Tietoturvapolitiikka

Voimaantulo 01.06.2026

KH 25.05.2026 § 142
YTNK 04.05.2026 § 31

Tietoturvallisuus on meidän yhteinen asia!

Tietoturvapolitiikka

1.6.2026

Sisällys

1. Johdanto

Kotkan kaupungin palveluiden perustana ovat kuntalaisten, kumppanien ja asiakkaiden tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn kaupungin ja sen konsernin toimintaympäristöissä. Kaupungin palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta.

Tietoturvan tärkeyttä lisäävät sähköisten palvelujen laajentuminen, tietojärjestelmien etä- ja mobiilikäyttö, kuntien yhteistyö, laaja palveluntuottajien verkosto sekä palvelutuotannon ja tietojenkäsittelyn nykyaikaiset menetelmät, kuten tekoälyn käyttö.

Kotkan kaupunkistrategiassa (Kotka 2035) tavoitteena on tarjota turvallinen ja sopeutumiskykyinen kaupunki, joka ennakoi ja varautuu mahdollisiin häiriötilanteisiin ja kyberuhkiin. Edistämme asukkaiden turvallisuutta ja hyvinvointia vahvistamalla yhteisöllisyyttä, arjen turvallisuutta ja valmiutta poikkeustilanteisiin.

Tietoturvapolitiikka määrittää Kotkan kaupungin tavoitteita tietoturvan osalta määrittelemällä kaupungin sitoutumisen tietojen suojaamiseen ja tietoturvan ylläpitämiseen sekä hallintajärjestelmän jatkuvaan parantamiseen. Politiikan tavoitteena on varmistaa yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietoturvatason toteuttamiseksi. Tietoturvapolitiikka toimii perustana Kotkan kaupungin tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa tässä annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietoturvapolitiikka koskee koko kaupunkikonsernia, sen jokaista työntekijää ja luottamushenkilöä sekä niitä Kotkan kaupungin sidosryhmien edustajia, jotka työnsä tai toimeksiantojensa puitteissa käsittelevät Kotkan kaupungin omistamaa tai hallinnoimaa tietoa. Politiikka kattaa kaupungin omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä politiikka on saatavissa kaupungin asianhallintajärjestelmässä ja intranetissa ja se liitetään tarvittaessa Kotkan kaupungin toimeksiantosopimuksiin ja huomioidaan hankinnoissa.

1.1 Tietoturvan merkitys Kotkan kaupungille

Lainsäädäntömuutokset mm. EU:n yleinen tietosuoja-asetus (GDPR), tietosuoja-, tiedonhallinta- ja kyberturvallisuuslaki, sekä EU:n saavutettavuusdirektiivi tähtäävät tietoturvan, tietosuojan, riskien arvioinnin ja yhteistoimivuuden huomioimiseen jo järjestelmien tai henkilötietojen käsittelyn suunnitteluvaiheessa sekä suunnittelun kautta saatavaan kustannustehokkuuteen, tietojen käytettävyyteen ja tietoturvallisuuden tilintekokykyisyyteen.

Tieto eri muodoissaan on tärkeä perusta kaupungin toiminnalle. Tietoturvalla tarkoitetaan eri muodoissa olevien tietojen suojaamista uhkatekijöiltä siten, että palveluiden laatu, luotettavuus ja jatkuvuus varmistuvat ja että palveluissa käsiteltäviin ja säilytettäviin tietoihin kohdentuvat riskitekijät minimoidaan.

Tietoturvan järjestämiseen ja hallintaan kuuluun merkittävästi digitaalinen turvallisuus, jonka tavoitteena on kaupungin toimintaympäristön turvallinen hallinta sekä luotettavuus myös häiriötilanteissa. Digitaalinen turvallisuus koostuu tietoturvallisuudesta, tietosuojasta, kyberturvallisuudesta, riskienhallinnasta sekä toiminnan jatkuvuudenhallinnasta ja varautumisesta.

Tietosuoja on merkittävä osa tietoturvaa ja se tarkoittaa ihmisten yksityisyyden kunnioittamista ja suojelemista oikeudellisia säännöksiä noudattavin periaattein ja käytännöin.

1.2 Tietoturvallisuuden määritelmä

Tietoturvallisuus koostuu toimista, joilla varmistetaan tietojen, tietojärjestelmien ja palvelujen turvaaminen niin, että niiden luottamuksellisuus, eheys ja saatavuus voidaan taata ja osoittaa toteutuneen.

- Eheys: Tieto on oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
- Luottamuksellisuus: Tieto on vain siihen oikeutettujen saatavilla.
- Saatavuus: Tieto on saatavilla tarvittaessa.
- Kiistämättömyys: Tietoon tehdyt muutokset sen käsittelyn eri vaiheissa pystytään tarvittaessa todentamaan.
- Todentaminen: Varmistetaan kohteen todenmukaisuus, oikeellisuus, alkuperä tai varmistetaan käyttäjän aitous määritellyllä luottamustasolla.

Hyvä tietoturvallisuustaso saavutetaan tietoturvapolitiikan, linjauksien ja ohjeiden mukaisilla toimintaperiaatteilla ja erilaisilla turvamekanismeilla, joita hallitaan ja katselmoidaan jatkuvan kehittämisen periaatteita noudattaen.

Tietosuojaa käsitellään tarkemmin Kotkan kaupungin tietosuojaohjeistuksessa.

1.3 Kyberturvallisuus

Kyberturvallisuudella tarkoitetaan tässä digitaalisen ja verkottuneen kaupungin turvallisuutta sekä vaikutusta kaupungin toimintoihin. Kyberturvallisuuden uhat eivät liity ainoastaan tiedon käsittelyyn, vaan ne voivat liittyä mihin tahansa kaupungin digitaalisten palveluiden ongelmiin, näistä esimerkkeinä sähkökatkot tai internetyhteyksien häirintä.

Kyberturvallisuuden varautumisen toimilla varmistetaan Kotkan kaupungin sisäistä turvallisuutta sekä sitä, ettei kaupungin tietojärjestelmiä tai -verkkoja käytetä kyberiskujen ja/tai hakkerointien suunnittelussa.

Kotkan kaupungin kyberturvallisuuteen varautuminen liitetään kaupungin valmius- ja riskienhallintasuunnitelmaan, jossa määritetään kaupungin kriittiset toiminnot, tuotettavat palvelut ja niihin liittyvät kriittiset järjestelmät, kuten laitteet ja ohjelmistot, joiden toiminta tulee varmistaa kaikissa tilanteissa (kriittisten toimintojen määrittely). Tehtyä suunnitelmaa, tulee harjoitella säännöllisesti.

Kuva 1. Tietoturvallisuuden ja kyberturvallisuuden suhde
Mukaellen lähdettä: Amit. 2016. Understanding difference between Cyber Security & Information Security,www-dokumentti.

Kuva 2. Tietoturvallisuus integroituu kuvan mukaisesti kaikkiin kokonaisuuden osa-alueisiin: turvallisuus, riskienhallinta sekä jatkuvuudenhallinta ja varautuminen.

1.4 Kotkan kaupungin toimintaympäristö ja tietoturvan kehittämisajatus

Kaupungin toimintaympäristö

Kotkan kaupungin palveluiden häiriötön toiminta on perusta arjen toimivuudelle ja uuden kehittämiselle. Digitaalisten palveluiden kehittäminen on yksi keskeisistä tavoitteista, jossa tiedon hyödyntämisen avulla parannetaan palveluiden laatua, tehokkuutta ja vaikuttavuutta.

Kaupungin tuottamat palvelut ovat riippuvaisia digitaalisen toimintaympäristön luotettavasta toiminnasta. Yhteiskunnan digitaalisen kehittymisen myötä kaupunkien toimintaympäristöt ja niihin liittyvät uhkatekijät ovat muuttuneet ja muutoksen myötä on tunnistettu uudenlaisia haasteita tietojen ja toimintojen turvaamisen näkökulmasta.

Digitaalisen palveluympäristön hallinta edellyttää suunnitelmallisuutta ja kyvykkyyttä varautua odottamattomiin tapahtumiin ja toipua niistä kriittiset toiminnot turvaten.

Tietoturvan kehittämisajatus

Tietoturva on kiinteä osa johtamista, riskienhallintaa ja palvelutoimintaa. Kotkan kaupunki pyrkii olemaan aktiivinen ja verkostoitunut digitaalisten palveluiden ja digitaalisen turvallisuuden kehittäjä. Henkilökunnan on tärkeä ymmärtää digitaalisen turvallisuuden merkitys työtehtävissään ja motivoitua noudattamaan yhteisesti sovittuja tietoturvallisia toimintatapoja.

1.5 Tietoturvatoimintaa ohjaavat tekijät

Kotkan kaupungin tietoturvallisuutta velvoittavat ja ohjaavat kansalliset ja kansainväliset yleiset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Lakivelvoitteiden lisäksi tietoturvallisuutta ohjaavat erilaiset määräykset ja ohjeet, kuten esimerkiksi toimittajien kanssa tehdyt turvallisuussopimukset. Kaupungin tietoturvallisuutta koskeva lainsäädäntö on lueteltu liitteessä 1.

Keskeinen asia on tunnistaa toimintaympäristön ne rakenteet, joiden toimimattomuus vaikeuttaisi merkittävästi Kotkan kaupungin tehtävien suorittamista, aiheuttaisi merkittäviä taloudellisia tai muita vahinkoja tai heikentäisi henkilöstön tai kuntalaisten turvallisuutta.

Digitaalinen turvallisuus tulee huomioida päivittäisessä toiminnassa ja palveluiden kehittämisessä, minkä avulla varmistetaan tietoturvan, tietosuojan ja lainsäädännön vaateiden toteutuminen ja varaudutaan erilaisiin uhkatilanteisiin.

Kaupungin johdon tehtävänä on ohjata tietoturvallisuuden kehittämistä strategisella tasolla.

2. Tietoturvan tavoitteet

Tietoturvatyö on kiinteä osa Kotkan kaupungin johtamista ja riskienhallintaa ja sen avulla luodaan yhdenmukaiset, yhdessä sovitut tietoturvakäytänteet. Tavoitteena on kehittää kaupungin toimintaympäristön digitaalisen turvallisuuden hallintaa ja sen avulla varmistaa palvelutoiminnan luotettavuus ja jatkuvuus. Tietojen oikeaoppinen ja tarkoituksenmukainen käsittely turvataan yhdenmukaisilla tietoturvakäytänteillä, jotka ovat tiedonhallintalain edellyttämiä. Tietoturvallisilla palveluilla ja tietosuoja huomioiden varmistetaan kuntalaisten luottamus Kotkan kaupungin palvelutuotantoon.

2.1 Tietoturvan uhkatekijöiden tunnistaminen ja hallinta

Tiedonhallintalaki velvoittaa Kotkan kaupunkia tunnistamaan merkittävät tietojenkäsittelyyn kohdentuvat riskitekijät ja hallitsemaan niiden tietoturvatoimenpiteitä riskilähtöisesti. Digitaalisen toimintaympäristön hallinnassa varmistetaan kyvykkyys tunnistaa tietoturvaan kohdentuvia uhkatekijöitä ja pyritään reagoimaan poikkeamiin proaktiivisesti. Tietoturvan hallinnan tason tulee noudattaa lainsäädännön velvoitteita ja sen tulee pystyä tukemaan kaupungin toimintaympäristön ja palveluiden asettamia vaatimuksia.

2.2 Palveluiden jatkuvuuden ja tietojen turvaaminen

ICT-järjestelmien keskeytymätön toiminta täytyy turvata. Tietojen luvaton käyttö sekä tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen täytyy havaita ja estää, ja näistä mahdollisesti aiheutuvat vahingot tulee minimoida.

Kriittisten toimintojen saatavuus varmistetaan sekä normaalioloissa että poikkeusolojen häiriötilanteissa mahdollisimman lyhyellä toipumisajalla. Palveluiden omistajat ja keskeiset sidosryhmät ylläpitävät tietoturvallisuuden hallintamallia määrittelemällä kriittisyysluokittelut ja hallinnalliset toimenpiteet tietojärjestelmille, tiedoille ja palveluille.

2.3 Henkilöstön tietoturvatietoisuuden, tietosuojan ja osaamisen kehittäminen

Tietoturvapolitiikka ja tietoturvallisuusohjeistukset sekä tietosuojakäytänteet sisällytetään osaksi kaupungin johtamista ja käytännön toimintaa. Toiminta vaatii henkilökunnalta tietoturvakäytänteiden tuntemista ja ohjeiden noudattamista. Tietoturva- ja tietosuojakoulutukset ovat osa säännöllistä kehittämis- ja perehdyttämistoimintaa. Jokainen työntekijä ja valtuutettu on velvollinen suorittamaan Kotkan kaupungin edellyttämät tietoturvallisuuskoulutukset.

Koulutusten lisäksi henkilöstöä ohjataan positiivisen tietoturvakulttuurin ylläpitämiseen. Tavoitteena on parantaa kaupungin kykyä vastata tietoturvan uhkakuviin ja ylläpitää kuntalaisten ja eri sidosryhmien luottamusta kaupungin tarjoamiin palveluihin sekä niiden tietoturvan, tietosuojan ja yksityisyydensuojan toteutumiseen.

2.4 Tietoturvan varmistaminen läpi toiminnan

Tietoturvallisen toimintaympäristön hallittavuus edellyttää yhteistyökumppanien sitouttamista ja velvoittamista sopimuksin noudattamaan kaupungin tietoturvakäytänteitä.

Hankinnoissa sopimuksen omistaja huomioi tietoturva- ja tietosuojasitoumusten laatimisen yhteistyökumppanien kanssa. ICT-sopimuksissa huomioidaan myös toiminnallinen vastuunjako tietoturvan, tietosuojan, palveluiden jatkuvuuden ja varautumisen osalta, esimerkiksi RACI-mallilla.

Sopimuksiin tulee olla kirjattu myös seuraavat asiat: säännöllinen raportointi palvelutason toteutumisesta, häiriötilanteiden hallinnasta ja tietoturvapoikkeamista sekä rikkomuksiin liittyvistä käytänteistä ja sanktioista.

2.5 Toiminnan kehittäminen tietoturvallisuustyö huomioiden

Tietoturva- ja tietosuojatyön tavoitteena on osaltaan varmistaa, että noudatamme kulloinkin voimassa olevia lainsäädännön vaateita, kansallisia tietoturvaohjeistuksia jokapäiväisessä työssä ja digitaalisten palveluiden kehittämisessä. Uusia palveluita hankittaessa tulee jo suunnitteluvaiheessa huomioida tietosuojan vaikutusten arvioinnin perusteet, mikäli palvelussa käsitellään henkilötietoja.

Toimintaympäristössä tapahtuvissa merkittävissä muutoksissa muutoksesta vastaava taho laatii tiedonhallinnan muutosvaikutusten arvioinnin (Laki julkisen hallinnon tiedonhallinnasta 906/2019). Arvioinnilla varmistetaan muutosten hallinnolliset, taloudelliset, toiminnalliset ja riskeihin perustuvat vaikutukset, millä pyritään varmistamaan järjestelmien yhteentoimivuus, tietoturvallisuus ja tietoaineistojen lainmukainen käsittely.

2.6 Tietosuojan varmistaminen

Tietosuoja on merkittävä osa toiminnan vaatimustenmukaisuutta, tietoturvallisuutta ja riskienhallintaa. Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata kuntalaisten, asiakkaiden, henkilöstön ja sidosryhmien henkilötietoja sekä varmistaa toiminnan läpinäkyvyys rekisteröidylle.

Kaupunki käsittelee henkilötietoja sisäänrakennetun ja oletusarvoisen tietosuojan toimintaperiaatteiden mukaisesti, kulloinkin voimassa olevaa lainsäädäntöä noudattaen.

Kotkan kaupungin tietosuojatyön toimintaperiaatteet ovat:

1. Keräämme ainoastaan käyttötarkoitusten kannalta tarpeellisia henkilötietoja kaupungin tehtävien suorittamiseksi ja palveluiden kehittämiseksi

2. Huolehdimme suunnitelmallisesti ja läpinäkyvästi henkilötietojen suojaamisesta ja elinkaarenhallinnasta
3. Varmistamme säännöllisen koulutuksen avulla, että työntekijöillä on riittävä tietosuojaosaaminen tehtävänkuvan mukaan
4. Mahdollistamme asiakkaillemme tiedonsaannin omiin henkilötietoihin ja informoimme kattavasti henkilötietojen käsittelyn periaatteita
5. Arvioimme säännöllisesti henkilötietojen käsittelyyn liittyviä riskejä yksilöiden oikeuksille ja vapauksille
6. Varmistamme sopimuksin, että kumppanimme noudattavat vähintään lainsäädännön edellyttämiä tietosuojaperiaatteita.

Tietosuojalla turvataan rekisteröidyn henkilön oikeuksien ja vapauksien toteutuminen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Henkilötietojen käsittelyssä määritellään aina rekisterinpitäjä. Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä, oikeushenkilöä tai viranomaista, jonka käyttöä varten henkilörekisteri perustetaan tai jonka tehtäväksi rekisterinpito on lailla säädetty.

Rekisterinpitäjällä on vastuu henkilötietojen käsittelyn lainmukaisuudesta ja velvollisuus tehdä tietosuojan vaikutustenarviointi ja laatia tietovirtakuvaukset osoitusvelvollisuuden toteuttamiseksi (Tietosuojalaki 1050/2018 ja EU:n yleinen tietosuoja-asetus 679/2016).
Rekisterinpitäjä määrittää, mihin käyttötarkoitukseen ja millä keinoin henkilötietoja käsitellään.

2.7 Lokitietojen hallinta

Lokitiedoilla valvotaan tietoturvan ja tietosuojan toteutumista ja jäljitettävyyttä, ennaltaehkäisten tai todentaen poikkeavia tapahtumia tai väärinkäytöksiä. Lokitiedot kerätään aina, kun tietojärjestelmän tai palvelun käyttö edellyttää tunnistautumista tai muuta kirjautumista.

Kerättävät lokitiedot määritellään osana tietojärjestelmien ja tietoaineistojen käsittelyn suunnittelua määrittelyvaiheessa tai tietojärjestelmäpalvelun hankinnan yhteydessä.
Lokien käsittely ja määrittely on ohjeistettu Lokiohjeessa.

2.8 Käyttövaltuuksien hallinta

Pääsynhallinnan ja käyttäjähallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään luvatonta käyttöä. Hallinnan tulee noudattaa vähimpien oikeuksien periaatteita ja sen on toteuduttava järjestelmän tai palvelun koko elinkaaren ajan.

Jokainen Kotkan kaupungin henkilöstöön kuuluva työntekijä sitoutuu tietojen ja tietojärjestelmien tietoturvalliseen ja ohjeiden mukaiseen käyttöön hyväksymällä tätä koskevan sähköisen tietoturvallisuussitoumuksen. Vastaavasti em. sitoumus edellytetään niiltä Kotkan kaupungin luottamushenkilöiltä ja muilta, joille sallitaan oikeus käyttää Kotkan kaupungin omistamia tietojärjestelmiä.

Tietojärjestelmissä ja laitteissa ei hyväksytä työntekijöiden yhteiskäyttötunnuksia, poikkeuksina järjestelmissä tarvittavat systeemitunnukset. Työaseman paikallisen järjestelmävalvojan tunnuksen käyttö edellyttää tietohallinnon hyväksyntää. Käyttövaltuushallintaa koskevat määräykset on kuvattu Käyttövaltuusohjeessa

Tietoturvallinen toimintatapa on kuvattu Tietoturvallisuutta henkilöstölle ohjeessa. Laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi Tietoturvarikkomusten seuraamustaulukon mukaisesti Liitteessä 5.

3. Tietoturvallisuuden organisointi ja vastuut

Kotkan kaupungin tietoturvavastuut on kuvattu liitteessä 2. Tietoturvavastuut ja niiden jakautuminen kaupungin ja keskeisten sidosryhmien ja yhteistyökumppaneiden osalta tulee kuvata ja sopia kirjallisesti. Tästä vastaavat palveluista vastaavat henkilöt.

Kotkan kaupungin kokonaisvaltaisen riskienhallinnan ja sitä kautta tietoturvan ja tietosuojan toteuttamisen kokonaisvastuu on kaupunginhallituksella ja kaupunginjohtajalla. Kaupungin johto sitoutuu tietoturvan ja tietosuojan jatkuvaan kehittämiseen ja huolehtii työn riittävästä resursoinnista ja jatkuvuudesta.

Kaupunginhallitus toimii rekisterinpitäjänä tilanteissa, joissa tieto on käytettävissä useammalla kuin yhdellä kaupungin toimialalla. Rekisterinpitäjä määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Lautakunnat vastaavat toimialueensa tietoturvallisesta toiminnasta ja tietosuojan järjestämisestä ja ovat vastuualueiden ja yksiköiden henkilötietojen käsittelyssä tietosuoja-asetuksen tarkoittamia rekisterinpitäjiä.

Tietoturvan ja tietosuojan ohjaaminen sekä tietoturvapolitiikan valmistelu kaupunginhallituksen päätettäväksi kuuluvat Tietoturvallisuus- ja julkisuusryhmän tehtäviin. Tietoturvallisuus- ja julkisuusryhmä hyväksyy tietoturvapolitiikkaan tehtävät vähäiset muutokset, jotka eivät edellytä

kaupunginhallituksen hyväksymistä. Tietoturvallisuusohjeet ja niitä koskevat muutokset hyväksytään Tietoturvallisuus ja julkisuusryhmässä.

Poikkeusluvan Kotkan kaupungin tietoturvapolitiikassa, standardeissa ja ohjeissa kuvattuihin menettelytapoihin myöntää Kotkan kaupunginhallitus. Kotkan kaupunginhallitus hyväksyy tietoturvapolitiikan ja määrittelee kaupungin johtamista, palveluja ja toimintoja koskevat tietoturvallisuuden periaatteet, vastuut ja tavoitteet.

4. Tietojen luokittelu

Kotkan kaupungin omistamat tiedot luokitellaan tietovarannon omistajan toimesta. Tietojen luokittelu perustuu lakiin viranomaisten toiminnan julkisuudesta ja Hallintoyksikön antamiin ohjeisiin lain soveltamisesta.

Pilvipalveluiden käytössä tulee huomioida, että luokittelematonta tietoa ei saa viedä pilvipalveluun. Sallitut pilvitallennuspaikat dokumentoidaan sekä ohjeistetaan ja tiedotetaan käyttäjille. Pilvipalvelun käyttö tallennuspaikkana ei saa olla ristiriidassa tietosuojaa, tietoturvaa tai tekijänoikeuksia määrittelevän lainsäädännön kanssa.

Tarkemmat määräykset löytyvät Tiedon käsittelyohje-dokumentista.

Kotkan kaupungin omistamat tietojärjestelmät tunnistetaan, luokitellaan kriittisyyden perusteella ja niille nimetään omistaja. Tietojärjestelmäluetteloa ylläpidetään tiedonhallintamallin kuvausjärjestelmässä.

5. ICT – ympäristön hankinnat, laitteet, tietoverkot ja järjestelmät

Uutta ICT-järjestelmää tai -palvelua ei saa hankkia, ennen kuin sille on määritetty omistaja. Omistajalla on aina virkavastuu. Omistaja vastaa, että hankinnassa huomioidaan tiedonhallintalain ja toiminnan vaatimukset tietoturvallisuudesta, varautumisesta, jatkuvuudesta, lokitietojen keräämisestä ja mahdollisesta tiedon siirtämiseen liittyvistä rajapinnoista.

Omistaja vastaa myös hankittavan ICT-järjestelmän tai – palvelun sopimuksesta ja sopimushallinnasta kaupungin ohjeistuksen mukaisesti. ICT-järjestelmien hankinnoissa noudatetaan Digikehittämisen toimintamallia. Uutta järjestelmää hankittaessa tulee myös huolehtia käytöstä poistuvan järjestelmän tietoaineiston käyttö- ja säilytystarpeesta.

Kotkan kaupungin tietojärjestelmä- ja tietoverkkoympäristöön saa liittää ja siinä käyttää ainoastaan tietohallinnon hyväksymiä laitteita.

Kotkan kaupungin henkilöstön käyttöön luovuttamat ICT-laitteet, ohjelmistot, tietojärjestelmät sekä tieto ovat tarkoitettuja vain työtehtävien hoitamiseen.

Kotkan kaupungin tietoverkko on tarkoitettu ainoastaan kaupungin palvelutuotannon käyttöön, sitä ei saa käyttää ulkopuolisten toimijoiden tarpeisiin, jotka eivät liity kaupungin palvelutuotantoon tai toimeksiantoihin.

Asennustyöt suorittavat Kotkan kaupungin kanssa sopimussuhteessa olevat toimijat. Kaupungin ja näiden toimijoiden välisissä sopimuksissa tulee huomioida tietoturvallisuuteen liittyvät vastuut ja velvoitteet.

6. Tietoturva-arvioinnit

Tietoturvatason arvioinnit ja auditoinnit ovat osa tietoturvallisuuden hallintaa. Toimenpiteiden tavoitteena on todentaa, miten tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta on huolehdittu.

Arvioinnit tuottavat tilannetietoa, jonka avulla tunnistetaan tietoturvaan mahdollisesti kohdentuvia uhkia ja haavoittuvuuksia. Arviointien tavoitteena on varmistaa palveluiden jatkuvuus ja toiminnan laatu.

Arviointeja voidaan kohdentaa myös ICT-palvelutuottajiin ja tämä tulee kirjata kaupungin ja palvelutoimittajan välisiin sopimuksiin.

Arviointikohteet vuosikellotetaan ja priorisoidaan kriittisyyden perusteella ja käsitellään tietoturvallisuus- ja julkisuusryhmässä. Tehdyt arvioinnit raportoidaan tietotilinpäätöksessä.

7. Tietoturvaosaamisen ja -tietoisuuden ylläpito

Jokaisen Kotkan kaupungin ICT-laitteita ja järjestelmiä käyttävän työntekijän tulee suorittaa tietoturvan perusteet sisältävän verkkokoulutuksen. Kotkan kaupungin tietoturvaohjeet löytyvät asianhallintajärjestelmästä ja intrasta.

Työntekijöiden tietoturvatietoisuuden ylläpitäminen tapahtuu intran tietoturvasivujen ja käytössä olevan koulutusportaalin kautta.

Tietoturvallisuuden ylläpidosta, kehittämisestä ja johtamisesta vastaaville tarjotaan mahdollisuus riittävän perus- ja jatkokoulutuksen hankkimiseen.

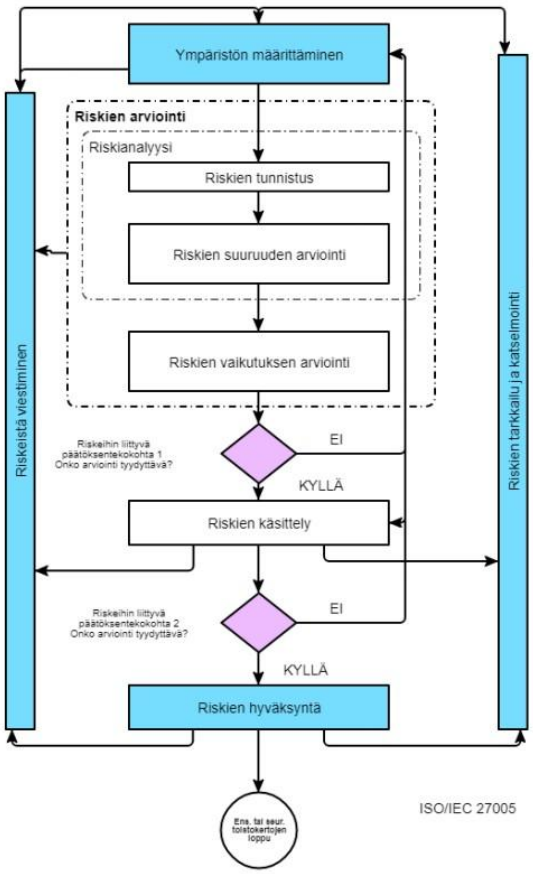
8. Tietoturvallisuudesta tiedottaminen

Tietoturvallisuuteen liittyvä henkilöstön tiedottaminen ajankohtaisasioista, ohjeista ja poikkeamatilanteista tehdään pääsääntöisesti intranetissä. Jokainen esihenkilö on velvollinen seuraamaan ja varmistamaan, että henkilöstö seuraa tiedotteita.

Teknistä tietoturvaa (esim. virustorjunta, palomuurit, roskapostisuodatus, valvonta) toteuttavien ICT - palveluntuottajan / -tuottajien kanssa sovitaan kirjallisesti poikkeamatilanteiden tiedotusmenettelyistä ja yhteyshenkilöistä.

9. Tietoriskien hallinta

Tietoriskien hallinnan perusta on riskien tunnistaminen ja vaikutusanalyysin muodostaminen sekä tarvittavista toimenpiteistä päättäminen riskien hallitsemiseksi.



Kuva 3. Kotkan kaupungin tietoriskien hallintaprosessi.

10. Toiminta poikkeustilanteissa ja -oloissa

Kaupungin toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Kaupungin palveluista vastaavat palvelu- ja vastuualueet sekä yksiköt ja tytäryhtiöt laativat kukin omat suunnitelmansa kriisien varalle. Suunnitelmat kootaan yhteen Kotkan kaupungin valmiussuunnitelman yleiseen osaan. Varautumistyötä johtaa kaupunginjohtaja yhdessä kaupunginhallituksen sekä valmiusjohtoryhmän kanssa.

Suunnittelussa tulee varautua pieneen, keskisuureen ja suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin. Poikkeusoloissa toimintaa johtaa viranomainen (johtovastuu voi muuttua tilanteen edetessä) ja kaupungin valmiussuunnitelma / häiriötilanteiden suunnittelu ja kaupunki tukevat sen toimintaa. Poikkeusolojen ja vakavien häiriötilanteiden varalta on päätökset käskyvaltasuhteiden muutoksista valmisteltava huolellisesti ennakolta, jotta tilanteen niin vaatiessa siirtyminen toimimaan linjaorganisaationa on nopeasti toteutettavissa. Huolellista ennakkovalmistelua edellyttävät erityisesti sopimusohjaustilanteet.

Kotkan kaupunginvaltuusto hyväksyy kaupunkikonsernia koskevat Sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa.

Kotkan kaupungissa on määritetty toimintaprosessi liittyen toimintaan tietoturvaloukkausten tapahtuessa ja se löytyy intranetistä, prosessikuvauksista sekä asianhallintajärjestelmästä. Tämän prosessin mukaista toimintatapaa noudatetaan tietoturvapoikkeamissa.

Kaupunki varautuu turvaamaan tiedonhallintaan liittyvien kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti.

10.1 Turvatoimien priorisointi

Kotkan kaupungin käytössä olevista tietojärjestelmistä ja palveluista on määriteltävä ja kuvattava suojattavat kohteet. Näiden toipumis- ja jatkuvuussuunnitelmissa tulee huomioida tietoturvallisuuteen kohdistuvat uhat ja toiminta poikkeamatilanteissa (esim. palvelunestohyökkäysten vaikutus). Suojattavat kohteet on priorisoitava.

11. Tietoturvallisuuden seuranta, ylläpito, kehittäminen ja resursointi

Kotkan kaupungin tietoturvallisuustyö perustuu toiminnan, teknologian ja osaamisen jatkuvaan kehittämiseen tietoturvan hallintamallin mukaisesti noudattaen jatkuvan kehittämisen periaatteita:

SUUNNITTELU: Tuotetaan johdon ja tietoturvasta vastaavien toimesta ohjeistuksia, periaatteita ja suunnitelmia. Tälle vaiheelle vaatimuksia asettavat mm. lainsäädäntö, riskienhallinnan tulokset, vaatimukset (sopimukset, asiakkaat ja sidosryhmät) sekä toimintaolosuhteet.

TOTEUTUS: Edellisen vaiheen päätökset ja suunnitelmat otetaan käyttöön, tiedotetaan ja jalkautetaan niin henkilökunnalle kuin myös kumppaneille ja asiakkaille.

SEURANTA: Suoritetaan tietoturvallisuuden teknistä valvontaa ja raportointia sekä arvioidaan ratkaisevatko toteutetut toimenpiteet tunnistettuja tietoturvariskejä ja vähenivätkö ne suunnitellulle tasolle.

MUUTOSHALLINTA: Toteutetaan muutoshallintaa seurantavaiheen tuloksista opitun perusteella.

Kuva 4. Kotkan kaupungin tietoturvallisuustyön jatkuva kehittäminen

RESURSOINTI: Resurssit suunnataan tietoturvallisuuden kannalta keskeisiin kohteisiin. Tietoturvallisuuden edellyttämät resurssitarpeet tulee huomioida taloussuunnittelussa sekä kehysprosessissa.

Liiteluettelo

Liite 1 Lakiluettelo
Liite 2 Tietoturvavastuut
Liite 3 Keskeiset käsitteet
Liite 4 Tietoturvallisuuden osa-alueet
Liite 5 Tietoturvarikkomusten seuraamustaulukko

Liite 1 Lakiluettelo
Julkinen

Tietoturvaan liittyvää lainsäädäntöä

Kyberturvallisuuslaki (124/2025)
Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta (125/2025)
AI Actia täydentävä kansallinen laki (valmisteilla, HE 46/2025)

Perustuslaki (731/1999)
Kuntalaki (410/2015)

Hallintolaki (434/2003)
Laki julkisen hallinnon tiedonhallinnasta (906/2019)
Laki digitaalisten palvelujen tarjoamisesta (306/2019)
Arkistolaki (831/1994)
Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
Laki viranomaisen toiminnan julkisuudesta (621/1999)

Tietosuojalaki (1050/2018)
Euroopan unionin yleinen tietosuoja-asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU 679/2016)

Laki yksityisyyden suojasta työelämässä (759/2004)
Laki kunnallisesta viranhaltijasta (304/2003)
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009)
Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
Rikoslaki (39/1889)
Työsopimuslaki (55/2001)
Valmiuslaki (1552/2011)
Tekijänoikeuslaki (404/1961)

Liite 2 Tietoturvavastuut
Julkinen

Tietoturvavastuut Kotkan kaupungissa

Tietoturvallisuuden vastuujärjestelyn tulee seurata kaupungin toiminnan mahdollisia muutoksia. Monet alla mainituista vastuista voivat kuulua samankin henkilön tehtäviin ja vastuisiin. Olennaista on, että näiden tehtävien hoito on järjestetty, myös varahenkilöiden osalta.

Yleinen vastuu tietoturvallisuuden valvonnasta ja ylläpitämisestä

Tietoturvallisuuden valvontaan ja ylläpitämiseen osallistuu jokainen kaupungin henkilöstöön ja järjestelmien ja palveluiden käyttäjiin kuuluva osana omaa yleistä toimintavastuutaan.

Turvallisuus on osa työtehtäviä

Suurin osa tietoturvallisuuden toteuttamiseksi tehdystä työstä sisältyy Kotkan kaupungissa työskentelevien normaaleihin tehtäviin. Tietoturvallisuuden ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityisasiantuntemusta ja nimettyjä turvallisuusvastuuhenkilöitä.

Tietoturvallisuuden erityisvastuut

Rooli	**Vastuu**	**valvontavastuu**
Kaupunginvaltuusto	Hallintosäännön hyväksyminen	
Kaupunginhallitus	Tietoturvapolitiikan hyväksyminen	Kaupunginvaltuusto
Kaupunginjohtajan johtoryhmä	Tietoturvapolitiikan käsittely Tietoturvan kehityshankkeiden hyväksyminen Poikkeustilanteiden koordinointi: valmiusjohtoryhmä	Talousjohtaja tai kansliapäällikkö vie johtoryhmän käsittelyyn.
Kansliapäällikkö	Tietoturvallisuus- ja julkisuusryhmän johtaminen	Kaupunginjohtaja
Talousjohtaja, tietohallinto	Kaupungin tietoturvaratkaisujen määrittäminen, kehittäminen, arviointi ja muutoksien hyväksyminen Vastaa keskitettyjen tietoturvallisuuden kehittämishankkeiden, ohjeistuksien ja koulutuksen valmistelusta ja toteutuksesta Avustaa johtoa ja yksiköitä tietoturvallisuuden toimeenpanossa yhteistyössä tietotyöryhmän kanssa Tietoturvapolitiikan valmistelu ja ylläpito	Kansliapäällikkö
Tietoturvallisuus- ja julkisuusryhmä	Kaupungin tietoturvaohjeiden- ja käytäntöjen ohjaaminen, koordinointi ja hyväksyntä Vastaa tietoturvaan liittyvien poikkeustilanteiden käsittelystä kuvatun prosessin mukaisesti Raportoi ylimmälle johdolle tietoturvallisuudesta	Kansliapäällikkö
Kiinteistöhallinto	Toimitilaturvallisuus ja vartiointi	Tekninen johtaja

Liite 2 Tietoturvavastuut
Julkinen

Vastuualueiden ja toimintayksiköiden johtajat, palveluyksikön johtaja tai päällikkö	Tietoturvallisuuden toteutuminen alaisessaan toiminnassa Tiedon ja tietojärjestelmien omistajien määrittäminen johtamisjärjestelmän vastuiden mukaisesti Oman yksikkönsä tietoturvakoulutukseen osallistumisesta huolehtiminen Vastaa, että yksiköllä on sen oman toiminnan erityisvaatimukset huomioiden tarkennetut tietoturvaohjeet Pääkäyttäjien määrittely	Kaupunginjohtaja kansliapäällikkö
Esihenkilö	Tietoturvan toteutumisen valvonta	Yksikönjohtaja tai ao. esihenkilö
Pääkäyttäjä	Tietojärjestelmien käyttövaltuuksien määrittely ja ohjeistus	Ao. esihenkilö
Alihankkijat ja konsultit	Ostopalvelut, joissa palvelun toteutus on sopimuspohjaisesti luovutettu, ICT–palvelun operatiivisesta ja teknisestä tietoturvasta ja sen ohjeistamisesta vastaaminen	Sopimuksen vastuuhenkilö(t)

Liite 3 Keskeiset käsitteet
Julkinen

Eheys (integrity)
Ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Fyysinen turvallisuus (physical security)
Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää mm. kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan.

Hallinnollinen tietoturva (administrative and organizational information security)
Tietoturvaan tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.

Henkilöstöturvallisuus (personnel security)
Henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen sekä työyhdistelmien järjestelyihin liittyvien turvallisuustekijöiden hoitamista.

Kyberturvallisuus (cyber security)
Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön (yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö) toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot.

Käytettävyys (availability)
Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Luottamuksellisuus (confidential)
Vain tietyn henkilön tai tiettyjen henkilöiden tietoon tarkoitettu.

Tietoaineistoturvallisuus (data security)
Tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Tietoturva (information security)
Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta.

https://termipankki.fi/tepa/fi/haku/tietoturva
Sanastokeskus TSK ry, SSN 1795-6323, Kyberturvallisuuden sanasto (TSK 52)

Liite 4 Tietoturvallisuuden osa-alueet
Julkinen

Tietoturvallisuuden osa-alueet

Hallinnollinen turvallisuus
Hallinnollinen tietoturva koostuu johdon hyväksymistä periaatteista, vastuunjaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista ja valvonnasta.

Ohjelmistoturvallisuus
Käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, pääsynvalvonta- ja varmistusmenettelyt, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.

Tietoaineistoturvallisuus
Tietoaineistoturvallisuudella säilytetään asiakirjojen, tietueiden ja tiedostojen luottamuksellisuus sekä estetään tietojen tuhoutuminen tai tahaton muuttuminen. Oleellista on myös tallenteiden suojaaminen ja oikeanlainen säilyttäminen.

Käyttöturvallisuus
Käyttöturvallisuutta ovat salasanat, käytössä olevien ohjelmien osaaminen ja virustentorjunta. Annettujen käyttöoikeuksien tulee olla mukautettu työtehtäviin. Käyttöturvallisuus koostuu järjestelmien turvallisista käyttöperiaatteista, tietojenkäsittelytapahtumien valvonnasta sekä jatkuvuuden turvaamisesta. Laitteiden käyttövarmuus on myös käyttöturvallisuutta. Toipumissuunnittelun vulla varmistetaan toiminnan jatkuminen jonkun yllättävän tilanteen ilmaantuessa.

Laitteistoturvallisuus
Tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi.

Tietoliikenneturvallisuus
Tietoliikenneturvallisuudella pyritään varmistamaan tietoturvan perustavoitteet eli verkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Keskeisenä tavoitteena on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus. Tietoliikenneturvallisuudessa on kyse kaikista niistä toimenpiteistä, joilla varmistetaan tietojen turvallisuus tiedon liikkuessa järjestelmän sisällä tai organisaatioiden välillä.

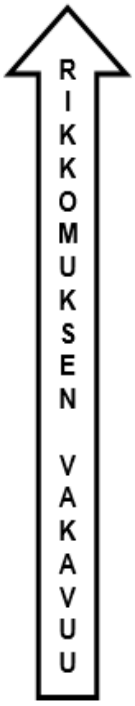
Henkilöstöturvallisuus
Henkilöstöturvallisuuden tavoite on, ettei työntekijä tietämättömyyden, huonon motivaation tai pahantahtoisuuden vuoksi pääse muuttamaan tai tuhoamaan tietoa, tai mahdollista jonkun ulkopuolisen käyttämään sitä. Henkilöstöturvallisuuden pääpaino on riskien välttäminen ennakkoon ja synnyn estäminen.

Fyysinen turvallisuus
Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden.

Tietoturvallisuus suojaa tietoja väärinkäytöltä, vahingoittumiselta ja katoamiselta, sekä varmistaa toiminnan jatkuvuuden.

Liite 5 Tietoturvarikkomusten seuraamustaulukko

Julkinen



	Tietämättömyys Osaamattomuus Huolimattomuus Vahinko Tahattomuus	Piittaamattomuus Törkeä huolimattomuus Välinpitämättömyys Tahallisuus Toistuvuus	Rikoksentekotarkoitus (vahingonteko, luvaton käyttö, vakoilu, salassapitorikos, aseman/väärinkäyttö) Hyötymistarkoitus
Vakava rikkomus/rikos Potilastiedon tai liikesalaisuuden luvaton käsittely ja luovuttaminen Hakkerointi, tunkeutuminen Rikoslain alaisen materiaalin oikeudeton käsittely Tekijänoikeuslain alaisen materiaalin laiton levittäminen Virusten tahallinen levittäminen	Esihenkilö käynnistää sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä. Esihenkilö harkitsee tutkintapyynnön tekemistä poliisille.	Esihenkilö käynnistää sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä. Esihenkilö tekee tutkintapyynnön poliisille.	Esihenkilö käynnistää sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä. Esihenkilö tekee tutkintapyynnön poliisille.
Rikkomus (vakava väärinkäyttö tai turvallisuuden vaarantaminen) Ohjelmien ja pelien luvaton kopiointi Luvattomien ohjelmien asentaminen Ylläpitäjän työkalujen luvaton hallussapito Palvelun luvaton pystytys Tunnuksen luovuttaminen Tiedon luottamuksellisuuden vaarantaminen	Esihenkilö käynnistää sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä.	Esihenkilö käynnistää sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä. Esihenkilö huolehtii käyttöoikeuksien perumisesta.	Esihenkilö käynnistää sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä. Esihenkilö tekee tutkintapyynnön poliisille.
Lievä rikkomus (väärinkäytös) Henkilökohtaisen tietoturvan laiminlyönti Epäasiallinen käytös Haitan aiheuttaminen Resurssien tuhlaus Virustorjunnan laiminlyönti Luvaton kaupallinen tai poliittinen toiminta Kulunvalvontasääntöjen rikkominen	Esihenkilö huolehtii puheeksi ottamisesta, opastuksesta ja perehdytyksestä. Esihenkilö käynnistää tarvittaessa sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä.	Esihenkilö huolehtii puheeksi ottamisesta, opastuksesta ja perehdytyksestä. Esihenkilö käynnistää tarvittaessa sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä.	Esihenkilö käynnistää sanktiomenettelyn kaupungin ohjeiden mukaisesti konsultoiden henkilöstöasioiden yksikköä. Esihenkilö harkitsee tutkintapyynnön tekemistä poliisille.