

**Tietoturvapolitiikan esimerkkipohja**

**Muutoshistoria**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Muutospäivä** | **Tekijä** | **Tehty muokkaus** | **Hyväksyjä** | **Versio** |
|  |  |  |  |  |
|  |  |  |  |  |

Sisällysluettelo

[**Yleistä** 3](#_Toc207016725)

[**Tietoturvan hallinnan tavoitteet ja periaatteet** 4](#_Toc207016726)

[**Tietoturvan hallinnan vastuut** 4](#_Toc207016727)

[**Koulutus ja viestintä** 5](#_Toc207016728)

[**Seuranta, mittaaminen ja poikkeamien käsittely** 6](#_Toc207016729)

# **Yleistä**

Tietoturva on osa kokonaisturvallisuutta, jota hallitaan turvallisuuspolitiikan mukaisesti. Tietoturvapolitiikkaa ja tämän alaisia ohjeistuksia sovelletaan kaikkeen vesihuoltolaitoksen omistamaan sekä hallinnoimaan tietoon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tietoturvapolitiikka toimii perustana vesihuoltolaitoksen tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja auttaa sen käytäntöön soveltamisessa. Tietoturvapolitiikka sisältää korkeimmat linjaukset tietoturvallisen toiminnan ylläpitämiseksi ja kehittämiseksi. Tämän päämääränä on yhdenmukaiset toimintaperiaatteet ja käytännöt tavoitellun tietoturvatason saavuttamiseksi ja toteuttamiseksi. Tietoturvapolitiikkaa täydennetään erikseen hyväksyttävillä linjauksilla ja toiminta- prosessi- ja menettelyohjeilla.

Tässä politiikassa esitettyjä periaatteita noudatetaan kaikessa tietojen ja materiaalin käsittelyssä, tilojen ja organisaation omaisuuden käytössä sekä viestinnässä. Tietoturvapolitiikka sekä sitä täydentävät muut politiikat ja ohjeet määrittää ne periaatteet, toimintatavat, vastuut, ja valvontajärjestelmän, joita noudattamalla luodaan edellytykset tietoturvan toteuttamisen ja kehittämisen toteutumiseen.

Tietoturvan hallinta ja toteutus nojaa tietoturvallisuuden perusperiaatteisiin jotka ovat:

"Luottamuksellisuus (confidentiality) - niiden tietojen ominaisuus, jotka ovat vain valtuutettujen henkilöiden tai järjestelmien käytettävissä.

Yrityksen hallussa olevien asiakas- ja henkilötietojen luottamuksellisuus pyritään varmistamaan jatkuvalla teknisen tietoturvallisuuden kehittämisellä, henkilöstön kouluttamisella, tiedottamisella ja tiedonkäsittelyyn liittyvien toimintaohjeiden jalkauttamisella."

"Eheys (integrity) - niiden tietojen ominaisuus, joita vain valtuutetut henkilöt tai järjestelmät saavat muuttaa sallituilla tavoilla.

Toimintaa ohjaavan tiedon eheys pyritään turvaamaan järjestelmien tarkistusten ja valvonnan kautta. Turvatoimien ja ohjeistuksen tavoitteena on varmistaa toiminnan perustuminen oikeaan tietoon kaikissa tilanteissa, sekä mahdollisen vahingon minimoiminen poikkeustilanteissa."

"Saatavuus (availability) - niiden tietojen ominaisuus, jotka ovat valtuutettujen henkilöiden käytettävissä niitä tarvittaessa.

Tietoturvallisuutta lisäävillä toimilla pyritään varmistamaan toimintakriittisten järjestelmien toiminta ja merkityksellisen tiedon saatavuus kaikissa tilanteissa. Tällaisia toimia ovat esimerkiksi teknisten järjestelmien jatkuva laadullinen arviointi ja kehittäminen sekä ammattitaitoisen henkilöstön varmistaminen."

# **Tietoturvan hallinnan tavoitteet ja periaatteet**

Tietoturvan tavoitteena on tämän osalta turvata vesihuoltolaitoksen kyvykkyys toteuttaa tämän ydintoimintoja asiakkaille ja sidosryhmille sekä estää tai minimoida omalle toiminnalle aiheutuvat seuraukset tietoturvallisuuteen liittyvien uhkien ja poikkeamien osalta. Lisäksi tietoturvallisuustoiminnalla varaudutaan riskeihin tietojen, tietojärjestelmien ja palveluiden jatkuvuuden osalta pyrkimällä takaamaan näiden keskeytymätön toiminta. Tavoitteena on suojata vesihuoltotoiminnan mainetta, omaisuutta ja henkilöstöä, varmistaa häiriötön toiminta ja toimintojen jatkuvuus sekä tunnistaa ja hallita tietoturvariskejä.

Normaalin jokapäiväiseen toimintaan liittyvän tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkiin ja niistä toipumiseen. Organisaation toiminta tukeutuu tälle kriittisesti keskeisten järjestelmien toimintaan ja systemaattinen tietoturvallisuuden kehittäminen on olennainen osa näiden jatkuvuuden hallintaa.

Tietoturvallisuus tulee ottaa huomioon mahdollisimman varhaisessa vaiheessa toimintaa suunniteltaessa. Toimintaympäristön riskeihin valmistaudutaan varustamalla työ- ja laitetilat tarvittavin kulunvalvonta- ja suojausratkaisuin.

Vesihuoltolaitoksen tietoturvavaatimukset määrittävät tietojärjestelmiltä ja sopimuskumppaneilta vaadittavan minimitason tietoturvan osalta. Laitoksen tulee varmistaa, että sisäiset sekä ulkoiset vaatimukset, kuten lakivelvoitteet ja sopimukset otetaan huomioon sekä, että toiminta on jäljitettävissä eli, että tehdyt päätökset ja muutokset tietoturvan käsittelyssä pystytään tarvittaessa todentamaan.

# **Tietoturvan hallinnan vastuut**

Tietoturvapolitiikka koskee kaikkea tietoturvan soveltuvuusalueen piirissä työskentelevää henkilöstöä. Jokainen työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteutumisesta sekä tietoturvaohjeiden noudattamisesta. Jokaisen työntekijän on noudatettava tätä politiikkaa, tietoturvaohjeita sekä voimassa olevaa lainsäädäntöä. Havaituista ja epäillyistä tietoturvapoikkeamista on ilmoitettava aina esihenkilölle ja tietoturvaryhmälle. Tietoturvakäytäntöjen noudattamatta jättämisestä voidaan määrätä kurinpitoseuraamuksia organisaation henkilöstöhallinnon käytäntöjen ja paikallisten lakien mukaisesti.

Ylin johto vastaa vesihuoltolaitoksen tietoturvapolitiikan ja -menettelyjen laatimisesta ja toimeenpanosta. Toimitusjohtaja vastaa tietoturvallisuuden toteuttamisen kokonaisuudesta sekä raportoinnista hallitukselle. Toimitusjohtaja hyväksyy yhtiötasoiset tietoturvalinjaukset ja ohjeet. Toimitusjohtajan tukena tietoturva-asioissa on operatiivinen johto ja yhtiön tietoturvaryhmä. Johdon vastuulla on varata vastuuhenkilöille kulloinkin tarpeelliset resurssit toimintojen toteuttamiseksi.

Operatiiviset johtajat vastaavat tehtäviensä mukaisesti tietoturvallisuuden toteutumisesta ja kehittämisestä yksiköissään. Päälliköt tarkastavat ja varmistavat, että heidän vastuualueensa tieto-omaisuuden tietoturvariskien käsittely ja menettelyt noudattavat asianmukaisia turvallisuuspolitiikkoja ja muita turvallisuusvaatimuksia. Esihenkilöt vastaavat työntekijöidensä perehdyttämisestä tietoturva- ja tietosuojaohjeisiin sekä ohjeiden noudattamisen valvonnasta.

Vesihuoltolaitoksen tietoturvaryhmään nimetyt henkilöt vastaavat tietoturvan ylläpito- ja kehittämistoimista. Tietoturvaryhmä toimii asiantuntijana tietoturvaa koskevissa asioissa, valmistelee johdolle esitykset tietoturvaohjeista, linjauksista ja ratkaisuista sekä tietoturvallisuuden hallinnan kokonaiskehittämisestä. Tietoturvaryhmä arvioi tietoturvariskejä ja ylläpitää tietoturvariskien arviointia ajan tasalla sekä, seuraavat tietoturvallisuuden yleistä kehittymistä sekä toimintaympäristön muutoksia ja tekevät siihen perustuen kehitysehdotuksia johdolle tietoturvallisuuden parantamiseksi.

Tietoturvaryhmän vastuulla on tietoturvan tekninen toteutus, yleisten tietoturvaohjeiden ja käytäntöjen laatiminen sekä niistä tiedottaminen. Ryhmän vastuulla on myös ohjeistaa ja tukea muita huomioimaan nämä periaatteet uusien prosessien suunnittelussa, tietojärjestelmien hankinnoissa sekä laadittaessa muita ohjeistuksia. Ryhmä vastuulla on lisäksi tietoturvatason seurannan ja raportoinnin järjestäminen sekä tietoturvariskien arviointi.

Tietoturvaryhmä käsittelee tietoturvapoikkeamat. Tietoturvaryhmä suunnittelee ja organisoi yhtiötason tietoturva- ja tietosuojakoulutuksia ja kokoaa tietoturvaa koskevat tiedot tilinpäätöstä varten. Tietoturvaryhmän jäsenet vastaavat myös yhteydenpidosta ja yhteistyöstä tietoturvaan liittyvissä ulkoisissa sidosryhmissä. Erityisesti operatiivisten järjestelmien hallinnassa on varmistettava henkilöstön riittävä pätevyys tehtävien suorittamiseen.

# **Koulutus ja viestintä**

Koko henkilöstölle järjestetään säännöllisesti tietoturvakoulutusta sekä -harjoituksia työtehtävien mukaisesti. Tietoturvakoulutukset sisältyvät koulutussuunnitelmaan ja niistä ylläpidetään koulutusrekisteriä. Koulutus auttaa henkilöstöä ymmärtämään tietoturvaohjeita, osallistumaan aktiivisesti tietoturvallisuuden ylläpitämiseen ja kehittämiseen sekä tunnistamaan poikkeamia.

Koulutus sisältää vähintään tietoturvapolitiikan läpikäynnin sekä tietoturvatapahtumien ja mahdollisten tietoturvauhkien ilmoitusmenettelyt. Asiaankuuluvat ohjeet ovat kaikkien työntekijöiden saatavilla ja tietoturvatietoisuutta parannetaan säännöllisesti. Henkilöstölle ja sidosryhmille viestitään säännöllisesti työtehtävien kannalta olennaisista tietoturva-asioista.

Tietoturvapoikkeamien sattuessa kaikille asiaankuuluville viranomaisille ja sidosryhmille ilmoitetaan tilanteesta ja heitä pidetään ajan tasalla poikkeamanhallintaprosessin aikana. Yhtiön tietoturvakäytäntöihin ja poikkeamatilanteisiin liittyvä viestiminen ulkopuolisille vaatii aina ylimmän johdon luvan.

# **Seuranta, mittaaminen ja poikkeamien käsittely**

Tietoturvatason ja tietoturvapolitiikan toteutumisen ylläpitäminen edellyttää toiminnan, prosessien ja tietojärjestelmien järjestelmällistä, systemaattista ja automatisoitua valvontaa.

Tietoturvallisuuden tilaa ja hallintatoimenpiteitä seurataan ja valvotaan jatkuvasti toimenpiteiden tehokkuuden arvioimiseksi ja poikkeamien havaitsemiseksi. Arvioimisessa käytetään erikseen määriteltyjä mittareita, kuten Kyberturvallisuuskeskuksen kybermittaripalvelua, sekä muita keinoja.

Seuranta kohdistetaan ensisijaisesti tärkeimpiin suojattaviin kohteisiin ja niihin kohdistuvien riskien ennaltaehkäisyyn sekä tietoturvan tavoiteltavaan tasoon valitun kriteeristön mukaan. Suojaustaso arvioidaan analysoimalla suojattavan tiedon luottamuksellisuus-, eheys- ja saatavuus-sekä mahdolliset muut vaatimukset.

Tietoturvapoikkeamien ilmoittamiselle ja käsittelemiselle on olemassa kuvattu prosessi, jonka mukaisesti varmistetaan riittävän tehokas reagoiminen poikkeamiin kulloisenkin kriittisyyden ja kiireellisuuden mukaisesti. Poikkeamaprosessi sisältää sekä toimenpiteet tapahtuman käsittelylle, että raportoinnin käytännöt johdolle.