

**Tietoturvariskienhallinnan esimerkkipohja**

**Muutoshistoria**

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

Sisällysluettelo

[**Tietoturvariskienhallinnan tavoitteet** 3](#_Toc207193574)

[**Tietoturvariskienhallinnan vastuut** 3](#_Toc207193575)

[Tietoturvariskienhallinnan prosessi 4](#_Toc207193576)

[Toimintaympäristön määritteleminen 4](#_Toc207193577)

[Tietoturvariskien kartoitus 5](#_Toc207193578)

[Riski- ja uhkalista 5](#_Toc207193579)

[Tietoturvariskien arviointi 5](#_Toc207193580)

[Tietoturvariskien käsittely 6](#_Toc207193581)

[Viestintä ja tiedonvaihto 7](#_Toc207193582)

[**Koulutus ja perehdyttäminen** 7](#_Toc207193583)

# **Tietoturvariskienhallinnan tavoitteet**

Tietoturvariskienhallinnan kautta tavoitteena on tunnistaa ja hallita tietoturvaan kohdistuvia heikkouksia ja epävarmuuksia sekä määrittää näiden pienentämiseksi tarvittavat toimenpiteet. Riskienhallinta tarkoittaa koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Se on systemaattista ja jatkuvaa toimintaa, jonka avulla tunnistetaan, arvioidaan, käsitellään ja seurataan riskejä. Säännöllisesti toteutettu tietoturvariskienhallinta parantaa vesihuoltolaitoksen toimintavarmuutta, tehokkuutta ja toiminnan yhdenmukaisuutta.

Tietoturvariskienhallinnan onnistumisen kannalta on tärkeää, että riskienhallintatyöhön osallistuvat päätöksentekijät, asiantuntijat ja sisäiset sekä tarvittaessa ulkoiset sidosryhmät. Toimiva ja läpinäkyvä riskienhallinta korostuu erityisesti muutoksissa, joissa kehitetään uusia toimintamalleja ja luovutaan vanhoista.

Riskienhallinta kattaa myös yhteistyökumppaneiden toiminnan. Palveluntuottajien riskienhallinnan järjestelyjen riittävä taso tulee varmistaa sopimuksilla.

# **Tietoturvariskienhallinnan vastuut**

Tietoturvapolitiikasta määritettyjä rooleja, käytetään myös tietoturvariskienhallinnassa.

Operatiivinen johto vastaa siitä, että heidän vastuullaan olevien toimintojen ja järjestelmien tietoturvariskit on arvioitu ja hallittu riittävässä laajuudessa vesihuoltolaitoksen riskienhallintaprosessin mukaisesti sekä siitä, että tunnistettuja riskejä koskeville hallintatoimille on määritelty vastuuhenkilöt ja aikataulu. Yksikön päälliköt ovat riskin omistajia, joilla on vastuu on vastuu tietoturvariskienhallinnan toteutumisesta.

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.

Vesihuoltolaitoksen ylin johto vastaa liikelaitoksen riskienhallinnan järjestämisestä koko organisaation tasolla ja vastaa riskienhallinnan toimeenpanosta ja tuloksellisuudesta sekä ohjaa tarvittaessa operatiivista.

Yhteistyökumppanien tietoturvariskien hallintaan liittyvät vastuut kirjataan sopimuksiin. Sopimusvastuiden noudattamista seurataan säännöllisesti, ja yhteistyökumppaneiden toimintaa auditoidaan tarvittaessa.

# Tietoturvariskienhallinnan prosessi

Tietoturvariskienhallinnan prosessi perustuu seuraaviin keskeisiin vaiheisiin alla olevan prosessikaavion mukaisesti:

* Toimintaympäristön määrittely
* Tietoturvariskien kartoitus
* Riskien arviointi
* Riskien käsittely
* Seuranta ja katselmointi



## Toimintaympäristön määritteleminen

Toimintaympäristöllä tarkoitetaan kokonaisuutta, jonka tietoturvariskejä käydään läpi. Tämä voi olla selkeästi rajattava järjestelmä, prosessi tai muu vesihuoltolaitoksen toiminto. Toimintaympäristön määrittelyn on tietoturvariskienhallinnassa keskeisessä osassa, sillä tässä määritellään mihin tietoturvariskien kartoitus, arviointi ja hallintakeinojen määrittely kohdistuu.

Kun toimintaympäristöä määritellään, on jokaisen toiminnon kohdalla tärkeää tunnistaa mistä järjestelmistä tämä muodostuu, että riskit varmana kohdistetaan ja arvioidaan oikein, sillä toiminto voi sisältää useita järjestelmiä sekä tällä voi olla useita rajapintoja esimerkiksi tietolähteinä, joita toiminto tarvitsee toimiakseen tai joidenka kautta järjestelmään voidaan vaikuttaa.

## Tietoturvariskien kartoitus

Kun vesihuoltolaitos tunnistaa tietoturvariskienkartoituksen kohteen, arvioidaan tämän hallinnollinen ja tekninen toteutus tietoturvariskien listauksen uhkia vasten, jossa tunnistetaan alustavasti mitenkä ja mitkä uhkat voivat toteutua järjestelmän osalta. Tarkastelussa tulee käydä ilmi, myös mitkä riskit eivät järjestelmään kohdistu, esimerkiksi jos järjestelmä ei sisällä tai tämä ei käsittele henkilötietoja, ei tietovuodon riski kohdistu tähän.

Tarkastelun jälkeen kaikki riskit, joidenka uhkat todettiin kohteen osalta mahdolliseksi kirjataan riskienhallintatyökaluun. Myös tietoturvariskit, jotka eivät järjestelmään kohdistu, kirjataan ylös, mutta näihin lisätään perustelu miksi riski ei kohdistu näihin sekä kirjauksen päivämäärä, jonka jälkeen riskit arkistoidaan.

### Riski- ja uhkalista

Vesihuoltolaitos käyttää riskien tunnistamisessa valmiiksi koottua tietoturvariskien listaa, jolla pyritään kattamaan kaikki uhkat menetelmä (eng. All hazards approach). Tietoturvariskien lista sisältää vesihuoltolaitoksen ennalta kokoaman riskilistauksen, jossa kuvataan mitkä uhkat riskissä käsitellään. Tietoturvan riskilistauksessa on myös kirjattuna vesihuoltolaitoksen soveltamat tietoturvan hallintakeinot.

Tietoturvariskien listaa päivitetään aina mikäli huomataan kartoittamaton hallintakeino tai tunnistamaton uhka, joka on jäänyt käsittelemättä, esimerkiksi tehdyn havainnon tai toteutuneen riskin myötä.

## Tietoturvariskien arviointi

Kun riskit ovat kirjattu riskienhallintatyökaluun aloitetaan näiden arviointi avainhenkilöiden kanssa.

Arvioinnissa on tarkoitus saada nykyhetken näkemys siitä kuinka todennäköisiä ja seurauksiltaan vakavia riskit, toteutettujen hallintakeinojen ja riskiarviointien mukaan, realisoituessaan olisivat järjestelmän luottamuksellisuudelle, eheydelle ja saatavuudelle. Luottamuksellisuudella tarkoitetaan järjestelmän tietojen suojausta siten, että vain tarkoituksenmukaiset tahot voivat näitä lukea ja käsitellä. Eheydellä tarkoitetaan, että tieto pysyy oikeana, ehjänä ja väärentämättömänä. Järjestelmän saatavuudella tarkoitetaan, että järjestelmä on käytettävissä eli kuinka jatkuvuusriskiin ollaan varauduttu.

Arviointia tehdessä on tärkeä huomioida, että todennäköisyys ja seuraus, jota tässä arvioidaan kohdistuu nimenomaan kohdejärjestelmään ja tämän tuottamaan toimintoon tai prosessiin. Vaikutus ja riski vesihuoltolaitoksen kokonaisvaltaiseen toimintaan tulee tehdä kokonaisriskienarvioinnissa, jossa huomioidaan tietoturvariskien lisäksi muita toimintaan vaikuttavia uhkatekijöitä.

Arvioinnissa käytetään riskienhallintatyökaluun kirjattuja arviointikriteerejä:

***Todennäköisyys***

*1: Ei riskiä, teoreettisesti mahdollinen mutta ei tiedetä tapahtuneen
2: Epätodennäköinen, on tapahtunut joskus muualla mutta ei meillä
3: Mahdollinen, on tapahtunut joskus meillä tai muualla
4: Todennäköinen, on tapahtunut usein meillä tai muualla tai on ollut useita "läheltä piti" -tilanteita
5: Hyvin todennäköinen, tapahtuminen meillä lähes varma*

Riskin ja tämän sisältämien uhkien todennäköisyyttä arvioidessa on tärkeää arvioida mikä on riskin realisoitumisen todennäköisyys teknologisesta ja käytännön näkökulmasta, sekä sen perusteella ovatko jotkin riskin sisältämistä uhkista jo aiemmin tapahtuneet tai ollut lähellä tapahtua vesihuoltolaitoksella tai muualla.

***Seuraus***

*1: Ei seurauksia, ei merkittäviä vaikutuksia
2: Häiriöitä toiminnalle, Lyhyt käyttökatko, pieni vahinko tai pieniä taloudellisia menetyksiä
3: Toiminnan häiriö toiminnassa, Toimintaan selkeitä vaikutuksia tai pidempi käyttökatko, taloudelliset menetykset kohtuullisia
4: Toiminnan huomattava vaikeutuminen, Merkittäviä vaikutuksia toimintaan, toiminnan palautus on vaikeaa, merkittäviä taloudellisia menetyksiä
5: Toiminnan lamaantuminen, riskistä täysin palautuminen on todella haastavaa tai mahdotonta, todella merkittäviä taloudellisia menetyksiä*

Kun riskin ja tämän sisältämien uhkien seurauksia arvioidaan tulee tätä katselmoida järjestelmälle aiheutuvan häiriön vaikuttavuuden, järjestelmän kehityksen ja ylläpidettävyyden tavoitteiden sekä riskin seurausten ja näistä palautumisesta koituvien taloudellisten menetysten näkökulmasta.

Riskit ja näiden käsittely priorisoituvat sen perusteella, kuinka todennäköisiä nämä ovat ja kuinka näiden toteutuminen vaikuttaisi järjestelmien toiminnallisuuteen. Riskien käsittelyn priorisoinnista vastaa loppukädessä järjestelmän omistaja yhteistyössä muiden toimijoiden kanssa ja viimekädessä ylin johto.

## Tietoturvariskien käsittely

Tietoturvariskejä hallitaan viidellä eri keinolla, joista keskeisin on riskien pienentäminen hallintakeinoilla. Kaikki tietoturvariskien käsittelytavat ovat seuraavat:

* Pienentäminen
	+ Mikäli tietoturvariski arvioidaan toimintavarmuuden kannalta korkeaksi voidaan tätä pyrkiä pienentämään hallintakeinoilla.
* Hyväksyminen
	+ Jos tietoturvariskin arvioidaan olevan tasolla, joka on järjestelmän toiminnan kannalta hyväksyttävällä tasolla, voidaan tämä päättää hyväksyä. Riski voidaan myös hyväksyä, jos tämän pienentämiseen ei ole käytössä hallintakeinoja tai hallintakeinot vaativat liian korkeita investointeja.
* Siirtäminen
	+ Tietoturvariskien siirtäminen ei ole lähtökohtaisesti käytettävä riskienhallinnan vaihtoehto, johtuen vesihuoltolaitoksen tuottamien yhteiskunnan kannalta kriittisten palveluiden keskeisyydestä. Vaikka esimerkiksi vakuutus korvaisi taloudelliset vahingot, on lakivelvoitteinen vastuu silti lähtökohtaisesti vesihuoltolaitoksella.
* Välttäminen
	+ Tietoturvariskejä ei pystytä täysin välttämään, mutta välttämisen avulla arvioitua riskitasoa voidaan madaltaa. Esimerkiksi jättämällä turvaton järjestelmän kehitysprojekti toteuttamatta tai ohjelma asentamatta, koska tämä nostaisi riskitasoa liian korkealle tai jokin järjestelmään liittyvä riskialtis toiminto lopetetaan.
* Poistaminen
	+ Riskien poistaminen on todella harvinainen riskin käsittelykeino, joka on usein mahdollista vain kun kyseinen järjestelmä, toiminto tai prosessi lakkautetaan täysin tai jokin, mahdollisesti turha, tieto poistetaan järjestelmästä.

Tietoturvariskien käsittelyssä on tärkeää pyrkiä oikeasuhtaiseen sekä perusteltuun toimintatapaan, sillä näiden käsittely on keskeinen osa koko vesihuoltolaitoksen tietoturvan kehitystä ja ylläpitoa. Lähtökohtaisesti kaikkia järjestelmän toimintavarmuutta vakavasti uhkaaviin riskeihin tulee reagoida näitä pienentämällä ja riskien hyväksymistä ja välttämistä tulisi käyttää ainoastaan tarkkaan harkituissa tilanteissa.

## Viestintä ja tiedonvaihto

Tietoturvariskien hallinta ja erityisesti arviointi edellyttää toimintaympäristöön ja riskeihin liittyvien eri osapuolten välistä viestintää. Viestinnän ansiosta tieto riskeistä tavoittaa ne, joiden tulee olla niistä tietoisia, ja riskienhallinnassa ja riskien käsittelyssä tarvittavaa tietoa saadaan jaettua toimenpiteistä ja valvonnasta vastuullisten kesken.

Riskienhallinnan viestintään sisältyvät kaikki oleelliset riskit ja käsittelytoimet. Tähän kuuluu myös riittävä tiedonvaihto yhteiskumppaneiden ja sidosryhmien välillä.

# **Koulutus ja perehdyttäminen**

Perustason käyttäjille pidetään riskienhallinnasta perustason koulutus. Tietoturvariskienhallinnassa mukana oleville tahoille tulee järjestää yksityiskohtainen koulutus tähän liittyvistä toimintatavoista ja prosesseista. Muille sidosryhmille osapuolille koulutuksen tarvetta tarkastellaan tapauskohtaisesti.

Tietoturvariskien arvioinnin ja riskienkäsittelysuunnitelman sisältö kuuluu työntekijöiden perehdytykseen.