

**Tietoturvapoikkeamaprosessi**

**Muutoshistoria**

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

Sisällysluettelo

[Tietoturvapoikkeamaprosessin ja tietoturvapoikkeaman määritelmä 3](#_Toc207877136)

[Roolit ja vastuut 3](#_Toc207877137)

[Ratkaisuryhmä 3](#_Toc207877138)

[Johtaja 4](#_Toc207877139)

[Järjestelmän omistaja ja pääkäyttäjä 4](#_Toc207877140)

[Viestintä 4](#_Toc207877141)

[Järjestelmätoimittaja 4](#_Toc207877142)

[Johdon edustaja 5](#_Toc207877143)

[Tietoturvapoikkeamaprosessin vaiheet 5](#_Toc207877144)

[Havainnointi 6](#_Toc207877145)

[Ratkaisu 7](#_Toc207877146)

[Viestittävät tahot ja sidosryhmät 9](#_Toc207877147)

[NIS ilmoitus 9](#_Toc207877148)

[Kyberturvallisuuskeskus 9](#_Toc207877149)

[Tietosuojavaltuutettu 9](#_Toc207877150)

[Poliisi 10](#_Toc207877151)

[Kehitys 10](#_Toc207877152)

# Tietoturvapoikkeamaprosessin ja tietoturvapoikkeaman määritelmä

Tietoturvapoikkeamaprosessi on tarkoitettu vesihuoltolaitoksen sisäisen tietoturvatyöskentelyn avuksi kuvaamaan kuinka vesihuoltolaitoksessa tietoturvapoikkeamia havaitaan ja ratkaistaan. Tietoturvapoikkeamalla tarkoitetaan tietoturvaan liittyvä tilannetta tai tapahtumaa, joka uhkaa, vaarantaa tai heikentää vesihuoltolaitoksen toimintavarmuutta tai toiminnan jatkuvuutta.

Tietoturvapoikkeama voi sisältää useita eri tilanteita ja tapahtumia, jotka voivat olla luonteeltaan aktiivisia tai passiivisia. Passiiviset tietoturvapoikkeamat ovat havaintoja, jotka merkittävästi nostavat tietoturvan uhkatasoa, kuten vakava haavoittuvaisuus, tietoturvapolitiikan tai tämän linjausten rikkominen, ennakkoon saatu uhkatieto, tietoturvapolitiikasta tai tietoturvalinjauksista poikkeaminen. Aktiivisessa tietoturvapoikkeamassa on taas kyse tilanteesta, joka suoraan joko uhkaa tai haittaa vesihuoltolaitoksen toiminnan jatkuvuutta. Näitä ovat esimerkiksi, tietomurto omaan tai yhteistyökumppanin järjestelmään, tahallinen tai tahaton tietojen vuotaminen, haittaohjelman leviäminen tai aktiivinen kyberhyökkäys.

# Roolit ja vastuut

Tietoturvapoikkeamat ovat aina kriittisiä ja ohittavat prioriteetiltaan kaikki muut ratkaisuvaiheeseen osallistuvien vesihuoltolaitoksen työntekijöiden työtehtävät ja nämä käsitellään aina välittömästi prosessin mukaisesti.

## Ratkaisuryhmä

Tietoturvapoikkeaman havainneen tahon ensisijainen tehtävä on muodostaa ratkaisuryhmä. Ryhmälle muodostetaan oma Teams keskustelu ja jokaista ryhmään kutsuttua henkilöä pyydetään vastaamaan viestillä, että tämä on saanut ja nähnyt viestin tapahtuneesta poikkeamasta. Mikäli Teams alusta ei ole käytettävissä käytetään puheluja ja tekstiviestejä korvaamaan alusta, kunnes tämä on jälleen käytettävissä. Ratkaisuryhmän vastuulla on tehdä tarvittaessa ensisijaiset lain velvoittamat ilmoitukset 24 tunnin sisällä sidosryhmille, jotka ovat kyberturvallisuuskeskus, henkilötietojen vaarantuessa tietosuojavaltuutettu ja vesihuollon toimintojen vaarantuessa NIS-ilmoitus.

Ratkaisuvaihe toteutetaan yhteistyössä, järjestelmätoimittajan, järjestelmän omistajien sekä pääkäyttäjien kanssa.

Ratkaisuryhmän tulee sisältää seuraavat roolit:

### Johtaja

Ratkaisuryhmän johtaja on toimii ryhmän puheenjohtajana, joka vastaa, että ryhmässä on asianmukaiset henkilöt ja ratkaisuun osallistuvilla henkilöillä on riittävät tieto ja ohjeistukset suoriutuakseen ratkaisusuunnitelman vaatimista tehtävistä. Ryhmän johtajalla on myös velvollisuus ilmoittaa tietoturvapoikkeamasta vesihuoltolaitoksen johdolle viestiä lain velvoittamille sidosryhmille 24 tunnin sisällä vesihuoltolaitoksen saatua tietoturvapoikkeama tietoonsa. Ryhmän johtajan vastuulla on tietoturvapoikkeaman kirjausten tekeminen.

### Järjestelmän omistaja ja pääkäyttäjä

Järjestelmän omistaja vastaa toimittajayhteistyöstä, vesihuoltolaitoksen toimintojen, joihin poikkeama vaikuttaa, sijaistoiminnoista ja operatiiviseen toimintaan kohdistuviin haasteisiin reagoimisesta. Järjestelmän pääkäyttäjä toimii ratkaisuryhmän tukena ja järjestelmän käytön asiantuntijana. Pääkäyttäjien vastuulla on myös tuoda esiin henkilöt ja ulkoiset sekä sisäiset tahot keihin poikkeama vaikuttaa ja viestiä poikkeaman aiheuttamista häiriöistä näille.

### Viestintä

Tietoturvapoikkeamista viestiminen vaatii usein aikaa, työtä ja viestinnän ammattitaitoa. Vesihuoltolaitoksen toimintavarmuuden kannalta on tarkoituksenmukaisempaa, että poikkeaman kohteena olevan järjestelmän asiantuntijat pystyvät keskittymään ratkaisun toteuttamiseen ja tilanteen johtamiseen, minkä vuoksi tulee ryhmässä tulee olla mukana viestintään keskittynyt henkilö. Viestijän vastuulla on varmistaa, että tarvittava tieto poikkeaman vaikutuksista saavuttaa vesihuoltolaitoksen sisäiset sidosryhmät sekä vastata julkisesta tiedottamisesta esimerkiksi verkkosivuilla. Viestijä kuitenkin tarvitsee tehtävistään suoriutumiseen ratkaisuryhmältä tiedon siitä mitä on tapahtunut, miten tämä vaikuttaa ja näkyy vesihuoltolaitoksen toiminnassa sekä kuinka tilanteen odotetaan etenevän, jonka vuoksi viestijä on hyvä kutsua mahdollisimman pian mukaan ratkaisuryhmään vaikka tapaus ei lopulta vaatisikaan viestintää.

### Järjestelmätoimittaja

Ratkaisuryhmän vastuulla on kartoittaa järjestelmätoimittajan kanssa ratkaisusuunnitelma ja toteuttaa omalta osalta ratkaisuun tarvittavat toimenpiteet.

Järjestelmätoimittajat usein tietävät järjestelmän teknisen toteutuksen paremmin kuin vesihuoltolaitoksen oma henkilöstö sekä vastaavat tämän ylläpidosta, muutoksista ja kehittämisestä. Poikkeaman kohteesta riippuen ratkaisuryhmään voi olla tarpeellista kutsua useampi järjestelmätoimittaja.

Ratkaisuryhmän pakollisten roolien lisäksi poikkeaman luonteesta, laajuudesta ja vakavuudesta riippuen ratkaisuryhmään voidaan kutsua lisäksi turvallisuudesta vastaavia tahoja sisäisistä ja ulkoisista sidosryhmistä. Tämä taho voi olla esimerkiksi:

### Johdon edustaja

Mikäli tietoturvapoikkeamalla on näkyviä tai laajamittaisia vaikutuksia vesihuoltolaitoksen toimintaan tulee ratkaisuryhmään kutsua mukaan vesihuoltolaitoksen johdon edustaja.

Johdon edustajan tehtävänä on ylläpitää tilannekuvaa sekä tarvittaessa päättää laajasti vesihuoltolaitoksen toimintaan vaikuttavien ratkaisutoimien toteuttamisesta.

Vesihuoltolaitoksen koko johtoryhmälle raportoidaan joka tapauksessa kaikista tapahtuneista tietoturvapoikkeamista säännöllisesti.

# Tietoturvapoikkeamaprosessin vaiheet

Tietoturvapoikkeamaprosessi on jatkuvasti käynnissä oleva prosessi, joka pitää sisällään kolme eri vaihetta: havainnointi, Ratkaisu ja Kehitys.

## Havainnointi

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, diagrammi

Tekoälyllä luotu sisältö voi olla virheellistä.

Havainnointi on prosessin vaihe, joka toteutuu pääasiassa automatisoiduilla valvontatyökaluilla sekä vesihuoltolaitoksen työntekijöiden ja sidosryhmien tietoturvaa koskevien havaintojen sekä ilmoituksien avulla. Tietoturvapoikkeamien havainnointiin liittyvien toimintojen sekä työkalujen tehokkuutta arvioidaan sekä kehitetään säännöllisesti vuosittain sekä jokaisen tietoturvapoikkeaman käsittelyn jälkeen.

Kaikki havainnot tutkitaan, jolloin arvioidaan havaintojen kriittisyys, potentiaalinen vakavuus sekä ovatko nämä virheellisiä vai todellisia havaintoja (eng. False Positive ja True Positive). Havainnot määritellään virheellisiksi, mikäli paljastuu, etteivät nämä ole tietoturvapoikkeamia, vaan esimerkiksi käyttäjä on yrittänyt kirjautua vahingossa liian useasti väärällä salasanalla, jolloin tästä muodostuu virheellinen havainto. Mikäli havaintojen perusteella todetaan kyseessä olevan tietoturvapoikkeama on kyseessä todellinen havainto, jolloin prosessissa siirrytään ratkaisuvaiheeseen. Havainnointivaihetta, ei kuitenkaan koskaan päätetä, vaan tämä jatkuu edelleen poikkeaman kehittymisen ja muiden mahdollisten poikkeamien havaitsemisen varalta.

## Ratkaisu

Kuva, joka sisältää kohteen teksti, kuvakaappaus, diagrammi, viiva

Tekoälyllä luotu sisältö voi olla virheellistä.

Tietoturvapoikkeaman ratkaisu on prosessin aktiivinen vaihe, jonka aikana tietoturvapoikkeama käsitellään ja tälle luodaan ratkaisusuunnitelma poikkeaman korjaamiseksi.

Ratkaisuryhmän ensisijaisena tehtävänä on muodostaa ja panna toimeen ratkaisusuunnitelma, jolla poikkeama saadaan hallintaan ja lopulta ratkaistua. Mikäli ratkaisu vaatii vesihuoltolaitoksen toiminnan rajoittamista tai pysäyttämistä, joillain operatiivisilla osa-alueilla tulee järjestelmän omistajien sekä johtajien olla tietoisia näistä toimista, joilta ensisijassa pyritään hakemaan lupa toiminnan rajoittamiselle. Mikäli päätöstä ei kuitenkaan saada tarpeeksi nopealla vasteella, ratkaisuryhmän vesihuoltolaitoksen edustajilla on oikeus antaa lupa ja toteuttaa ensisijaiset toimet itsenäisesti, mikäli näiden voidaan arvioida merkittävästi vähentävän poikkeamasta koituvia vahinkoja.

Ratkaisusuunnitelman muodostamista varten tulee ratkaisuryhmän selvittää ja kirjata Teams keskusteluun seuraavat asiat:

* **Mitä on tapahtunut ja miten tietoturvapoikkeama vaikuttaa?**

Ensimmäisenä kaikkien ryhmän jäsenten tulee olla tietoisia siitä mitä ryhmä lähtee ratkaisemaan ja mitä vaikutuksia tällä on vesihuoltolaitoksen toimintaan.

* **Millä toimenpiteillä poikkeama saadaan hallintaan, mitä vaikutuksia toimenpiteillä on ja kenelle tästä viestitään?**

Seuraavaksi ryhmän tulee selvittää kuinka poikkeaman leviäminen, eskaloituminen ja uusiutuminen saadaan estettyä ja kuinka toimintaa johon poikkeama vaikuttaa jatketaan sekä keille vesihuoltolaitoksen sisäisille ja julkisille sidosryhmille poikkeaman vaikutuksista viestitään.

Poikkeaman hallintaan saamisella on usein joitain seurauksia tietoturvanpoikkeaman kohteena olevan järjestelmän ja tätä myötä vesihuoltolaitoksen toimintaan, joka tulee myös selvittää.

* **Miten poikkeama tullaan ratkaisemaan ja mitenkä ratkaisu tulee vaikuttamaan?**

Kun tietoturvapoikkeama on hallinnassa ja ryhmä on varmistunut, että tämä ei pysty enää leviämään tulee poikkeaman aiheuttaneet juurisyyt korjata, ettei tämä pääse enää uusiutumaan ja ettei poikkeamalla enää ole vaikutuksia vesihuoltolaitoksen toimintaan.

Poikkeama saattaa joissain tapauksissa tulla myös ratkaistuksi samalla kun tämän vaikutukset saadaan hallintaan.

Ratkaisussa oleva poikkeama todetaan ratkaistuksi vasta, kun poikkeaman aiheuttama uhka on käsitelty, haitalliset toimet torjuttu ja näistä koitunut vahinko toiminnalle on korjattu sekä varmistettu, että kaikki tunnistetut hallintakeinot ovat kartoitettu poikkeaman uusiutumisen ehkäisemiseksi.

Ratkaisuvaiheessa selvitetään aina poikkeamaan johtaneet tapahtumaketju ja juurisyyt. Kaikkia tapahtuvia tietoturvapoikkeamia ei kuitenkaan välttämättä aina saada täysin lopullisesti selvitettyä esimerkiksi todistusaineiston tai lokitietojen puutteellisuuden vuoksi. Myöskään kaikkien poikkeamien uusiutumista ei voida täysin estää, sillä esimerkiksi käyttäjävirheestä seuraavan virustartunnan tai tunnusten vuotamisen uusiutuminen on teoriassa aina mahdollista.

## Viestittävät tahot ja sidosryhmät

Yhteiskunnan kannalta kriittisenä toimijana vesihuoltolaitoksella lain edellyttämä velvollisuus ilmoittaa tietoturvaloukkauksista, jotka voivat vaarantaa vesihuollon toiminnan. Pääasiallinen vastuu ilmoitusten tekemisestä on ratkaisuryhmän johtajalla, mutta tämä voi myös ohjeistaa toisen ratkaisuryhmän jäsenen tekemään nämä, mutta vastuu ilmoitusten toteutumisesta on myös tällöin ratkaisuryhmän johtajalla.

### NIS ilmoitus

Vesihuoltolaitoksella on EU:n kyberturvallisuusdirektiivin kannalta yhteiskunnan kannalta keskeisenä tai tärkeänä toimijana lain määräämä velvollisuus tehdä merkittävistä aktiivisista tietoturvapoikkeamista 24 tunnin kuluessa ensi-ilmoitus ELY-Keskukselle, joka toimii vesihuoltolaitoksen valvovana viranomaisena. Ilmoituksen tulee sisältää poikkeamasta alustavat tiedot ja poikkeaman kohde sekä sen hetkisen ratkaisuryhmän johtajan yhteystiedot. Ensi-ilmoituksen jälkeen tulee poikkeamasta tehdä jatkoilmoitus viimeistään 72 tunnin kuluessa ja loppuraportti kuukauden kuluessa.

Ilmoitus vastuullinen: Ratkaisuryhmän johtaja  
Internetlomake: <https://eservices.traficom.fi/ContactForms/form/NIS2-Ilmoitus?langid=fi>

### Kyberturvallisuuskeskus

Mahdollisen tuen saamiseksi ja viranomaisviestinnän avaamiseksi tulee tietoturvapoikkeamasta tehdä ilmoitus kyberturvallisuuskeskukselle internetlomakkeella ja täydentävästi sähköpostilla.

Ilmoitus vastuullinen: Ratkaisuryhmän johtaja  
Sähköposti: [cert@traficom.fi](mailto:cert@traficom.fi)   
Internetlomake: <https://www.kyberturvallisuuskeskus.fi/fi/ilmoita>

### Tietosuojavaltuutettu

Mikäli tietoturvapoikkeama vaarantaa tai tämän seurauksena on mahdollisesti päässyt paljastumaan henkilötietoja, tulee tästä ilmoittaa 72 tunnin kuluessa tietosuojavaltuutetulle. Tietosuojavaltuutetulle internetlomakkeella ilmoittamisesta vesihuoltolaitoksessa vastaa ratkaisuryhmän johtaja.

Ilmoitus vastuullinen: Ratkaisuryhmän johtaja   
Sähköposti:   
Internetlomake: <https://turvaviesti.om.fi/ilmoitus-tietoturvaloukkauksesta>

### Poliisi

Tietoturvapoikkeamista tulee viimeistään ratkaisusuunnitelman täytäntöönpanon jälkeen tehdä rikosilmoitus poliisille. Rikosilmoituksen voi tehdä ratkaisuryhmän johtaja tai toimitusjohtaja.

Ilmoitus vastuullinen: Ratkaisuryhmän johtaja tai toimitusjohtaja  
Sähköposti:   
Internetlomake: <https://asiointi.poliisi.fi/yritys/rikos>

## Kehitys

Kuva, joka sisältää kohteen teksti, kuvakaappaus, käyntikortti, diagrammi

Kuvaus luotu automaattisesti

Poikkeamaprosessin kehitysvaihe on osa organisaation sisällä tapahtuvaa jatkuvaa toimintaa, jonka ensisijainen tarkoitus on parantaa vesihuoltolaitoksen toimintavarmuutta varautumalla tietoturvapoikkeamiin ja ennaltaehkäisemällä näitä sekä pyrkiä estämään näiden uusiutuminen. Poikkeamaprosessin kehitysvaiheeseen liittyvää toimintaa toteutetaan myös ennakoivasti säännöllisesti tietoturvan kokonaisvaltaisen kehittämisen yhteydessä.

Jos tietoturvapoikkeaman ratkaisun yhteydessä havaitaan tietoturvaan liittyviä teknisiä tai toiminnallisia puutteita, käsitellään nämä ratkaisuvaiheen jälkeen prosessin kehitysvaiheessa, jossa kartoitetaan uusia ja arvioidaan olemassa olevia tietoturvan hallintakeinoja. Järjestelmän omistajan vastuulla on käydä kartoitetut hallintakeinot läpi. Järjestelmän omistajan vastuulla on myös varmistaa, että hallintakeinot siirtyvät toteutukseen järjestelmän pääkäyttäjille ja järjestelmätoimittajille. Vastuu järjestelmään tai toimintatapoihin tehtävien toimenpiteiden ja hallintakeinojen toteuttamisesta kuuluu järjestelmän omistajalle, mutta lopullinen vastuu havaittujen hallintakeinojen toteutumisesta ja näiden toteuttamisen päättämisestä on vesihuoltolaitoksen johdolla.