

TIETOTURVAPOLITIIKKA

Versiohallinta

Versio	Pvm	Toimet	Tekijä	Hyväksyntä
1.0	20.5.2025	Luonnos	Mika Halme	
2.0	21.5.2025	Valmis	Marjo Säärelä, hallintojohtaja	21.5.2025
2.0			Kaupunginhallitus	

Sisällysluettelo

1. Vastuullisuus ja vaatimuksenmukaisuus	4
2. Kattavuus	4
3. Tavoitteet, suojattavat kohteet ja hyväksyttävä käyttö	4
4. Vastuut ja organisointi	5
5. Ylläpito ja kehitys	6
6. Jatkuva parantaminen	7

1 VASTUULLISUUS JA VAATIMUKSENMUKAISUUS

Tämä dokumentti määrittää Kemijärven kaupungin toiminnoissa noudatettavan tietoturvaläpöitiikan. Tietoturvaläpöitiikka tarkoittaa tässä dokumentissa kaikkien tietoturvaläpöitiikun eri osa-alueiden kokonaisvaltaista hallintaa.

Kemijärven kaupungin toiminnassa suhtaudutaan vastuullisesti tietoturvaläpöitiikun suhteen. Samalla jokaisen toimintaan osallistuvan työntekijän edellytetään toimivan vastuullisesti. Noudatamme kaikessa toiminnassamme sitä koskevia säädöksiä, määräyksiä ja muita velvoitteita ottaen huomioon julkishallinnon erityisvaatimukset.

Asukkaiden, kaupungin henkilöstön, yhteistyökumppaneiden ja asiakkaiden tietoa-aineistojen käsittelyssä noudatamme erityistä huolellisuutta tietoturvaläpöitiikun ja tietosuojan korkean tason varmistamiseksi.

2 KATTAVUUS

Tietoturvaläpöitiikka on kaupunginhallituksen hyväksymä sekä sitä sovelletaan kaikkiin Kemijärven kaupungin tietoja käsitteleviin osapuoliin, luottamushenkilöihin, yhteistyökumppaneihin, ostopalvelujen tuottajiin ja konserniyhtiöihin, sekä henkilökuntaan.

Kaupungin sisäisissä ja ulkoisissa palveluissa mukana olevilta alihankkijoilta ja toimittajilta edellytämme korkealla tasolla hoidettua tietoturvaa ja tietosuojaa sekä lainmukaisuutta. Toimittajille on laadittu oma tietoturvaläpöitiikun- ja tietosuojan vaatimukset - tarkistuslista.

3 TAVOITTEET, SUOJATTAVAT KOHTEET JA HYVÄKSYTTÄVÄ KÄYTTÖ

Turvallisuustoimintamme perustuu säännöllisesti toteutettavaan riskienarviointiin, jonka avulla tunnistamme ja hallitsemme toimintaamme liittyviä tietoturvaläpöitiikun riskejä. Varmistamme henkilöstömme riittävän tietoturvaosaamisen perehdyttämisen, kouluttamisen ja ohjeistuksen avulla. Varaudumme ennalta mahdollisiin tietoturvahäiriöihin ja meillä on olemassa prosessit häiriöiden selvittämiseksi. Tuotamme ja ylläpidämme kaupunkilaisille

tietoturvallisia palveluita ja varmistamme käyttäjien / asukkaiden luottamuksen palveluihimme.

Tärkeimmät kaupungin tietoturvatoinnilla suojattavat kohteet ovat tiedot ja varsinaiseen toimintaan liittyvät prosessit, toiminnot, palvelut ja tietojärjestelmät sekä näitä tukevat resurssit ja infrastruktuuri. Tietoturvallisuustoimenpiteillä (kuten Ohjelmistojen ja järjestelmien päivittäminen, käyttöoikeuksien hallinta, varmuuskopiointi, monivaiheinen tunnistautuminen, salasanojen hallinta) huolehditaan kaupungin omien ja sen hallussa olevien tietojen ja niiden käsittelyn hallinnollisesta, teknisestä ja fyysisestä tietoturvallisuudesta (eheys, saatavuus, luottamuksellisuus, kiistämättömyys) tietojen olomuodosta ja sijainnista riippumatta. Tietoturvallisuustoimenpiteillä tuetaan myös tietosuojanäkökohtien toteutumista.

Kaupungin toimintaan liittyviä suojattavia tietoaineistoja, tietojärjestelmiä, työvälineitä ja muuta suojattavaa omaisuutta käytetään työtehtävien mukaisiin hyväksytyjä tarpeita palveleviin tarkoituksiin. Lähtökohtana on työtehtäviin perustuva tarve esimerkiksi käsitellä tietoja tai päästä suojattuihin tietojärjestelmiin.

4 VASTUUT JA ORGANISOINTI

Tietoturvallisuuden sekä tietosuojan korkean tason ylläpito on oleellinen osa jokaisen kaupungin työntekijän päivittäistä toimintaa. Tietosuojan tason takaamiseksi kaupungilla on erillinen tietosuojapolitiikka.

Työntekijä vastaa oman työskentelynsä tietoturvallisuudesta, annettujen ohjeiden noudattamisesta sekä havaitsemiensa tietoturvallisuusongelmien, väärinkäyttötapausten ja tietoturvallisuuteen liittyvien epäkohtien kirjaamisesta raportointijärjestelmään.

Esihenkilö vastaa oman yksikkönsä tai tiiminsä tietoturvallisuusasioiden toteuttamisesta. Tietohallinto vastaa kaupungin tietoturvallisuuden ylläpidosta ja kehittämisestä operatiivisella tasolla ja raportoi näistä hallintojohtajalle.

5 YLLÄPITO JA KEHITYS

Kaupungin koko henkilöstö osallistuu tietoturvallisuuden ylläpitoon ja kehittämiseen. Tärkeä osa tätä ylläpito- ja kehitystyötä on henkilöstön systemaattinen ja pitkäjänteinen perehdyttäminen, ohjeistaminen ja kouluttaminen.

Ylläpidämme tietoturvatietoisuutta ja parannamme tietoturvakulttuuria myös aktiivisella sisäisellä viestinnällä.

Noudatamme kaupunginhallituksen vahvistamaa ja hyväksymää tietoturvapoliittikkaa.

Seuraamme ja analysoimme toimintaamme kohdistuvia tietoturvallisuusriskejä ja kehitämme toimintaamme tämän tiedon mukaan. Arvioimme toimintaamme kohdistuvia riskejä säännöllisesti ja teemme tarvittavat riskienhallintatoimenpiteet.

Seuraamme aktiivisesti toimintaamme kohdistuvaa lainsäädäntöä ja kehitämme toimintaamme pysyäksemme voimassa olevien säädösten mukaisena.

Luomme ja ylläpidämme kaupungin jatkuvuus- ja toipumissuunnitelmia uhkatilanteiden varalle. Seuraamme myös tietoturvallisuuden kansallista ja kansainvälistä kehitystä hyödyntäen uusinta tietoa toiminnassamme. Käytämme vain sellaisia laitteistoja ja ohjelmistoja, joiden tietoturvallisuus on varmistettu ja joihin on tarvittavat käyttöoikeudet. Haittaohjelmien torjuntaan käytämme aina ajantasaisia ohjelmistoja ja muita välineitä.

Ylläpidämme ja kehitämme järjestelmällisesti yhteistyötä tärkeimpien sidosryhmiemme kanssa tietoturvallisuuden eri osa-alueilla.

Määritettyjen tietoturvavaatimusten toteutumista sekä menettelyiden ja ohjeiden noudattamista seurataan ja arvioidaan. Jokaisen toimintaan osallistuvan velvollisuutena on ilmoittaa havaitsemistaan tietoturvapuutteista ja heikkouksista sekä tapahtuneista häiriöistä tai niiden epäilyistä ja läheltä piti tilanteista asianmukaiselle vastuutaholle, jonka velvollisuutena on ryhtyä tarvittaviin toimenpiteisiin ilman aiheetonta viivettä.

Vaatimusten, menettelyiden ja ohjeiden vastaiseen toimintaan puututaan korjaavilla ja kehittävillä toimenpiteillä ja tarvittavilla seuraamusmenettelyillä.

6 JATKUVA PARANTAMINEN

Tietoturvallisuuteen liittyvien prosessien ja menettelyiden on edustettava hyvää hallintokäytäntöä ja oltava jatkuvan parantamisen kohteena. Jatkovaa parantamista toteutetaan muun muassa säännöllisen riskienarvioinnin ja kehitystoimenpiteiden avulla. Seuraamme tietoturvapoliitikan toteutumista ja tietohallinto raportoi asiasta tarvittaessa kaupungin hallintojohtajalle.

Tämä suunnitelma päivitetään vuosittain tai tarvittaessa.