PUOLANGAN KUNNAN TIETOTURVAPOLITIIKKA

Voimassa 1.10.2022 alkaen

Kunnanhallitus 18.8.2022

PUOLANKA
SITKEÄÄ SORTTIA

Sisällys

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. Politiikka toimii perustana kunnan tietoturvallisuutta ja tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja auttaa niiden käytäntöön soveltamisessa. Tietoturvapolitiikka 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. Politiikka kattaa kunnan käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta 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 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 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)

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:

- Kuntia velvoittavat lait ja asetukset, mm. Laki julkisen hallinnon tiedonhallinnasta (906/2019)

• EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR)

• 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

Tietoturvallisuus on osa kunnan 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.

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.

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. Kunta mahdollistaa asiakkaille tiedonsaannin omiin henkilötietoihinsa sekä informoi henkilötietojen käsittelystä kunnan verkkosivuilla. Kunnan henkilörekistereitä käsittelevät sopimuskumppanit velvoitetaan noudattamaan vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

4 Tietoturvallisuustavoitteet

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.

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 ohjeistus.

5 Organisointi ja tietoturvavastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu kunnan sääntöjen mukaisesti.

Kunnanhallitus seuraa tietoturvallisuuden toteutumista kunnassa. Kunnanhallitus hyväksyy tietoturvapolitiikan 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. Kunnanjohtajan tukena tietoturvallisuusasioissa on kunnan tietoturva- ja tietosuojatyöryhmä.

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

Esimies vastaa tietoturvallisuuden toteutumisesta omalla vastuualueellaan. Esimiehen keskeisimpinä tehtävinä on huolehtia:

• oman organisaationsa perehdyttämisestä kunnan tietoturvaohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin tietoturvavastuisiin.

• työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:

o kunnan tiedon ja muun omaisuuden palauttamisesta

o 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 Atean asiakastukeen ja omalle esimiehelleen. 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 henkilön esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho. Tietojärjestelmän omistaja on tietojärjestelmästä vastaava toimialan tulosalueen tai toimintayksikön esimies.

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

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 kunnan tietoturvapolitiikkaa sekä sopimusten tietoturva- ja tietosuojaliitteitä.

6 Tiedon ja tietojärjestelmien käyttö

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

Käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Käyttöoikeudet toteutetaan kunnalla roolipohjaisesti käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan. Vastuu käyttöoikeuksista on aina sillä toimialalla tai liikelaitoksella, joka ne myöntää. Tärkeintä on varmistaa, että käyttäjätunnusten elinkaari on hallittavissa siten, että kaikki käyttäjätunnuksiin ja käyttövaltuuksiin tehdyt muutokset ovat asianmukaisesti esimiehen valtuuttamia, dokumentoituja ja valvottuja. Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi kunnan ohjeita. Henkilötietojen käsittelyssä noudatetaan voimassa olevaa lakia ja tietosuojaa ohjaavia periaatteita.

Esimiehen tulee huolehtia käyttöoikeuksien asianmukaisuudesta ja ajantasaisuudesta. Työntekijän palvelussuhteen päättyessä tai tehtävien muuttuessa esimies huolehtii työntekijän käyttöoikeuksien ja -valtuuksien poistamisesta.

Tiedolla on aina omistaja. Tiedon omistaja vastaa tiedon luokittelusta ja oikeasta käsittelystä. Kunnan tietojen käsittelynohjeita 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. Tietoturvatoimia tulee mitoittaa sekä järjestelmän tietosisällön, että kunnan kriittisten prosessien näkökulmasta. Tietoaineistoihin, tietovarantoihin ja tietojärjestelmiin kohdistuvia riskejä tulee tarkastella osana kokonaisturvallisuuteen liittyvää riskianalyysiä 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.

Esimies 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.

Kunnan työntekijät suorittavat omatoimisen 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 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 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 palvelutuottajia tai muita henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet. Käsittelyn on täytettävä tietosuoja-asetuksen vaatimukset ja varmistettava rekisteröidyn oikeuksien suojelu. Lähtökohtaisesti kunnan sopimuksissa ja hankinnoissa käytetään kunnan 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 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.

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

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.

Tietoturvapolitiikka katselmoidaan vuosittain ja päivitetään tarvittaessa.

LIITE 1: Puolangan kuntaa koskevat tarkennukset

Mitä edellä todetaan kunnanjohtajasta, tarkoittaa Puolangalla pormestaria. Puolangan kunnalla ole liikelaitoksia. Mitä edellä todetaan ATEA:sta koskisi palveluntuottajan mahdollisesti vaihtuessa kunnan silloista ICT-palveluiden tuottajaa.

Kunnan tietoturva- ja tietosuojatyöryhmällä tarkoitetaan pormestaria, tiedonhallinta-asiantuntijaa, hallintojohtajaa ja kunnan ICT-palveluiden tuottajan tietosuojasta vastaavaa henkilöä. Lisäksi 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 riskinhallinasta vastaa myös talous- ja henkilöstöhallinnon palveluntuottaja.

Tietosuojavastaavana toimii tiedonhallinta-asiantuntija ja tietosuojavastaavan sijaisena hallintojohtaja.

Henkilöstöä koskeva tietoturva

Tietoturvapolitiikka ja sen liitteet sisältävät koko kunnan henkilöstölle tarkoitetut tietoturvallisuuteen liittyvät perusasiat sekä neuvoja tietoturvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tilanteissa.

Tietosuoja- tietoturvasitoumus

Työasemien, tietoliikenneverkon ja atk-järjestelmien 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 esimiehet. Kunnalla on oikeus seurata ja rajoittaa tunnusten käyttöä.

Kunnan sähköpostin käyttäminen

Kunnan sähköpostia on mahdollista käyttää työasemalta tai mobiililaitteella. Tällöin sähköpostia käytetään älypuhelimella tai kannettavan tietokoneen kautta.

Liikkuva työ ja mobiililaitteet

Liikkuvassa työssä 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.

PUOLANKA
SITKEÄÄ SORTTIA

LIITE 2: Tiedonhallintalain mukaisten tietoturvatoimenpiteiden toteuttaminen Puolangan kunnassa

Pykälä	Kuvaus	Lähde	Toteutusvastaava	Toteutustapa	Riski
Elinkaaren huomioiminen tietojen käsittelyssä 13§	Tietoturvallisuus tietoaineistojen elinkaaressa muodostaa kokonaisuuden, johon kuuluvat tiedon luokittelu, riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen. Tiedonhallintayksikön tulee arvioida tietoaineistoihin liittyviä riskejä säännöllisesti tietoaineistojen koko elinkaaren ajan sekä huomioitava muuttuneiden riskien edellyttämät toimenpiteet tietoturvaa koskevissa suunnitelmissa ja toteutuksissa. Ennen tiedon tuottamista tai vastaanottamista tulee huomioida tiedon määrittely, jossa arvioidaan tiedon ominaisuuksiin, turvallisuuteen ja metatietoihin liittyviä ominaispiirteitä. Tiedon määrittelyvaiheen perusteella muodostuvat tiedon käsittelyperiaatteet koko elinkaaren ajalle.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Hallintojohtaja; Tietosuojavastaava	Määritellään tiedon ominaispiirteet tiedonhallintajärjestelmää apuna käyttäen. Kunnalla käytössä myös yhteinen tietoturvapolitiikka.	Kyberhyökkäys; Tilaturvallisuus; Salaamattomat sähköpostit; Sähköverkon toimintakatko

Elinkaaren huomioiminen tietojärjestelmissä 13§	Tietoturvallisuus tietojärjestelmien elinkaaressa muodostaa kokonaisuuden, johon kuuluvat riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen. Tiedonhallintayksikkö arvioi tietojärjestelmiin liittyviä riskejä säännöllisesti niiden koko elinkaaren ajan sekä huomioi muuttuneiden riskien edellyttämät toimenpiteet tietoturvallisuuden suunnittelussa ja toteutuksessa.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Hallintojohtaja; Johtoryhmä; Tietosuojavastaava	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta.	Kyberhyökkäys; Tilaturvallisuus; Salaamattomat sähköpostit; Sähköverkon toimintakatko

Hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet 13,4§	Hankintoja ohjaaviin asiakirjoihin tulisi sisällyttää: hankinta-asiakirjojen käsittelyä koskevat ohjeet, joista ilmenee, mitä tietoturvallisuustoimenpiteitä hankinta-asiakirjojen käsittelyssä on noudatettava tiedonhallintayksikössä tarjouspyynnön mallipohja, joka sisältää tiedot tiedonhallintayksikössä noudatettavista yleisistä tietoturvallisuustoimenpiteistä riippumatta hankintakohteesta sopimusmallin, jonka perusteella hankintakohdekohtaisesti hankintaan suunnittelevan vastuuhenkilön on kuvattava asianmukaiset tietoturvallisuusvaatimukset ja -toimenpiteet tarvittavilta osin niin henkilö-, tietoliikenne-, tietojärjestelmä-, tietoaineisto- kuin toimitilaturvallisuuden osalta.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Atea; Hallintojohtaja; Pormestari; Tietosuojavastaava; Kunnanhallitus	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta.	Varkaus; Huolimattomuus; Kyberhyökkäys; Vaitiolovelvollisuuden rikkominen; Salaamattomat sähköpostit
Julkisuus ja salassapitorakenne on huomioitu tietovarantojen tietoraken	Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.	Tiedonhallintalaki	Hallintojohtaja; Tietosuojavastaava; Atea; Pormestari	Käytössä asianhallintajärjestelmä sekä tiedonhallintajärjestelmä	Varkaus; Huolimattomuus; Kyberhyökkäys; Vaitiolovelvollisuuden rikkominen; Salaamattomat sähköpostit

teissa, 13.3§					
Käyttöoikeudet on määritelty ja hallittu tietojärjestelmissä, 16§	Ainoastaan oikeutetuille käyttäjille sekä järjestelmille myönnetään pääsy- ja käyttöoikeus tietoihin ja tietojärjestelmiin. Käyttöoikeuksien hallinnan tulee noudattaa vähimpien oikeuksien periaatetta ja sen on katettava järjestelmien koko elinkaari. Vähimpien oikeuksien periaate tarkoittaa, että käyttäjälle annetaan tietojärjestelmiin vain sellaiset käyttöoikeudet ja -valtuudet, jotka ovat työtehtävien kannalta tarpeellisia. Käyttäjätilien hallintaa ja käyttöä seurataan ja valvotaan poikkeamien ja uhkien havaitsemiseksi sekä niihin reagoimiseksi. Seurannassa ja valvonnassa on huomioitava lokitietojen keräämistä ja käyttöä koskevat suositukset. Käyttöoikeuksien hallinnan edellytys on esimerkiksi, että käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Hallintojohtaja; Tietosuojavastaava; Pormestari	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta.	

Salassa pidettävät tiedot on suojattu yleisessä tietoverkossa tietoja siirrettäessä, 14.1§	Salausratkaisujen tulee perustua salassa pidettävän tiedon luokitteluun ja riskiarvioon. Salaus tulee toteuttaa kulloinkin voimassa olevien viranomaisvaatimusten ja suositusten mukaisesti. Tietoliikenne tulisi ideaalitilanteessa salata päästä päähän, eli esimerkiksi käyttäjältä tietojärjestelmään tai kahden tietojärjestelmän välillä. Mikäli tämä ei ole mahdollista, voidaan organisaatioiden verkkojen välinen yleisen tietoverkon osuus salata esimerkiksi VPN-ratkaisuilla, jolloin organisaatioiden sisäisten verkkojen osuus jää salaamatta. Lakitekstissä puhutaan salassa pidettävästä tiedosta ja yleisestä tietoverkosta. Lähtökohtaisesti kannattaa kuitenkin käsitellä kaikkea tietoa niin kuin se olisi salassa pidettävää ja salata tietoliikenneyhteydet aina oletusarvoisesti. Vastaavasti organisaatioiden omia verkkoja kannattaa käsitellä turvattomina verkkoina ja salata liikenne myös siellä samojen periaatteiden mukaan. Esimerkiksi avoimen HTTP-protokollan käyttöä sisäverkon julkistakin tietoa käsittelevissä järjestelmissä tulisi välttää. Lähtökohtaisesti tiedon vastaanottaja (ja pääsääntöisesti myös lähettäjä) tulisi tunnistaa vahvasti. Mikäli kyseessä on tietojärjestelmien välinen tietojensiirto, tapahtuu tämä tyypillisesti varmenteiden (sertifikaattien) avulla.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Hallintojohtaja; Tietosuojavastaava; Atea	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta. Organisaatiossa salassapidettäviä tietoja lähetetään vain suojatussa sähköpostissa.	Ilkivalta; Kyberhyökkäys; Vaitiolovelvollisuuden rikkominen; Salaamattomat sähköpostit; Sähköverkon toimintakatko

Tarpeelliset lokitiedot on kerätty tietojärjestelmien käytöstä ja luovutuksista, 17§	Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Lokitietojen perusteella voidaan selvittää virhetilanteita ja valvoa tietojärjestelmien käyttöä muun muassa oikeusturvan toteuttamiseksi, häiriötilanteesta toipumiseksi, virkavastuun todentamiseksi sekä häiriöiden ja riskin muodostavien poikkeamien tunnistamiseksi. Lokitietoja tarvitaan sekä normaali- että poikkeamatilanteissa. Normaalitilanteissa lokien avulla toteutetaan muun muassa toiminnan häiriöttömyyden seurantaa, käytönvalvontaa, tilastointia ja laskutusta. Poikkeustilanteissa lokeja käytetään muun muassa syiden selvittämiseen, tilanteen normalisointiin sekä tapahtumien ja niiden osapuolten tunnistamiseen. Lokitietoja ei kerätä ja käsitellä summittaisesti, vaan määritellyn tarpeen pohjalta laadittujen lokiperiaatteiden ja -suunnitelman mukaisesti. Lokitietoja tuotetaan ja kerätään tietojärjestelmän käytöstä ja tietojen luovutuksista, mutta missä laajuudessa ja mitä lokitietoja, perustuu tiedonhallintalain mukaiseen tarpeellisuusarviointiin. Tarpeellisuusarvioinnin tekee tietojärjestelmästä vastuussa oleva viranomainen.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Hallintojohtaja; Atea; Tietosuojavastaava	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta. Tietojen luovutukset on kuvattu tiedonhallintamallissa.	Ilkivalta; Kyberhyökkäys; Vaitiolovelvollisuuden rikkominen; Salaamattomat sähköpostit; Sähköverkon toimintakatko

Tehtävät, joiden suorittaminen edellyttää henkilöiltä erityistä luotettavuutta on tunnistettu, 12§	Erityistä luotettavuutta edellyttäviä tehtäviä voidaan tunnistaa esimerkiksi määrittämällä tilanteet, joissa henkilö käsittelee turvallisuusluokiteltavia tai merkittävässä määrin ja säännöllisesti salassa pidettäviä tietoja tai työskentelee tiloissa, joissa henkilön tietoon voi tulla muutoin kuin satunnaisesti turvallisuusluokiteltavia tai salassa pidettäviä tietoja.	Suosituskokoelma tiettyjen tietoturvaäännösten soveltamisesta, 8.11.2021	Atea; Johtoryhmä; Pormestari; Tietosuojavastaava	Työntekijä sitoutuu työ- virkasuhteessa vaitiolosopimukseen.	Varkaus; Huolimattomuus; Vaitiolovelvollisuuden rikkominen; Salaamattomat sähköpostit
Tietoaineistoja käsitellään riittävän turvallisissa tiloissa, 15.2§	Viranomaisen tulisi määritellä kullekin tietoaineistolle hyväksytyt sijainnit, joissa sähköisessä muodossa ja paperisina olevia aineistoja ja tietovarantoja voidaan käsitellä, säilyttää ja arkistoida. Sijaintien määrittelemisessä pitää huomioida palvelujen toteuttamistapa, kuten palveluntuottajat, pilvipalvelut ja tiedon käsittelyn fyysinen sijainti. Tyypillisesti palveluntarjoajat säilyttävät ja ylläpitävät tietojen ja tietojärjestelmien käsittelyssä tarvittavia fyysisiä tiloja ja laitteita. Tällöin palveluntarjoajien kanssa on varmistettava fyysisen turvallisuuden vaatimusten toteutuminen. Viranomaisen tulee huomioida, että erityyppisiin tietoaineistoihin (esim. salassa pidettävät tai henkilötiedot) kohdistuu erilaisia suojausvaatimuksia, jotka voivat aiheuttaa lisävaatimuksia palveluntarjoajaa tai viranomaista kohtaan.	Suosituskokoelma tiettyjen tietoturvaäännösten soveltamisesta, 8.11.2021	Atea; Johtoryhmä; Tietosuojavastaava	Käytössä tiedonhallintamalli, jossa eri arkistojen sijainnit on lueteltu.	Varkaus; Huolimattomuus; Ilkivalta; Kyberhyökkäys; Tilaturvallisuus; Salaamattomat sähköpostit

Tietoaineistojen turvallisuus on varmistettu, 15§	Tietoaineistojen turvaamiseen liittyvät toimenpiteet voidaan jakaa karkeasti kolmeen luokkaan: teknisiin, toiminnallisiin, hallinnollisiin. Teknisillä toimenpiteillä tarkoitetaan esimerkiksi palomuureja, salausmenetelmien käyttöä ja järjestelmien vahvistamista. Toiminnalliset tietoturvatoimenpiteet ovat esimerkiksi prosessikuvauksia. Hallinnolliset toimenpiteet ovat esimerkiksi ohjeistuksia, koulutuksia tai käyttöoikeuksien rajauksia. Tiedonhallintayksiköt voivat hyödyntää edellä mainittuja toimenpiteitä varmistaessaan tietoaineistojensa turvallisuutta.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Atea; Hallintojohtaja; Pormestari; Tietosuojavastaava	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta.	Ilkivalta; Kyberhyökkäys; Vaitiolovelvollisuuden rikkominen; Tilaturvallisuus; Salaamattomat sähköpostit; Sähköverkon toimintakatko
Tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettu, 13.2§	Olennaiset tietojärjestelmät kartoitetaan niitä varten laaditaan kriittisyysluokitus, jota tulee myös ylläpitää. Luokituksessa on huomioitava lakisääteiset tehtävät sekä riippuvuus muista järjestelmistä. Vikasietoisuttaa varmistetaan esimerkiksi testauksella ennen käyttöönottoa, järjestelmätestauksella ja hyväksymistestauksella, kuormitustestauksella, koodikatselmoinneilla, tietoturvatestauksilla, toipumissuunnittelulla Toiminnallisen käytettävyyden turvaamiseksi on varmistettava esimerkiksi, että tietojärjestelmä on helposti opittava ja toimintalogiikka on helposti muistettava, tietojärjestelmä tukee työtehtäviä, joihin sitä käytetään ja edistää käytön virheettömyyttä.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Hallintojohtaja; Atea; Tietosuojavastaava	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta.	Kyberhyökkäys

Tietoriskien hallinta ja siihen perustuvat tietoturvat oimet on järjestetty, 13.1§	Tietoriskien hallinta on jatkuvaa toimintaa, johon liittyvät tavoitteet, periaatteet, vastuut ja keskeiset menettelyt tiedonhallintayksikön on hyvä kuvata. Johdon vastuulla on tietoriskien hallinnan organisointi ja resursointi. Hallintaprosessi vaikuttaa tiedonhallintayksikön toiminnan ja tavoitteiden arviointiin ja suunnitteluun. Tietoriskien hallinnassa havaitut riskit vaikuttavat tiedonhallintayksikön toimenpiteisiin koko sen toiminnan ajan.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Atea; Hallintojohtaja; Pormestari; Tietosuojavastaava	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta.	Ilkivalta; Kyberhyökkäys; Salaamattomat sähköpostit
Toimintaympäristön tietoturvallisuustilaa seurataan, 13.1§	Hyvänä käytäntönä tiedonhallintayksikössä on seurata toimintaympäristön turvallisuustilannetta viranomaislähteistä, viranomaiskontaktien ja mediaseurannan avulla sekä valvomalla jatkuvasti tietojärjestelmiä ja tietovarantoja. Tämä tulee tehdä ottaen huomioon mahdollinen erityislainsäädäntö, käytännesäännöt, muu informaatioohjaus, tulosohjaus ja taloudelliset voimavarat. Keskeisiä viranomaistietolähteitä ovat Kyberturvallisuuskeskuksen raportit sekä rikosasioissa Poliisi.	Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta, 8.11.2021	Atea; Hallintojohtaja; Tietosuojavastaava	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta.	Varkaus; Ilkivalta; Kyberhyökkäys; Sähköverkon toimintakatko

Turvallisuusluokitelta vista asiakirjoista ja niiden käsittelystä on huolehdittu, 18§	Valtion virastoissa ja laitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan.	Tiedonhallintalaki	Hallintojohtaja; Tietosuojavastaava	Toimitaan yhteistyössä Atean ja Sofigaten sekä Monetran kanssa ja arvioidaan riskejä myöskin oman toiminnan kautta. Turvallisuusluokiteltu tieto on voitu kuvata tarpeen mukaan tiedonhallintasuunnitelmassa.	Tilaturvallisuus