Tietoturva ja tietosuojapolitiikka LUONNOS

LUONNOS
Laatinut:
Johanna Viuhko
tietosuojavastaava

Sisällysluettelo

1. Johdanto

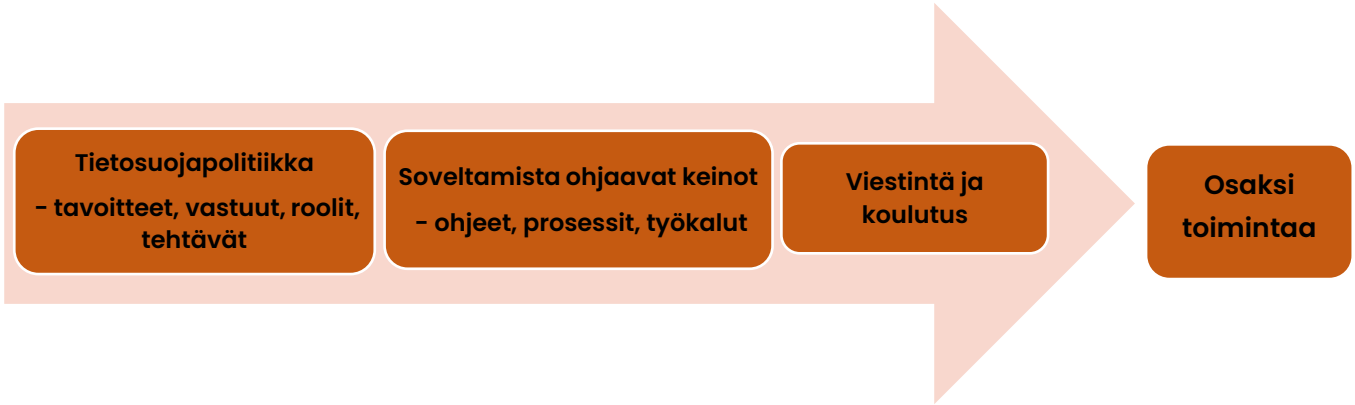
Tietoturva ja tietosuoja ovat tärkeä osa Askolan kunnan toimintaa ja palveluita. Ne liittyvät osana kunnan päivittäiseen toimintaa kaikilla organisaatiotasoilla, toiminnoissa ja palveluissa. Tässä asiakirjassa määritellään, mitä tietoturva ja tietosuoja Askolan kunnassa tarkoittavat. Kuvataan kunnan tietoturvan ja tietosuojan keskeiset periaatteet, tavoitteet, roolit ja vastuut.

Politiikka on perusta kunnan tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja ohjata toimintaa käytännössä. Asiakirja on henkilöstön saatavilla intranetissä ja myös kuntalaisten saatavilla kunnan kotisivuilla. Politiikka on kunnanhallituksen hyväksymä xxx ja koskee jokaista kunnan työntekijää, viranhaltijaa, luottamushenkilöä ja sidosryhmän edustajaa, joka toimeksiantonsa tai työnsä puitteissa käsittelee Askolan kunnan omistamaa tai hallinnoimaa tietoa. Politiikkaa sovelletaan kaikkeen tietoon riippumatta sen muodosta, esitystavasta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotavasta. Tietoturva- ja tietosuojapolitiikkaa katselmoidaan vuosittain ja päivitetään tarvittaessa.

2. Politiikan tavoitteet ja hyödyt

Politiikan tavoite on sitouttaa organisaation johto ja henkilöstö tietoturvalliseen toiminta-kulttuuriin ja -tapaan. Se kuvaa miten tietoturva ja -suojaperiaatteet soveltuvat ja miten niitä toteutetaan. Se määrittää vastuut ja tehtävät sekä ohjaa toimintaa lakien, asetusten ja tietoturvaohjeiden edellyttämällä tavalla sekä varmistaa osoitevelvollisuuden täyttymisen. Lisäksi politiikka luo viitekehyksen tietosuojan hallintamalille, jolla sovitut toimintaperiaatteet toteutuvat käytännössä.

- Sisäinen organisoituminen tietoturvan ja -suojan hoitamiseksi
- Tavoitteet ja toimintaperiaatteet henkilötietojen käsittelyssä
- Suunnittelu, raportointi ja jatkuva kehitys



2.1. Keskeisiä käsitteitä

Henkilötiedot: kaikki tieto, josta yksin tai yhdessä muun tiedon kanssa ihminen voidaan tunnistaa.

Tietosuoja: perusoikeus, joka turvaa rekisteröidyn oikeuksia ja vapauksia henkilötietojen käsittelyn toteuttamisessa. Tietosuojan tarkoitus on osoittaa milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Tietoturva: osa-alueita ovat fyysinen turvallisuus esimerkiksi tilojen suojaaminen, hallinnollinen tietoturvallisuus esimerkiksi ohjeet, linjaukset ja organisointi ja henkilöstöturvallisuus (osaaminen ja luotettavuus). Teknisiin toteutuksiin liittyvät kuten käyttöturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja tietoliikenneturvallisuus.

Henkilötiedon käsittely: käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen, haku, kysely, käyttö, katselu, tietojen luovuttaminen, tietojen yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

Henkilötietojen käsittelijä: taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun ja toimii rekisterinpitäjän alaisuudessa ja ohjeiden mukaan. Esim. IT-palveluntarjoajat, jotka käsittelevät henkilötietoja asiakkaansa puolesta.

3. Tietoturvallisuus

Tietoturvallisuus kattaa sekä tietoturvaan että tietosuojaan liittyvät toteutukset. Sillä tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kunnan omistamaa tai hallinnoimaa tietoa sekä normaalitilanteissa, normaaliolojen häiriötilanteissa, että poikkeusoloissa. Sitä noudatetaan kaiken kunnan käsittelemän tiedon suhteen sen tallennusmuodosta riippumatta. Tietoturvallisuus on tietojen, tietojärjestelmien ja tietoverkkojen suojaamista luvattomalta käytöltä sekä tietovuodoilta, vahingoittumisilta sekä muilta tietoturvariskeiltä suojautumista.

Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toimintaa suunniteltaessa. Tietoturvallisuuskäytäntöjen tulee kattaa kaikki kunnan tietojenkäsittelytehtävät, ottaen huomioon toimialojen ja tulosalueiden tietoturvatarpeet. Niitä noudatetaan koko tiedon elinkaaren ajan, tietojen arkistointiin tai turvalliseen hävittämiseen asti.

Tietoturvatyö tarkoittaa tiedon suojaamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista Se perustuu Askolan kunnan strategiaan, jonka peruspilareita ovat ajanmukainen palveluverkko, turvallinen ja viihtyisä elinympäristö, osallistava ja avoin toimintatapa, hyvinvoivat asukkaat ja henkilöstö sekä kunnan arvoihin turvallisuus ja kestävyys. Käytännössä se näkyy seuraavasti:

- **Asenne:** Tiedon käsittelijä ymmärtää tietoturvan merkityksen ja omat vastuunsa, sekä on motivoinut noudattamaan tätä politiikkaa sekä tästä politiikasta johdettuja tietoturvaohjeita ja -määräyksiä.
- **Luottamuksellisuus:** Tietoja suojataan luvattomalta käytöltä. Tämä tarkoittaa esimerkiksi käyttöoikeuksien hallintaa ja fyysisen pääsyn rajoittamista tietoresursseihin.
- **Eheys:** Tieto, tietojärjestelmät ja arkistot ovat luotettavia, oikeellisia ja ajantasaisia. Toisin sanoen tieto ei ole muuttunut teknisen vian seurauksena tai tietoa ei ole muutettu ihmisen toimesta tahallisesti tai tahattomasti.
- **Saatavuus:** Tieto ja tietojärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille ja tietojärjestelmille, sovituilla tavoilla ja sovittuun aikaan.
- **Pääsynvalvonta:** Tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa eikä arkistotiloihin tai vastaaviin pääse ilman kontrolloitua pääsynvalvontaa.
- **Tietoturvasuunnittelu:** Tietoturva huomioidaan jo tietojärjestelmien ja - sovellusten suunnitteluvaiheessa.
- **Koulutus ja tietoisuus:** Käyttäjiä ja henkilökuntaa on koulutettava tunnistamaan tietoturvauhat ja toimimaan niiden mukaisesti.
- **Säädökset ja määräykset:** Tietoturvallisuusvaatimuksiin on noudatettava sovellettavia lakeja ja asetuksia. Tietoturvallisuus vaatii jatkuvaa päivitystä ja kehitystä vastatakseen muuttuviin uhkiin ja haasteisiin.

3.1. Tietosuojan periaatteet

Tietosuoja perustuu EU:n yleiseen tietosuoja-asetukseen GDPR (679/2016) ja tietosuojalakiin (1050/2018). Tietosuoja on osa toiminnan vaatimustenmukaisuutta, tietoturvallisuutta ja riskienhallintaa. Hyvin organisoitu tietosuojatyö on nykyaikaisen organisaation tuottavuuden, luotettavuuden ja tehokkuuden yksi tärkeä tekijä.

Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista ja henkilötietojen oikeaoppista käsittelyä niin, että henkilön yksilöivää tietoa ei paljastu siihen oikeudettomille missään tiedon elinkaaren vaiheessa. Kunnassamme tämä tarkoittaa henkilöstön, asiakkaiden sekä sidosryhmien henkilötietojen suojaamista. Tietosuoja kattaa myös vaitiolovelvollisuuden piiriin kuuluvan tiedon käsittelyn.

Rekisterinpitäjä on vastuussa henkilötietojen lainmukaisesta käsittelystä ja myös määrittelee mihin tarkoituksiin ja millä keinoin henkilötietoja käsitellään. Rekisterinpitäjällä on osoitusvelvollisuus toiminnan lainmukaisuudesta, jota toteutetaan dokumentaation avulla (mm. tietosuojaselosteet).

EU:n tietosuoja-asetuksen mukaisesti henkilötietoja:

- Kerätään ainoastaan ennalta määriteltyjen käyttötarkoitusten kannalta tarpeellisia henkilötietoja kunnan tehtävien suorittamiseksi ja palveluiden kehittämiseksi.

- On selkeä kokonaiskuva hallussa olevista henkilötiedoista ja niiden käsittelyyn sisältyvistä riskeistä.
- Huolehditaan suunnitelmallisesti ja läpinäkyvästi henkilötietojen elinkaaren hallinnasta ja suojaamisesta.
- Varmistetaan säännöllisten koulutusten avulla, että henkilöstöllä on riittävä tietosuojaosaaminen tehtävänkuvan mukaisesti.
- Asiakkailla on mahdollisuus omien henkilötietojen tiedonsaantiin ja heitä informoidaan henkilötietojen käsittelyperiaatteista.
- Arvioidaan jatkuvasti henkilötietojen käsittelyyn liittyviä riskejä yksilöiden oikeuksille ja vapauksille.
- Varmistetaan, että sopimuskumppanimme noudattavat vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

4. Roolit ja vastuut

Tietoturva ja -suojapolitiikka koskee kaikkea Askolan kunnan toimintaa ja se velvoittaa Askolan kunnan koko henkilöstöä, johtoa, luottamushenkilöitä, viranhaltijoita, sekä muita kunnan tietoja käsitteleviä henkilöitä. Tietoturvan ja tietosuojan toteuttaminen on jatkuvaa, tarkoittaen hyvien periaatteiden ja yhteisten ohjeiden noudattamista sekä tietoturvan ja -suojan huomioimista kaikessa tekemisessä. Kunnan tietoturva- ja tietosuojaperiaatteita sovelletaan myös hankkeisiin ja esimerkiksi pilotointeihin. Kunnanhallituksella ja kunnanjohtajalla on ylin vastuu tietoturvasta ja -suojasta, riskienhallinnasta sekä varautumisesta.

Kunnanhallitus	• Toimii kunnassa ylimpänä kokonaisturvallisuudesta päättävänä elimenä ja omistajana • Hyväksyy politiikkatasoiset asiakirjat • Kokonaisturvallisuuden toteutumisen seuranta ja ohjaus
Kunnanjohtaja	• Luo edellytykset tietosuojan asianmukaiselle toimeenpanolle • Raportoi kunnanhallitukselle
Toimialajohto	• Vastaa tietosuojan toteutuksesta johtamansa toiminnan osalta. • Nimeää vastuualueensa tietojärjestelmien omistajat • Ylläpitää tietoutta tietosuojaan vaikuttavista laeista ja säädöksistä johtamansa toiminnan osalta

Tietoturvan ja tietosuojan työryhmä	• Kehittää ja edistää organisaation tietoturvan ja tietosuojan toteutumista ja seuraa sitä vuosikellon mukaisesti • Seuraa tietoturvallisuuden ja tietosuojan yleistä kehittymistä, toimintaympäristön ja lainsäädännön muutoksia ja arvioi kokonaisvaltaisesti tietoturva- ja tietosuojariskejä • Koordinoi tietoturvariskien ja tietoturvapoikkeamien hallinnointia • Toteuttaa ja tukee tietoturvallisuuteen liittyvää viestintää
Esihenkilöt	• Vastaa omassa yksikössään annettujen ohjeiden ja määräysten noudattamisesta • Huolehtii työntekijöidensä perehdytyksestä, sitoumusten allekirjoittamisesta ja vuosittaisten koulutuksen suorittamisesta tietosuojan osalta • Huolehtii tietojärjestelmien käyttöoikeuksien hakemisesta, hyväksymisestä, muuttamisesta ja poistamisesta • Ilmoittaa mahdollisista tietosuojapoikkeamista tietosuojavastaavalle • Ilmoittaa mahdollisista tietoturvapoikkeamista it-tukeen
Henkilöstö/ jokainen työntekijä	• Käsittelee tietoja annettujen ohjeiden ja määräysten mukaisesti • Allekirjoittaa tietosuojasitoumuksen ja suorittaa vuosittaisen koulutuksen sovitussa aikataulussa • Ilmoittaa viipymättä havaitsemistaan tietoturvan/tietosuojan poikkeamista, ongelmista tai ohjeiden vastaisesta menettelystä.
Luottamushenkilöt	• Huolehtii tietoturvan toteutumisesta omissa luottamustehtävissään.
Asiakirjahallinnosta vastaava	• Ohjaa ja kehittää asiakirjahallintoa osana koko kunnan tiedonhallintaa, tietoturvallisuus huomioiden • Ohjaa toimialoja asiakirjahallinnon hoidossa, jotta arkistolain 7§ toteutuu oikeusturva ja tietosuoja huomioituna • Hyväksyy asiakirjallisten tietoaineistojen hallinnan edellyttämät arkistonmuodostus- ja tiedonohjaussuunnitelmat

	• Vastaa päätearkistoon luovutetusta pysyvästi säilytettävästä tietoaineistosta ja sen tietoturvallisuudesta ja tietosuojasta
Tiedon tai tietojärjestelmän omistaja	• Vastaa omistukseensa liittyvästä käyttäjien ja heidän käyttöoikeuksiensa määrittelystä ja hyväksynnästä • Riskienhallinnan toteuttamisesta • Vastaa tiedon eheydestä ja luokittelusta (julkisuuden ja salassapidon määrittely sekä arkistonmuodostus) käyttäen apuna tarvittavia asiantuntijoita
Tietosuojavastaava	• Neuvoo henkilötietojen lainmukaisessa käsittelyssä ja auttaa henkilötietojen käsittelyn erityisasiantuntijana kunnan johtoa rekisterinpitäjän velvoitteiden toteuttamisessa • Valvoo tietosuojalainsäädännön ja hyvien tietosuojakäytänteiden noudattamista ja toimii yhteyspisteenä valvontaviranomaiselle
Tietotekniikan henkilöstö	• Soveltavat ja toteuttavat tietoturva ja -suojapolitiikkaa • Vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä
Rekisteröidyt	• Ovat tietoisia oikeuksistaan sekä vastuussa antamiensa tietojen oikeellisuudesta
Ulkoiset palveluntuottajat	• Sitoutuvat noudattamaan kunnan tietoturva- ja suojaohjeistusta

5. Tiedon ja tietojärjestelmien käyttö

Kunnassa käytetään tietojärjestelmiä, laitteita ja ohjelmistoja, joiden tietoturvallisuus on varmistettu. Ennen uusien ratkaisujen käyttöönottoa tulee varmistaa niiden tietoturvallisuus suhteessa käyttötarkoitukseen. Jokaiselle käyttöjärjestelmälle tulee nimetä pääkäyttäjä ja arvioida järjestelmään liittyvät riskit ja kriittisyys.

Käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myöntää esihenkilö kunkin työtehtävän hoitoa vaativassa laajuudessa. Käytettävät tietojärjestelmät ja laitteet on tarkoitettu vain työtehtävien hoitamiseen eikä niitä saa käyttää niin, että kunnan omistama tai hallinnoima tieto vaarantuu. Vaarantumisen aiheuttaja on ensisijaisesti korvausvastuussa kunnalle tai sen toiminnalle mahdollisesti aiheutetusta haitasta.

Vastuu käyttöoikeuksista on oikeudet myöntävällä toimialalla. Käyttäjätunnusten elinkaari on varmistettava niin, että kaikki käyttäjätunnuksiin ja käyttövaltuuksiin tehdyt muutokset ovat asianmukaisesti esihenkilön valtuuttamia ja valvomia. Esihenkilö huolehtii myös työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta, kun työntekijän palvelussuhde päättyy tai tehtävä muuttuu.

6. Tietoturvallisuuden osaaminen

Tietoturvallisuus merkitsee sitä, että koko kunnan henkilöstö ymmärtää, on tietoinen ja sitoutuu henkilötietojen käsittelyyn lain ja asetuksen sekä organisaation tietoturva- ja tietosuojapolitiikan ja annettujen ohjeiden mukaisesti. Tietoturva- ja tietosuojaosaamista ylläpidetään ja kehitetään aktiivisesti viestinnän, henkilöstön koulutuksen sekä ajantasaisen ohjeistuksen avulla.

Keskeistä on, että tietoturva- ja tietosuojaohjeistus sisältyy koko kunnan henkilöstön perehdytysprosessiin. Tarvittavien ulkoisten sidosryhmien tietoturva- ja tietosuojaosaamisesta vastaa kyseisen toimialan johto. On tärkeää, että kaikki, jotka käsittelevät kunnan omistamaa tai hallinnoimaa tietoa, saavat riittävät edellytykset tiedon asianmukaiseen käsittelyyn.

Jokainen työntekijä allekirjoittaa palvelussuhteen alkaessa tietoturva- ja tietosuojasitoumuksen ja esihenkilö huolehtii uudessa tehtävässä aloittavan työtekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin sekä työntekijän omissa työtehtävissä tarvittavaan erityisosaamiseen. Esihenkilö huolehtii myös siitä, että työntekijät suorittavat vuosittain tietoturvan ja tietosuojan perusteista Navisec-verkkokoulutuksen ja -testin sekä osallistuvat mahdollisesti muihin tarvittaviin tietosuojakoulutuksiin. Työnantajan tulee huolehtia, että tietosuojaohjeet ovat kaikkien työntekijöiden saatavilla intranetissä. Tietoturvallisuuden ja tietosuojan ylläpidosta, kehittämisestä ja johtamisesta vastaaville tulee myös tarjota riittävä koulutus tehtävien hoitamista varten.

7. Ohjaava lainsäädäntö

Tärkeimmät lait, asetukset ja valtakunnalliset ohjeistukset:

- EU:n yleinen tietosuoja-asetus (679/2016)
- Tietosuojalaki (1050/2018)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Arkistolaki (831/1994)
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- Laki digitaalisten palvelujen tarjoamisesta (306/2019)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- VAHTI-ohjeet

- Tiedonhallintalautakunnan suositukset ja ohjeet https://vm.fi/tiedonhallinta-lautakunta

Uudistuvat säädöstekstit löytyvät ajantasaisina mm. Valtion säädöstietopankki – sivustolta (www.finlex.fi)

Myös tiedonhallintalaki (906/2019) ohjaa laajasti tiedon käsittelyä kunnassa. Siinä on määritelty osa-alueita ja tehtäviä kunnalle:

1. Tiedonhallintayksikön perustaminen ja vastuiden määrittely, tiedonhallintamallin laatiminen ja muutosvaikutusten arviointi.

- Tämä tietoturva- ja tietosuojapolitiikka on osa tiedonhallintalain edellyttämää dokumentointia ja vastuiden määrittelyä.
- Lain edellyttämä ohjeistus tietoturvan ja tietosuojan osalta on kuvattu dokumentin lopussa.
- Tiedonhallintamallissa kuvataan tiedon käsittelyn, tietojärjestelmien, tietoturvan ja myös tietosuojan hallinta organisaatiossa. Se antaa kuvan tiedon elinkaaresta, sen keruusta tiedon hävittämiseen saakka.

2. Tietoturvavaatimukset (voimaan 1.1.2023).

- Kunnassa tulee olla lain edellyttämällä tasolla mm. tietojärjestelmien turvallisuus, tietojen turvallinen siirtäminen tietoverkoissa, tietoaineistoturvallisuus, henkilöstöturvallisuusselvitykset, käyttöoikeuksien hallinta sekä lokien kerääminen.
- 3) Tietoaineistojen digitalisointi, digitaalisen tiedon käsittely, luovuttaminen ja vastaanottaminen.
- Kunta valmistautuu tiedon sähköiseen siirtoon viranomaisten välillä valtakunnallisen ohjeistuksen mukaisesti ja edistää tiedon säilyttämistä sähköisessä muodossa.

8. Menettely tietoturvallisuuden vaarantuessa

Tietoturvallisuuden vaarantuessa toimintatapa riippuu siitä, onko kyseessä henkilötietoja vai ei. Tietosuojaloukkaukseksi katsotaan henkilötietojen käsittelyä koskevien lakien ja asetusten, tämän politiikan sekä kunnan tarkempien periaatteiden ja ohjeistusten vastaista toimintaa. Jokaisella kunnan työntekijällä on velvollisuus ilmoittaa havaitessaan mahdollisen tietosuoja- tai tietoturvaloukkauksen. Ilmoitus tehdään omalle esihenkilölle, joka tarvittaessa vie asian eteenpäin it-tukeen ja/tai tietosuojavastaavalle. Pelkkä epäily tietosuoja- tai tietoturvaloukkauksesta riittää asian selvittämiseen. Ilmoituskynnyksen tulee olla matala ja työntekijöillä tieto siitä, miten tilanteessa toimitaan.

Jos tietosuojaloukkauksesta todennäköisesti aiheutuu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski, rekisterinpitäjän on ilmoitettava siitä rekisteröidyille ja

valvontaviranomaiselle ilman aiheetonta viivytystä. Askolan kunnan tietosuojavastaava toimii yhteyshenkilönä valvontaviranomaiselle (tietosuojavaltuutettu). Tarvittaessa ilmoittaminen rekisteröidyille, joita tietosuojaloukkaus koskee, tapahtuu tietosuojavastaavan, rekisterin vastuuhenkilön ja tietojärjestelmän pääkäyttäjän yhdessä sopimalla tavalla. Poikkeamisen tai rikkomuksen käsittelyssä on tärkeää käydä läpi, miten ja missä virhe on tapahtunut. Virheiden paljastuminen on tärkeää, pahempaa on, jo ne jäävät huomaamatta tai ilmoittamatta. Tilanteista on tärkeä ottaa opiksi ja kehittää toimintaa niin, ettei sama virhe pääse tapahtumaan toiste.

Tietoturvarikkomuksista ja tietosuojaloukkauksista voi olla seurauksena käyttöoikeuksien rajoituksia, palvelussuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä seuraamuksia. Palvelussuhteeseen vaikuttavista seuraamuksista on säädetty ensi sijassa työsopimuslaissa ja viranhaltijalaissa. Sovellettavaksi voivat tulla myös rikos- ja vahingonkorvauslainsäädäntö. Seuraamuksia arvioitaessa moitittava toiminta, sen vaikutukset ja seuraukset käsitellään kokonaisuutena.

Tietoturva- ja tietosuojapoikkeamien sekä mahdollisten väärinkäytöksien selvittämisessä ovat mukana tietosuojavastaava, toimialajohto sekä tarvittaessa tietotekniikan asiantuntijat. Asian ja tehtävän selvittämiseksi heille on mahdollistettava pääsy tarvittavaan tietoon.

9. Tietoturvallisuus on osa kokonaisturvallisuutta

Turvallisuusnäkökulma tulee huomioida kaikissa varautumiseen ja jatkuvuudenhallintaan liittyvissä suunnitelmissa kuten,

- Jatkuvuussuunnitelmat toiminnan kannalta elintärkeille palveluille, toiminnoille ja tietojärjestelmille niiden jatkuvuuden turvaamiseksi.
- Toipumissuunnitelmat kriittisille tietojärjestelmille ja -verkoille niiden mahdollisimman nopean toipumisen, toiminnan uudelleenaloittamisen ja jatkamisen varmistamiseksi.
- Valmiussuunnitelma toiminnan, palveluiden ja järjestelmien hallinnoimiseksi häiriö- ja poikkeusoloissa (kriittiset tietojärjestelmät nimetään valmiussuunnitelmassa).
- Lakisääteiset pelastussuunnitelmat ihmisten ja omaisuuden suojelemiseksi, sekä vahinkojen minimoimiseksi onnettomuustilanteissa.

Varautumista toteutetaan testaamalla, harjoittelemalla ja ylläpitämällä tarvittavia valmius- ja muita suunnitelmia myös tietoturvallisuuden osalta. Jolloin toiminnan häiriöihin ja keskeytyksiin voidaan varautua niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, rajoittaa häiriöiden haittavaikutuksia sekä toipua häiriöistä mahdollisimman nopeasti.

EU:n yleinen tietosuoja-asetus edellyttää vaikutuksen arvioinnin (DPIA) tekemistä. Vaikutustenarvioinnin tarkoituksena on kuvata henkilötietojen käsittelyä, arvioida käsittelyn tarpeellisuutta ja oikeasuhteisuutta sekä arvioida henkilötietojen käsittelystä aiheutuvia riskejä ja tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutusten arviointia on tehtävä, kun henkilötietojen käsittelyyn kohdistuu korkea riski, esimerkiksi silloin, kun käsitellään suuria määriä arkaluonteisia tietoja tai käytetään uutta teknologiaa. Vaikutustenarviointi tulee ottaa osaksi toiminnan ja hankintojen suunnittelua niin, että mahdollisimman aikaisessa vaiheessa tiedostetaan, milloin vaikutustenarviointi on tarpeen tehdä.

10. Seuranta, ylläpito ja kehittäminen

Askolan kunta suunnittelee ja seuraa tietosuojatyötä laaditun vuosikellon mukaisesti. Suunnitelmassa toteutettavat tehtävät on jaettu toteutettavaksi pitkin vuotta. Vuosisuunnitelman pohjalta tehtäviä voidaan delegoida vastuussa oleville henkilöille. Vuoden lopussa kunnan tietosuojatyö kootaan tietotilinpäätökseen. Tietotilinpäätös on kunnan tilinpäätöksen liitteenä, jonka hyväksyy kunnan valtuusto.

11. Voimassa olevat ohjeet ja sitoumukset

- Tietosuoja ja salassapitositoumus
- Työaseman käyttäjän tietoturvaohje
- Ohje sähköposteista