Tietoturvapolitiikka

Varkauden kaupunki

Versio 1.0

17.10.2013

Sisällysluettelo

Muutoshistoria:

Versio	Tekijä	Sisältö
1.0	Tietohallinnon johtoryhmä	Kaupunginhallituksen hyväksymä versio

1 Johdanto

Tietoturva on tärkeä osa Varkauden kaupunkikonsernin (myöh. kaupunki) toiminnan ja palveluiden laatua. Tietoturvaan liittyvä työ kaupungissa on päivittäistä kaikille organisaatiotasoille, toimintoihin ja palveluihin sulautettua toimintaa. Tietoturvatyö tarkoittaa tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja sen mukaista toteuttamista.

Tässä politiikassa ja sen liitteissä määritellään mitä tietoturva kaupungissa tarkoittaa. Lisäksi politiikassa ja sen liitteissä kuvataan kaupungin keskeiset tietoturvaperiaatteet, -tavoitteet, -roolit ja -vastuut.

Tämä politiikka katselmoidaan vuosittain ja on kokonaisuudessaan henkilöstön saatavilla intranetissä.

2 Tietoturvapolitiikan tarkoitus ja tausta

Tämä politiikka toimii kaupungin ylimpänä turvallisuusasiakirjana, sekä perustana toimialojen omille politiikoille ja ohjeille jotka tarkentavat tässä politiikassa annettuja määräyksiä.

Tämä politiikka kuvaa tietoturvan roolin kaupungin toiminnoissa ja palveluissa, perustuen tehtyihin riskiarvioihin ja toimintaa säätelevien lakien vaatimuksiin. Politiikassa on lisäksi huomioitu kaupunkistrategiassa (KV, 17.6.2013) määritellyt painopistealueet ja niiden tietoturvatyölle asettamat vaatimukset. Tietoturvan kannalta keskeisimpiä on nähty ’Kaupunkilaiset asiakkaina ja toimijoina’ sekä ’Henkilöstöresurssit / osaava ja hyvinvoiva henkilöstö’.

3 Keitä tietoturvapolitiikka koskee

Tämä tietoturvapolitiikka on kaupunginhallituksen hyväksymä ja koskee koko kaupunkiorganisaatiota sekä niitä sidosryhmiä (yhteistyö- ja sopimuskumppanit) jotka käsittelevät kaupungin omistamaa tai hallinnoimaa tietoa.

Politiikassa esitetyt periaatteet ja käytännöt koskevat kaikissa elinkaaren vaiheissa (luonti, säilytys, siirto, poisto) ja kaikissa muodoissa (mm. paperi, sähköinen, optinen, puhuttu) olevaa tietoa.

4 Tietoturvallisuus

Tietoturvallisuus kattaa tietoturvaan ja tietosuojaan liittyvät toteutukset. Tietoturvalla kaupungissa tarkoitetaan kaikissa muodoissa olevan tiedon (sekä tietojärjestelmien, tietoliikenteen, palveluiden ja niiden käyttöympäristöjen) turvaamista siten, että tiedon luottamuksellisuus, eheys ja saatavuus kyetään varmistamaan.

Tietosuojalla kaupungissa tarkoitetaan henkilön yksityisyyden ja henkilötietojen suojaamista niin, että henkilön yksilöivää tietoa ei paljastu siihen oikeudettomille tiedon elinkaaren missään vaiheessa (Henkilötietolaki 22.4.1999/523).

Periaatteena on, että tietoturvallisuuskäytännöt kattavat kaikki kaupungin tietojenkäsittelytehtävät sisältäen myös asiakirjahallinnon sekä arkistoinnin ottaen huomioon toimialojen ja työyksiköiden perusluonteen ja tietoturvatarpeet. Tietoturvallisuus pyritään integroimaan kiinteästi kaupungin palveluihin ja toimintaan, sekä jokaisen käyttäjän työtapoihin.

Tietoturvallisuutta toteutetaan käytännössä seuraavilla:

- **Asenne**: Tiedon käsittelijä ymmärtää tietoturvan merkityksen ja omat vastuunsa, sekä on motivoinut noudattamaan tätä politiikkaa sekä tästä politiikasta johdettuja tietoturvaohjeita ja -määräyksiä.
- **Eheys:** Tieto, tietojärjestelmät ja paperiasiakirjojen arkistot ovat luotettavia, oikeellisia ja ajantasaisia. Toisin sanoen tieto ei ole muuttunut teknisen vian seurauksena tai tietoa ei ole muutettu ihmisen toimesta tahallisesti tai tahattomasti.
- **Kiistämättömyys:** Tiedonkäsittelytoimenpiteiden suorittamista siten, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa sekä toimenpiteiden aikana että jälkikäteen.
- **Luottamuksellisuus:** Tieto on vain siihen oikeutettujen saatavissa eikä sitä paljasteta tai muutoin saateta sivullisten tietoon. Tiedon käsittelyssä noudatetaan julkisuuslakia sekä erikseen, toiminnoittain/järjestelmittäin, hyväksyttyjä tietojen turvaluokituksien mukaisia sääntöjä ja ohjeita.
- **Pääsynvalvonta:** Tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa ja ettei arkistotiloihin tai vastaaviin pääse ilman kontrolloitua pääsynvalvontaa.
- **Saatavuus:** Tieto ja tietojärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille ja tietojärjestelmille, sovituilla tavoilla ja sovittuun aikaan.

Kaupungin tietoturvatyön periaatteet ja toteutukset perustuvat ensisijassa Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohjeisiin ja suosituksiin, Tietoturvatasojen määrittelemiin Perustaso -vaatimuksiin (Tietoturvallisuusasetus 681/2010) ja tietosuojavaltuutetun toimiston antamiin ohjeisiin. Tietoturvatoteutukset koskien henkilöstö-, tietoaineisto-, fyysistä, tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuutta kuvataan tietoturvasuunnitelmassa.

5 Kokonaisturvallisuus

Kaupungin kokonaisturvallisuus koostuu riskienhallintaan, varautumiseen ja turvallisuuteen liittyvistä prosesseista ja niiden toteutuksista. Tietoturvapolitiikka on osa kaupungin kokonaisturvallisuuden hallintaa.

6 Riskienhallinta

Riskienhallinta toimii kaupungin kokonaisturvallisuuden perustana. Riskienhallinnan avulla kaupungin palveluihin ja toimintoihin kohdistuvia riskejä hallitaan järjestelmällisesti ja koko organisaation laajuisesti. Riskienhallinta kuuluu jokaisen työntekijän vastuulle.

7 Varautuminen ja jatkuvuudenhallinta

Kaupungin tavoitteena on varautua erilaisiin, toimintaa häiritseviin tai toiminnan keskeyttäviin uhkatilanteisiin, kriiseihin ja niistä toipumiseen ennakolta. Tämä tapahtuu kehittämällä ja ylläpitämällä seuraavia varautumiseen ja jatkuvuudenhallintaan liittyviä suunnitelmia:

- Jatkuvuussuunnitelmat toiminnan kannalta kriittisille palveluille ja toiminnoille niiden jatkuvuuden turvaamiseksi
- Toipumissuunnitelmat kriittisille tietojärjestelmille ja -verkoille niiden mahdollisimman nopean toipumisen, toiminnan uudelleenaloittamisen ja jatkamisen varmistamiseksi
- Valmiussuunnitelma toiminnan, palveluiden ja järjestelmien hallinnoimiseksi poikkeusoloissa
- Lakisääteiset pelastussuunnitelmat ihmisten ja omaisuuden suojelemiseksi, sekä vahinkojen minimoimiseksi onnettomuustilanteissa

8 Turvallisuus

Tietoturvan ja tietosuojan ohella keskeisimpiä turvallisuuden osa-alueita kaupungissa ovat:

Turvallisuusjohtaminen on turvallisuuden toteutumisen ohjaamista ja valvomista kaikilla tietoturvaprosessin kuvaamilla osa-alueilla.

Henkilöstöturvallisuus on kaupungin ja sidosryhmien henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskien hallintaa. Periaatteena on, että tietoturva huomioidaan työ- / virkasuhteen kaikissa vaiheissa.

Fyysinen turvallisuus koostuu järjestelyistä joilla kaupungin tiloja, ihmisiä, tietoa ja muuta omaisuutta suojataan vahingoilta ja vahingoittamisyrityksiltä.

9 Tietoturvatyö ja -prosessi

Kaupungin tietoturvatyö perustuu tietoturvaprosessissa kuvattuun kokonaisturvallisuuden jatkuvan kehittämisen malliin. Tietoturvatyö toteutuksineen sisältää organisointiin, ohjaukseen ja seurantaan liittyvän tekemisen, sekä niihin liittyvät menetelmät, toimenpiteet, asiakirjat ja kontrollit.

10 Tietoturvatavoitteet

Hyväksyessään tietoturvapolitiikan kaupunginhallitus asettaa seuraavat, kaupunkistrategiaa tukevat ja koko organisaatiota koskevat pitkän tähtäimen tietoturvatavoitteet:

1. Osaava ja hyvinvoiva henkilöstö: Koko kaupungin henkilökunta on osallistunut ’Tietoturvan perusteet’ -koulutukseen
2. Kaupunkilaiset asiakkaina ja toimijoina: Salassa pidettävää tai luottamuksellista tietoa ei paljastu tietoon oikeudettomille
3. Tietoturvan hallinnolliset ja tekniset järjestelyt täyttävät keskeisiltä osin Tietoturvatasojen Perustaso -vaatimukset (Tietoturvallisuusasetus 681/2010)

11 Roolit ja vastuut

Tietoturvan toteuttaminen on jatkuvaa, laaja-alaista ja kaikille toimijoille kuuluvaa toimintaa. Periaatteena on, että tietoturvan toteuttamiseen osallistuvat kaupungin ja sidosryhmien henkilöstö, osana omaa yleistä toimintavastuutaan. Käytännössä tämä tarkoittaa hyvien tiedonhallintatapojen, tietoturvamääräysten ja -ohjeiden noudattamista, sekä tietoturvan huomioimista kaikessa tekemisessä.

Ylin vastuu tietoturvasta, riskienhallinnasta ja varautumisesta on kaupunginhallituksella ja kaupunginjohtajalla. Tietoturvan ohjaus- ja kehittämistyössä tarvittava muu erityisasiantuntemus ja nimetyt turvallisuusvastuut kuvataan liitteessä 1.

12 Tietojärjestelmien käyttö

Kaupungin periaatteiden mukaisesti, käytettävät tietojärjestelmät on tarkoitettu työtehtävien hoitamiseen eikä niitä tule käyttää kaupungin omistaman tai hallinnoiman tiedon vaarantumiseen johtavaan toimintaan. Kaupungille tai sen toiminnalle mahdollisesti aiheutetun haitan korvausvastuussa on ensisijassa vaarantumisen aiheuttaja.

Käyttäjien toimintaa ohjataan tästä politiikasta johdetuilla tietoturvamääräyksillä ja -ohjeilla. Tiedon ja tietojärjestelmien väärinkäyttöön puututaan kaupungin normaalein kurinpitomenettelyin.

13 Tietoturvan seuranta, ylläpito ja kehittäminen

Kaupungin tietoturvatavoitteiden toteutumista seurataan säännöllisesti. Seuranta perustuu tietoturvaprosessin mukaisiin mitattaviin tavoitteisiin ja raportointikäytäntöihin, sekä yhteisesti sovittuihin teknisen valvonnan keinoihin.

Tietoturvan ylläpidossa ja kehittämisessä keskeisessä roolissa on osaaminen mitä toteutetaan säännöllisillä koulutus- ja viestintäkäytännöillä. Tässä politiikassa kuvatut määräykset ja periaatteet koulutetaan koko kaupungin henkilöstölle normaalin perehdytysprosessien mukaisesti.

Tarvittavien ulkoisten sidosryhmien tietoturvaosaamisesta vastaa kyseisen toimialan johto. Periaate on, että kaikki jotka käsittelevät kaupungin omistamaa tai hallinnoimaa tietoa saavat riittävät edellytykset tiedon asianmukaiseen käsittelyyn.

Tietoturvatoteutukset sekä asetettujen tietoturvatavoitteiden edellyttämät hallinnolliset, fyysiset ja tekniset ratkaisut kuvataan tietoturvaperiaatteet ja käytännöt -dokumentissa.

LIITE 1: ROOLIT JA VASTUUT

Luottamushenkilöstö

- Tietoturvallisuuden toteutuminen omissa luottamustehtävissään

Kaupunginhallitus

- Toimii kaupungin ylimpänä kokonaisturvallisuudesta päättävänä tahona
- Politiikkatason asiakirjojen hyväksyntä
- Kokonaisturvallisuuden toteutumisen seuranta ja ohjaus

Kaupunginjohtaja

- Edellytysten luominen tietoturvallisuuden toteutumiselle
- Raportointi ja kehitysehdotukset kaupunginhallitukselle

Tietohallinnon johtoryhmä

- Tietoturvan tekniset linjaukset
- Yhteisten tietoturvaperiaatteiden ja käytäntöjen hyväksyntä
- Tietoturvalinjausten tarkistaminen tietohallinnon vuosikellon mukaisesti
- Tietoturvapolitiikan ja ohjeistuksen kehittäminen tietoturvapäällikön johdolla
- Tietoturvatietouden edistäminen yhdessä toimialojen ja konsernin johdon kanssa
- Tietoturvallisuuden kehittäminen, sekä toteutumisen ohjaus ja valvonta kaupungin laajuisesti
- Tietoriskien ja tietoturvapoikkeamien hallinnan koordinointi
- Tietoturvallisuuteen liittyvän viestinnän tukeminen ja toteuttaminen yhdessä tietoturvapäällikön kanssa

Tietoturvapäällikkö

- Riskienhallinta- / tietoturvapolitiikan ja -periaatteiden määrittelyyn osallistuminen
- Tietoturvan kehittäminen tietoturvapolitiikan mukaisesti
- Henkilöstön tietoturvatietouden ylläpito ja tietoturvakoulutuksen järjestelyt
- Tietoturvaprosessin omistajuus ja prosessin mukaisen tietoturvan toteutuksen ohjaus
- Konsernijohdolle ja toimialajohdolle raportointi tietoturvan toteutumisesta, vuosikellon mukaisesti
- Yhteisten tietoturvaperiaatteiden ja käytäntöjen valmistelu, sekä tietoturvasuunnitelman omistajuus
- Yhteistyö ulkoisten sidosryhmien kanssa

Tietosuojavastaava

- Henkilötietojen suojaamisessa, hyvän henkilötietojen käsittelytavan ja mahdollisten lakien edellyttämän tietosuojan tason saavuttamisessa tukeminen ja ohjeistaminen
- Tietosuojan toteutumisesta ja kehitystarpeista raportointi valvoville viranomaisille ja toimialan johdolle
- Henkilötietojen käsittelyn ja niiden suojausmenetelmien seuranta ja valvonta
- Tietosuojaan liittyvän koulutusmateriaalin tuottaminen ja kouluttaminen

- Henkilötietojen käsittelyä koskeva suunnittelutoiminta, tietohallinnon johtoryhmän jäsenenä

Toimialojen johto ja konsernijohto

- Tietoturvallisuuden toteuttaminen ja toteutumisen seuranta omassa organisaatiossaan ja kaikessa alaisessaan toiminnassa
- Tietoturva- ja tietosuojavastuiden toteuttaminen tytäryhtiöissä
- Toimintaa säätelevien lakien, säädösten, direktiivien ja määräysten huomioiminen omassa organisaatiossaan (tietoturvallisuuden osalta)
- Sisäisen valvonnan raportin tuottaminen vuosittain

Esimies

- Tietoturvallisuuden toteuttaminen ja toteutumisen seuranta omassa organisaatiossaan ja kaikessa alaisessaan toiminnassa
- Oman organisaationsa tietoturvaan ja tietosuojaan liittyvän osaamisen ja koulutuksen toteutumisen varmistaminen

Tiedon tai tietojärjestelmän omistaja

- Omistamansa tiedon tai tietojärjestelmän suojaamistarpeen määrittäminen, sekä käyttöoikeuksien hyväksyntä ja säännöllinen katselmointi
- Riskienhallinta omistuksensa puitteissa
- Kriittisten järjestelmien turvajärjestelyjen testauksen toteuttaminen

Henkilöstöhallinto

- Henkilöstöturvallisuuden toteuttaminen virka- / työsuhteen kaikissa vaiheissa

Arkistotointa johtava viranhaltija

- Osallistuu asiakirjallisen tietoaineiston käsittelyn kehittämiseen ja tietoturvallisuuden toteuttamiseen
- Ohjaa hallintokuntia arkistotoimen hoidossa, jotta arkistolain 7§ toteutuu oikeusturva ja tietosuoja huomioiden
- Hyväksyy asiakirjallisten tietoaineistojen hallinnan edellyttämät arkistonmuodostussuunnitelmat
- Vastaa päätearkistoon luovutetusta pysyvästi säilytettävästä tietoaineistosta ja niiden tietoturvallisuudesta

Toimialojen arkistovastaavat

- Vastaa asiakirjallisen tietoaineiston käsittelyn kehittämisestä ja tietoturvallisuuden toteuttamisesta arkistovastaavan tehtävissä
- Ohjaa omalla vastuualueellaan arkistotoimen hoitoa arkistolain 7 § huomioiden
- Vastaa omalla vastuualueellaan arkistonmuodostussuunnitelman ajantasaisuudesta myös tietoturvallisuuden toteutumiseksi
- Vastaa omalla vastuualueellaan päätearkistoon ja käsiarkistoihin luovutetun tietoaineiston säilyttämisestä ja tietoturvallisuudesta

Tietotekniikan tukihenkilöstö

- Tietoturvapolitiikan soveltaminen ja toteuttaminen omaa erikoisasiantuntemusta hyödyntäen
- Tietoturvatoimenpiteiden huomioiminen omalla vastuualueellaan
- Teknisen valvonnan toteuttaminen tietoturvapäällikön ohjauksessa ja valvonnassa, yhteistyömenettelyssä sovittujen toteutusten mukaisesti

Tietojärjestelmän pää- ja varapääkäyttäjä

- Tiedon tai tietojärjestelmän suojaamistarpeen määrittäminen ja toteuttaminen, yhdessä tiedon tai tietojärjestelmän omistajan kanssa
- Tietojärjestelmäkuvauksien ylläpito, yhdessä tiedon tai tietojärjestelmän omistajan kanssa (tietojärjestelmä- ja henkilörekisteriselosteet)
- Käyttöoikeuksien hallinta tietojärjestelmän omistajan valtuuttamana

Viran- tai toimenhaltija

- Tietoturvallisuuden toteutuminen omissa työtehtävissään
- Havaitsemiensa tietoturvaan liittyvien ongelmien, uhkien, poikkeamien tai ohjeiden vastaisen menettelyn raportointi