



SUOMUSSALMEN KUNNAN TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Sisällys

1	Johdanto	1
2	Tietoturvallisuus	1
3	Tietosuoja	3
4	Tietoturvallisuustavoitteet	4
5	Organisointi ja tietoturvavastuut	4
6	Tiedon ja tietojärjestelmien käyttö.....	6
7	Riskiperusteinen lähestymistapa.....	7
8	Tietoturvaosaamisen varmistaminen	7
9	Tietoturva- ja tietosuoja hankinnoissa ja sopimuksissa.....	7
10	Lokitietojen kerääminen	8
11	Tietoturvapoikkeamien käsittely ja niistä tiedottaminen	9
12	Tietoturvallisuuden seuranta, ylläpito ja kehittäminen.....	9
13	Tekoäly	10
14	Suomussalmen kunnan henkilöstöä koskevat tarkennukset	11

SUOMUSSALMEN KUNNAN TIETOTURVA- JA TIETOSUOJAPOLITIikka

1 Johdanto

Tieto on keskeisessä roolissa Suomussalmen 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 Suomussalmen 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 Suomussalmen kunnan intranetissä.

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

2 Tietoturvallisuus

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

Tietoturvallisuus on kiinteä osa Suomussalmen kunnan johtamista, palveluita ja toimintoja. Se ulottuu jokaisen henkilöstön arkipäivän työtehtäviin ja työtapoihin sekä luottamushenkilöiden toimintaan Suomussalmen kunnan asioiden käsittelijöinä.

Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Tietoturvallisuuteen liittyvillä vastuutuksilla ja käytännöillä pyritään varmistamaan, että Suomussalmen 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.

Suomussalmen 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)
- Suomussalmen kunnan omat voimassa olevat strategiat, hallinto- ja ohjesäännöt, riskienhallinta-, valmius- ja viestintäsuunnitelmat (tietoturvallisuutta koskevilta tai sivuavilta osiltaan) sekä näistä johdetut vaatimukset
- Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) suositukset
- Valtionhallinnon Tietoturvallisuuden johtoryhmän (VAHTI) ohjeet
- EU:n tekoälydirektiivi

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

Suomussalmen 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 tietoturvatyömenpiteitä. Tietoturvan hallinnan taso on asetettu noudattamaan lainsäädännöllisiä velvoitteita. Suomussalmen kunta tunnistaa 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.

Suomussalmen 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. Suomussalmen kunta mahdollistaa asiakkaille tiedonsaannin omiin henkilötietoihinsa sekä informoi henkilötietojen käsittelystä kunnan verkkosivuilla. Suomussalmen kunnan henkilörekistereitä käsittelevät sopimuskumppanit veloitetaan noudattamaan vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

4 Tietoturvallisuustavoitteet

Suomussalmen 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.

Suomussalmen 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 Suomussalmen kunnan sääntöjen mukaisesti.

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

Kunnanjohtajalla on kokonaisvastuu tietoturvallisuuden toteuttamisesta ja tietoturvallisuuden toteutumisen raportoinnista kunnanhallitukselle. Kunnanjohtaja omistaa tietoturvapoliittikan ja esittelee muutokset kunnanhallitukselle. Kunnanjohtaja hyväksyy organisaation tasoiset ohjeet ja linjaukset ellei hallintosäännössä toisin määrätä. Kunnanjohtajan tukena tietoturvallisuusasioissa ovat vastuualuejohtajat.

Vastuualuejohtajat vastaavat vastuualueidensa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta.

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

- oman organisaationsa perehdyttämisestä Suomussalmen kunnan tietoturvaohjeisiin sekä jokaisen työntekijän ja viranhaltijan työtehtäviin liittyviin tietoturvavastuisiin.
- työntekijän tai viranhaltijan palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin:
 - o Suomussalmen 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 ICT-palveluntuottajan asiakastukeen ja omalle esihenkilölleen tai keskitetysti hallintojohtajalle. 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 esihenkilön tai keskitetysti hallintojohtajan hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho. Tietojärjestelmän omistaja on tietojärjestelmästä vastaava kunnanjohtaja ja vastuualuejohtajat.

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

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

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

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 Suomussalmen kunnan tietoturvapoliittikkaa sekä sopimusten tietoturva- ja tietosuojaliitteitä.

6 Tiedon ja tietojärjestelmien käyttö

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

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

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

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

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

Etätyössä tulee noudattaa Suomussalmen kunnan etätyöohjeistuksen tietoturvakäytäntöjä.

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. Tietoturvatyötoimia tulee mitoittaa sekä järjestelmän tietosisällön, että Suomussalmen 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.

Esihenkilö huolehtii uudessa tehtävässä aloittavan työntekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin ja siihen, miten tietoturvallisuus tulee huomioida hänen omissa työtehtävissään. Tietoturvallisuuden peruskoulutusta tarjotaan säännöllisesti, ja tietoturva- ja tietosuojaohjeet pidetään koko henkilöstön saatavilla. Koulutukset kattavat tietoturvan perusperiaatteet, ajankohtaiset uhkat ja parhaat käytännöt.

Suomussalmen kunnan henkilöstö suorittaa omatoimisen tietoturva- ja tietosuojakoulutuksen kunnan laatiman suosituksen mukaisesti.

9 Tietoturva- ja tietosuoja hankinnoissa ja sopimuksissa

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

Tietosuojan osalta tietosuoja-asetus edellyttää, että Suomussalmen 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 suojeleminen.

Lähtökohtaisesti Suomussalmen kunnan sopimuksissa ja hankinnoissa käytetään Suomussalmen kunnan tietosuojaliitettä. Tietosuojaliite tai muut tietosuoja-asetuksen 28 artiklan vaatimukset täyttävät ehdot sisällytetään kaikkiin uusiin sopimuksiin, joiden perusteella käsittelijä käsittelee henkilötietoja Suomussalmen 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. Väärinkäyttöksiin puututaan.

Sekä odottamattomista että ennalta tiedetyistä palvelukatkoksista ja muista tietojärjestelmien käytön häiriöistä tiedotetaan Suomussalmen 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 Suomussalmen 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.

13 Tekoäly

Tekoälyteknologioiden käyttö Suomussalmen kunnan 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 tietoturvauhkien tunnistamisen ja niihin varautumisen.
- Jatkuva seuranta ja arviointi: Tekoälyjärjestelmien toimintaa tulee seurata ja arvioida jatkuvasti, jotta voidaan varmistaa niiden tietoturvallisuus ja tietosuoja.

Suomussalmen kunnan tietoturvapolitiikassa 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. On varmistettava, että käyttäjät ymmärtävät, miten tekoälyjärjestelmät toimivat.

Suomussalmen kunnan tekoälypolitiikka on laadittu yhdessä Kainuun kuntien ja Kainuun liiton kanssa. Yhteinen tekoälypolitiikka Kainuun kuntia ja Kainuun liittoa varten on tämän asiakirjan liitteenä (Liite 1).

14 Suomussalmen kunnan henkilöstöä koskevat tarkennukset

Tämä kunnan henkilöstöä ja toimintaa koskeva tietoturva- ja tietosuojapolitiikka sisältää koko kunnan henkilöstölle tarkoitetut tietoturvallisuuteen liittyvät perusasiat sekä neuvoja tietoturvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tilanteissa.

Kunta osallistuu Kainuun kuntien ja Kainuun liiton tiedonhallinnan ja tietosuojan ohjausryhmän toimintaan. Talous- ja henkilöstöhallinnan ohjelmien riskinhallinnasta vastaa myös talous- ja henkilöstöhallinnon palveluntuottaja. Tietosuojavastaavana toimii ICT-sihteerin ja tietosuojavastaavan sijaisena toimistotyöntekijä.

Työasemien, tietoliikenneverkon ja tietojärjestelmien käyttöoikeudet annetaan vain niille, jotka ovat kuntaan palvelussuhteessa ja salassapitovelvollisia. Tästä pääsäännöstä voidaan poiketa ainoastaan perustellusta syystä, kuten kunnallisen luottamushenkilön osalta. Kunnan henkilöstölle sallitaan vain sellaisten tietojärjestelmien käyttäminen, joita määrättyjen tehtävien suorittaminen edellyttää. Kunnalla on oikeus seurata ja rajoittaa tunnusten käyttöä.

Kunnan työntekijä tai viranhaltija ei saa käyttää väärin tietoja, joita hän työssään käsittelee. Henkilöstöön kuuluva ei saa tarpeettomasti käsitellä tai katsoa tietoa, johon hänellä on pääsy, jos hän ei sitä omia työtehtäviään hoitaessa tarvitse. Tietoturva- ja suojarikkomuksista voi olla seurauksena käyttöoikeuksien rajoituksia, työsuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä seuraamuksia.

Jos tietojen väärinkäyttöä tai urkkimista havaitaan, käsitellään asia väärinkäytöstä tai urkinnasta epäillyn kanssa. Mikäli väärinkäyttö tai urkinta on vähäistä, eivät tiedot ole arkaluonteisia tai salassa pidettäviä, annetaan huomautus. Jos edellä mainittu tahalliseksi todettu toiminta jatkuu, huomautuksen jälkeen annetaan kirjallinen varoitus. Tietojen väärinkäytöstä tai urkinnasta epäiltyä on aina kuultava tilanteessa, jotta inhimilliset erehdykset, järjestelmävirheet ja muut selittävät tekijät voidaan tunnistaa. Salassa pidettävän tiedon tahallisesta urkkimisesta tai väärinkäytöstä voidaan antaa suoraan kirjallinen varoitus, minkä lisäksi tapauksesta riippuen voi tulla myös rikos- ja vahingonkorvauslainsäädännön mukaisia seuraamuksia. Palvelussuhteeseen vaikuttavista seuraamuksista on säädetty ensisijassa työsopimuslaissa ja viranhaltijalaissa.

Etätyössä tulee noudattaa Suomussalmen kunnan etätyöohjeistuksen tietoturvakäytäntöjä. Etätyössä tulee käyttää vain hyväksytyjä laitteita ja ohjelmistoja. Kaikki yhteydet tulee suojata vahvalla salauksella organisaation VPN-palvelua käyttämällä. Etätyössä tai muualla työskennellessään on myös arvioitava etätyöympäristön turvallisuutta. Esim. mobiilisähköpostin käyttäminen voi mahdollistaa sähköpostin käyttäjän ollessa poissa työasemansa äärestä. Tällöin on kiinnitettävä erityistä huolellisuutta laitteen säilytykseen ja tilaturvallisuuteen.

Henkilöstön on sitouduttava noudattamaan etätyössä samaa salassapitovelvollisuutta, jota työssä ollessa normaalistikin edellytetään. 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 työtehtäviin. Luottamuksellisen tiedon hävittäminen pitää tapahtua tietoturvaohjeiden mukaisesti.

Liitteet

Liite 1: Yhteinen tekoälypolitiikka Kainuun kuntia ja Kainuun liittoa varten