Puumala
SAIMAAN KAUNEIN

PUUMALAN KUNNAN
TIETOSUOJA- JA TIETOTURVAPOLITIIKKA

Muutokset:
Tämä asiakirja korvaa kunnanhallituksen 20.2.2017 § 37 hyväksymän tietoturvapolitiikan

Sisällys

1 Johdanto

Tieto on keskeisessä roolissa organisaatioiden toiminnassa ja palvelutuotannossa. Tiedon tulee olla hyödynnettävissä tarpeen mukaisesti ja tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tietojenkäsittelyn turvallisuus, luotettavuus ja virheettömyys ovat tärkeitä toiminnan jatkuvuuden sekä palveluiden laadun ja tehokkuuden kannalta.

Tietosuoja suojaa ihmisten yksityisyyttä. Inhimillisenä toimintana tietojenkäsittelyyn liittyy aina riskejä, joita pyritään minimoimaan ohjeistuksilla, koulutuksella ja teknisillä ratkaisuilla. Tietoturvariskeistä pystytään minimoimaan teknisin ratkaisuin vain osa, tärkeintä ovat päivittäisessä tietojenkäsittelyssä tehdyt ratkaisut ja toimenpiteet.

Tietoturva suojaa henkilötietoja ja muita tietoja luvattomalta käytöltä. Se käsittää keskeisiin toimintoihin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky hallita ennakoivasti uhkia ja tarvittaessa sietää niiden vaikutuksia. Riskien tunnistamisen ja hallinnan sekä vaikutusten minimointi on osa organisaation aktiivista tietoturvan toteuttamista.

Poikkeamatilanteisiin varautumisen ensisijainen vastuu on organisaation ylimmällä johdolla, jonka on varmistettava tietoturvatyön riittävä resursointi ja seuranta. Panostaminen tietoturvaan sekä yleisellä että tekniikan tasolla ovat strategisia päätöksiä, joilla vaikutetaan myös organisaation toimintakykyyn. Lisäksi lainsäädäntö edellyttää tietoturvan asianmukaista hoitamista. Edut ovat häiriötön toiminta, toiminnan laatu ja positiivisen julkisuuskuvan säilyminen. Tietoturvan ja tietotekniikan ammattilaisilla on keskeinen merkitys johdon neuvon antajina.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi ja sitä voidaan tarvittaessa täydentää tai päivittää, kuten lainsäädännön tai muiden ohjeistusten muuttuessa. Tietoturva- ja tietosuojapolitiikka on julkinen asiakirja.

2 Tietoturvan ja tietosuojan periaatteet

Tietoturvatyö on osa yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturvan ja tietosuojan toteutuminen varmennetaan vuosittain tietoturvaorganisaation raportoinnilla johdolle.

Tietoturva- ja tietosuojapolitiikka määrittää periaatteet, toimintatavat, vastuut, toimivallat, valvonnan ja seuraamusjärjestelmän, joita noudatetaan tietoturvan toteuttamiseksi ja kehittämiseksi, sitä sovelletaan kaikessa toiminnassa ja koko henkilöstöön sekä sidosryhmiin.

Tietoturvaperiaatteita noudatetaan kaikissa tiedon elinkaaren vaiheissa ja tämän edistämiseksi tietoturva- ja tietosuojaperiaatteet ovat osa henkilöstön perehdytystä ja koulutusta. Teknisin ratkaisuin varmistetaan toiminnan ja työtehtävän kannalta tarpeellisten tietojen käsittely.

3 Tietoturva

Tietoturvasta huolehditaan asianmukaisesti, joka tarkoittaa tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Tietoturvatoimenpiteet koskevat sekä sähköistä, että manuaalista tietojenkäsittelyä. Tietoturvalliseen toimintatapaan ohjeistetaan ja sen tulee olla jokapäiväistä niin työpaikalla kuin sen ulkopuolella.

Tietoturva koostuu:

- **Tiedon luottamuksellisuudesta**, eli siitä, että tiedot ovat vain niihin oikeutettujen henkilöiden ja organisaatioiden saatavilla eivätkä ne päädy ulkopuolisten tietoon.
- **Tiedon eheydestä**, joka tarkoittaa tietojen muuttumattomuutta tai muutoksen havaitsemista ja säilyvyyttä huolimatta laitteisto- tai järjestelmäviasta tai inhimillisen toiminnan virheistä.
- **Tiedon saatavuudesta**, jolloin tieto on oikeutettujen henkilöiden saatavilla tai käytettävissä silloin kun niitä tarvitaan.
- **Todentamisesta ja kiistämättömyydestä,** joilla tarkoitetaan käyttäjän todentamista ja käyttäjien tietojen käytön kiistämätöntä todistamista.

3.1 Tietojärjestelmä

Tietojärjestelmä on kokonaisuus, joka koostuu tietovarannoista, niitä käsittelevistä sovelluksista ja laitteista sekä tietoverkoista, tietojen käyttöä määrittävistä ohjeista, käyttäjistä sekä liittymistä toisiin tietojärjestelmiin. Tietojärjestelmään kuuluu oleellisena osana käsiteltävien tietojen turvallisuus ja tietoturvan yleinen hallinta ja valvonta. Poikkeama missä tahansa kokonaisuuden osassa merkitsee häiriötä järjestelmän toiminnassa.

Puumalan kunnassa käytössä olevista tietojärjestelmistä ylläpidetään tietojärjestelmäluetteloa yhteistyössä Etelä-Savon tietosuojavastaavan kanssa.

3.2 Tietoturvan hallinnolliset periaatteet

Hallinnollinen tietoturva on tietoturvatoimintojen johtamista ja organisointia, ja sillä tarkoitetaan tietoturvatoimintojen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Hallinnollinen tietoturva pyrkii ennakoimaan riskit sekä arvioimaan ja hallitsemaan riskien mahdollisia vaikutuksia. Tavoitteena on tietoturvan toteutuminen sekä johdon ja henkilöstön sitoutuminen sen suunnitelmalliseen hoitamiseen ja kehittämiseen.

Palveluiden hankinnoissa edellytetään tiedon käsittelyyn liittyvien suojatoimien, vastuiden ja teknisten tietoturvavastuiden sisältyvän palvelusopimuksiin, lisäksi henkilötietojen käsittelystä tulee sopia EU:n yleisen tietosuoja-asetuksen mukaisesti.

Tietoturvaan liittyvillä tehtävillä on omat vastuuhenkilöt. Vastuuhenkilöillä on resurssit ja toimivalta toteuttaa vastuulleen annetut tehtävät. Tietoturvaperiaatteet viedään käytäntöön ohjeistuksin, koulutuksin ja tiedottein.

3.3 Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöiden toimista johtuvia ja heihin kohdistuvien tietoturvauhkien hallintaa. Tavoitteena on luotettava ja tehtäväänsä soveltuva henkilöstö, joka tuntee oman roolinsa mukaisesti hänelle asetetut tietoturvavaatimukset. Henkilöstön, opiskelijoiden, harjoittelijoiden, luottamushenkilöiden ja organisaatiolle ostopalveluita tuottavien henkilöiden ja toimijoiden tulee noudattaa tietoturvallisia toimintatapoja tehtävässään. Henkilöstöturvallisuuden toteutumiseksi on myös vaaralliset työyhdistelmät eliminoitava.

Työtehtävän mukainen käyttöoikeus järjestelmiin ja ohjelmistoihin annetaan tai poistetaan esimiehen pyynnöstä. Esimies vastaa työtehtävän määrittelystä tehtäväkuvauksessa. Käyttöoikeudet ja -rajoitukset toteuttavat ict-asiantuntija tai ko. ohjelmistojen pääkäyttäjät.

Henkilökunnan koulutus, valmennus ja perehdyttäminen ovat tärkeä osa henkilökunnan tietoturvatietoisuuden ylläpidossa. Uusi henkilöstö perehdytetään ja koulutetaan tehtäväänsä esimiehen tai hänen määräämänsä henkilön toimesta. Jokainen Puumalan kunnan tietojärjestelmiä käyttävä henkilökuntaan kuuluva sekä luottamushenkilönä toimiva on velvoitettu tekemään vuosittain Tietoturva- ja tietosuoja -testin. Testi tehdään Navisec Flex -koulutusjärjestelmässä. Toimialajohtajat seuraavat suorituksia ja ict-asiantuntija raportoi tunnusluvuista tietotilinpäätöksessä.

3.4 Fyysinen tietoturva

Fyysinen tietoturvan keinoin pyritään suojaamaan organisaation hallussa olevia tietoja ja tietovarantoja fyysisten uhkien, kuten rakenteiden ja niiden vikojen aiheuttamilta vahingoilta ja luvattomien tai rikollisten toimien seurauksilta. Fyysisen tietoturvan suunnittelussa kartoitetaan ja huomioidaan tärkeimmät suojattavat kohteet ja varmistetaan teknisten järjestelmien toiminta.

Puumalan kunnan fyysinen tietoturva sisältää mm. kulun- ja tilojen valvonnan, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirikuljetusten ja tietoaineistoja sisältävien postilähetysten suojaamisen vahinkoja ja asiatonta toimintaa vastaan.

3.5 Tietoaineistoturvallisuus

Tietojen käsittely sekä luokittelu ja säilyttäminen perustuvat tiedonhallintaa ohjaavaan lainsäädäntöön ja ohjeisiin. Perusteena henkilötietojen käsittelylle on lakisääteisyys tai käyttäjän tehtävästä johtuva asiayhteys asiakkaaseen ja häntä koskeviin tietoihin.

Tietojen saatavuus ja käytettävyys varmistetaan teknisin toimin ja estetään tietojen tahaton tai tahallinen tuhoutuminen tai vääristyminen. Teknisillä toimilla pyritään varmistamaan toiminnan

jatkuvuus häiriöttä ja varaudutaan mahdollisista häiriöistä toipumiseen. Tietoturvatoimia sovelletaan tietoaineiston koko elinkaaren ajan, tiedon syntymisestä sen hävittämiseen.

Organisaation tiedonhallintaohjeistus toimii käytännön ohjeena kaikille asiakirjojen käsittelyyn osallistuville. Asiakirjahallinnon johtavan viranhaltijan ja toimialojen arkistovastaavien vastuulla on asiakirjojen käytettävyyden, säilyttämisen ja lainmukaisen luovuttamisen sekä säilyttämisen toteuttaminen tiedonhallintaohjeistuksen mukaisesti.

3.6 Laitteistoturvallisuus

Laitteistoturvallisuudella suojataan organisaation laitteistojen elinkaarta ja turvallista käyttöä, siihen kuuluvat laitteiston asennuksen, suojauksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja sopimukset sekä laitteistojen turvallinen poisto niiden elinkaaren lopussa.

Laitteiden elinkaareen liittyvät palvelusopimukset pidetään ajan tasalla ja laitteiston elinkaaren päättyessä huolehditaan tietojen asianmukaisesta tuhoamisesta. Tietojärjestelmätoimittajilla ja tietoinfrastruktuurin ylläpitäjällä on omat vastuunsa laitteistoturvallisuuden osalta ja nämä huomioidaan hankinnoissa ja sopimuksissa.

Teknisin toimin pyritään varmistamaan tietojen keskeytyksetön käyttö ja toiminnan jatkuvuus sekä varaudutaan mahdollisista häiriöistä toipumiseen. Kriittisille laitteistoille taataan katkoton sähkönsyöttö ja ylläpidon korkea palvelutaso.

Toimialajohtajat tai vastuualueiden esimiehet hyväksyvät vastuualueidensa ict-laitehankinnat ja laitteiden hankinnasta, ohjelmistoasennuksista, suojauksesta ja ylläpidosta vastaa ict-asiantuntija.

3.7 Ohjelmistoturvallisuus

Pääsynhallinnalla ja sen suunnittelulla estetään tietoaineiston, ohjelmien ja järjestelmien luvaton käyttö. Ohjelmistojen tietoturvaan kiinnitetään huomiota jo niiden hankintavaiheessa, jolloin varmistutaan ohjelmistojen tietoturvasta ja vaatimustenmukaisuudesta. Esimies vastaa siitä, että hänen alaisuudessaan olevat käyttäjät perehdytetään ohjelmistojen käyttöön.

Uuden ohjelman hankinnan lähtökohta on sen tekninen ja toiminnallinen yhteensopivuus käytössä olevien ohjelmistojen ja arkkitehtuurin kanssa. Lisäksi huomioidaan EU:n yleisen tietosuoja-asetuksen asettamat vaatimukset. Ohjelmiston valmistajan ja myyjän vastuu ohjelmistotuotteista määräytyy hankinta- ja käyttöoikeussopimuksissa.

3.8 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella varmistetaan viestinnän häiriöttömyys, tiedonsiirtoyhteyksien käytettävyys, tiedonsiirron suojaaminen ja salaus sekä käyttäjien tunnistaminen. Tietoliikenneturvallisuus kattaa tietoverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan, jonka tuloksena ovat turvatut ja luotettavat tiedonsiirtoyhteydet.

Tietoliikenneturvallisuuden ylläpito on keskitetty MPY Oy:lle ja Wintunix Oy:lle palvelusopimusten mukaisesti.

3.9 Käyttöturvallisuus

Käyttöturvallisuus tarkoittaa turvallisen käytön toimintaolosuhteita, tekniikan toimivuuden valvontaa, käytön ja lokien valvontaa, ohjelmistotukea, ylläpitoa ja huollon turvallisuustoimenpiteitä, varmuuskopiointia sekä häiriöraportointia.

Tietoturva on suuressa määrin käyttäjien toiminnasta riippuvaista. Käyttöturvallisuuden perustana on osaava ja sitoutunut henkilöstö sekä ajantasaiset ohjeistukset, joita toiminnassa noudatetaan. Tietojen oikeudeton käyttö estetään tietojen käsittelyn suunnittelulla ja käyttöoikeuksien hallinnalla.

Tietosuojatyöryhmä yhdessä tietosuojavastaavan kanssa huolehtii tietoturva- ja tietosuojaohjeiden ajantasaisuudesta. Esimiehet ja ohjelmien pääkäyttäjät opastavat ja kouluttavat henkilöstöä ohjelmistojen käyttöön ja tietoturvaan liittyvissä asioissa. Laitteiden ja ohjelmien käyttäjien on perehdyttävä annettuihin ohjeisiin ja noudatettava niitä.

3.10 Liikkuva työ

Liikkuva työ tarkoittaa kaikkea organisaation toimitilojen ulkopuolella tehtävää työtä. Etätyötä tehtäessä huolehditaan puhelinten ja muiden mobiililaitteiden käytön turvallisuudesta sekä tietojen salassa pidon toteutumisesta. Kaikessa organisaation toimitilojen ulkopuolella tehtävässä työssä on noudatettava tietoturvavaatimuksia.

Etätyötä tehtäessä työntekijän ja työnantajan välillä tehdään etätyösopimus.

3.11 Seuranta, valvonta ja raportointi

Tietoturvan kehittäminen ja ylläpito vaativat jatkuvaa seurantaa. Tähän kuuluvat tietoturvan valvonta sekä poikkeamien raportointi ja tilastointi. Seurannan toteuttaminen kuuluu tietosuojavastaavalle ja tietosuojatyöryhmälle. Sisäisen valvonnan ja riskienhallinnan ohjeen mukainen jatkuva seuranta ja valvonta kuuluu nimettyjen henkilöiden lisäksi kaikille esimiehille. Lisäksi valvontaa tehdään rekisteröidyn pyynnöstä tai työntekijän ilmoituksen perusteella.

4 Tietosuoja

Tietosuoja on olennainen osa tietoturvaa. Tietosuoja määrittelee henkilön yksityisyyden suojaamista ja sillä turvataan oikeuksia, tietoja ja luottamusta. Tietosuojan lähtökohtana on suojata henkilöiden perusoikeudet ja -vapaudet sekä erityisesti henkilötiedot ja varmistaa yksityisyyden suoja.

Tietosuojaa ja sen vaatimuksia määrittelee EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö, joka velvoittaa rekisterinpitäjän suunnittelemaan ja osoittamaan henkilötietojen käsittelyn lainmukaisuuden.

Suojaamistoimet kattavat kaiken tiedon käsittelyn, siirron ja säilytyksen, riippumatta niiden tallennusmuodosta tai niihin kohdistuvan uhan luonteesta. Uhat voivat olla tahallisia tai tahattomia, kuten tietojen urkinta, huolimattomuus, järjestelmäviat, tapaturmat tai luonnonkatastrofit. Henkilötietojen turvallinen käsittely korostuu alueellisten ja kansallisten yhteisjärjestelmien käytössä.

Rekisterinpitäjä seuraa tietosuojan toteutumista ja puuttuu havaitsemaansa asiattomaan käyttöön, myös työntekijällä on velvollisuus ilmoittaa havaitsemistaan tietoturvaongelmista. Tietojen luvattomasta käytöstä saattaa seurauksena olla oikeudellisia seurauksia tai erilaisia työnantajan menettelyjä, riippuen tilanteen vakavuudesta.

4.1 Henkilötietojen kerääminen ja käsittely

Henkilötietoja käsitellään siinä laajuudessa kuin se on tarpeen palvelun tai työtehtävän kannalta. Käsittelytoimet suunnitellaan ja määritellään tiedon elinkaari huomioiden. Henkilötietojen käyttö on sallittua vain lainsäädännön nojalla tai henkilön suostumuksen perusteella. Tietojen säilytys ja käyttö toteutetaan siten, ettei ulkopuolisten ole mahdollista saada niitä tietoonsa.

Henkilötietojen tulee säilyä virheettöminä ja niiden tulee olla saatavilla tarpeen mukaisesti. Henkilötietoihin pääsy on rajattu työtehtävän mukaiseksi. Mikäli henkilötietoja luovutetaan, tulee siirron olla tietoturvallinen. Tietoja voidaan luovuttaa lakien ja asetusten nojalla tai rekisteröidyn suostumuksella. Rekisteröidyllä on EU:n yleisen tietosuoja-asetuksen mukainen oikeus tarkistaa itseään koskevat tiedot.

Suomessa henkilötietojen käsittelyä ohjaa ja valvoo tietosuojavaltuutettu, joka käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröidyn oikeuksien toteutumisesta. Yhteyshenkilönä organisaation ja tietosuojavaltuutetun välillä toimii tietosuojavastaava.

5 Tietoturvariskeihin varautuminen

Tietoturvariskejä arvioidaan ja niihin varaudutaan ennalta. Uhkia aiheuttavat mm. tietoisesti tehdyt väärinkäytökset, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset ja haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat. Tietoturvaan kohdistuvat uhat voivat aiheuttaa riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Laitetason ratkaisuilla voidaan vaikuttaa tietoturvan toteutumiseen vain rajallisesti, henkilöstön osaaminen ja tietoisuus ovat suuressa roolissa tietoturvan toteutumisessa. Kouluttaminen sekä tietoisuuden lisääminen tietoturvasta ovat merkittävä tekijä uhkien pienentämisessä. Esimiesten vastuulla on huolehtia henkilöstön perehdyttämisestä.

Tietoturvariskien arviointi sekä niiden hallinnan ja valvonnan periaatteet sisältyvät organisaation sisäisen valvonnan ja riskienhallinnan ohjeeseen.

5.1 Riskien arviointi

Tietoturvariskejä arvioitaessa on huomio kiinnitettävä erityisesti tietojen käsittelyn sisältämiin riskeihin. Riskejä syntyy aina kun tietoja käsitellään, erityisesti silloin, jos tietoja on tarpeen siirtää. Riskejä ovat myös tietojen vahingossa tapahtuva tai tarkoituksellinen tuhoaminen, muuttaminen, luvaton luovuttaminen tai tietoihin oikeudettomasti pääseminen.

Järjestelmien luokittelu tapahtuu niiden kriittisyyden mukaan. Järjestelmien turvajärjestelyt tarkastetaan säännöllisesti ja tarvittaessa niiden toimivuus testataan.

Tietoturvariskejä tulee arvioida ja hallita riskienhallinnan ohjeistuksen mukaisesti ja tietoturvan suurimmat riskit tulee sisällyttää organisaation riskienhallintasuunnitelmaan.

Tiivistetysti riskienhallinnassa tunnistetaan riskit, suojataan tiedot, havaitaan rikkomukset, toimitaan tilanteen vaatimalla tavalla ja varmistetaan toiminnan vaikutukset.

5.2 Tietoturvapoikkeamat

Jokaisen henkilön vastuulla on ilmoittaa, mikäli havaitsee tietoturvaan kohdistuvia uhkia tai ohjeistuksen vastaista toimintaa. Poikkeamista on raportoitava esimiehelle, ict-asiantuntijalle tai tietosuojavastaavalle. Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation tietovarantoihin ja palveluihin kohdistuu uhka, joka vaarantaa tiedon ja palvelun eheyden, luottamuksellisuuden tai saatavuuden.

Tietoturvarikkomukset ja tietoturvapoikkeamat käsitellään tietosuojatyöryhmässä, jossa esitetään jatkotoimet kunnanjohtajalle. Tietoturvarikkomusten ja väärinkäytösten rangaistusta määritettäessä sovelletaan Tietosuojarikkomusten seuraamustaulukkoa (Kuva 1).

Työntekijän velvollisuus on viedä asia eteenpäin, mikäli esimerkiksi asiakas siitä hänelle ilmoittaa.

Mikäli kyse on henkilötietoihin kohdistuneesta tapahtumasta, tulee arvioida tapahtuneen vakavuus ja se, tuleeko tapahtuneesta tehdä ilmoitus tietosuojavaltuutetun toimistolle ja rekisteröidyille. Tilanteen arvioinnin ja päätöksen ilmoituksesta tekee tietoturvatyöryhmä ja tietosuojavastaava.

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi:

- hävinnyt tiedonsiirtoväline, kuten USB-tikku
- varastettu tietokone
- hakkerointi

- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa
- tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen. Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Tällaiset lisätiedot täytyy säilyttää huolellisesti erillään henkilötiedoista.

5.3 Tietoturvarikkomusten seuraamukset

Tietoturvarikkomuksista säädetään työsopimuslaissa sekä viranhaltijalaissa. Henkilötietoihin kohdistuvien rikkomusten osalta asiaa säätää lisäksi EU:n yleinen tietosuoja-asetus sekä kansalliset lait ja asetukset.

Seurauksena rikkomuksista, niiden tapauskohtaisen vakavuuden mukaisesti, voi olla käyttöoikeuteen kohdistuvia rajoituksia, palvelusuhteeseen vaikuttavia seuraamuksia sekä rikoslaissa määriteltyjä seuraamuksia. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin.

TAHALLISUUDEN ASTE / RIKKOMUKSEN VAKAVUUS	**Tietämättömyys, osaamattomuus, erehdys, vahinko, huolimattomuus**	**Piittaamattomuus, tahallisuus, toistuvuus**
Vakava rikkomus **(lain mukaan rikkomuksena tai rikoksena ttava teko)**	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään	- tehdään rikosilmoitus - palvelusuhteen päättämismenettelyn käynnistys
Rikkomus **(vakava väärinkäyttö tai turvallisuuden rikkominen)**	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus	- kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään - palvelussuhteen päättämismenettelyn käynnistys
Lievä rikkomus **(asiaton toiminta tai väärinkäytös)**	- puheeksi ottaminen ja opastus - suullinen huomautus	- suullinen huomautus - kirjallinen varoitus - palvelussuhteen päättämismenettelyn käynnistys

Kuva 1: Tietosuojarikkomusten seuraamustaulukko

5.3.1 Vakava rikkomus

Lain mukaan rikkomuksena tai rikoksena tuomittava teko.

- salassa pidettävien tietojen oikeudeton käsittely ja luovuttaminen (esim. potilastietojen katsominen ilman oikeudellista perustetta)

- 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. virusten tahallinen levittäminen tai palvelun tahallinen estäminen)
- vakoilu
- virka-aseman väärinkäyttö
- hyötymistarkoitus

5.3.2 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 tai potilastiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä)
- ylläpito-oikeuksien luvaton hallussapito
- ohjelmien ja pelien luvaton kopiointi
- luvattomien ohjelmien asentaminen
- luvattomien laitteiden lisääminen verkkoon

5.3.3 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)

6 Vastuut ja organisointi

Tietosuoja ja tietoturva on organisaation yhteinen asia ja se koskettaa koko henkilöstöä.

Tietosuoja- ja tietoturvatoimintaa johtaa **kunnanjohtaja** ja ylintä vastuuta niistä kantaa **kunnanhallitus.** Ylimmän johdon tehtävänä on valvoa kokonaisuutta sekä riskienhallinnan ja sisäisen valvonnan toteutusta. Lisäksi kunnanhallitus vastaa ja antaa tarkemmat ohjeet sopimusten hallinnasta sekä määrää sopimusten vastuuhenkilöt. Tietosuoja- ja tietoturvatyöhön huolehditaan riittävä resursointi ja tietosuojavastaavan työ mahdollistetaan organisaation

toimenpitein. Hallintopäällikkö vastaa teknisen ja hallinnollisen tietoturvan yleisestä järjestämisestä, kehittämisestä ja seurannasta.

Tietosuojavastaava auttaa johtoa velvoitteidensa toteuttamisessa rekisterinpitäjänä. Tietosuojavastaava osallistuu suunnittelutoimintaan, valmistelee ohjeita ja ylläpitää niitä sekä kouluttaa tietosuoja-asioita henkilöstölle. Tietosuojavastaava tukee henkilökuntaa ja rekisteröityjä tietosuoja-asioissa ja seuraa sekä valvoo henkilötietojen käsittelyä ja suojausmenettelyä. Tietosuojavastaavalla on oikeus suorittaa tehtävänsä ja niihin liittyvä suunnittelu, seuranta ja raportointi itsenäisesti. Lisäksi tietosuojavastaavalla on oikeus organisoida henkilötietojen käsittelyn valvonta, ylläpitää käyttöloki- ja luovutuslokirekistereitä sekä ryhtyä jatkotoimenpiteisiin tietosuojan ongelmatilanteissa.

Tietoturvatyöryhmä toimii yhteistyössä tietosuojavastaavan kanssa tietoturvan toteuttamisessa ja suunnittelussa. Työryhmää johtaa hallintopäällikkö ja ryhmän jäsenistö koostuu edustajista hallinto-, hyvinvointi- ja teknisistä palveluista. Tietoturvatyöryhmä käsittelee tietoturvan linjaukset ja ohjeet sekä huolehtii tietoturvan toteuttamisen vastuuttamisesta. Ryhmä seuraa ja toteuttaa tietoturvan eri vastuualueiden suunnitelmien, ohjeiden, selosteiden ja lomakkeiden laadintaa sekä ottaa tarvittaessa kantaa käytäntöihin ja kehittämishankkeisiin ja seuraa yleisesti tietoturvatilannetta.

Hallintopäällikkö johtaa asiakirjahallintoa ja laatii tiedonhallinnan ohjeet yhteistyössä hallintoasiantuntijan kanssa sekä valvoo, että tehtävät hoidetaan annettujen ohjeiden mukaisesti sekä huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta. Asiakirjahallinnon johtavan viranhaltijan ja toimialojen arkistovastaavien vastuulla on asiakirjojen käytettävyyden, säilyttämisen ja lainmukaisen luovuttamisen sekä säilyttämisen toteuttaminen tiedonhallintaohjeistuksen mukaisesti.

Esimiehet vastaavat tulosalueittain sekä toimintayksiköittäin tietoturvan toteutumisesta ja siihen liittyvästä tiedottamisesta sekä valvonnasta. Esimiesten vastuulla on perehdyttää tietoturva- ja tietosuojamääräykset henkilöstölle ja valvoa näiden noudattamista.

Työntekijät ja luottamushenkilöt ovat velvollisia ilmoittamaan havaitsemistaan tietoturvapuutteista, uhista tai menettelyvirheistä tietosuojavastaavalle. Samoin jokainen työntekijä ja luottamushenkilö on omalta osaltaan vastuussa tietoturvan toteuttamisesta toiminta-alueellaan.

Kunnalle palveluja tuottavat kolmannet osapuolet velvoitetaan noudattamaan kunnan ja lakien määrittelemiä tietoturvaperiaatteita ja sopimuksiin tehdään tarvittaessa velvoittavat kirjaukset.

7 Lisätietoja

Tämä tietoturva- ja tietosuojapolitiikka pohjautuu kansalliseen lainsäädäntöön ja EU:n yleiseen tietosuoja-asetukseen. Lisätietoa löydät mm. seuraavista:

Tietosuojalaki
https://finlex.fi/fi/laki/ajantasa/2018/20181050?search%5Btype%5D=pika&search%5Bpika%5D=tietosuoja

Tietosuoja-asetuksen 5 artikla
https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679&qid=1637319193404

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän VAHTI-ohjeet
https://dvv.fi/vahti

Liikenne- ja viestintävirasto Traficom Kyperturvallisuuskeskus
https://www.kyberturvallisuuskeskus.fi/fi/

Tietosuojavaltuutetun toimisto
www.tietosuoja.fi

Kuntaliitto
https://www.kuntaliitto.fi/laki/tietosuoja

Työelämän tietosuojalain 24 §:n rangaistussäännökset
https://www.kt.fi/palvelussuhde/tyoelaman-kaytannot/tietosuoja/rangaistukset