Kh xx.xx.2025 § xx
17.3.2025

Ristijärven kunnan tietoturva ja tietosuojapolitiikka

Johdanto

Tieto on keskeisessä roolissa Ristijärven kunnan toiminnassa ja palvelutuotannossa. Jotta tieto on tehokkaasti hyödynnettävissä, tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa.

Tietoturva- ja tietosuojapolitiikassa Kainuun kunnat ovat yhteistyössä Kainuun liiton kanssa määritelleet tietoturvallisuutta koskevat periaatteet, vastuut ja tavoitteet. Politiikka toimii perustana Ristijärven kunnan tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja auttaa niiden käytäntöön soveltamisessa. Tietoturva- ja tietosuojapolitiikka ja sen soveltamisohjeet pidetään käyttäjien saatavilla Ristijärven kunnan intranetissä.

Tietoturva- ja tietosuojapolitiikka koskee koko Ristijärven kunnan organisaatiota – niin työntekijöitä kuin luottamushenkilöitäkin – sekä niitä Ristijärven kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Ristijärven kunnan omistamaa tai hallinnoimaa tietoa. Politiikka kattaa Ristijärven kunnan käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tietoturvallisuus

Ristijärven kunnassa tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan Ristijärven kunnan omistamaa tai hallinnoimaa tietoa sekä normaalitilanteissa, normaaliolojen häiriötilanteissa, että poikkeusoloissa. Tietoturvallisuus kattaa käsitteenä sekä kyberturvallisuuden että tietojen fyysisen suojaamisen.

Tietoturvallisuus on kiinteä osa Ristijärven kunnan johtamista, palveluita ja toimintoja. Se ulottuu jokaisen työntekijän arkipäivän työtehtäviin ja työtapoihin sekä luottamushenkilöiden toimintaan Kainuun liiton asioiden käsittelijöinä. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Tietoturvallisuuteen liittyvillä vastuilla ja käytännöillä pyritään varmistamaan, että Ristijärven kunnan omistama ja hallinnoima tieto

- on oikeaa ja eheää, eikä muuttunut teknisen tai inhimillisen toiminnan seurauksena (eheys)
- on vain siihen oikeutettujen saatavilla (luottamuksellisuus)
- on saatavilla, kun sitä tarvitaan (käytettävyys)

- on käsitelty niin, että käsittelyn osapuolet voidaan tunnistaa toimenpiteiden aikana ja jälkikäteen (kiistämättömyys)
- on mahdollista varmistaa sen todenmukaisuus, oikeellisuus, alkuperä ja/tai varmistetaan käyttäjän aitous määritellyllä luottamustasolla (todentaminen)

Tähän liittyen tulee tiedon käsittelyprosessien omistajuus ja käyttöoikeudet määritellä sekä huolehtia tiedon elinkaaren hallinnasta niin, että tietoon sen käsittelyn eri vaiheissa tehdyt muutokset voidaan tarvittaessa jäljittää ja todentaa.

Hyvän tietoturvallisuuden aikaansaaminen ja ylläpito edellyttävät tietoista johtamista ja hyvän hallintotavan noudattamista kunnan kaikissa toiminnoissa. Tietoturvallisuuden osalta tämä kokonaisuus sisältää suunnitteluun, toteutukseen, seurantaan ja ohjaukseen liittyvät prosessit, asiakirjat, kontrollit ja vastuut.

Ristijärven kunnan tietoturvatyötä ohjaavat, soveltuvilta osin, seuraavat viitekehykset:

- Julkisia organisaatioita velvoittavat lait ja asetukset, mm. Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR)
- Ristijärven kunnan omat voimassa olevat strategiat, hallinto- ja ohjesäännöt, riskienhallinta-, valmius- ja viestintäsuunnitelmat (tietoturvallisuutta koskevilta tai sivuavilta osiltaan) sekä näistä johdetut vaatimukset
- Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) suositukset
- Valtionhallinnon Tietoturvallisuuden johtoryhmän (VAHTI) ohjeet
- EU:n tekoälydirektiivi

Tietoturvallisuus on osa Ristijärven kunnan riskienhallintaa, varautumista ja kokonaisturvallisuutta. Riskienhallintaa toteutetaan Ristijärven kunnan sisäisen valvonnan ja riskienhallinnan ohjeen mukaisesti.

Ristijärven kunta varautuu turvaamaan ensi sijassa kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia valmius- ja muita suunnitelmia. Varautumiseen liittyvät roolit ja vastuut kuvataan em. suunnitelmissa. Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

Tiedonhallintalaki velvoittaa tunnistamaan merkittävät tietojenkäsittelyyn kohdistuvat riskit ja hallitsemaan niihin liittyviä ennakoivia tietoturvatoimenpiteitä. Tietoturvan hallinnan taso on asetettu noudattamaan lainsäädännöllisiä velvoitteita. Ristijärven kunta tunnistaa ja hallitsee tietoturvan uhkatekijöitä proaktiivisesti. Uhkatekijöiden hallinta perustuu jatkuvaan seurantaan ja analysointiin, jotta poikkeamat voidaan havaita ja käsitellä ajoissa.

Tietosuoja

Tietosuoja on oleellinen osa tietoturvallisuutta. Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten ihmisten yksityisyyden, oikeuksien ja oikeusturvan varmistamiseksi. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä.

Ristijärven kunta käsittelee henkilötietoja vain perusteltuun käyttötarkoitukseen ja vain siinä määrin ja niin kauan, kun se on käyttötarkoituksen kannalta tarpeellista. Käytettävien tietojen oikeellisuus pyritään varmistamaan ja tietoja päivitetään. Henkilötietoja säilytetään ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Tietosuojaa ohjaavina periaatteina ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä tietojen eheys ja luottamuksellisuus.

Toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Henkilöstön tietosuojaosaamisesta huolehditaan koulutuksilla sekä työroolin mukaisilla ohjeistuksilla. Ristijärven kunta mahdollistaa asiakkaille tiedonsaannin omiin henkilötietoihinsa sekä informoi henkilötietojen käsittelystä Ristijärven kunnan verkkosivuilla. Ristijärven kunnan henkilörekistereitä käsittelevät sopimuskumppanit velvoitetaan noudattamaan vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

Tietoturvallisuustavoitteet

Ristijärven kunnan tavoitteena on saavuttaa Tiedonhallintalain (906/2019) asettamat tietoturvallisuutta koskevat vaatimukset. Tässä yhteydessä otetaan huomioon, että tiedonhallintaa koskeva lainsäädäntö ja siihen liittyvät kansalliset suositukset ovat muutoksessa ja sisältävät useita siirtymäaikoja.

Ristijärven kunta päivittää tietoturvaa koskevia tavoitteita ja tähän liittyviä toimintaprosessejaan suhteessa muuttuvaan lainsäädäntöön osana tietoturvan kokonaissuunnittelua. Toiminnan suunnittelussa ja kehittämisessä otetaan huomioon Valtiovarainministeriön Tiedonhallintalautakunnan, valtionhallinnon tietoturvallisuuden johtoryhmän (Vahti) ja Suomen Kuntaliiton päivittyvät suositukset sekä muu kansallinen julkishallinnon tietoturvaa koskeva lainsäädäntö ja ohjeistus.

Organisointi ja tietoturvavastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu Ristijärven kunnan hallintosäännön mukaisesti.

Kunnanhallitus seuraa tietoturvallisuuden toteutumista kunnassa. Kunnanhallitus hyväksyy tietoturva- ja tietosuojapolitiikan ja siihen ehdotetut muutokset. Kunnanhallituksella on vastuu kunnan sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Kunnanjohtajalla on kokonaisvastuu tietoturvallisuuden toteuttamisesta ja tietoturvallisuuden toteutumisen raportoinnista kunnanhallitukselle. Kunnanjohtaja omistaa tietoturvapolitiikan ja esittelee muutokset kunnanhallitukselle. Kunnanjohtaja hyväksyy kuntatasoiset ohjeet ja linjaukset ellei hallintosäännössä toisin määrätä. Kunnanjohtajan tukena tietoturvallisuusasioissa on tietosuojavastaava ja hallintopäällikkö, sekä palveluiden toimittajat siinä osin, kuin se on palvelusopimuksissa määritelty.

Toimialuepäälliköt vastaavat toimialueidensa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

Esihenkilö vastaa tietoturvallisuuden toteutumisesta omalla vastuualueellaan.
Esihenkilön keskeisimpinä tehtävinä on huolehtia:

- oman organisaationsa perehdyttämisestä Ristijärven kunnan tietoturvaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturvavastuisiin.
- työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
    - Ristijärven kunnan tiedon ja muun omaisuuden palauttamisesta
    - työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta ja vähintään näiden muutoksien ilmoittamisesta ohjelmistojen pääkäyttäjälle.

Henkilöstö vastaa tietoturvan ja -suojan toteuttamisesta omalta osaltaan. Jokaisen on edesautettava omalla tekemisellään turvallisuuden tavoitteiden toteutumista mm. noudattamalla tietosuojaa ja tietoturvaa koskevia ohjeita. Jokaisen velvollisuus on tuoda esille mahdolliset turvallisuuspoikkeamat, epäkohdat sekä havaitsemansa uhkat ja riskit ja raportoida niistä välittömästi Atean asiakastukeen ja omalle esihenkilölleen, tai keskitetysti tietosuojavastaavalle. Henkilöstö on velvollinen pyytämään apua tietoturvaa ja -suojaa koskevissa kysymyksissä sitä tarvitessaan. Tietoturvatavoitteet saavutetaan vain, jos kaikki noudattavat yhteisesti sovittuja periaatteita.

Tiedon omistaja vastaa tiedon elinkaaren hallinnasta, tiedon luokittelusta (julkisuuden ja salassapidon määrittely), eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön. Tiedon omistaja on se, joka tiedon tuottaa ja joka vastaa sen oikeellisuudesta.

Tietojärjestelmän omistaja vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmään hyväksyy työntekijän esihenkilön tai hänen valtuuttamansa taho. Tietojärjestelmän omistaja on tietojärjestelmästä vastaava palvelualueen esihenkilö tai tietojärjestelmän pääkäyttäjä.

Prosessin omistaja vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Lisäksi hän vastaa prosessin riippuvaisuuksien tunnistamisesta ja kriittisyyden arvioinnista.

Pääkäyttäjät ovat keskeisessä roolissa tietojärjestelmien hallinnassa ja käytössä. Heidän vastuullaan on varmistaa, että tietojärjestelmät toimivat asianmukaisesti ja että käyttäjät saavat tarvitsemansa tuen ja ohjeistuksen.

Tietosuojavastaava antaa tietoa ja neuvoja tietosuojaan liittyvissä asioissa, seuraa tietosuojaasetuksen ja kansallisten tietosuojaa koskevien lakien noudattamista, tekee yhteistyötä valvontaviranomaisen kanssa ja toimii valvontaviranomaisen ja rekisteröityjen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tietosuojavastaava vastaa tietosuojaan liittyvästä viestinnästä.

Palveluntuottajat vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumisesta ICT-ympäristössä ja tietojärjestelmissä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin. Milloin tietosuojalainsäädäntö edellyttää tietosuojan vaikutustenarvioinnin (dpia) tekemistä, vastaa palveluntuottaja vaikutustenarviointiprosessiin osallistumisesta omalta osaltaan. Palveluntuottajat noudattavat Ristijärven kunnan tietoturvapolitiikkaa sekä sopimusten tietoturva- ja tietosuojaliitteitä.

Tiedon ja tietojärjestelmien käyttö

Ristijärven kunnan tietojärjestelmäympäristössä käytetään kunnan hyväksymiä ja hallinnoimia tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Uusien ratkaisujen käyttöönoton yhteydessä tulee varmistua, että ne ovat Atean tiedossa ja hyväksymiä.

Käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon, fyysisiin tiloihin- esimerkiksi päätearkistoon, sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Käyttöoikeudet toteutetaan kunnalla roolipohjaisesti käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan. Vastuu käyttöoikeuksista on aina sillä toimialalla, joka ne myöntää.

Tärkeintä on varmistaa, että käyttäjätunnusten elinkaari on hallittavissa siten, että kaikki käyttäjätunnuksiin ja käyttövaltuuksiin tehdyt muutokset ovat asianmukaisesti esihenkilön valtuuttamia, dokumentoituja ja valvottuja. Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi Ristijärven kunnan sisäisiä ohjeita. Henkilötietojen käsittelyssä noudatetaan voimassa olevaa lakia ja tietosuojaa ohjaavia periaatteita.

Esihenkilön tulee huolehtia käyttöoikeuksien asianmukaisuudesta ja ajantasaisuudesta. Työntekijän palvelussuhteen päättyessä tai tehtävien muuttuessa esihenkilö tai keskitetysti hallintojohtaja huolehtii työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta.

Tiedolla on aina omistaja. Tiedon omistaja vastaa tiedon luokittelusta ja oikeasta käsittelystä. Ristijärven kunnan tietojen käsittelynohjeita tulee noudattaa. Ristijärven kunnan tietojen käsittelyohjeita sekä tietoturva- ja tietosuojaperiaatteita ja ohjeita sovelletaan myös hankkeisiin ja pilotteihin.

Pilvipalveluiden käytössä tulee noudattaa Ristijärven kunnan tietoturvaohjeita. Tietojen suojaaminen pilvipalveluissa on varmistettava käyttämällä vahvoja salausmenetelmiä ja valitsemalla luotettavia pilvipalveluntarjoajia, jotka täyttävät tietoturvavaatimukset. Pilvipalveluiden käsittelemä data tulisi olla EU/ETA-alueella erityisesti henkilötietoja käsittelyssä.

Etätyössä tulee noudattaa Ristijärven kunnan etätyöohjeistuksen tietoturvakäytäntöjä.

Tämä tulee liittää myös etätyöohjeeseen: *Henkilöstön tulee käyttää vain hyväksyttyjä laitteita ja ohjelmistoja, ja kaikki yhteydet tulee suojata vahvalla salauksella. Tietoja ei saa paljastaa ulkopuolisille, eikä työnantajan tietokoneita tai laitteita saa luovuttaa ulkopuolisten käyttöön. Ulkopuolisilla tarkoitetaan myös perheenjäseniä. Kotona tai toimiston ulkopuolella käsiteltävän tietoaineiston täytyy liittyä työntekijän tehtäviin. Luottamuksellisen tiedon hävittäminen pitää tapahtua tietoturvaohjeiden mukaisesti. Työntekijän on sitouduttava noudattamaan etätyössä samaa salassapitovelvollisuutta, jota häneltä työssä ollessa normaalistikin edellytetään.*

Riskiperusteinen lähestymistapa

Tietoturvallisuustoimet tulee perustaa vaatimuksiin, joita toiminta ja palvelut asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle. Tietoturvallisuustoimet tulee suhteuttaa suojattavaan tietoon; julkisen tiedon suojaamiseksi ei tarvita samanlaisia toimenpiteitä kuin salassa pidettävien tietojen suojaamiseksi. Tietoturvatoimia tulee mitoittaa sekä järjestelmän tietosisällön, että Kainuun liiton kriittisten prosessien näkökulmasta. Tietoaineistoihin, tietovarantoihin ja tietojärjestelmiin kohdistuvia riskejä tulee tarkastella osana kokonaisturvallisuuteen liittyvää riskianalyysiä ja suunnittelua.

Tietoturvaosaamisen varmistaminen

Johdon tehtävänä on varmistaa koulutuksen ja ohjeiden avulla, että henkilöstön tietoturvaosaaminen on riittävää. Myös osaamisen ylläpidosta on huolehdittava niin, että se vastaa kulloinkin vallitsevia tilanteita ja toimintaympäristön vaatimuksia.

Esihenkilö huolehtii uudessa tehtävässä aloittavan työtekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin ja siihen, miten tietoturvallisuus tulee huomioida hänen omissa työtehtävissään. Tietoturvallisuuden peruskoulutusta tarjotaan säännöllisesti, ja tietoturva- ja tietosuojaohjeet pidetään kaikkien työntekijöiden saatavilla Ristijärven kunnan intrassa. Koulutukset kattavat tietoturvan perusperiaatteet, ajankohtaiset uhkat ja parhaat käytännöt. Ulkoistettujen palveluiden osalta (mm. talous- ja henkilöstöhallinto) paveluntarjoaja huolehtii salassapitosopimusten ajantasaisuudesta.

Ristijärven kunnan työntekijät suorittavat omatoimisen tietoturva- ja tietosuojakoulutuksen kunnan laatiman suosituksen mukaisesti.

Tietoturva- ja tietosuoja hankinnoissa ja sopimuksissa

Hankinnoissa tulee noudattaa hankintalainsäädäntöä, Ristijärven kunnan hankintaohjeistusta sekä julkishallinnon yleisiä suosituksia ICT-hankintojen ja hankinnan kohteiden tietoturvan huomioimisesta. Erityistä huomiota tulee kiinnittää siihen, että tieto- ja viestintätekniset hankinnat sopivat Ristijärven kunnan tiedonhallintamallissa määriteltyyn kokonaisarkkitehtuuriin. Tieto- ja viestintäteknisissä hankinnoissa tulee hankintalainsäädännön asettamissa puitteissa pyrkiä mahdollisimman yhdenmukaisiin, olemassa olevaa osaamista hyödyntäviin hankintoihin kokonaistaloudellisuus ja riskit huomioon ottaen.

Hankintoja suunniteltaessa tulee määritellä tarvittavat asianmukaiset tietoturvajärjestelyt ja tietoturvan toteutumisen valvonta sekä varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Vaadittavien tietoturvajärjestelyiden tulee perustua käsiteltävien tietojen laatuun ja kriittisyyteen kunnan palveluiden jatkuvuuden hallinnan sekä tietosuojan näkökulmista. Huomioon tulee ottaa tiedon elinkaari, normaaliolojen häiriötilanteisiin ja poikkeusoloihin varautumiseen liittyvät vaatimukset sekä muu asiaa sääntelevä lainsäädäntö.

Hankintasopimuksissa määritellään, kuinka tietoturva huomioidaan palvelutuotannossa mukaan lukien se, minkä tasoinen häiriönhallintakyky palveluntuottajalta ostetaan. Hankintasopimukseen tulee lisäksi liittää Ristijärven kunnan tietoturva- ja tietosuojaliitteet. Kyseisten sopimusvelvoitteiden lisäksi hankinnassa tulee huomioida tietoturvavaatimukset tarkemmalla tasolla tämän tietoturva- ja tietosuojapolitiikan mukaisesti.

Tietosuojan osalta tietosuoja-asetus edellyttää, että Ristijärven kunta saa käyttää ainoastaan sellaisia palvelutuottajia tai muita henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet. Käsittelyn on täytettävä tietosuoja-asetuksen vaatimukset ja varmistettava rekisteröidyn oikeuksien suojelu.

Lähtökohtaisesti Ristijärven kunnan sopimuksissa ja hankinnoissa käytetään Ristijärven kunnan *tietosuojaliitettä.* Tietosuojaliite tai muut tietosuoja-asetuksen 28 artiklan vaatimukset täyttävät ehdot sisällytetään kaikkiin uusiin sopimuksiin, joiden perusteella käsittelijä käsittelee henkilötietoja Ristijärven kunnan lukuun.
Tietosuojalainsäädännön asettamia ehtoja ja niiden toteutumista tulee valvoa.

Lokitietojen kerääminen

Silloin kun tieto- ja viestintäjärjestelmän toiminta tai todennetun käyttäjän toimet pitää osoittaa kiistämättömästi, tulee tarvittava tapahtumakirjanpito toteuttaa tietojen eheyden säilyttävillä teknisillä ratkaisuilla (lokijärjestelmät). Lokitietojen kerääminen edellyttää, että käyttöoikeudet ovat henkilökohtaisia.

Lokien keräämiselle tulee olla peruste ja käsittelytavat sekä vastuut määritelty.
Lokeihin tallentuvien tietojen tyypit ja suojaustarpeet tulee tunnistaa ja määritellä. Pääsyä lokitietoihin tulee kontrolloida pääsyoikeushallinnalla ja lähtökohtaisesti käyttäjien pääsy tulee olla evätty, silloin kun henkilön työtehtävät eivät pääsyä edellytä. Luottamuksen säilyttämiseksi lokeja ei tule oikeudettomasti muuttaa tai tuhota.

Kun tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista, tulee tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätä tarpeelliset lokitiedot. Lokitietoja käytetään seuraamaan tietojärjestelmissä olevien tietojen käyttöä ja luovuttamista sekä selvittämään tietojärjestelmien teknisiä virheitä. Lokitietojen käsittelyssä tulee huomioida tiedonhallintalainsäädännön mukainen tarpeellisuusarviointi sekä tietosuojalainsäädäntö.

Tietoturvapoikkeamien käsittely ja niistä tiedottaminen

Tietoturva- ja tietosuojaohjeiden noudattamista valvotaan sekä säännöllisin rutiinein tai automaattisesti että pistokokein. Väärinkäytöksiin puututaan.

Sekä odottamattomista että ennalta tiedetyistä palvelukatkoksista ja muista tietojärjestelmien käytön häiriöistä tiedotetaan Kainuun liiton tavanomaisia tiedotuskanavia hyödyntäen. Järjestelmän omistaja tiedottaa käyttöhäiriöistä niiden edellyttämässä laajuudessa.

Tietoturvapoikkeamat käsitellään ja niistä raportoidaan johdolle erikseen ohjeistetulla tavalla. Muulle organisaatiolle havaituista poikkeamista tiedotetaan niiden luonteen ja laajuuden edellyttämällä tavalla.

Tietoturvaloukkauksissa noudatetaan EU:n yleisen tietosuoja-asetuksen määräyksiä henkilötietojen tietoturvaloukkauksen ilmoittamisesta valvontaviranomaiselle ja rekisteröidylle artiklojen 33 ja 34 mukaisesti.

Liite: prosessi tietoturvapoikkeamien käsittelyä varten

Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Tarvittaessa tehdään tietoturva-auditointeja, joiden avulla varmistetaan tietoturvakäytäntöjen noudattaminen ja tunnistetaan mahdolliset kehityskohteet.

Tietoturvallisuustyön tulee olla suunnitelmallista ja käytännön toteutusten tulee vastata toiminnan tarpeisiin, lainsäädännön vaatimuksiin sekä Kainuun liiton riskienhallintatyössä asetettuihin muihin tavoitteisiin, ulkoiset toimintaolosuhteet huomioiden.

Seurannan ja muutoshallinnan keinoin varmistetaan, että tietoturvallisuuteen liittyvät kokemukset, palaute ja muutokset vaatimuksissa tai olosuhteissa tulevat oikea-aikaisesti huomioon otetuiksi.

Tietoturva- ja tietosuojapolitiikka katselmoidaan vuosittain ja päivitetään tarvittaessa.