



TIETOTURVA- JA TIETOSUOJAPOLITIikka

VERSIO 1.1

12. JOULUKUUTA 2022

TIETOHALLINTO

VARKAUDEN KAUPUNKI

Ahlströminkatu 6, 78250 Varkaus



SISÄLLYS

1	Johdanto	2
2	Tietoturva- ja tietosuojapolitiikan tarkoitus ja rakenne	2
3	Keitä tietoturva- ja tietosuojapolitiikka koskee	3
4	tiedonhallinta	3
5	Tietoturvallisuus	3
6	Tietosuoja	4
7	Kokonaisturvallisuus	5
8	Riskienhallinta	5
9	Varautuminen ja jatkuvuudenhallinta	6
9.1	Menettely tietosuojan tai tietoturvan vaarantuessa	6
10	Turvallisuus	7
11	Roolit ja vastuut	7
12	Tietojärjestelmien käyttö	7
13	Tietoturvan ja tietosuojan seuranta, ylläpito ja kehittäminen	8
	Roolit ja vastuut	9
	Tietoturva- ja tietosuojasitoumus	12
	Liitteet	13



1 JOHDANTO

Tietoturva ja tietosuoja ovat yhdessä tärkeä osa Varkauden kaupunkikonsernin (myöh. kaupunki) toiminnan ja palveluiden laatua. Niihin liittyvä työ kaupungissa on päivittäistä kaikille organisaatiotasoisille, toimintoihin ja palveluihin sulautettua toimintaa.

Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista ja henkilötietojen oikeaoppista käsittelyä niin, että henkilön yksilöivää tietoa ei paljastu siihen oikeudettomille tiedon elinkaaren missään vaiheessa.

Tietoturvatyö tarkoittaa tiedon suojaamiseksi tehtävien toimenpiteiden suunnittelua ja sen mukaista toteuttamista.

Tässä politiikassa ja sen liitteissä määritellään mitä tietoturva ja tietosuoja Varkauden kaupungissa tarkoittaa. Lisäksi politiikassa kuvataan kaupungin tietoturvan ja tietosuojan keskeiset periaatteet, tavoitteet, roolit ja vastuut.

Tämä politiikka katselmoidaan vuosittain ja on kokonaisuudessaan henkilöstön saatavilla intranetissä. Julkinen versio julkaistaan kaupungin kotisivuilla.

2 TIETOTURVA- JA TIETOSUOJAPOLITIIKAN TARKOITUS JA RAKENNE

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

Tämä politiikka kuvaa tietoturvan ja tietosuoja roolit kaupungin toiminnoissa ja palveluissa, perustuen tehtyihin riskiarvioihin ja toimintaa säätelevien lakien ja asetusten vaatimuksiin.

Tietoturvakäytännöt ovat tietoturvapoliitiikan alaisia ohjeistusdokumentteja.

Tietoturvakäytäntöjen on tarkoitus ohjata tietoturvan ja tietoturvaratkaisujen toteuttamista käytännönläheisesti ja konkreettisesti. Tietoturvakäytännöt ja niihin liittyvän dokumentaation hyväksyy tietohallinnon johtoryhmä.

Tietoturvapoliitikkaa toteutetaan seuraavilla tietoturvakäytännöillä:

- ICT Varautumissuunnitelma
- Jatkuvuudenhallintakäytäntö
- Pääsynhallintakäytäntö
- Työasemien ja oheislaitteiden käytäntö
- Tietoverkon ylläpitokäytäntö
- Palvelinympäristön hallintakäytäntö
- Opas sähköiseen työympäristöön



3 KEITÄ TIETOTURVA- JA TIETOSUOJAPOLITIikka KOSKEE

Tämä politiikka 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 tiedon elinkaaren vaiheissa (tuottaminen, kerääminen, säilytys, siirto, luovuttaminen, hävittäminen) ja kaikissa muodoissa (mm. paperi, sähköinen, optinen, puhuttu) olevaa tietoa.

4 TIEDONHALLINTA

Vuoden 2020 alussa voimaan tullut tiedonhallintalaki asettaa julkiselle hallinnolle tiedon hallintaan liittyviä vaatimuksia. Varkauden kaupunki noudattaa nykyisiä lakien ja asetusten mukaisia vaatimuksia.

Varkauden kaupunki on laatinut tiedonhallintamallin, jota katselmoidaan vuosittain. Tiedonhallintalain edellyttämä asiakirjajulkisuuskuvaus on julkaistu kaupungin verkkosivustolla. Kaupungilla on myös käytössä sähköiseen arkistointiin soveltuva arkistointiratkaisu.

Virka- tai työsuhteen, työharjoittelun tai luottamustehtävän päättyessä tehtävää hoitaneen henkilön tulee luovuttaa kaikki haltuunsa annetut Varkauden kaupunkia, sen tytäryhtiöitä tai asiakkaita koskevat, liike- ja ammattisalaisuuksia ja/tai muuta taloudellista arvoa sisältävät dokumentit (pöytäkirjat, muistiot, piirustukset, tietovälineet ja -ohjelmat, suunnitelmat, keskeneräiset dokumentit yms.) takaisin Varkauden kaupungille.

5 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 alkuperäisyys, luottamuksellisuus, eheys, saatavuus ja käytettävyys kyetään varmistamaan.

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

Tietoturvallisuuden toteutumiselle asetetaan seuraavat käytännön tavoitteet:



- **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 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 voimassa olevia lakeja sekä erikseen, toiminnoittain/järjestelmittäin, hyväksytyjä tietojen turvaluokitusten mukaisia sääntöjä ja ohjeita.
- **Pääsynvalvonta:** Tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa ja ettei arkistotiloihin tai vastaaviin pääse ilman kontrolloitua pääsynvalvontaa. Pääsynvalvontaa ohjataan pääsynhallintakäytännöillä (1.1. Pääsynhallintakäytäntö).
- **Saatavuus:** Tieto ja tietojärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille ja tietojärjestelmille, sovituilla tavoilla ja sovittuun aikaan.

Kaupungin tietoturvatyön periaatteet ja toteutukset perustuvat voimassa olevan lainsäädännön lisäksi julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeisiin, tiedonhallintalautakunnan ohjeisiin ja suosituksiin (mm. julkisen hallinnon tietoturvallisuuden arviointikriteeristö), sekä tietosuojavaltuutetun toimiston antamiin ohjeisiin.

6 TIETOSUOJA

Varkauden kaupunki noudattaa laissa ja asetuksissa voimassa olevia velvollisuuksia rekisterinpitäjänä ja henkilötietojen käsittelijänä, sekä sitoutuu turvaamaan rekisteröidyn oikeudet. (Euroopan unionin yleinen tietosuojasetus (EU 679/2016), Tietosuojalaki (2018), Tiedonhallintalaki (2019).

Henkilötietoja kerätään vain siinä laajuudessa kuin kaupungin tarjoamien palveluiden tuottaminen edellyttää. Henkilötietojen käsittelijöillä on käyttöoikeus vain niihin tietoihin, joita palvelun tuottamisessa tarvitaan. Tietoja voidaan luovuttaa kolmansille osapuolille lakeihin perustuvien luovutustarpeiden nojalla eikä tietoja luovuteta muihin tarkoituksiin ilman asiakkaalta pyydettyä käyttötarkoitukselta lupaa.

Toiminnassa muodostuvista henkilörekistereistä on julkisesti tarjolla tietosuoja-asetteet, joista käy ilmi rekistereiden sisältämät tiedot ja käyttötarkoitus. Rekisterinpitäjänä on se toimija, jonka käyttötarkoitusta varten henkilötiedot on kerätty.

Varkauden kaupungin toimiessa rekisterinpitäjänä palveluntarjoaja voi siirtää henkilötietoja Euroopan unionin, Euroopan talousalueen tai muiden maiden, joiden Euroopan Komissio on todennut takaavan riittävän tietosuojan tason, ulkopuolelle ainoastaan Varkauden kaupungin etukäteisellä kirjallisella suostumuksella.



Varkauden kaupunki tekee sopimuksen kumppaneiden ja palveluntarjoajien kanssa henkilötietojen käsittelystä tietoturva- ja tietosuojaryhmän suositusten mukaisesti.

Varkauden kaupunki edellyttää, että henkilöstö on osallistunut tietoturva- ja tietosuojakoulutuksiin ja todentaa osaamisen vuosittain verkko-oppimisympäristössä suoritettua testin avulla. Lisäksi henkilöstö allekirjoittaa tietoturva- ja tietosuojasitoumuksen, jossa jokainen sitoutuu noudattamaan kaupungin tietoturvasääntöjä. Liitteessä 'Tietoturva- ja tietosuojasitoumus' listataan tietosuojasitoumuksen asiat. Tietosuojasitoumus allekirjoitetaan sähköisesti ESSI järjestelmään.

Varkauden kaupunki rekisterinpitäjänä vastaa siitä, että henkilötietojen käsittelyä koskevia periaatteita on noudatettu (asetuksen mukainen osoitusvelvollisuus):

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus

7 KOKONAISTURVALLISUUS

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

8 RISKIENHALLINTA

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

Varkauden kaupungin tietoturva- ja tietosuojaryhmä sekä tietohallinto muodostavat turvallisuusriskeistä kokonaiskuvaa. Tärkeimpiä lähteitä ovat kyberturvallisuuskeskus, media, auditoinnit, oma ICT-riskiarvio sekä Varkauden kaupungin poikkeamienhallintatyökalu.

Tiedonhallinnan riskien arviointi on osa ICT varautumissuunnitelman käytäntöjä (Liite: ICT varautumissuunnitelma). Läheisesti ICT varautumissuunnitelmaan liittyy myös jatkuvuuden hallinta ja palautuminen tilanteesta, kun joku riski toteutuu. Tarkemmin varautumisesta ja jatkuvuudenhallinnasta on kohdassa 8. Varautuminen ja jatkuvuudenhallinta. Varkauden kaupunkiin kohdistuneista tieturvapoikkeamista raportoidaan tietotilinpäätöksessä.



Erilaisiin uhkatilanteisiin ennalta varautuminen pienentää mahdollisuutta riskien toteutumiselle. Riskienhallinnan tulee olla kiinteä osa tiedon hallinnan prosesseja. Riskiarviointien tekeminen tulee myös olla säännöllistä ja toistuvaa toimintaa.

EU:n yleinen tietosuoja-asetus edellyttää vaikutuksen arvioinnin (DPIA) tekemistä.

Vaikutustenarvioinnin tarkoituksena on kuvata henkilötietojen käsittelyä, arvioida käsittelyn tarpeellisuutta ja oikeasuhteisuutta sekä arvioida henkilötietojen käsittelystä aiheutuvia riskejä ja tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutustenarviointi on tehtävä ennen käsittelyn aloittamista, kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski.

Vaikutustenarvioinnin tarkoituksena on auttaa rekisterinpitäjää tietosuoja-asetuksen vaatimusten noudattamisessa ja noudattamisen osoittamisessa.

9 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:

- ICT Valmiussuunnitelma kuuluu Varkauden kaupungin valmiussuunnitelman yleisen osan alaisuuteen sekä saman sisältöisenä tietoturvapoliittikan käytäntöihin. Valmiussuunnitelma kuvaa varautumistoimenpiteet palveluiden ja järjestelmien hallintaan häiriö- ja poikkeusoloissa.
- Jatkuvuudenhallintakäytäntö kuuluu tietoturvapoliittikan alaisuuteen. Käytäntö kuvaa hallintatoimet toiminnan kannalta kriittisten tietojärjestelmien ja tietoverkkojen jatkuvuuden turvaamiseksi normaaliolojen häiriötilanteissa. Toipumissuunnitelmat mahdollisimman nopean toipumisen, toiminnan uudelleenaloittamisen ja jatkamisen varmistamiseksi ovat osa jatkuvuudenhallintakäytäntöä.

9.1 MENETTELY TIETOSUOJAN TAI TIETOTURVAN VAARANTUESSA

Tietosuoja-/tietoturvaloukkaukseksi katsotaan kaikki henkilötietojen käsittelyä koskevien lakien ja asetusten, tämän politiikan sekä kaupungin tarkempien periaatteiden ja ohjeistuksien vastainen toiminta.

Jokaisella työntekijällä on velvollisuus ilmoittaa huomattessaan mahdollisen tietoturva- tai tietosuojaloukkauksen. Ilmoitus tehdään tietohallintoon ja tietosuojavastaavalle. Jo pelkkä epäily tietosuoja- tai tietoturvaloukkauksesta johtaa asian selvittämiseen.

Jos henkilötietojen tietosuojaloukkauksesta todennäköisesti aiheutuu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski, rekisterinpitäjän on ilmoitettava siitä rekisteröidyille ja valvontaviranomaiselle ilman aiheutonta viivytystä (72h). Varkauden kaupungin tietosuojavastaava toimii yhteyshenkilönä valvontaviranomaiselle sekä rekisteröidyille, joita tietosuojaloukkaus koskee.



Tietoturvarikkomuksista ja tietosuojaloukkauksista voi olla seurauksena käyttöoikeuksien rajoituksia, palvelussuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä seuraamuksia. Palvelussuhteeseen vaikuttavista seuraamuksista on säädetty ensi sijassa työsopimuslaissa ja viranhaltijalaissa. Jos tietosuojaloukkaus arvioidaan lainsäädännön perusteella rangaistavaksi toiminnaksi tai rangaistavuudesta on olemassa riittävä epäily, asian käsittely annetaan viranomaiselle. Seuraamuksia arvioitaessa moitittava toiminta, sen vaikutukset ja seuraukset käsitellään kokonaisuutena.

10 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 ja tietosuoja huomioidaan työ- / virkasuhteen kaikissa vaiheissa.

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

11 ROOLIT JA VASTUUT

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

Ylin vastuu tietoturvasta, tietosuojasta, riskienhallinnasta ja varautumisesta on kaupunginhallituksella ja kaupunginjohtajalla. Ohjaus- ja kehittämistyössä tarvittava muu erityisasiantuntemus ja nimetyt turvallisuusvastuut kuvataan liitteessä 'Roolit ja vastuut'.

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 periaatteilla ja ohjeilla. Tiedon ja tietojärjestelmien väärinkäyttöön puututaan kaupungin normaalein kurinpitomenettelyin.

13 TIETOTURVAN JA TIETOSUOJAN SEURANTA, YLLÄPITO JA KEHITTÄMINEN

Kaupungin tietoturva- ja tietosuojatavoitteiden toteutumista seurataan säännöllisesti laaditun vuosikellon mukaisesti. Seuranta perustuu tietoturva- ja tietosuojaprosessin mukaisiin mitattaviin tavoitteisiin ja raportointikäytäntöihin (mm. tietotilinpäätös), sekä yhteisesti sovittuihin teknisen valvonnan keinoihin.

Tietotilinpäätös on raportti, joka syntyy organisaation sisäisen tarkastelun tuloksena. Se käsittää tilinpäätösluonteisen tarkastelun ulottamisen tietovarantoihin, tietojohdamiseen, tietojenkäsittelyyn ja tietoturvaluuteen.

Tietoturvan ja tietosuojan ylläpidossa ja kehittämisessä keskeisessä roolissa on osaaminen, mitä toteutetaan säännöllisillä koulutus- ja viestintäkäytännöillä. Tämä politiikka sisällytetään koko kaupungin henkilöstön perehdytysprosessiin.

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



ROOLIT JA VASTUUT

Luottamushenkilöstö

- Vastaa tietoturvallisuuden toteuttamisesta omissa luottamustehtävissään

Kaupunginhallitus

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

Kaupunginjohtaja

- Edellytysten luominen tietoturvallisuuden toteutumiselle
- Raportointi ja kehitysehdotukset kaupunginhallitukselle

Tietohallinnon johtoryhmä

- Tietoturvan ja tietosuojan tekniset linjaukset
- Yhteisten periaatteiden ja käytäntöjen, mm. tietoturvakäytäntö-dokumentation hyväksyntä
- Tietoturva- ja tietosuojalinjausten tarkistaminen tietohallinnon vuosikellon mukaisesti
- Tietoturva- ja tietosuojapolitiikan ja ohjeistuksen kehittäminen
- Tietoturvatietouden edistäminen yhdessä toimialojen ja konsernin johdon kanssa
- Tietoturvallisuuden kehittäminen, sekä toteutumisen ohjaus ja valvonta kaupungin laajuisesti
- Tietoturvariskien ja -poikkeamien hallinnan koordinointi
- Tietoturvallisuuteen liittyvän viestinnän tukeminen ja toteuttaminen yhdessä tietoturvapäällikön kanssa

Tietoturva- ja tietosuojaryhmä

- käsittelee, kommentoi, antaa lausuntoja ja kannanottoja tietosuojaan, tietoturvaan ja kyberturvallisuuteen liittyen
- tarkastaa henkilötietoja sisältävien sopimusten tietoturvan ja tietosuojan
- käsittelee tietosuojaan ja tietoturvaan liittyvät merkittävät poikkeamat
- käsittelee ja hyväksyy osaltaan projektit sovitussa tarkastuspisteissä
- kehittää ja edistää organisaation tietoturvan ja tietosuojan toteutumista

Tietoturvapäällikkö

- Riskienhallinta- / tietoturvapoliitiikan ja -periaatteiden määrittelyyn osallistuminen
- Tietoturvan kehittäminen tietoturvapoliitiikan 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

- antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja



- antaa pyydettyä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoo sen toteutusta 35 artiklan mukaisesti
- tekee yhteistyötä valvontaviranomaisen kanssa ja toimii yhteyspisteenä käsittelyyn liittyvissä kysymyksissä
- henkilötietojen käsittelyä koskeva suunnittelu- ja kehittämistoiminta, tietoturva- ja tietosuojaryhmän jäsenenä
- osallistuu rekisterinpitäjän hyväksymiä tietosuoja- ja tietoturvaohjeita koskevaan valmisteluun ja ylläpitoon
- seuraa ja valvoo henkilötietojen käsittelyä ja niiden suojausmenetelmiä
- raportoi suoraan organisaation johdolle tietosuojan (ja tietoturvallisuuden) tilasta ja kehittämistarpeista (sisäiset auditoinnit ja käytönvalvonta)

Toimialojen johto ja konsernijohto

- Tietoturvallisuuden toteuttaminen ja toteutumisen seuranta omassa organisaatiossaan ja kaikessa alaisessaan toiminnassa
- Tietoturva- ja tietosuojavastuiden toteuttaminen tytäryhtiöissä
- Tietoturvaa ja tietosuojaa säätelevien lakien, säädösten, direktiivien ja määräysten huomioiminen omassa organisaatiossaan
- Sisäisen valvonnan raportin tuottaminen vuosittain

Esihenkilö

- vastaa oman yksikkönsä osalta annettujen määräysten ja ohjeistusten noudattamisesta sisältäen niin työntekijöiden perehdyttämisen kuin toteutumisen seurannan
- raportoi mahdollisista poikkeamista tietosuojavastaavalle
- tietojärjestelmien käyttöoikeuksien hakeminen, hyväksyminen, muuttaminen ja poisto- ja passivointipyyntöjen tekeminen

Tiedon tai tietojärjestelmän omistaja

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

Henkilöstöhallinto

- Henkilöstöturvallisuuden toteuttaminen virka- / työsuhteen kaikissa vaiheissa

Asiakirjahallinnosta vastaava

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



Toimialojen arkistovastaavat

- Vastaa asiakirjallisen tietoaaineiston käsittelyn kehittämisestä ja tietoturvallisuuden toteuttamisesta arkistovastaavan tehtävissä
- Ohjaa omalla vastuualueellaan asiakirjahallinnon hoitoa arkistolain 7 § huomioiden
- Vastaa omalla vastuualueellaan arkistonmuodostus- ja tiedonohjaussuunnitelman ajantasaisuudesta myös tietoturvallisuuden toteutumiseksi
- Vastaa omalla vastuualueellaan päätearkistoon ja käsiarkistoihin luovutetun tietoaaineiston säilyttämisestä ja tietoturvallisuudesta ja tietosuojasta

Tietotekniikan tukihenkilöstö

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

Tietojärjestelmän pää- ja varapääkäyttäjät

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

Henkilöstö

- Käsittelee tietoja annettujen ohjeiden ja määräysten mukaisesti
- Havaitsemiensa tietoturvaan ja tietosuojaan liittyvien ongelmien, uhkien, poikkeamien tai ohjeiden vastaisen menettelyn raportointi

Rekisteröidyt

- ovat tietoisia oikeuksistaan sekä vastuussa antamiensa tietojen oikeellisuudesta

Ulkoiset palveluntuottajat

- Sitoutuvat noudattamaan kaupungin tietoturva- ja tietosuojapolitiikkaa
- Palveluntuottajien vastuut henkilötietojen käsittelyssä sovitaan palvelukohtaisissa sopimuksissa
- Palveluntuottajien tulee nimetä tietoturva- ja tietosuoja-asioihin yhteyshenkilö



TIETOTURVA- JA TIETOSUOJASITOUMUS

1. Noudatan tietojen ja tietojärjestelmien käyttöön liittyviä velvoitteita ja määräyksiä.
2. Käytän organisaation järjestelmiä ja laitteita vain työtehtävien hoitamiseen ellei käytöstä ole työnantajan kanssa muuta erikseen sovittu.
3. Vastaan käytössäni olevista laitteista niin, etteivät ne tai niissä olevat tiedot joudu väärin käsiin. Työsuhteen päättyessä palautan laitteeni annettujen ohjeiden mukaisesti.
4. Varmistan esimieheni kanssa, että saan tarvittavan koulutuksen laitteiden ja järjestelmien käyttöön.
5. Käsittelen vain työtehtävieni kulloinkin edellyttämiä tietoja ja vain siinä laajuudessa kuin asian käsittely vaatii.
6. En luovuta sivullisille salassa pidettäviä tietoja ilman asianmukaista lupaa tai lain perustetta.
7. Käsittelen salassa pidettäviä tietoja vain niissä järjestelmissä, jotka tällaisten tietojen käsittelyyn on tarkoitettu.
8. Tulostan salassa pidettäviä tietoja vain perustelluista syistä. Varmistan tulostinta käyttäessäni, että tiedot eivät joudu ulkopuolisten käsiin. Hävitän tulosteet ainoastaan tietosuojajätteen käsittelyyn tarkoitettuihin säiliöihin.
9. Noudatan sähköisten viestintävälineiden käytöstä annettuja ohjeita. Salassa pidettäviä tietoja lähetän vain suojatulla sähköpostiyhteydellä.
10. Hoitaessani työtehtäviä työpaikkani ulkopuolella vastaan siitä, että sivulliset eivät näe ja kuule työhön liittyviä asioita.
11. Huolehdin esimieheni kanssa siitä, että minulla ei ole tarpeettomia käyttöoikeuksia tietojärjestelmiin.
12. Tietojärjestelmien käyttöoikeudet ovat henkilökohtaisia. Vastaan siitä, että käytän järjestelmiä minulle toimitetuilla tunnuksilla, tunnistekorteilla, koodeilla yms. Säilytän myönnetyt tunnukset huolellisesti siten, että ne eivät paljastu ulkopuolisille.
13. Kirjaudun ulos tietojärjestelmistä tai lukitsen laitteen, kun laite ei ole valvonnassani.
14. Omien ohjelmistojen asentaminen työnantajan laitteisiin on kielletty. Jos tarvitsen jotain erillistä ohjelmaa, otan yhteyttä esimieheeni.
15. Olen tietoinen, että järjestelmien käytöstä ja tiedon käsittelystä syntyy ns. lokitietoa. Tietojen käyttöä valvotaan ja myös asiakkaalla on oikeus saada tieto heidän tietojaan käsitelleistä henkilöistä.
16. Ilmoitan havaitsemistani tietoturvaan, tietosuojaan tai tietojärjestelmiin liittyvistä epäkohdista ja ongelmista tietosuojavastaavalle ja esimiehelleni.



LIITTEET

Seuraavat liitteet eivät ole julkisia:

ICT Varautumissuunnitelma
Jatkuvuudenhallintakäytäntö
Pääsynhallintakäytäntö
Työasemien ja oheislaitteiden käytäntö
Tietoverkon ylläpitokäytäntö
Palvelinympäristön hallintakäytäntö
Opas sähköiseen työympäristöön