



TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Kunnanhallitus 30.4.2025

Sisällys

1. Johdanto	3
2. Tietoturvallisuus	3
3. Tietosuoja	5
4. Tietoturvaluustavoitteet	5
5. Organisointi ja tietoturvastuut	5
6. Tiedon ja tietojärjestelmien käyttö	7
7. Riskiperusteinen lähestymistapa	7
8. Tietoturvaosaamisen varmistaminen	8
9. Tietoturva ja tietosuoja hankinnoissa ja sopimuksissa	8
10. Lokitietojen kerääminen	9
11. Tietoturvapoikkeamien käsittely ja niistä tiedottaminen	9
12. Tietoturvallisuuden seuranta, ylläpito ja kehittäminen	9
13. Tekoälyteknologioiden käyttäminen	10
14. Puolangan kunnan henkilöstöä koskevat tarkennukset	11
<i>Henkilöstöä koskeva tietoturva</i>	<i>11</i>
<i>Tietosuoja- ja tietoturvasitoumus</i>	<i>11</i>
<i>Käyttäjähallinta</i>	<i>11</i>
<i>Kunnan sähköpostin käyttäminen</i>	<i>11</i>
<i>Etätyö / Liikkuva työ ja mobiililaitteet</i>	<i>11</i>

1. Johdanto

Tieto on keskeisessä roolissa 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. Poliitiikka toimii perustana 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 kunnan intranetissä.

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

2. Tietoturvallisuus

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

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

Tietoturvallisuuteen liittyvillä vastuutuksilla ja käytännöillä pyritään varmistamaan, että Puolangan 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.

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)
- Kunnan voimassa oleva strategia, hallintosääntö, sisäisen valvonnan ja riskienhallinnan ohje, valmius- ja viestintäsuunnitelma (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 organisaation riskienhallintaa, varautumista ja kokonaisturvallisuutta. Riskienhallintaa toteutetaan kunnan sisäisen valvonnan ja riskienhallinnan ohjeen mukaisesti.

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 tietoturvatoumenpiteitä. Tietoturvan hallinnan taso on asetettu noudattamaan lainsäädännöllisiä veloitteita. Organisaatio tunnistaa ja hallitsee tietoturvan uhkatekijöitä proaktiivisesti. Uhkatekijöiden hallinta perustuu jatkuvaan seurantaan ja analysointiin, jotta poikkeamat voidaan havaita ja käsitellä ajoissa.

3. 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.

Kunta käsittelee henkilötietoja vain perustellun käyttötarkoituksen vuoksi 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.

Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Henkilöstön tietosuojaosaamisesta huolehditaan koulutuksilla sekä työroolin mukaisilla ohjeistuksilla. Kunta mahdollistaa asiakkaille tiedonsaannin omiin henkilötietoihinsa sekä informoi henkilötietojen käsittelystä kunnan verkkosivuilla. Kunnan henkilörekistereitä käsittelevät sopimuskumppanit velvoitetaan noudattamaan vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

4. Tietoturvallisuustavoitteet

Kunta noudattaa Tiedonhallintalain (906/2019) asettamia vaatimuksia. Tässä yhteydessä otetaan huomioon, että tiedonhallintaa koskeva lainsäädäntö ja siihen liittyvät kansalliset suositukset ovat muutoksessa ja sisältävät useita siirtymäaikoja.

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.

5. Organisointi ja tietoturvavastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu kunnan sääntöjen mukaisesti.

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

Kunnan johdolla on kokonaisvastuu tietoturvallisuuden toteuttamisesta. Tietoturvallisuuden toteutumisen raportoinnista kunnanhallitukselle vastaa hallintojohtaja. Tukena tietoturvallisuus-asioissa ovat toimialajohtajat sekä tiedonhallinta-asiantuntija.

Toimialojen johtajat vastaavat vastuualueidensa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

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

- ✓ oman toimialansa perehdyttämisestä kunnan tietoturvaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturvavastuuihin.
- ✓ työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
 - kunnan tiedon ja muun omaisuuden palauttamisesta
 - työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta.

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 tietosuojavastaavalle, ICT-palveluntuottajan asiakastukeen ja omalle esihenkilölleen. 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 hakee työntekijän esihenkilö tai muu vastaava henkilö hakemuksen perusteella. Tietojärjestelmän omistaja on tietojärjestelmästä vastaava toimialajohtaja.

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

Tietosuojavastaava antaa tietoa ja neuvoja tietosuojaan liittyvissä asioissa, seuraa tietosuoja-asetuksen ja kansallisten tietosuoja koskevien lakien noudattamista, tekee yhteistyötä valvontaviranomaisen kanssa ja toimii valvontaviranomaisen ja rekisteröityjen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tietosuojavastaava vastaa tietosuojaan liittyvästä viestinnästä. Tietosuoja säännösten noudattaminen on aina rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla. Tietosuojavastaava ei ole erikseen henkilökohtaisesti vastuussa tietosuoja-asetuksen rikkomisesta.

Palveluntuottajat vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumisesta ICT-ympäristössä ja tietojärjestelmissä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.

Palveluntuottajat noudattavat Puolangan kunnan tietoturvapoliittikkaa sekä sopimusten tietoturva- ja tietosuojaliitteitä.

6. Tiedon ja tietojärjestelmien käyttö

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 kunnan tiedossa ja hyväksymiä.

Käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon, fyysisiin tiloihin sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Käyttöoikeudet toteutetaan kunnassa roolipohjaisesti käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan. Vastuu käyttöoikeuksien myöntämisestä on aina kunnalla. Tärkeintä on varmistaa, että käyttäjätunnusten elinkaari on hallittavissa siten, että kaikki käyttäjätunnuksiin ja käyttövaltuuksiin tehdyt muutokset ovat asianmukaisesti kunnan valtuuttamia, dokumentoituja ja valvottuja. Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi kunnan 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. Kunnan tietojen käsittelyohjeita tulee noudattaa. Kunnan tietojen käsittelyohjeita sekä tietoturva- ja tietosuojaperiaatteita ja ohjeita sovelletaan myös hankkeisiin ja pilotteihin.

7. 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. Tietoturvatoinimia tulee mitoittaa sekä järjestelmän tietosisällön, että kunnan kriittisten prosessien näkökulmasta. Tietoaineistoihin, tietovarantoihin ja tietojärjestelmiin kohdistuvia riskejä tulee tarkastella osana kokonaisturvallisuuteen liittyvää riskianalyysyä ja suunnittelua.

8. 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 työntekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin ja siihen, miten tietoturvallisuus tulee huomioida hänen omissa työtehtävissään. Tietoturvallisuuden peruskoulutusta tarjotaan säännöllisesti. Tietoturva- ja tietosuojaohjeet pidetään kaikkien työntekijöiden saatavilla. Koulutukset kattavat tietoturvan perusperiaatteet, ajankohtaiset uhat ja parhaat käytännöt.

Työntekijät suorittavat tietoturva- ja tietosuojakoulutuksen kunnan laatiman suosituksen mukaisesti.

9. Tietoturva ja tietosuoja hankinnoissa ja sopimuksissa

Hankinnoissa tulee noudattaa hankintalainsäädäntöä, kunnan hankintaohjeistusta sekä julkishallinnon yleisiä suosituksia ICT-hankintojen ja hankinnan kohteiden tietoturvan huomioimisesta. Erityistä huomiota tulee kiinnittää siihen, että tieto- ja viestintätekniset hankinnat sopivat 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 tietoa-aineistojen 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 kunnan tietoturva- ja tietosuojaliitteet. Kyseisten sopimusvelvoitteiden lisäksi hankinnassa tulee huomioida tietoturvavaatimukset tarkemmalla tasolla tämän tietoturva- ja tietosuojapolitiikan mukaisesti.

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

Lähtökohtaisesti kunnan sopimuksissa ja hankinnoissa käytetään kunnan omaa tietosuojaliitettä. Tietosuojaliite tai muut tietosuoja-asetuksen 28 artiklan vaatimukset täyttävät

ehdot sisällytetään kaikkiin uusiin sopimuksiin, joiden perusteella käsittelijä käsittelee henkilötietoja kunnan lukuun. Tietosuojalainsäädännön asettamia ehtoja ja niiden toteutumista tulee valvoa.

10. 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 eväty, 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.

11. 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 kunnan 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.

12. 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 kunnan 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 virkatyönä. Merkittävät muutokset tietosuoja- ja turvapolitiikkaan käsitellään kunnanhallituksessa.

13. Tekoälyteknologioiden käyttäminen

Tekoälyteknologioiden käyttö organisaation toiminnassa edellyttää erityistä huomiota tietoturvaan ja tietosuojaan. Tekoälyjärjestelmien kehittämisessä ja käytössä tulee noudattaa seuraavia periaatteita:

- **Läpinäkyvyys:** Tekoälyjärjestelmien toiminnan tulee olla läpinäkyvää ja selitettävää. Käyttäjille tulee tarjota riittävästi tietoa tekoälyn toiminnasta ja sen päätöksenteon perusteista.
- **Tietojen anonymisointi:** Tekoälyjärjestelmissä käytettävät henkilötiedot tulee anonymisoida aina kun mahdollista, jotta yksityisyyden suoja voidaan varmistaa.
- **Eettisyys:** Tekoälyn käyttöön liittyvät eettiset kysymykset tulee huomioida ja varmistaa, että tekoälyjärjestelmät toimivat oikeudenmukaisesti ja syrjimättömästi.
- **Riskienhallinta:** Tekoälyjärjestelmien käyttöön liittyvät riskit tulee arvioida ja hallita huolellisesti. Tämä sisältää mahdollisten tietoturvaauhkien tunnistamisen ja niihin varautumisen.
- **Jatkuva seuranta ja arviointi:** Tekoälyjärjestelmien toimintaa tulee seurata ja arvioida jatkuvasti, jotta voidaan varmistaa niiden tietoturvallisuus ja tietosuoja.

Kunnan tietoturvapoliitikassa on huomioitava tekoälyjärjestelmien riskienhallinta ja varmistettava, että tekoälyjärjestelmät ovat turvallisia ja luotettavia. Tekoällysäädös korostaa henkilötietojen suojaa ja edellyttää, että tekoälyjärjestelmät noudattavat GDPR:n vaatimuksia. On varmistettava, että tekoälyjärjestelmät käsittelevät henkilötietoja asianmukaisesti ja että tietosuoja on otettu huomioon kaikissa tekoälyjärjestelmissä. Tekoällysäädös vaatii, että tekoälyjärjestelmät ovat läpinäkyviä ja selitettäviä. On varmistettava, että käyttäjät ymmärtävät, miten tekoälyjärjestelmät toimivat.

14. Puolangan kunnan henkilöstöä koskevat tarkennukset

Kunta osallistuu Kainuun kuntien ja Kainuun liiton tiedonhallinnan ja tietosuojan ohjausryhmän toimintaan. Lisäksi Puolangan kunta hankkii ICT-asioissa neuvonantajapalvelua kolmannelta osapuolelta.

Talous- ja henkilöstöhallinnan ohjelmien riskinhallinnasta vastaa myös talous- ja henkilöstöhallinnon palveluntuottaja.

Tietosuojavastaavana toimii tiedonhallinta-asiantuntija ja tietosuojavastaavan sijaisena hallintojohtaja.

Henkilöstöä koskeva tietoturva

Tietoturvapoliittikka sisältää koko kunnan henkilöstölle tarkoitetut tietoturvallisuuteen liittyvät perusasiat sekä neuvoja tietoturvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tilanteissa.

Tietosuoja- ja tietoturvasitoumus

Työasemien, tietoliikenneverkon ja tietojärjestelmien käyttöoikeudet annetaan vain niille, jotka ovat allekirjoittaneet työsopimuksen ja tässä yhteydessä salassapitositoumuksen.

Käyttäjähallinta

Henkilöstölle sallitaan vain sellaisten tietojärjestelmien käyttäminen, joita hän työnsä puolesta tarvitsee. Käyttöoikeuslomakkeita voivat käyttää ja muokata esihenkilöt. Kunnalla on oikeus seurata ja rajoittaa tunnusten käyttöä.

Kunnan sähköpostin käyttäminen

Kunnan sähköpostia on mahdollista käyttää työasemalta tai mobiililaitteilla.

Etätyö / Liikkuva työ ja mobiililaitteet

Etätyössä tulee noudattaa Puolangan kunnan etätyöohjeistuksen tietoturvakäytäntöjä. Tietoturvallisuudessa noudatetaan voimassa olevia lakeja ja määräyksiä. Työntekijän on sitouduttava noudattamaan etätyössä samaa salassapitovelvollisuutta, jota häneltä työssä ollessa normaalistikin edellytetään.

Etätyössä tai muualla työskennellessään työntekijän on myös itse arvioitava etätyöympäristön turvallisuutta. Esim. mobiilisähköpostin käyttäminen voi mahdollistaa sähköpostin käyttämisen käyttäjän ollessa poissa työasemansa äärestä. Tällöin on kiinnitettävä erityistä huolellisuutta laitteen säilytykseen ja tilaturvallisuuteen.

Etätyössä työntekijän tulee käyttää vain hyväksyttyjä laitteita ja ohjelmistoja. Kaikki yhteydet tulee suojata vahvalla salauksella organisaation VPN-palvelua käyttämällä.

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.