YLIVIESKAN KAUPUNGIN TIETOTURVA- JA TIETOSUOJAPOLITIIKKA 2023–2027

Kaupunginhallitus 22.1.2024 § xxx

YLIVIESKA
kasvun ihmeitä

YLIVIESKA

Sisällys

Ylivieskan kaupungin tietoturva- ja tietosuojapolitiikka

Johdanto

Tämä tietoturva- ja tietosuojapolitikkaa kuvaa ne Ylivieskan kaupungin tietoturvallisuuden ja tietosuojan tavoitteet, vastuut ja toteuttamiskeinot, jotka Ylivieskan kaupungin johto on hyväksynyt. Johto sitoutuu noudattamaan tietoturvaan ja tietosuojaan liittyvää lainsäädäntöä ja uusimpia viranomaisvaatimuksia. Ylivieskan kaupunki ottaa tietoturvan huomioon kaikessa toiminnassaan ja edellyttää samaa myös henkilökunnaltaan ja sidosryhmiltään.

Tietoturvan ensisijainen tarkoitus on varmistaa tietojen asianmukainen ja luotettava käsittely organisaatiossa. Päivittäisessä työssä tämä tarkoittaa pääasiassa sitä, että tietoja voivat käyttää ainoastaan niitä virka- ja työtehtävissään tarvitsevat henkilöt. Järjestelmähankintoja ja käyttöönottoja suunniteltaessa otetaan huomioon järjestelmille asetettavat käytettävyys-, tietosuoja- ja tietoturvavaatimukset kaupungin hankintaohjeen ja -prosessien mukaisesti.

Tämä tietoturva- ja tietosuojapolitiikka on julkinen asiakirja. Johto sitoutuu parantamaan tietoturvaa ja tietosuojaa jatkuvasti ja asettaa vuosittain tietoturvan ja tietosuojan kehittämistavoitteet. Mahdolliset tietoturva- ja tietosuojapolitiikkaan liittyvät huomautukset ja kehittämiskohteet pyydetään toimittamaan tietoturvapäällikölle ja tietosuojavastaavalle.

1. Tietoturva- ja tietosuojapolitiikan tavoitteet

1.1. Tietoturvallisuuden käsite ja merkitys

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä tunnistettavuudesta eli pääsynvalvonnasta sekä kiistämättömyydestä. Tietoturvatoimet koskevat tiedon käsittelyä, kuten tallennusta, luovutusta ja siirtoa.

Tietoturvatoimilla suojataan manuaaliset ja automaattiset tietojärjestelmät ja niiden toiminta ja sisältö. Päämääränä on turvata Ylivieskan kaupungin keskeytymätön ja luotettava toiminta. Tietoturvan osalta tätä päämäärää tavoitellaan siten, että estetään tietojen ja tietojärjestelmien valtuudeton käyttö sekä tiedon tahaton tai tahallinen tuhoaminen ja vääristyminen. Ylivieskan kaupungin kriittiset tiedot, tietojenkäsittelyjärjestelmät ja palvelut pidetään asianmukaisesti suojattuna sekä normaali- että poikkeustilanteissa. Luettelo kriittisistä kohteista ja niiden suojauksista on salassa pidettävä. Uhka- ja poikkeustilanteisiin varaudutaan etukäteen riskianalyysillä ja toipumissuunnitelmalla, jotta mahdolliset vahingot saadaan minimoitua.

1.2. Tavoitteet

Tavoitteena on turvata tietojenkäsittelyn turvallisuus siten, että sekä Ylivieskan kaupungin henkilökunta että sidosryhmät voivat luottaa tietojenkäsittelyn asianmukaisuuteen ja että koko henkilökunta on sitoutunut huolehtimaan omalta osaltaan turvallisuudesta. Samalla turvataan ensisijaisen toiminnan mahdollisimman sujuva ja häiriötön toiminta.

Näiden päämäärien saavuttamiseksi:
Kaikkien tietoa käsittelevien henkilöiden on ymmärrettävä tietojenkäsittelyn periaatteet: mitä tietoa saa käsitellä, missä tarkoituksessa tietoa saa käsitellä ja milloin tietoa saa käsitellä.
Organisaation kaikkien työntekijöiden tietoturvatietoisuus on oltava riittävä. Kaikki ymmärtävät oman merkityksensä sekä tehtävänsä ja velvollisuutensa

tietoturvallisuuden ylläpidossa.

Tietoturvaa toteutetaan kaikilla tasoilla siten, että tietoturva on mukana kaikessa toiminnassa. Tällä toimintatavalla varmistetaan tietoturvallisen työkulttuurin toteutuminen.
Tietojen luottamuksellisuuden, eheyden ja saatavuuden vaatimus toteutuu kaikessa tietojenkäsittelyssä ja se mahdollistaa tietoturvallisen asioinnin ja tietojen käytön.

Tietoturvallisuuden vaatimukset otetaan huomioon kaikessa kehittämistoiminnassa sekä hankinnoissa. Tietoturvallinen toimintatapa on mukana jokapäiväisessä toiminnassa sekä toimintaprosesseissa ja tietojärjestelmissä niin, että helpoin ja luontevin tapa tehdä jokin asia on myös tietoturvallisuuden kannalta paras. Tietoturvallisuuteen sekä tietosuojaan liittyvissä kysymyksissä voi kääntyä tietosuoja- ja tietoturvavastaavien puoleen.

1.3. Tietosuoja

Tietosuojalla turvataan henkilötietojen käsittelyä. Se on perusoikeus, joka turvaa henkilön oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Vaatimukset tietosuojan toteuttamiselle tulevat yleisestä EU:n tietosuoja-asetuksesta. Tietosuoja-asetuksen tavoitteena on turvata henkilötietojen käsittelyn läpinäkyvyys ja oikeasuhtaisuus sekä varmistaa rekisteröityjen oikeudet ja tietosuojan toteutuminen.
Kansallinen lainsäädäntö ja EU:n tietosuoja-asetus velvoittavat rekisterinpitäjän suunnittelemaan henkilötietojen käsittelyn ja osoittamaan käsittelyn lainmukaisuuden. Rekisterinpitäjän on suojattava rekisteröidyn tiedot asiattomalta käsittelyltä. Suojaustoimet on ulotettava kaikkeen tiedon käsittelyyn, siirtoon ja säilytykseen tallennusmuodosta riippumatta.
Tietosuojan toteutumista seurataan aktiivisesti ja kaikkeen asiattomaan käyttöön puututaan. Jokaisen työntekijän on ilmoitettava esimiehelleen havaitsemistaan tietosuojaan liittyvistä ongelmista.

Tietojen oikeudettoman käytön seurauksena saattaa olla työnantajan antama huomautus, varoitus tai oikeudellisia seurauksia teon vakavuuden mukaan.

1.4. Henkilötietojen käsittely

Henkilötietoja käsittelevät Ylivieskan virkamiehet ja työntekijät, joiden virka- tai työtehtäviin ko. henkilötietojen käsittely kuuluu. Henkilötietoja voivat käsitellä myös esim. sopimuskumppanit tai järjestelmien ylläpitäjät, siinä laajuudessa kuin se on tarpeen käsittelyn tarkoituksen kannalta henkilötietojen käsittelyä koskevan sopimuksen perusteella.

Käsittelytoimet suunnitellaan ja määritellään tiedon elinkaari huomioiden. Henkilötietojen käyttö on sallittua vain lainsäädännön nojalla tai henkilön suostumuksen perusteella. Tietojen säilytys ja käyttö tapahtuu tietoturvaperiaatteita noudattaen.

Henkilötietojen tulee säilyä virheettöminä ja niiden tulee olla saatavilla tarpeen mukaisesti. Henkilötietoihin pääsy on rajattu työtehtävän mukaiseksi. Mikäli henkilötietoja luovutetaan, tulee siirron olla tietoturvallinen ja perustua lakiin tai suostumukseen. Tietoja voidaan luovuttaa lakien ja asetusten nojalla tai rekisteröidyn suostumuksella.

2. Tietoturvan ja tietosuojan organisointi ja vastuut

Tietoturvan ja tietosuojan vastuiden ylätasot kuvataan tässä tietoturvapolitiikassa. Tarkemmat vastuiden kuvaukset ja sisällöt löytyvät "Tietoturvavastuut" dokumentista.

2.1. Organisaatio

Tietoturvallisuus on osa Ylivieskan kaupungin kokonaisturvallisuutta ja tietoturvan eri osa-alueille määritellään vastuuhenkilöt. Tietoturvallisuusorganisaation keskeisimmät toimijat ja roolit sekä heidän vastuunsa ja velvollisuutensa on kerrottu erillisessä Ylivieskan kaupungin tietoturvavastuu-dokumentissa. Luettelon vastuuhenkilöistä voi pyytää kirjaamosta.

2.2. Johdon vastuut

Kaupungin johto on vastuussa tietoturvan linjauksista ja johtamisesta. Se määrittelee tietoturvan tavoitetason ja ne hyödyt, joita tieto-omaisuuden turvaavalla toiminnalla saavutetaan. Kaupunginhallitus nimeää ne vastuuhenkilöt, joiden tehtävänä on toteuttaa turvallisuusjohtamiseen liittyviä tehtäviä. Johto hyväksyy ulkopuoliset palvelutahot, mikäli tietoturvatyössä tarvitaan ulkoisia asiantuntijoita ja ammattilaisia. Johto on vastuussa siitä, että kaikki kaupungin työntekijät ovat tietoisia kaupungin tietoturva- ja tietosuojapolitiikasta ja periaatteista. Johto on vastuussa myös siitä, että tietoturvavastuut ovat sidosryhmien tiedossa ja tietoturvaohjeita noudatetaan siten, että myös asiakkaiden ja yhteistyökumppaneiden tietoturva ei vaarannu. Johdon tehtävä on integroida tietoturvallisuus osaksi organisaation johtamisjärjestelmää siten, että tietoturva otetaan huomioon kaikessa toiminnassa.

2.3. Tietoturvaorganisaatio

Ylivieskan kaupungin tietoturvaorganisaatioon kuuluvat tietoturva- ja tietosuojaryhmä, tietoturvapäällikkö, tietosuojavastaava ja toimialojen tietoturvavastaavat.

Tietoturvapäällikkö toimii tietoturva- ja tietosuojaryhmän puheenjohtajana ja

ryhmä valitsee keskuudestaan sihteerin. Tietoturva- ja tietosuojaryhmä kokoontuu vähintään neljä kertaa vuodessa ja tarvittaessa useammin.
Tietoturva- ja tietosuojaryhmä vastaa kaupungin keskeisten toimintojen tietoturvan ja tietosuojan kehittämisestä, tietoturva- ja tietosuojatyön koordinoinnista ja toimenpiteistä tietoturva- ja tietosuojaloukkauksien osalta.

2.4. Työntekijöiden vastuut

Jokaisella kaupungin työntekijällä on vastuu toimia siten, että kaupungin tietoturva säilyy loukkaamattomana. Jokainen työntekijä on velvollinen raportoimaan havaituista poikkeamatilanteista esimiehelleen, joka vie asian eteenpäin tietoturvapäällikölle ja tietosuojavastaavalle. Myös työtehtävissä havaitut tietoturvallisuuteen liittyvät puutteet raportoidaan.

2.5. Organisaation yhteistyökumppaneiden vastuut

Sidosryhmät ja yhteistyökumppanit sitoutuvat omalta osaltaan turvalliseen tiedonkäsittelyyn asioidessaan Ylivieskan kaupungin kanssa. Tilaajaan velvollisuus on huolehtia, että kaikkiin tarjouspyyntöihin ja palvelusopimuksiin sisällytetään tietohallinnon ylläpitämät yleiset tietoturvavaatimukset täydennettynä kyseisen palvelun erityisvaatimuksilla sekä häiriötilanteiden toimintamallit ja selkeä vastuunjako läpi koko palveluketjun. Tietotekniikan käyttöohjeiden ja tietoturva- ja tietosuojapolitiikan noudattamisesta tehdään tarvittaessa kirjallinen sopimus.

3. Tietoturvallisuuden laajuus ja periaatteet

3.1. Tietoturvan perustason määrittely

Perustasolla häiriöitä voivat aiheuttaa mm. ihmisten huolimattomuus, tahallisen ilkivallan tekijät, järjestäytyneet rikolliset, laiteviat, onnettomuudet, valtiolliset toimijat tai luonnonmullistukset. Tietoturvaa hallitaan arvioimalla näiden riskien esiintymisen todennäköisyyttä ja tiheyttä ja valitsemalla sopivia menetelmiä, joilla tietoturvauhkia voidaan hallita.

Tietoturvasuunnitelmia pidetään yllä ja suunnitelmiin liittyviä käytäntöjä harjoitellaan, jotta niistä tulee osa organisaation toimintaa.
Jatkuvuussuunnitelmia tulee kehittää ja toteuttaa käytännössä, jotta voidaan varmistua siitä, että toimintaprosessit saadaan palautettua toimintaan vaaditussa ajassa.

Ylivieskan kaupunki osallistuu tietoturvan perustason määrittämiseen kansallisilla ja alueellisilla yhteistyöalustoilla. Yhteistyöllä varmistamme tietoturvallisuuteen liittyvien hyvien käytänteiden käyttöönoton ja läpiviennin.

3.2. Tietoturvan periaatteet

Hallinnollista tietoturvaa toteutetaan luomalla periaatteet kaupungin tietoturvatyölle. Johto arvioi riskit ja luo puitteet tietoturvan hallinnan muiden osa-alueiden menettelytavoille. Hallinnollisen tietoturvan toimenpiteitä ovat resurssien nimeämiset, vastuiden jakamiset, salassapito- ja turvallisuussopimusten tekeminen. Tietoturvallinen ajattelutapa pyritään sisällyttämään kaupungin jokapäiväisiin toimiin.

Henkilöturvallisuus pyritään pitämään korkealla tasolla valitsemalla oikeat henkilöt työtehtäviin, perehdyttämällä ja kouluttamalla henkilöt toimimaan oikein prosessien mukaan sekä noudattamalla sovittuja menettelyjä irtisanomistilanteissa. Näitä periaatteita sovelletaan sekä vakituisiin että tilapäisiin

työntekijöihin.

Tietotekniikan käyttöympäristö laitteineen ja tiedonsiirtovälineineen suojataan fyysisin turvallisuustoimenpitein. Kiinteistöt, toimitilat, laitteet ja tietovarastot suojataan asiaankuulumattomilta henkilöiltä sekä erilaisilta vahingoilta ja onnettomuuksilta. Jotta toiminnan jatkuminen voidaan taata ajan kuluessa, riskien havaitsemiseen ja vähentämiseen tähtääviä toimenpiteitä kehitetään siten, että ne muodostuvat arkirutiineiksi.

Laitteistoturvallisuudessa otetaan huomioon laitteiden koko elinkaari, takuut, sopimukset ja tukipalvelut. Laitteistoturvallisuus taataan laitteiston suojauksella ja asianmukaisilla asennus-, ylläpito- ja poistotoimenpiteillä. Lisäksi laitteille määritellään omistaja ja laitteen turvaluokka sekä suunnitellaan laitteiden valvonta ja kapasiteetit.
Ohjelmistoturvallisuus taataan oikeanlaisilla ohjelmistoihin kohdistuvilla toimilla. Tähän kuuluvat ohjelmistojen päivitykset, pääsynvalvonta- ja lokimenettelyt sekä varmuuskopiot. Ohjelmistoja saa asentaa vain tietohallinnon luvalla. Tämä koskee erityisesti ilmaisohjelmia. Ohjelmistopäivitysten julkaisuja seurataan aktiivisesti ja päivitysten kriittisyys arvioidaan ennakolta, jos mahdollista. Kriittiset päivitykset asennetaan välittömästi viivytyksettä. Kriittisten komponenttien, palvelinten, työasemien, käyttöjärjestelmien sekä ohjelmistojen turvatoimet ja -päivitykset on kuvattu tietoturvasuunnitelmassa.

Tietoliikenneturvallisuus suojataan tarvittavilla toimenpiteillä siten, että tietojen siirto järjestelmästä toiseen on turvallista. Kriittiset viestit ja dokumentit välitetään luokitusten vaatimin salausmenettelyin. Viestinvälityksen tietosuojaa koskevat vaatimukset ja vastuut on määritelty kaupungin ja viestinvälitysoperaattorin välisissä sopimuksissa.

Tietoaineistoturvallisuutta pidetään yllä luokittelemalla tietoja niiden kriittisyyden perusteella ja antamalla käsittelyoikeudet luokittelujen perusteella sekä valvomalla tiedonkäsittelyä. Käyttöturvallisuutta parannetaan luomalla ja ylläpitämällä

turvalliset toimintaolosuhteet huolehtimalla käytön ja tekniikan toimivuuden valvonnasta, käyttöoikeuksista, sekä ohjelmistotuesta ja varmuus- ja suojakopioinnista sekä häiriöraportoinnista. Käyttöturvallisuus otetaan myös huomioon ylläpito-, huolto- ja kehittämistoimintoihin liittyvissä toimenpiteissä.

Tietoturvapoikkeamista, haitallisista ja toimintaa vaarantavista tapahtumista raportoidaan kaikilla tasoilla viivytyksettä poikkeamien hallintaprosessin mukaisesti.

Palveluja ulkoistettaessa huolehditaan Suomen ja EU:n lainsäädännön mukaisesta luottamuksellisen aineiston käsittelystä.

3.3. Tietoturvallisuuden toteutumista tukevia käytäntöjä

Ylivieskan kaupungin tietoturvallisuuden toteutumista varmistetaan käyttämällä seuraavia toimenpiteitä:

- Tietojen merkityksen arviointi
- kriittisen tiedon tunnistaminen
- Tiedon käytettävyys, eheys ja luottamuksellisuus
- Tiedon luokittelua ja käsittely
- luokittelutavat
- käsittelyohjeet
- Hallinnollisen tietoturvallisuuden käytäntöjen omaksuminen
- Käyttö- ja pääsyoikeuksien hallinta
- Turvallisuusselvitykset
- Turvallisuussopimukset
- Salassapitosopimukset
- Henkilöstön osaaminen (tietoturva- ja sovellusosaaminen)
- Tieto- ja yksityisyydensuojan noudattaminen
- Henkilötietojen käsittely
- Yksityisyydensuoja työelämässä
- Viestinnän suoja

- Teknisen tietoturvallisuuden toteuttaminen ja ylläpito
- Palomuurit yms. ratkaisut
- Haittaohjelmien torjunta
- Tiedonsiirron suojaaminen
- Päätelaitteiden suojaus
- Salaustekniikan hyödyntäminen
- Laitteisto- ja ohjelmistoturvallisuus
- Varmuuskopiointi ja muut varmistukset
- Käyttöturvallisuus (ohjeet ja tuki)
- Järjestelmien ja prosessien toiminnan jatkuvuuden varmistaminen
- Havainnointikyvyn kehittäminen
- Sieto- ja palautumiskyvyn kehittäminen
- Ympäristön fyysinen turvallisuus
- Jatkuva havainnointi, lokiseuranta Muutoksenhallinta
- Vaikutuksenarviointi
- Tiedonhallintamallin kehittäminen
- Varautuminen häiriöihin

4. Suojattavat kohteet ja niiden turvatoimien priorisointi

Suojattavat kohteet tunnistetaan ja tietoturvakriittisyys arvioidaan ja perustellaan. Kriittiset kohteet luetteloidaan ja priorisoidaan ja kohteille tehdään riski- ja vaikutustenarviointi kriittisyysjärjestyksessä. Riskien kontrollit arvioidaan ja valitaan toimintaympäristöön parhaiten soveltuvat tietoturvakontrollit. Tietoturvakontrollien toteuttamiseen osoitetaan vastuutahot. Riskien hallinta ja tietoturvakontrollien käyttöönotto ja vastuut kuvataan riskienhallintasuunnitelmassa.

5. Tietoturvallisuuden hallintajärjestelmä

Ylivieskan kaupungin tietoturvan hallintaan liittyvä dokumentaatio säilytetään dokumenttien hallintajärjestelmässä ja tulostettu kopio arkistossa.

Tietoturvallisuuden toteuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten,

fyysisten ja teknisten ratkaisujen avulla. Tietoturvallisuusmääritykset tarkistetaan ja arvioidaan vähintään vuosittain tai merkittävien muutosten yhteydessä. Tietoturvan hallintajärjestelmän ja kehittämissuunnitelman hyödyllisyys ja toimivuus käsitellään johdon katselmoinnissa ja johto päättää tarvittavista laajavaikutteisista muutoksista. Tietoturvallisuuskuvausten teknisestä ylläpidosta tietosuojan osalta vastaa tietosuojavastaava yhdessä tietoturvapäällikön johdon kanssa.

5.1. Tietoturvan kehittämisvisio

Ylivieskan kaupungilla on vuonna 2027 käytössä kokonaisvaltainen tietoturvan hallintajärjestelmä. Henkilöstö on tietoturvatietoista, motivoitunutta ja sitoutunutta yhteistoiminnassa asetettuihin tietoturvatavoitteisiin.

6. Tietoturvakoulutus ja -ohjeet

Ylivieskan kaupunki kouluttaa johtoa ja henkilökuntaa säännöllisesti tietoturvaan ja tietosuojaan liittyvissä asioissa. Henkilökunta osallistuu säännöllisesti verkkokoulutuksiin ja tarpeen mukaan luokkahuonekoulutuksiin sekä seminaareihin tai työpajoihin. Koulutukset kuvataan tarkemmin koulutussuunnitelmassa. Uusien työntekijöiden perehdytyskoulutuksiin sisältyy tietoturvakoulutus. Tietoturvakoulutuksien toteutumista seurataan. Mikäli tietojärjestelmiin tai organisaatiorakenteisiin tehdään merkittäviä uudistuksia tai hankintaan uusia tietojärjestelmiä, arvioidaan tietoturvakoulutuksen tarve erikseen näissä tilanteissa.

7. Tietoturvallisuudesta tiedottaminen

Kaupungin johto tiedottaa ja ohjeistaa henkilökuntaa, mikäli organisaatiossa esiintyy tietoturvapoikkeamia. Johto varoittaa ja ohjeistaa henkilökuntaa myös varautumaan, mikäli tietyt tietoturvaloukkauksen lisääntyvät ajoittain.

8. Tietoturvallisuuden ja tietosuojan seuranta

Jokainen työntekijä on velvollinen ilmoittamaan havaitsemistaan tietoturvapuutteista. Toimialojen vastuuhenkilöiden tehtävänä on valvoa, että tietoturva toteutuu käytännössä ja ryhtyä toimiin, mikäli henkilökunta ilmoittaa tietoturvaan liittyvästä epäilystä tai epäkohdasta. Tietoturvaohjeistukseen liittyvien laiminlyöntien sattuessa

seurauksena voi olla teon vakavuudesta ja tahallisuudesta johtuen huomautus tai kirjallinen varoitus, rikosilmoitus tai jopa palvelussuhteen purkaminen. Tietoturva- ja tietosuojarikkomuksista on yksityiskohtaisempaa tietoa kohdassa ”Tietojärjestelmien valvonta ja seuraamukset”.

Tietoturvavastuista tehdään laite- ja sovellustoimittajien sekä palveluntarjoajien kanssa erilliset sopimukset.

Tietoturvakäytännöille tehdään vertaisarviointeja saman toimialueen toimijoiden kanssa ja/tai niitä katselmoidaan erillisissä auditointitilaisuuksissa.

9. Poikkeamien hallintaprosessi

Poikkeamien käsittely on kuvattu jatkuvuus- ja toipumissuunnitelmassa. Kun havaitaan poikkeamaepäily, noudatetaan suunnitelman mukaisia toimia. Mikäli poikkeamaa ei ole riskikartoituksessa osattu ennakoida, toimitaan nopeasti tilanteen edellyttämällä tavalla vahinkojen minimoimiseksi. Jokainen poikkeamatilanteeseen osallistuva dokumentoi tilannetta vaihe vaiheelta kirjaamalla päiväyksen, kelloajan ja tehtävän, jonka tehnyt poikkeamaepäilyyn liittyen. Tilanteen mentyä ohi, tietoturvan kokonaiskuva dokumentoidaan ja tallennetaan poikkeamien hallintaan.

Kaikki merkittävät haitalliset tapahtumat kirjataan tulevien kehittämistoimien perustaksi. Myös ns. ”läheltä piti” –tapaukset rekisteröidään. Onnettomuuksien, turvallisuusrikkomusten ja palvelujen keskeytysten seuraukset analysoidaan. Haitallisista tietoturvatapahtumista kerätään jatkuvasti ajan tasalla olevaa tilannekuvaa yhdyshenkilöverkoston ja teknisten valvontatietojen avulla. Tilannekuva havainnollistaa tietoturva-poikkeamatilanteen ja niiden aiheuttamat vaikutukset. Kerättyä dataa käytetään tulevissa arvioinneissa apuna tietoturvatoimien suunnittelussa ja priorisoinnissa.

Tietoturvaloukkauksesta ilmoitetaan tarpeen vaatiessa myös Traficomin Kyberturvallisuuskeskukseen nettilomakkeella. Tarvittaessa tietoturvarikoksesta tehdään rikosilmoitus poliisille. Tietosuojaan kohdistuvista loukkauksista tehdään ilmoitus tietosuojavaltuutetun toimistolle.

10. Tietojärjestelmien valvonta ja seuraamukset

Tietojen ja tietojärjestelmien käyttöä valvotaan olemassa olevien lakien ja asetusten mukaisesti huomioiden yksityisyyden suoja työelämässä. Tietojärjestelmien lokivalvontaa suoritetaan tietosuojavastaavan laatiman ja tietoturva- ja tietosuojaryhmän hyväksymän lokivalvontasuunnitelman mukaisesti.

Kaikki tietoturvarikkomukset käsitellään asianmukaisesti. Tietoturvarikkomusta lieventää merkittävästi, mikäli rikkomuksen tehnyt henkilö on välittömästi rikkomuksen huomattuaan ottanut yhteyttä esimieheensä sekä tietoturva- tai tietosuojavastaavaan, eikä käytä missään olosuhteissa väärin saamaansa tietoa. Tietoturvarikkomuksesta seuraa varoitus tai sen perusteella on mahdollista päättää työ- tai virkasuhde. Tietoturvarikkomuksesta voi seurata myös rikosoikeudellinen vastuu. Yksityiskohtaisempaa tietoa tietoturva- ja tietosuojarikkomuksesta seuraamustaulukosta.

Toiminnan oikeellisuus on varmistettava ensisijaisesti lähiesimieheltä tai tietoturva- ja tietosuojavastaavilta.

YLIVIESKA

Tietoturva- ja tietosuojarikkomusten seuraamustaulukko

TAHALLISUUDEN ASTE RIKKOMUKSEN VAKAVUUS	**Tietämättömyys, osaamattomuus, erehdys, vahinko, huolimattomuus**	**Piittaamattomuus, tahallisuus, toistuvuus**	**Rikoksentekotarkoitus (vahingonteko, luvaton käyttö, vakoilu, salassapitorikos, aseman/väärinkäyttö hyötymistarkoitus)**
Vakava rikkomus **(lain mukaan rikkomuksena tai rikoksena tuomittava teko)**	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään	- tehdään rikosilmoitus - työnantaja käynnistää palvelussuhteen päättämismenettelyn	– tutkintapyyntö poliisille – työnantaja käynnistää palvelussuhteen päättämismenettelyn
Rikkomus **(vakava väärin-käyttö tai turvallisuuden rikkominen)**	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus	- kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään - työnantaja käynnistää palvelussuhteen päättämismenettelyn	- tutkintapyyntö poliisille - työnantaja käynnistää palvelussuhteen päättämismenettelyn
Lievä rikkomus **(asiaton toiminta tai väärinkäytös)**	- puheeksi ottaminen ja opastus - suullinen huomautus	- suullinen huomautus - kirjallinen varoitus - työnantaja käynnistää palvelussuhteen päättämismenettelyn	– tutkintapyyntöä poliisille harkitaan – kirjallinen varoitus – työnantaja käynnistää palvelussuhteen päättämismenettelyn

- **Vakava rikkomus (lain mukaan rikkomuksena tai rikoksena tuomittava teko)**
    - Salassa pidettävien tietojen oikeudeton käsittely ja luovuttaminen
    - Tietojen luvaton käyttö (esim. tekijänoikeuden loukkaus tai rikoslain alaisen materiaalin oikeudeton käsittely ja hallussapito, kuten mm. rasistinen aineisto tai lapsiporno)
    - Hakkerointi ja tunkeutuminen tietojärjestelmiin
    - Vahingonteko (esim. haittaohjelmien tahallinen levittäminen tai palvelun tahallinen estäminen)
    - Vakoilu
    - Virka-aseman väärinkäyttö

- Hyötymistarkoitus

- **Rikkomus (vakava väärinkäyttö tai turvallisuuden rikkominen)**
  - Ohjeiden vastainen laitteistojen tai ohjelmien käyttö
  - Tunnuksen luovuttaminen (esim. salasanan kertominen toiselle käyttäjälle tai avoimen työaseman luovuttaminen niin, että toinen pääsee valvomatta käyttämään luovuttajan tunnusta)
  - Tiedon luottamuksellisuuden vaarantaminen (esim. työaseman jättäminen auki valvomatta)
  - Ylläpito-oikeuksien luvaton hallussapito
  - Ohjelmien ja pelien luvaton kopiointi

- **Lievä rikkomus (asiaton toiminta tai väärinkäytös)**
  - Henkilökohtaisen tietoturvan/tietosuojan laiminlyönti (esim. käyttäjätunnuksen huolimaton käyttö, salasanan jättäminen näkyviin, salassa pidettävien asiakirjojen jättäminen näkyviin)
  - Haitan aiheuttaminen (esim. laitteiden/ohjelmien lukitseminen ja toisten oikeutetun pääsyn estäminen)
  - Resurssien tuhlaus (esim. työajan väärinkäyttö, kuten asiaton surffailu internetissä)
  - Luvaton kaupallinen tai poliittinen toiminta (esim. sähköpostin käyttäminen henkilökohtaiseen markkinointiin)
  - Kulunvalvontaohjeiden rikkominen (esim. avainten luovuttaminen toisen käyttöön)