Tietoturvapolitiikka

Sipoon kunta

SIPOO
SIBBO

Sisällys

1 Tietoturvapolitiikan keskeisiä käsitteitä

Tietoturva	Tietoturvalla varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys. Tietoturvaan sisältyy muun muassa tietojen, tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen, tilojen ja toiminnan turvaaminen. Tietoturva liittyy läheisesti tietosuojaperiaatteiden toteuttamiseen.
Tietosuoja	Tietosuoja tarkoittaa perusoikeutta, joka turvaa jokaisen oikeuksia ja vapauksia henkilötietojen käsittelyssä. Tietosuoja määrittelee ne periaatteet, milloin, millä edellytyksillä ja miten henkilötietoja voidaan käsitellä.
Luottamuksellisuus	Luottamuksellisuus eli se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Tiedot suojataan luotettavasti ja oikeus käsitellä tietoja perustuu työtehtävien mukaiseen tarpeeseen ja vähimpien oikeuksien periaatteeseen. Tietojen ja järjestelmien käyttäjät tunnistetaan luotettavasti.
Eheys	Eheys eli se, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut. Tietojen ja tietojen käsittelymenetelmien oikeellisuus, laatu ja kiistämättömyys varmistetaan. Tieto suojataan luvattomalta tai vahingossa tapahtuvalta tiedon muuttamiselta tai poistamiselta.
Käytettävyys	Käytettävyys eli se, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Tiedot ja niihin perustuvat palvelut ovat niihin valtuutettujen henkilöiden käytettävissä oikea-aikaisesti.
Tekniset ja organisatoriset toimet	Teknisillä ja organisatorisilla toimilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutusta, ohjeita ja määräyksiä, salassapito-sopimuksia, tilavalvontaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, auditointeja, teknisiä rajoituksia ja kontrolleja, tarkastus- ja valvontajärjestelmiä, käytännesääntöjä ja sertifikaattien käyttöönottoa.
Tietoturvaloukkaus	Tietoturvaloukkaus on tietoturvajärjestelmään kohdistuva fyysinen tai tekninen loukkaus. Tyypillisiä tietoturvaloukkauksen muotoja ovat esimerkiksi tietomurto, palvelunestohyökkäys ja haittaohjelmat. Tietoturvaloukkauksessa organisaation tietojärjestelmän tietoihin murtaudutaan tai tunkeudutaan ja varastettua tietoa käytetään hyväksi. Tietoturvaloukkaus ei aina kohdistu henkilötietoihin.
Henkilötietojen tietoturvaloukkaus	Henkilötietojen tietoturvaloukkaus eli tietoturvaloukkaus, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

2 Tietoturvapolitiikan merkitys

Tietoturvapolitiikka on ylin tietoturvan toteutusta ja hallintaa määrittävä dokumentti. Tietoturvallisuuden tavoitteena on tukea Sipoon kunnan strategisten tavoitteiden toteutumista. Sipoon kunnan tietoturvapolitiikka määrittää vastuut, periaatteet ja toimintatavat tietojen käsittelyyn ja suojaamiseen.

Tietoturvallisuus perustuu lainsäädäntöön, normiohjaukseen ja sopimuksiin. Tietoturvapolitiikan soveltaminen ei ole sidoksissa tiedon muotoon tai sen käsittely- tai esitystapaan ja sitä sovelletaan kaikkiin tiedon elinkaaren eri vaiheisiin.

Tietoturvapolitiikka koskee kaikkea Sipoon kunnan toimintaa. Tietoturvapolitiikka tulee huomioida myös kunnan käyttämien palveluntuottajien ja sidosryhmien toiminnassa. Tietoturvapolitiikka velvoittaa Sipoon kunnan henkilöstöä, johtoa, luottamushenkilöitä, viranhaltijoita, sekä muita kunnan tietoja käsitteleviä henkilöitä, kuten konsultteja, alihankkijoita ja sidosryhmiä riippumatta siitä, missä muodossa käsiteltävä tieto on.

Tietoturvapolitiikan mukaisia periaatteita ja niiden soveltamista tarkennetaan linjauksilla ja vaatimuksilla, käytännöillä, ohjeistuksilla ja muulla tietoturvan dokumentaatiolla.

Kunnanhallitus on hyväksynyt tietoturvapolitiikan. Tietoturvapolitiikkaa katselmoidaan vuosittain ja tarvittaessa useammin merkittävien muutosten johdosta tietoturva- tai tietosuojakäytännöissä, lainsäädännössä tai viranomaisohjeistuksessa. Katselmoinnin tarkoituksena on varmistaa politiikan ajantasaisuus ja vaikuttavuus. Tietoturvapolitiikan katselmoinnista vastaa tietosuoja- ja tietoturvaryhmä.

3 Tietoturvan roolit ja vastuut

Tietoturvan roolit ja vastuut jakautuvat Sipoon kunnassa alla olevan taulukon mukaisesti:

Kunnanhallitus	Vastaa tietoturvan johtamisesta ja resursoinnista sekä valvonnasta.
Kunnanjohtaja	Toimii tietoturvan omistajana kunnassa luoden edellytykset tietoturvan asianmukaiselle toimeenpanolle. Tarvittaessa kunnanjohtaja asettaa ryhmän seuraamaan tietoturvan ja -suojan toteutumista, tekemään kehitysehdotuksia sekä toimimaan toimialojen tietosuojavastaavien sekä järjestelmien pääkäyttäjien tukena.
Toimialan johto	Vastaa tietoturvan toteutuksesta johtamansa toiminnan osalta.
Esimiehet	Vastaavat tietoturvan toteutumisesta alaisessaan toiminnassa. Esimiehet raportoivat näistä asioista toimialajohdon lisäksi tietoturvatiimille.
Tietoturvatiimi	Vastaa tietoturvaprosessien ohjauksesta ja integroimisesta muihin kokonaisturvallisuuden osa-alueisiin sekä tietoturvaa koskevasta viestinnästä johdolta saamiensa resurssien ja toimivaltuuksien puitteissa. Tehtävään sisältyy tietoturvatyön suunnittelu, ohjeistus, seuranta ja kehittäminen sekä tietoturvariskien ja -poikkeamien hallinnan koordinointi. Chief Digital Officer raportoi kunnanjohtajalle. Tietoturvatiimi ja tietotekniikan palveluntuottajat tiimin ohjeistamana vastaavat tietoturvallisuuden ja teknisen valvonnan

	toteutumisesta tietojärjestelmäympäristössä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.
Viranhaltijat, työntekijät, luottamushenkilöt ja muut työntekijäsuhteeseen rinnastettavat henkilöt	Vastaavat omalta osaltaan tietoturvan toteutumisesta omissa työtehtävissään. Jokaisen vastuulla on havaitsemiensa tietoturvaan liittyvien uhkien, riskien tai rikkomusten ilmoittaminen viipymättä esimiehelle, palvelusta tai toiminnasta vastuulliselle taholle ja tietoturvatiimille.
Tiedon, tietojärjestelmän tai palvelun omistaja	Vastaa omistukseensa liittyvästä käyttäjien ja heidän käyttöoikeuksiensa määrittelystä ja hyväksynnästä, riskienhallinnan toteuttamisesta, tiedon eheyden varmistamisesta, tietojen luokittelusta (julkisuuden ja salassapidon määrittely sekä arkistonmuodostus) sekä tiedon hävittämisestä.

4 Tietoturvaperiaatteet

Tietoturvaperiaatteita noudatetaan kaikissa tietojen käsittelyn elinkaaren eri vaiheissa ja tiedon kaikissa olomuodoissa. Tiedon elinkaarella tarkoitetaan kaikkia tiedon käsittelyn vaiheita tiedon keräämisestä tiedon hävittämiseen.

Tietoturvaperiaatteilla varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys ja tätä kautta kunnan palvelutuotannon, prosessien ja muiden toimintojen luotettavuus, laatu sekä jatkuvuus. Lähtökohtana tietoturvaa koskevissa päätöksissä ovat viranomaissäädökset sekä hyvä tiedonhallinta- ja -käsittelytapa.

Tiedon suojaaminen on oleellinen osa kunnan kokonaisturvallisuutta ja päivittäistä toimintaa. Tietoturvallisuuden perustana on osaava ja tietoturvaan sitoutunut henkilöstö. Tietoturvaperiaatteilla ohjataan tietojen suojaamista ja niitä edistetään tuomalla tietoturvaperiaatteet osaksi henkilöstön perehdytystä ja koulutusta.

Tietoturvaperiaatteiden noudattaminen on edellytys tietosuojaperiaatteiden toteutumiselle ja uuden teknologian turvalliseen käyttämiseen.

Alla olevassa taulukossa esitellään Sipoon kunnan keskeisimmät tietoturvaperiaatteet:

Hallinnollinen tietoturva	Hallinnollinen tietoturva koostuu johdon hyväksymistä periaatteista, vastuunjaosta, toimintatavoista, ohjeistuksista, tarkoitukseen varatuista resursseista sekä riskien arvioinnista ja valvonnasta.
Henkilöstöturvallisuus	Henkilöstöturvallisuuden pääpaino on riskien välttäminen ennakkoon varmistamalla työprosessien ja käsittelyketjujen tietovirtojen turvallisuus, työtehtävien riittävä eriyttäminen, jatkuva valvonta sekä varmistamalla henkilöstön riittävä ja ajantasainen tietoturvaosaaminen.
Fyysinen tietoturva	Fyysiseen tietoturvaan kuuluvat kaikki ne keinot, joilla pyritään suojaamaan henkilöiden, tietoaineistojen, laitteiden, toimitilojen ja omaisuuden turvallisuus. Fyysinen turvallisuus turvataan muun muassa rakennus- ja toimitilaratkaisuilla, fyysisen ja teknisen

	kulunvalvonnan, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan turvallisuuskäytännöillä.
Tietoaineistoturvallisuus	Tietoaineistoturvallisuus sisältää tietoaineistojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamisen. Tavoitteena on estää tietojen tuhoutuminen tai tahaton muuttuminen sekä varmistaa tietoaineistojen luokitus, suojaaminen, oikeanlainen käsittely, säilyttäminen ja hävittäminen.
Käyttöturvallisuus	Käyttöturvallisuuteen sisältyy muun muassa järjestelmien turvalliset käyttöperiaatteet, käytössä olevien järjestelmien osaaminen, tietojenkäsittelytapahtumien valvonta, laitteiden käyttövarmuus ja tietoturvapäivitykset, salasanakäytännöt, työtehtäviin perustuvien käyttöoikeuksien hallinta, jatkuvuuden turvaaminen sekä keskeisimpien toimintojen ja prosessien kuvausten ja ohjeistusten ylläpito.
Laitteistoturvallisuus	Laitteistoturvallisuus sisältää tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi.
Ohjelmistoturvallisuus	Ohjelmistoturvallisuus sisältää käyttöjärjestelmiin ja ohjelmistoihin kohdistuvat ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja valvontatoimet, lokimenettelyt, laadunvarmistusmenettelyt sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden varmistamiseksi.
Tietoliikenneturvallisuus	Tietoliikenneturvallisuudella varmistetaan verkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys tiedon liikkuessa järjestelmän sisällä tai organisaatioiden välillä. Keskeisenä tavoitteena on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus.

4.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sipoon kunta noudattaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen mukaisia henkilötietojen käsittelyn periaatteita ja muuta henkilötietojen käsittelyyn soveltuvaa sääntelyä.

Teknisillä ja organisatorisilla toimilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kannalta tarpeellisia tietoja. Tietosuojaperiaatteet huomioidaan kaikessa toiminnassa mahdollisimman varhaisesta vaiheesta lähtien ja riskitasoon nähden asianmukaiset tekniset ja organisatoriset toimenpiteet toteutetaan.

Tietosuojaperiaatteiden noudattaminen henkilötietojen keräämisessä ja käsittelyssä toteutetaan muun muassa varmistamalla, että

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja käsitellään vain suunnitellun käsittelytarkoituksen kannalta
- tietoja ei kerätä suurempia määriä eikä niitä säilytetä kauemmin kuin on välttämätöntä kyseiseen käyttötarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville

- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin.

Tietosuojaa käsitellään tarkemmin Sipoon kunnan tietosuojapolitiikassa.

4.2 Toimittajahallinta

Tietoturvaan ja tietosuojaan liittyvät vastuut ja velvoitteet huomioidaan kunnan ja eri osapuolten välisissä sopimuksissa. Riskiarvion edellyttämien tietoturvavaatimusten täyttyminen sopimusehdoissa varmistetaan sopimuksia tehdessä. Hankinta- ja ulkoistussopimuksia tekevät vastaavat siitä, että tietoturvan taso vastaa ostopalveluissa määräyksiä, ohjeita ja voimassa olevia säännöksiä sekä sopimuksen tekohetkellä että toimeksiannon aikana. Sopimuksilla varataan toimittajaan kohdistuva auditointioikeus ja tätä oikeutta käytetään tarvittaessa. Toimittajan kanssa pidetään säännöllisesti suunnittelu- ja seurantapalavereita, joissa käsitellään myös tietoturvallisuusasiat.

4.3 Toiminnan jatkuvuuden hallinta

Kunnan toiminnassa tunnistetaan jatkuvuutta uhkaavat riskit sekä varaudutaan niihin jatkuvuus- ja toipumissuunnitelmilla sekä niihin liittyvillä varajärjestelyillä. Jatkuvuuden varmistamisessa keskitytään ongelmien ja riskien ennalta ehkäisyyn sekä nopeaan toipumiseen poikkeamatilanteista. Jatkuvuuden hallintaan sisältyy kyberuhkiin varautuminen ja kyberturvallisuuden suojauskäytäntöjen riittävyyden arviointi. Myös sopimuskumppaneilta edellytetään toiminnan jatkuvuutta uhkaavien riskien säännöllistä tunnistamista sekä ajan tasaisia jatkuvuus- ja toipumissuunnitelmia.

4.4 Tietoturvan tai tietosuojan rikkomukset

Tietoturva- ja -suojajärjestelyt toteutetaan siten, että turvallisuusloukkausten selvittäminen on jälkikäteen kohtuudella mahdollista. Tietoturvallisuushäiriöt, -poikkeamat ja tietoturvaloukkaukset hallinnoidaan hallintaprosessin mukaisesti. Jokaisella organisaation työntekijällä on velvollisuus ilmoittaa huomaamastaan tietoturvaan kohdistuvasta riskistä, havaitsemastaan poikkeamasta tai muusta vastaavasta tilanteesta. Tietoturvatiimi huolehtii, että tietoturvaloukkaukset kirjataan, selvitetään viipymättä ja havaitut riskit saatetaan hallintaan.

Henkilötietojen tietoturvaloukkausten ilmoittamisessa valvontaviranomaisille ja rekisteröidylle toimitaan lainsäädännön ja kunnan ohjeistuksen mukaisesti. Sipoon kunnan tietosuojavastaava toimii yhteyshenkilönä valvontaviranomaisen suuntaan.

5 Riskiperusteinen lähestymistapa ja tietoturvariskien hallinta

Kunta rekisterinpitäjänä arvioi tietojenkäsittelyyn ja henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallinta- ja tietoturvallisuustoimenpiteet.

Tietoturvan toteutumista tarkastellaan riskilähtöisesti. Kunnan järjestelmät luokitellaan niiden kriittisyyden mukaan. Kriittisten järjestelmien turvajärjestelyt tarkistetaan säännöllisesti ja niiden toimivuus testataan tarvittaessa.

Tietoturvallisuutta ja sen hallintakeinoja kehitetään jatkuvasti tietoturvariskien arvioinnin ja analysoinnin, käytännön kokemusten ja tietoturvallisuuden yleinen kehitys huomioiden.

6 Koulutus ja tietoisuuden lisääminen

Tietoturvaan liittyvää koko kuntaa ohjaavaa ohjeistusta laaditaan hallinnollisessa yhteistyössä. Tietoturvaan liittyvää ohjeistusta sisällytetään kunnan muihin ohjeistuksiin ja prosessien eri vaiheisiin tämän politiikan periaatteet huomioiden.

Sipoon kunnan tulee osoittaa, että henkilöstön tietoturva- ja tietosuojaosaaminen on ajantasaista. Tietoturva- ja tietosuojaosaaminen osoitetaan toteutetulla perehdytyksellä, erilaisilla koulutustodistuksilla sekä osaamista seuraamalla. Esimiesten valvontaoikeuteen ja -velvollisuuteen kuuluu tietoturvallisuusohjeiden noudattamisen valvonta.

Sipoon kunta velvoittaa jokaisen työntekijän hyväksymään tietoturvasitoumuksen palvelussuhteen alkaessa. Osaamisen varmistamiseksi koko henkilöstöltä edellytetään vuosittain tietoturva- ja tietosuojakoulutuksen suorittamista. Tietoturva- ja tietosuojakoulutusta edellytetään myös luottamushenkilöiltä. Lisäksi järjestetään vuosittain tietoturva- ja tietosuojakoulutusta kohdennetuille henkilöstöryhmille.

6.1 Tietoturva-asioista tiedottaminen

Tietoturvapolitiikka määrittää voimassa olevat tietoturvan periaatteet ja dokumentista tiedotetaan koko henkilöstöä. Hyväksytty politiikka julkaistaan kunnan intranetissä ja verkkosivuilla ja siitä tiedotetaan henkilöstöä myös muilla keinoilla. Yleisesti tietoturva-asioissa tiedottaminen tapahtuu tietoturvatiimin ja johtoryhmien kautta.

7 Dokumentin tiedot ja versiohistoria

Dokumentin tiedot	Selite
Dokumentin nimi	Sipoon kunnan tietoturvapolitiikka
Omistaja	Tietoturvatiimi
Hyväksyjä	Kunnanhallitus
Hyväksymispäivämäärä	24.10.2022
Dokumenttia päivitetty	21.7.2022

Versio	Pvm.	Muutokset	Tekijä
1.0	24.10.2022	Ensimmäinen hyväksytty versio	Tietoturvatiimi