
PARKANON KAUPUNGIN TIETOTURVAPOLITIikka

Politiikan lähtökohdat

Tietoturvapoliitikka määrittelee organisaation tietoturvallisuuden päämäärät, tavoitteet, vastuut ja toteutuskeinot.

Tietoturvapoliitikan onnistumisen ehdoton edellytys on, että johto sitoutuu olemaan mukana prosessissa sekä ymmärtää tietoturvan ja suojausmekanismien tärkeyden toiminnan jatkuvuuden kannalta. Johdon on oltava tietoinen suojausten toteuttamisen tärkeydestä ja sen on tuettava tietoturvallisuuden edistämistä.

Tietoturvapoliitikka vahvistetaan kaupunginhallituksen päätöksellä.

Tietoturvapoliitikka annetaan tiedoksi kaikille kaupungilla työskenteleville.

Tietoturvapoliitikkaa täydentävät tietoturvasuunnitelma sekä yksityiskohtaiset määräykset ja ohjeet.

Päämäärä ja tavoitteet

Tietoturvallisuustyön päämäärä on turvata kaupungin toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida mahdollisesti aiheutuvat vahingot.

Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Kaupungin tiedot, tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmukaisesti suojattuina sekä normaali, että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla.

Tietoturvallisuustyön tavoitteena on, että tietoturvallisuuden perustaso kattaa kaupungin kaiken tietojenkäsittelyn huomioiden yksikköjen perusluonteen ja mahdollisen tarpeen tietoturvallisuuden tehostamiseen.

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Toimintaan kuuluvat tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet. Tietoturvallisuus kattaa kaikki kaupungin tietojenkäsittelytehtävät sisältäen myös toimistotyön tehtävät.

Tietoturvallisuustoimet koskevat sähköisessä ja kirjallisessa muodossa olevan tiedon käsittelyä, luovutusta ja siirtoa.

Tietoturvallisuus

Tietoturvallisuus tietojenkäsittelyn turvaamista. Tietoturvallisuus rakentuu seuraavien perustekijöiden varaan; tiedon luottamuksellisuus, tiedon eheys ja käytettävyys, tiedon saatavuus, tiedon säilyvyys sekä tiedon tarkastettavuus. Edelleen tietoturvallisuus jaotellaan seuraaviin pienempiin kokonaisuuksiin.

- hallinnollinen tietoturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus.

Vastuut

Tietoturvallisuus on osa kokonaisturvallisuutta.

Parkanon kaupungin tietohallinto vastaa tietoturvallisuuden kehittämisestä, toteutuksen valvonnasta ja tietoturvatietouden edistämisestä.

Jokainen kaupungin tietoja käsittelevä, tietojärjestelmien- ja tietoverkkojen ylläpitäjä ja käyttäjä on viime kädessä vastuussa tietoturvallisuuden toteutumisesta omalta osaltaan.

Kukin tietojärjestelmien ja niiden sisältämien tietojen haltija vastaa tietojensa ja tietojärjestelmiensä suojaamisesta.

Toteutuskeinot

Tietoturvallisuuden tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten, fyysisten ja teknisten ratkaisujen avulla. Käyttäjien toimintaa ohjataan niihin sisältyvillä käytösäännöillä ja toimintaohjeilla sekä tietoturvakoulutuksella.

Tieto luokitellaan tärkeyden mukaisesti erilaisiin turvallisuusluokkiin. Kullekin turvallisuusluokalle määritellään vaadittava tietoturvallisuustaso ja sen mukaiset tietoturva toimenpiteet.

Jokaiselle tietojärjestelmälle tai sen osalle on oltava yksiselitteinen vastuuhenkilö, jota sanotaan järjestelmän pääkäyttäjäksi.

Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely

Parkanon kaupungin tietohallinto tekee kaupungin tietojärjestelmien tietoturvallisuuden kartoitusta ja tekee tai esittää tehtäväksi tarpeelliset toimenpiteet havaittujen puutteiden korjaamiseksi. Jokainen kaupungin tietojenkäsittelyjärjestelmien käyttäjä on velvollinen noudattamaan tietokoneiden ja tietoverkkojen käytösäntöjä sekä tietoturvaohjeita.

Työnantajalla on velvollisuus perehdyttää käyttäjä tietojenkäsittelyjärjestelmien käyttöön ja tietoturvallisuuden huomioon ottamiseen.

Käyttäjien ja tietojen ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista esimiehelleen, sekä tietoturvavastaavalle.

Tietoturvan organisointi

Tietoturvaa johtaa ja valvoo kaupunginhallitus, joka myös päättää kokonaisturvallisuuden ja kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvavastaavan.

Tietoturvavastaava vastaa tietoturvatyön kokonaisuudesta. Hän vastaa myös tietoturva-asioista tiedottamisesta organisaation ulkopuolelle ja organisaation sisällä yleisellä tasolla. Tietoturvavastaava vastaa kaupungin tietoturvallisuustason määrittelystä ja arvioinnista ja raportoinnista sekä muusta hallinnollisesta tietoturvasta. Hän vastaa tietoturvan kehittämissuunnitelmien tekemisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta toimintayksikössä ja sen ostamissa palveluissa sekä raportoinnista johdolle. Tietoturvavastaava vastaa myös laitteisto- ja ohjelmistoturvallisuudesta. Tietohallintojohtaja on työnsä puolesta tietoturvavastaava.

Tietosuojavastaava vastaa henkilörekisterien suojauksesta ja valvonnasta sekä muusta käyttöturvallisuudesta. Arkistonhoitaja on työnsä puolesta tietosuojavastaava.

Kaupungin keskeisten toimintojen turvanäkemyksiä edustaa ICT-tietoturvaryhmä, jonka asettaa kaupunginjohtaja. Tietoturvaryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään hyväksyttäväksi.

Jokaisella tietojärjestelmällä on omistajayksikkö ja vastuhenkilö. Tietojärjestelmän vastuuhenkilön velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn) määrittely sekä käyttöoikeuksien myöntäminen ja valvonta.

Tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa yksikön esimies.

Parkanon kaupunginhallitus

Hyväksytty 18.12.2017 § 302
