

Tietoturvakartoitus-kysymyslista

- Mikä on yritykselle arvokasta tietoa?
- Mikä on yritykselle elintärkeän arvokasta tietoa?
- Kuinka tietoja valvotaan?
- Mitä tietoa tarvitaan päivittäin?
- Mitä tietoa tarvitaan kuukausittain tai harvemmin?
- Onko yritykselle tehty tietoturvallisuuden riskianalyysi?
- Jos yrityksen tietokone varastetaan, voiko joku hyödyntää siinä olevaa tietoa?
- Jos tapahtuu sähkönjakeluhäiriö, voivatko päivän aikana luodut tiedostot hävitä?
- Jos kiinteistössä syttyy tulipalo, voivatko tiedot tuhoutua ja liiketoiminta pysähtyä?
- Jos tietokone ei tunnista käyttäjää, voiko konetta käyttää petokselliseen toimintaan?
- Onko etätyön tietoturvasta huolehdittu?
- Jos työntekijä kertoo junassa tutulleen tuotekehityksen tuloksista, voiko tieto olla merkittävä takana istuvalle kilpailijalle?
- Jos yrityksessä työskentelevä ulkopuolinen työntekijä kuljettaa tietoa ulkopuolelle, voivatko tiedot joutua niitä hyödyntäville tahoille?
- Jos työntekijä irtisanotaan, voiko hän tuhota tärkeitä tietoja tai viedä ne eteenpäin ja hyötyä niistä?
- Onko turvallisuuden kehittämistarpeet tunnistettu?
- Onko turvallisuuden kehittämistarpeet kirjattu kehittämissuunnitelmaksi?
- Onko yrityksellänne selkeä johdon hyväksymä tietoturvallisuuspolitiikka?
- Onko kehittämiskustannukset arvioitu?
- Onko päätetty miltä osin toiminta vakuutetaan?
- Onko henkilökunta perehdytetty yrityksen tietoturvan käytäntöihin?
- Onko tietoturvavastuut määritelty?
- Onko tehtävät vastuutettu?

- Miten huolehditaan tärkeiden tehtävien varahenkilöjärjestelyistä?
- Saako jokainen työntekijä käyttöoikeudet vain niihin tietoihin, joita työtehtävä edellyttää?
- Miten toimitaan, jos epäillään väärinkäytöksiä?
- Kuinka usein varmistetaan palautusten, varmenteiden ja varajärjestelmien toimivuus?
- Missä tilanteissa käytetään sähköpostiviestien salakirjoitusmenetelmiä?
- Säilytetäänkö turvakopiot eri kiinteistöissä?
- Mikä on yrityksenne tietoturvallisuuden tilanne tänään?

Pohdintakysymyksiä henkilötietojen käsittelyyn liittyen

- Käsittelekö yritys henkilötietoja?
- Käsittelekö se niitä itsenäisenä rekisterinpitäjänä vai toimeksiannosta toisen lukuun?
- Onko henkilötietojen käsittelyn tarkoitus ja siihen liittyvät prosessit suunniteltu henkilötietolain (523/1999) 6 §:n edellyttämällä tavalla?
- Onko henkilötietojen suojaamisesta huolehdittu kaikissa niiden käsittelyvaiheissa (sekä sähköisen että manuaalisen aineiston osalta)?
- Onko työntekijät perehdytetty henkilötietojen käsittelyyn ja siihen liittyviin vastuisiin (mm. salassapito- ja vaitiolovelvollisuuteen)?