# Tietoturvallisuuspolitiikan mallipohja

**Tässä dokumentissa on kuvattu esimerkinomaisesti, millainen yrityksen kirjallinen tietoturvallisuuspolitiikka voi olla. Tietoturvallisuuspolitiikan tulisi olla 1-2 sivun mittainen dokumentti, jossa on kerrottu yrityksen tietoturvallisuuteen liittyvistä asioista. Tietoturvallisuuspolitiikka sisältää muun muassa sen velvoittavuuden, perusteet, tavoitteet, pääperiaatteet, vastuut ja organisoinnin sekä tiedottamisen. Alla on tarkempi malliteksti.**

## Velvoittavuus

Tämä tietoturvallisuuspolitiikka koskee kaikkia yritykseen X työsuhteessa olevia henkilöitä sekä yrityksen tiloissa työskenteleviä yhteistyökumppanien ja toimittajien työntekijöitä. Tietoturvallisuuden toteuttamiseksi annettuja ohjeita ovat velvollisia noudattamaan myös muut yrityksessä asioivat henkilöt, kuten vierailijat ja asiakkaiden edustajat.

## Yritysjohdon perusteet tietoturvallisuudelle

Yrityksen X toiminta perustuu tuotteiden korkeaan laatuun, asiakastyytyväisyyteen, toiminnan jatkuvaan parantamiseen ja toimintaa tukevien tietojärjestelmien tehokkaaseen hyödyntämiseen. Näiden tavoitteiden saavuttamiseksi on olennaisen tärkeää, että tietojärjestelmät toimivat luotettavasti ja virheettömästi kaikissa tilanteissa. Tietojen ja tietojärjestelmien turvaamiseksi tulee toteuttaa tarvittavia hallinnollisia, toiminnallisia ja teknisiä ratkaisuja, koulutusta ja tiedottamista. Lisäksi yrityksessä on varauduttava todennäköisiin uhkatilanteisiin ja toimintaan uhkatilanteiden toteutuessa (toipumis- ja jatkuvuussuunnittelu). Yrityksen tietoturvallisuutta pyritään jatkuvasti arvioimaan ja parantamaan.

## Tavoitteet

Tietoturvallisuuden tavoitteena on ylläpitää ja kehittää yrityksen tietojen ja tietojärjestelmien käytettävyyttä, luotettavuutta ja eheyttä hyvän tietohallintotavan, lainsäädännön ja yrityksen liiketoimintastrategian vaatimusten mukaisesti. Tavoitteena on myös estää yrityksen resurssien luvaton käyttö, kehittää toiminnan laatua, turvata yrityksen luotettavuus ja maine yhteistyökumppanina sekä varautua uhkatilanteisiin ja niistä toipumiseen.

## Pääperiaatteet

Tietoturvallisuuden toteuttaminen on osa yrityksen riskienhallintaa. Organisaation eri tasoilla arvioidaan säännöllisesti vuosittain toimintaan kohdistuvia tietoriskejä osana yrityksen riskienhallintatoimintaa. Riskienarvioinnin perusteella suunnataan eniten resursseja ja tarvittavia toimenpiteitä uhanalaisimmille tai yrityksen toiminnan kannalta kriittisimmille osa-alueille. Käytännön tietoturvallisuustoimenpiteet kirjataan vuosittain tehtävään yrityksen tietoturvallisuuden kehittämissuunnitelmaan. Henkilöstölle ja yhteistyökumppaneille jaetaan asiaa koskevia toimintaohjeita ja järjestetään tarvittavaa koulutusta.

## Vastuut ja organisointi

Tietoturvallisuus on osa kunkin työntekijän jokapäiväistä toimintaa. Tämän vuoksi jokainen yrityksen työntekijä ja toimitiloissa työskentelevä on vastuussa oman toimintansa tietoturvallisuudesta. Viime kädessä toiminnasta vastaa yrityksen johto. Vastuu tietoturvan käytännön toteutuksesta, ohjauksesta ja valvonnasta on yrityksen linjaorganisaatiossa, lisäksi jokaisella tietojärjestelmällä on omistaja, joka vastaa järjestelmän tietojen käytöstä. Yrityksen johtoryhmä käsittelee säännöllisesti kokouksessaan ajankohtaisia yrityksen tietoturvallisuuteen liittyviä seikkoja.

Yritykseen on nimetty tietoturvallisuuspäällikkö ja tietoturvallisuusryhmä, jotka toimivat linjaorganisaation apuna kehittäen, koordinoiden ja ohjeistaen tietoturvallisuuden käytännön toteuttamista. Tietoturvallisuuspäällikkö raportoi yrityksen tietoturvallisuustilanteesta johtoryhmälle neljännesvuosittain ja muutenkin tilanteen niin vaatiessa.

## Tiedottaminen

Yrityksen tietoturvallisuudesta ja mahdollisista tietoturvallisuustapahtumista tiedottamisesta huolehtii tietoturvallisuusryhmä yrityksen johdon antamien ohjeiden mukaisesti. Muut yksiköt tai henkilöt eivät anna mitään tiedonantoja yrityksen ulkopuolelle.