttävät työtehtäviensä suorittamiseen

- Vastaa työntekijöiden yhteisessä käytössä olevien toimiston sisäverkkoon kytkeytyvien laitteiden tietoturvasta, esim. verkkotulostimista

### **Palvelinympäristöjen ja verkkolaitteiden tietoturvasta vastaava**

- Vastaa toimiston sisäverkon ja ulkoverkkoon pääsyn mahdollistavien laitteiden tietoturvasta, esim. reitittimet, kytkimet ja palomuuuri
- Vastaa yrityksen käytössä olevien palvelimien tietoturvasta, esim. yrityksen omat palvelimet sisäverkossa ja ulkoverkon kautta saatavilla olevat ostetut palvelimet muilta
- Vastaa yrityksen verkko-osoitepalveluiden tietoturvasta

### **Tehden-ohjelmistojen tietoturvasta vastaava**

- Vastaa Tehdenin tuottamien ohjelmistojen kehittämisestä ja toiminnasta tietoturvallisesti
- Valvoo tietoturvan toteutumista liittyen Tehden-ohjelmistossa hyödynnettyjen 3. tahon ohjelmistoihin ja palveluihin, esim. tekstiviesti- ja sähköpostipalveluihin

### **Henkilökunnan käyttämien ohjelmistojen tietoturvasta vastaava**

- Valvoo tietoturvan toteutumista henkilökunnan käyttämissä ohjelmissa ja ohjeistaa näistä asioista pääkäyttäjiä

## 5. Tietoturvan toteutus

Tietoturvan toteuttamisen perusta on tämä Tehden Oy:n hallituksen hyväksymä kirjallinen tietoturvapoliittikka, joka annetaan tiedoksi työntekijöille.

Tietoturvaryhmä pitää säännöllisiä kokouksia, joissa pidetään pöytäkirjaa. Tietoturvaryhmä kirjaa kokouspöytäkirjan esityslistalle esille nousseet tietoturvaryhmän käsittelyä vaativat tietoturvaan ja tietosuojaan liittyvät huomiot ja kysymykset. Kiireelliset tietoturvaryhmän käsittelyä vaativat asiat tietoturvaryhmä ottaa käsittelyyn viivytyksettä. Tietoturvaryhmä ylläpitää ja kehittää kanavia, joissa yhtiön henkilökunta tavoittaa tietoturvaryhmän esille nousevissa kysymyksissä ja huomioissa, ja joissa tietoturvaryhmä tiedottaa ja ohjeistaa ajankohtaisista tietoturvaan ja tietosuojaan liittyvistä asioista.

Tietoturvaryhmä tarkastaa vuosittain yhtiön sisäisen **tietoturvasuunnitelman** yhtiön hallituksen asettamien tavoitteiden pohjalta. Lisäksi tietoturvasuunnitelmaa päivitetään tietoturvaryhmän toimesta tarpeen mukaan havaintojen perusteella.

Tietoturvasuunnitelma sisältää:

- Kuvauksen tietoturvan toteuttamisesta ja ylläpidosta
- Kuvauksen niistä hallinnollisista ja teknisistä ratkaisuista, joilla toteutetaan jatkuva prosessi tietoturvan tavoitteiden saavuttamiseksi
- Yleiset kehittämiskohteet, joilla tietoturvaan ja tietosuojaan liittyviin asetettuihin tavoitteisiin päästään

Tietoturvaryhmän puheenjohtaja esittelee vuosittain sekä muiden päivitysten yhteydessä tietoturvasuunnitelman toimitusjohtajalle ja yhtiön hallitukselle. Hallitus hyväksyy tietoturvasuunnitelman.

Työntekijöiden toimintaa ohjataan tietoturvasuunnitelmaan sisältyvillä toimintaohjeilla sekä tietoturvakoulutuksella.