KEURUU

Tietoturvaperiaatteet

Kh 2.11.2026 §

SISÄLLYSLUETTELO

Versiohistoria **2**
1. Tarkoitus ja tavoitteet **3**
2. Soveltamisala ja toimintaa ohjaavat vaatimukset **3**
3. Tietoturvan periaatteet **3**
3.1. Riskiperusteisuus 4
3.2. Tiedon suojaaminen 4
3.3. Käyttöoikeudet ja pääsynhallinta 5
3.4. Turvalliset tietojärjestelmät ja palvelut 5
3.5. Jatkuvuus, varautuminen ja kyberturvallisuus 5
3.6. Tietoturvapoikkeamien hallinta 6
4. Tietoturvan johtaminen, organisointi ja vastuut **6**
5. Tietoturvatietoisuus ja toimintakulttuuri **8**
6. Tietoturvaperiaatteiden valvonta, ylläpito ja kehittäminen **8**

Lapsi-ystävällinen kunta | unicef

Versiohistoria

Päivämäärä	Tekijä	Versionumero	Muutoksen lyhyt kuvaus
02.10.2026	Timo Ahonen	0.1	Alustava luonnos
13.10.2026 27.10.2026	Timo Ahonen Päivi Vauhkonen	1.0	Esitys kaupunginhallitukselle

1. Tarkoitus ja tavoitteet

Keuruun kaupungin tietoturvaperiaatteissa määritellään tietoturvallisuuden keskeiset suuntaviivat sekä tietoturvallisuuden organisoinnin, vastuiden ja seurannan yleiset periaatteet. Asiakirjalla ohjataan kaupungin hallintosäännön 67 §:n mukaisia tietoturvallisuusjärjestelyjä. Se on kaupungin ylin tietoturvallisuutta ohjaava asiakirja, jota täydennetään erillisillä tietoturvaohjeilla ja tarvittaessa toimialakohtaisilla ohjeilla.

Tietoturvallisuuden tavoitteena on suojata kaupungin tietoja, tietojärjestelmiä, palveluita ja niiden käyttöympäristöjä niihin kohdistuvilta uhkilta sekä varmistaa tietojen luottamuksellisuus, eheys ja saatavuus. Tietoturvallisuutta toteutetaan riskiperusteisesti osana kaupungin johtamista, toimintaa, riskienhallintaa, jatkuvuudenhallintaa ja varautumista.

Tietoturvallisuus kattaa myös kyberturvallisuuden, jolla turvataan kaupungin digitaalista toimintaympäristöä ja palveluiden jatkuvuutta. Kyberturvallisuuteen kuuluu digitaalisiin palveluihin, tietojärjestelmiin ja tietoverkkoihin kohdistuvien uhkien ehkäiseminen ja havaitseminen sekä häiriötilanteisiin varautuminen, niissä toimiminen ja niistä palautuminen.

2. Soveltamisala ja toimintaa ohjaavat vaatimukset

Tietoturvaperiaatteet täydentävät ja toteuttavat kaupunginvaltuuston 26.10.2026 hyväksymiä sisäisen valvonnan ja riskienhallinnan perusteita tietoturvallisuuden ja kyberturvallisuuden osalta.

Tietoturvaperiaatteita sovelletaan Keuruun kaupungin kaikessa toiminnassa ja kaikilla organisaatiotasoilla. Periaatteet velvoittavat kaupungin henkilöstöä, viranhaltijoita ja luottamushenkilöitä sekä soveltuvin osin muita henkilöitä, joilla on oikeus käsitellä kaupungin tietoja tai käyttää kaupungin tietojärjestelmiä ja palveluita. Periaatteita sovelletaan soveltuvin osin myös kaupungin tietoja käsittelevien palveluntuottajien, yhteistyökumppaneiden ja muiden ulkopuolisten toimijoiden kanssa toimittaessa. Ulkopuolisten tahojen kanssa toimittaessa tietoturvan vaatimukset ja vastuut määritellään tarvittavilta osin sopimuksissa ja osapuolia velvoittavissa asiakirjoissa.

Tietoturvaperiaatteet koskevat kaupungin hallinnassa tai vastuulla olevia tietoja, tietoaineistoja, tietojärjestelmiä, digitaalisia palveluita ja niiden käsittely-ympäristöjä riippumatta tiedon muodosta, sijainnista tai käsittelytavasta. Tietoturvallisuudesta huolehditaan tiedon ja palveluiden koko elinkaaren ajan.

Keuruun kaupungin tietoturvallisuuden toteuttamista ohjaavat voimassa oleva lainsäädäntö, viranomaismääräykset ja -ohjeet sekä kaupungin omat määräykset, päätökset ja ohjeet. Tietoturvallisuuden toteuttamisessa huomioidaan lisäksi soveltuvat kansalliset ja kansainväliset tietoturvallisuuden suositukset ja hyvät käytännöt.

Näitä periaatteita täydentävissä tietoturvaohjeissa ja muissa alemman tason ohjeissa määritellään tarkemmin tietoturvallisuuden käytännön vaatimukset ja näiden toteutustavat.

3. Tietoturvan periaatteet

Tietoturvallisuuden pääperiaatteina Keuruun kaupungin toiminnassa ovat toiminnan jatkuvuuden varmistaminen, tietoturvariskien hallinta sekä ennaltaehkäisy ja toteutuneiden riskien vaikutuksien rajoittaminen. Tietoturvallisuuden toteuttamisella pyritään suojaamaan kaupungin tietoja, tietojärjestelmiä ja palveluita niiden koko elinkaaren ajan. Olennaisia toimenpiteitä

toteutetaan riskiperusteisesti ja siten suojaustoimenpiteet valitaan oikeasuhteisesti tiedon käyttötapojen mukaan.

Tietoturvallisuus tulee huomioida luonnollisena osana kaupungin toiminnan suunnittelussa, kehittämisessä ja hankinnoissa. Tietoturvallisuudesta huolehditaan siten ennakoivasti ja sitä kehitetään olosuhteiden muuttuessa toimintaympäristön, uhkien tai riskien kehityksen mukaisesti.

Tietoturvallisuuden periaatteet koskevat tiedon käsittelyä olomuodosta, sijainnista ja käsittelytavasta riippumatta. Periaatteita ja sitä tarkentavia ohjeistuksia tulee noudattaa kaikissa tiedon käsittelyn vaiheissa ja ympäristöissä.

3.1. Riskiperusteisuus

Keuruun kaupungin tietoturvallisuuden riskienhallinta on osa kaupungin kokonaisvaltaista sisäistä valvontaa ja riskienhallintaa. Tietoturvariskejä hallitaan kaupungin hallintosäännön 13 luvun sekä Sisäisen valvonnan ja riskienhallinnan perusteiden (KH 21.09.2026 § 285) mukaisesti osana johtamista, toiminnan suunnittelua, päätöksentekoa ja seurantaa. Tietoturvallisuuteen liittyvät toiminnan kannalta olennaiset riskit tunnistetaan ja arvioidaan järjestelmällisesti. Arvioinnissa huomioidaan riskien toteutumisen todennäköisyys ja vaikutukset sekä määritellään tarvittavat riskienhallintatoimenpiteet ja niihin liittyvät vastuut.

Riskienhallinnan tavoitteena on saattaa riskit kaupungin toiminnan kannalta hyväksyttävälle tasolle. Tietoturvariskejä arvioidaan erityisesti tietojärjestelmien ja digitaalisten palvelujen suunnittelun, hankinnan, käyttöönoton ja käytön yhteydessä sekä toiminnan, järjestelmien tai toimintaympäristön olennaisesti muuttuessa. Kaupungin toimijoiden tulee tunnistaa omaan toimintaansa liittyviä tietoturvariskejä ja ilmoittaa havaitsemistaan riskeistä sovittujen toimintatapojen mukaisesti. Tunnistettujen riskien käsittely ja hallintatoimenpiteet mitoitetaan riskin merkittävyyden perusteella. Riskien ja niiden hallintatoimenpiteiden tilaa seurataan ja arvioidaan säännöllisesti. Hallintatoimenpiteiden jälkeen jäljelle jäävät merkittävät jäännösriskit käsitellään ja hyväksytään kaupungin määrittelemän toimivallan ja vastuunjaon mukaisesti.

3.2. Tiedon suojaaminen

Tietoturvallisuuden periaatteet tulee huomioida välineestä riippumatta eli ne eivät liity vain tietotekniikkaan. Paperiset asiakirjat, sähköiset tietovarannot, tietojärjestelmät, tietotekniset laitteet, tietoverkot ja niihin liittyvät palvelut on pidettävä asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa. Tietoturvallisuuden saavuttamiseksi toteutetaan sopivia turvamekanismeja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista ja ohjelmisto- ja laitteistotoiminnoista. On varmistettava, että luottamukselliset, arkaluonteiset ja muut salassa pidettävät tiedot kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu. Jokaisen esimiehen on huolehdittava, että tietoturvamääräykset ja ohjeet koulutetaan ja perehdytetään henkilöstölle.

Tietojen suojaamisessa varmistetaan niiden luottamuksellisuus, eheys ja saatavuus koko elinkaaren ajan. Suojaustoimenpiteet suhteutetaan tiedon, tietojärjestelmän tai palvelun merkitykseen ja siihen kohdistuviin riskeihin. Pääsy tietoihin ja tietojärjestelmiin sallitaan vain työtehtävien ja käyttötarpeen edellyttämässä laajuudessa.

3.3. Käyttöoikeudet ja pääsynhallinta

Käyttöoikeuksien jakamisessa ja pääsynhallinnassa toteutetaan pienimpien oikeuksien periaatetta. Käyttöoikeudet kaupungin tietojärjestelmiin ja tietoihin myönnetään pääsääntöisesti tehtävien hoidon vaatimalla tasolla ja siten, että ne ovat perusteltavissa määriteltyjen tehtävien hoitamisella (Laki julkisen hallinnon tiedonhallinnasta, 16 §). Käyttöoikeudet ovat lähtökohtaisesti henkilökohtaisia ja niiden elinkaarta hallitaan siten, että oikeuksia muokataan perustellusta tarpeesta ja niitä poistetaan käyttötarpeen päättyessä. Ylläpitäjän oikeuksia myönnetään ja hallinnoidaan asianmukaisesti korkeamman riskin edellyttämällä tavalla.

Käyttöoikeuksia ja niiden käyttöä voidaan valvoa teknisin ratkaisuin ja niitä voidaan auditoida jälkikäteen. Pääsyoikeuksia katselmoidaan säännöllisesti ja katselmointien tuloksena löydetyt poikkeamat korjataan viivytyksettä.

3.4. Turvalliset tietojärjestelmät ja palvelut

Tietoturvallisuus huomioidaan tietojärjestelmien ja digitaalisten palveluiden koko elinkaaren ajan suunnittelusta ja hankinnasta niiden ylläpitoon ja käytöstä poistamiseen. Tietojärjestelmille ja palveluille asetettavat tietoturvavaatimukset määritellään niiden käyttötarkoituksen, käsiteltävien tietojen ja tunnistettujen riskien perusteella. Tietoturvavaatimukset huomioidaan myös hankinnoissa ja palveluntuottajien kanssa tehtävissä sopimuksissa.

Tietojärjestelmiä ja palveluita ylläpidetään suunnitelmallisesti ja niiden tietoturvallisuudesta huolehditaan koko käyttöiän ajan. Havaitut tietoturvapuutteet ja haavoittuvuudet käsitellään niiden aiheuttaman riskin edellyttämällä tavalla. Palveluiden ja tietojärjestelmien käytöstä poistaminen toteutetaan hallitusti siten, että tiedot poistetaan ja käyttöoikeudet käsitellään asianmukaisesti.

3.5. Jatkuvuus, varautuminen ja kyberturvallisuus

Yhtenä tietoturvallisuuden pääperiaatteista Keuruun kaupungilla on jatkuvuuden varmistaminen hallintosäännön seitsemännen luvun mukaisesti varautumalla poikkeustilanteisiin. Tietoturvallisuuden näkökulmasta varautumista tulee toteuttaa siten, että kriittiseksi luokitelluista tietojärjestelmistä ja toiminnoista toteutetaan asianmukaiset jatkuvuussuunnitelmat. Jatkuvuussuunnitelmien mukaisen toiminnan toteuttamista harjoitellaan ja harjoitusten tulosten pohjalta tehdään korjauksia havaittuihin puutteisiin perustuen. Jatkuvuussuunnitelmat pidetään ajan tasalla säännöllisen katselmoinnin avulla ja niissä huomioidaan kriittisten toimintojen ja palveluiden palautuminen sekä toiminnan kannalta olennaiset riippuvuudet ja vastuut.

Keuruun kaupunki huolehtii digitaalisen toimintaympäristönsä turvallisuudesta osana tietoturvallisuutta, riskienhallintaa ja varautumista. Kyberturvallisuuden tavoitteena on suojata kaupungin tietoverkkoja, tietojärjestelmiä, laitteita ja digitaalisia palveluita niihin kohdistuvilta uhkilta sekä turvata kaupungin toiminnan ja palveluiden jatkuvuus.Kaupunki tunnistaa ja arvioi kyberturvallisuuteen liittyviä riskejä sekä toteuttaa niiden perusteella tarkoituksenmukaisia suojaustoimenpiteitä. Kyberturvallisuudessa huomioidaan myös palveluntuottajiin, toimitusketjuihin ja muihin toiminnan kannalta olennaisiin riippuvuuksiin liittyvät riskit.

Kaupunki ylläpitää kykyä havaita ja käsitellä kyberturvallisuuspoikkeamia, rajoittaa niiden vaikutuksia sekä palauttaa toimintansa häiriötilanteen jälkeen. Häiriötilanteisiin varautumista ja niissä toimimista harjoitellaan säännöllisesti yhteistyössä tarvittavien toimijoiden kanssa.Käytännön suojaustoimet, kuten päivitykset, monivaiheinen tunnistautuminen, varmuuskopiointi ja palauttamisen testaus, voidaan kuvata periaatteita täydentävässä tietoturvaohjeessa ja jatkuvuussuunnitelmissa.

3.6. Tietoturvapoikkeamien hallinta

Keuruun kaupungin tietojenkäsittelyn yhteydessä tapahtuvia tai epäiltyjä tietoturvapoikkeamia tunnistetaan, ilmoitetaan, käsitellään ja selvitetään tarkoituksenmukaisilla tavoilla. Jokaisen kaupungin tietoja, tietojärjestelmiä tai palveluita käsittelevän henkilön tulee ilmoittaa havaitsemastaan tai epäilemästään tietoturvapoikkeamasta viivytyksettä määriteltyä ilmoitusmenettelyä käyttäen. Poikkeamiin reagoidaan vakavuuden ja vaikutusten edellyttämällä tavalla. Niiden hallinnassa pyritään rajoittamaan vaikutuksia, turvaamaan toiminnan jatkuvuus sekä selvittämään poikkeaman syyt ja seuraukset.

Tietoturvapoikkeamista saatua tietoa hyödynnetään tietoturvallisuuden, toimintatapojen ja suojaustoimenpiteiden kehittämisessä sekä vastaavien poikkeamien ennaltaehkäisemisessä. Tarvittavat ilmoitukset viranomaisille ja muille tahoille tehdään sovellettavien velvoitteiden mukaisesti. Poikkeamien selvittäminen mahdollistaa toiminnan ja prosessien kehittämisen.

4. Tietoturvan johtaminen, organisointi ja vastuut

Keuruun kaupungin tietoturvallisuuteen liittyvät roolit ja vastuut ovat seuraavat:

Kaupungin valtuusto:

- Päättää kaupungin ja kaupunkikonsernin sisäisen valvonnan ja riskienhallinnan perusteista.

Kaupunginhallitus:

- Tietoturvaperiaatteiden hyväksyminen.
- Huolehtii hallintosäännön sekä sisäisen valvonnan ja riskienhallinnan perusteiden mukaisesti kaupungin sisäisestä valvonnasta ja riskienhallinnan järjestämisestä.
- Vastaa kaupungin ylimmällä tasolla tietoturvallisuuden johtamisesta, valvonnasta ja resursoinnista.

Kaupunginjohtaja:

- Vastaa hallintosäännön mukaisesti sisäisen valvonnan ja riskienhallinnan toimeenpanosta ja tuloksellisuudesta toimialallaan ja tulosalueellaan, ohjeistaa alaisiaan tulosyksiköitä sekä raportoi kaupunginhallituksen antamien ohjeiden mukaisesti.
- Vastaa tietoturvallisuuden toimeenpanon edellytysten luomisesta.
- Johtaa toimintaa vakavissa häiriö- ja poikkeustilanteissa.
- Varmistaa tietoturvallisuustyön resurssien riittämisen.

Konsernipalvelujohtaja:

- Vastaa hallintosäännön mukaisesti kaupungin sisäisen valvonnan ja konsernin riskienhallinnan toteuttamisen käytännön toimenpiteistä, sekä valmistelee tarkastussuunnitelman.

Toimialajohtajat:

- Vastaavat sisäisen valvonnan ja riskienhallinnan toimeenpanosta ja tuloksellisuudesta toimialallaan.

- Vastaavat tietoturvallisuuden toteutumisesta omalla toimialallaan.
- Vastaavat tietoturvalinjausten toimeenpanosta.
- Vastaavat oman toimialansa järjestelmien, tietojen ja tietovarantojen turvallisuudesta.

Tietosuojavastaava:

- Vastaa Euroopan unionin yleisen tietosuoja-asetuksen (GDPR) määräämistä tehtävistä.
- Opastaa ja neuvoo henkilötietojen tietoturvallisessa käsittelyssä.
- Toimii asiantuntijana järjestelmähankinnoissa, missä käsitellään henkilötietoja.
- Toimii yhteyshenkilönä valtakunnalliseen tietosuojavaltuutettuun.

Tietojärjestelmän, tiedon tai prosessin omistaja:

- Vastaavat omistamansa järjestelmän, tiedon tai prosessin tietoturvan toteutumisesta.
- Kartoittavat tietojärjestelmiensä toimintaan liittyvät riskit sekä käytössä että kehitteillä olevien sovellusten osalta.
- Määrittelevät tehtävien hoitoon vaadittavat käyttöoikeustasot.
- Toteuttavat vastaamansa järjestelmän jatkuvuussuunnitelmat.

Esihenkilö

- Vastaa henkilökuntansa perehdyttämisestä tietoturvallisuusasioihin ja kaupungin ohjeistuksiin.
- Vastaa oman henkilökuntansa osalta ohjeiden noudattamisen valvonnasta.
- Huolehtii henkilökuntansa osalta käyttöoikeuksien ajantasaisuudesta.
- Raportoi havaitsemistaan mahdollisista tietoturvapoikkeamista tietohallinnolle.

Tietohallintopäällikkö

- Vastaa kyberturvallisuuden teknisestä suunnittelusta, koordinoinnista, seurannasta ja kehittämisestä sekä kyberturvallisuuspoikkeamien hallinnan koordinoinnista yhteistyössä toimialojen ja palveluntuottajien kanssa.
- Vastaa tietoturvallisuuden teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.
- Vastaa käyttövaltuushallinnan järjestämisestä.
- Tietohallintopäällikkö raportoi tietoturvallisuuden tilasta, merkittävistä riskeistä ja poikkeamista sekä olennaisista kehittämistarpeista ja korjaavien toimenpiteiden etenemisestä kaupungin johtoryhmälle.

Henkilöstö

- Vastaa tietoturvaperiaatteiden ja -ohjeiden noudattamisesta omassa toiminnassaan.
- Vastaa henkilökohtaisten käyttöoikeuksien ja tiedon asianmukaisesta käytöstä.
- Osallistuu vaadittuihin tietoturvallisuuden koulutuksiin.
- Ilmoittaa viipymättä havaitsemistaan riskeistä, puutteista ja tietoturvapoikkeamista tietohallinnolle.

Palveluntuottajat ja yhteistyökumppanit

- Vastaavat tietoturvallisuudesta ja tietosuojasta sopimuksissa ja muissa velvoittavissa asiakirjoissa määritellyssä laajuudessa.
- Raportoivat viivytyksettä havaitsemansa tietoturvapoikkeamat.

5. Tietoturvatietoisuus ja toimintakulttuuri

Tietoturvallisuus on osa Keuruun kaupungin päivittäistä toimintaa ja jokaisen kaupungin tietoja ja tietojärjestelmiä käsittelevän henkilön vastuuta. Jokaisen tulee tuntea omaan tehtäväänsä liittyvät tietoturvavastuut ja -ohjeet sekä toimia niiden mukaisesti. Tietoturvallisuutta edistetään osana johtamista, esihenkilötyötä ja toimintojen kehittämistä.

Riittävä tietoturvaosaaminen varmistetaan henkilöstön perehdytyksellä, koulutuksella ja ajankohtaisella tietoturvaa koskevalla viestinnällä. Tietoturvaosaamisen tason tulee vastata tehtävien ja vastuiden vaatimuksia, ja osaamista ylläpidetään tarvittaessa toimintaympäristön ja uhkien muuttuessa. Kaupungin henkilöstöä rohkaistaan ilmoittamaan tietoturvallisuuteen liittyvistä riskeistä, puutteista ja poikkeamista viivytyksettä. Havaintojen ja poikkeamien pohjalta toimintaa, osaamista ja tietoturvallisuutta voidaan kehittää jatkuvan kehityksen keinoin.

6. Tietoturvaperiaatteiden valvonta, ylläpito ja kehittäminen

Keuruun kaupungin tietoturvaperiaatteiden ja täydentävien ohjeiden toteutumista seurataan ja arvioidaan säännöllisesti. Seurannan keinoina käytetään muun muassa tietoturvallisuuden tilannekuvaa, tarkastuksia, auditointeja, riskien arviointia sekä tietoturvapoikkeamista, havainnoista ja palautteesta saatavaa tietoa.

Tietoturvallisuutta kehitetään jatkuvasti ja riskiperusteisesti. Kehittämisessä huomioidaan tunnistetut riskit, havaitut puutteet ja poikkeamat, tarkastusten ja auditointien tulokset sekä toimintaympäristön, lainsäädännön, viranomaisvaatimusten ja teknologian muutokset. Havaitut puutteet ja kehittämistarpeet arvioidaan, priorisoidaan ja vastuutetaan niiden riskin ja vaikutusten perusteella. Vakavat tai välitöntä reagointia edellyttävät puutteet käsitellään viipymättä, ja muut korjaavat toimenpiteet toteutetaan suunnitelmallisesti määritellyssä aikataulussa.

Tietoturvaperiaatteet katselmoidaan vähintään kerran vuodessa ja päivitetään tarvittaessa. Periaatteiden toteutumista katselmoidaan lisäksi silloin, kun kaupungin toiminnassa, organisaatiossa, toimintaympäristössä, lainsäädännössä, tietoturvavaatimuksissa tai riskeissä tapahtuu merkittäviä muutoksia. Periaatteisiin tehtävät merkittävät sisällölliset muutokset hyväksyy kaupunginhallitus. Katselmoinnit ja muutokset dokumentoidaan politiikan yhteydessä ylläpidettävään versiohistoriaan.

Ajantasaiset tietoturvaperiaatteet julkaistaan kaupungin asianmukaisissa tiedotuskanavissa, ja sen hyväksymisestä sekä olennaisista muutoksista tiedotetaan henkilöstölle. Politiikan toimeenpanoa täsmennetään erillisellä tietoturvaohjeella ja muilla tarvittavilla ohjeilla, joissa kuvataan periaatteiden soveltaminen käytännön toiminnassa.

Tietoturvallisuuden tilasta, merkittävistä riskeistä ja poikkeamista sekä olennaisista kehittämistarpeista ja korjaavien toimenpiteiden etenemisestä raportoidaan kaupungin johtoryhmälle säännöllisesti ja tarvittaessa kaupunginhallitukselle tässä politiikassa määriteltyjen vastuiden mukaisesti.