HAAPAVEDEN KAUPUNGIN TIETOTURVAPOLITIIKKA

Tämä tietoturvapolitiikka korvaa kaupunginhallituksessa 15.12.2008 hyväksytyn tietoturvapolitiikan.

Luotu 10.10.2023

Sisällys

1. Johdanto

Tässä dokumentissa kuvataan Haapaveden kaupungin tietoturvapolitiikka. Tietoturvapolitiikka määrittelee Haapaveden kaupungin tietoturvan toteuttamisessa ja kehittämisessä käytettävät toimintaperiaatteet, toimintatavat sekä vastuut. Lisäksi tietoturvapolitiikka määrittelee tietoturvan toteutumisen seurannan ja valvonnan. Tietoturvapolitiikka toimii ylätason dokumenttina, johon erilliset tietoturvaohjeistukset pohjautuvat. Organisaation yksittäiset tietoturvaohjeet täydentävät tietoturvapolitiikkaa. Politiikalla luodaan yhdenmukaiset ohjeet ja käytännöt hyvän tietoturvan toteuttamiseksi koko organisaatiolle. Tietoturvapolitiikka pohjautuu useaan eri lakiin. Tietoturva ilmenee organisaatiossa monella eri tavalla ja se on suurimmaksi osaksi muuta kuin teknisiä ratkaisuja.

2. Käsitteet

Tietoturvalla tarkoitetaan tiedon suojaamista erilaisilta uhkilta ja toimintaa tai tietoja uhkaavien riskien minimointia. Tietoturvallisuus käsittää erilaiset tiedon käsittelyn, siirron, luovutuksen ja arkistoinnin toimenpiteet. Tieto voi olla useassa eri muodossa, kuten sähköisessä, puhutussa tai kirjallisessa muodossa. Tietoturvallisuus kattaa tiedon kaikissa sen ilmenemismuodoissa.

Tietojen turvaamisessa omina osa-alueinaan huomioidaan hallinnollinen, henkilöstö-, toimitila-, tietoaineisto- ja tietojärjestelmäturvallisuus. Tietojärjestelmäturvallisuus jaetaan tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuuteen. Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, tiedon eheydestä ja tiedon käytettävyydestä.

Arkaluonteinen tieto	Yksilöä koskeva tieto, jonka rekisteröintiä tai käyttöä on rajoitettu lain tai asianomaisen vaatimuksesta. Arkaluonteista tietoa ovat henkilötiedot, joilla kuvataan rotua, etnistä alkuperää, uskontoa, terveydentilaa, seksuaalista suuntautuneisuutta jne.
EDPB	European Data Protection Board, Euroopan tietosuojaneuvosto, joka voi antaa sitovia päätöksiä tietosuoja-asetuksen soveltamisessa.
Eheys	Tietojen ja tietojärjestelmien aitous, riidattomuus, väärentämättömyys, ajantasaisuus. Tietoa ei ole valtuudettomasti muutettu tai väärennetty.
Fyysinen turvallisuus	Laitteiden, tilojen, tietovarastojen ja toimitilojen suojaamista tuhoja ja vahinkoja vastaan. Tukijärjestelmien, kuten sähkön, ilmanvaihdon ja veden saannin varmistamista.
GDPR	General Data Protection Regulation, EU:n 24.5.2016 voimaantullut tietosuojauudistus.
Hallinnollinen turvallisuus	Yleinen tietoturvallisuuden organisointi, joka sisältää suunnittelun, tiedottamisen, valvonnan, vastuiden määrittelyn, ohjeistuksen ja koulutuksen järjestämisen.

Henkilöstöturvallisuus	Oman ja ulkopuolisen henkilökunnan turvallisuuden hallinta. Henkilöstön soveltuvuuden ja luotettavuuden sekä toimenkuvien, tiedon käyttöoikeuksien, henkilöstön suojaamisen ja henkilöstön koulutuksen muodostama kokonaisuus.
Järjestelmäturvallisuus	Tietojenkäsittelylaitteiden, tietokantojen ja tietoliikennelaitteiden käytettävyyden ja toiminnan varmistaminen.
Käytettävyys	Tiedot ja tietojenkäsittelyjärjestelmät ovat käytettävissä ja käyttökelpoisia käyttäjille, joilla on niihin pääsyoikeus.
Luottamuksellisuus	Tietojen säilyttäminen luottamuksellisina. Tiedot ja tietojärjestelmät ovat vain tietoon oikeutettujen käytössä.
Rekisterinpitäjä	Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä vastaa siitä, että henkilötietoja käsitellään lainmukaisesti.
Rekisteröity	Henkilö, jonka henkilötietoja käsitellään.
Tietosuoja	Yksityisyyden suoja ja yksityisyyttä turvaavat oikeudet.
Tietoturva	80 % toimintamalleja, prosesseja, vastuita, organisointia, asenteita, motivaatiota, käytännön toimintaa. 20 % teknisiä ratkaisuja.
Tietoturvapolitiikka	Organisaation johdon näkemys tietoturvallisuuden päämääristä ja tavoitteista.

3. Kehykset ja lait

Tietoturvallisuudesta huolehditaan kansallisten tietoturvaa ja tietosuojaa koskevien lakien ja säädösten mukaisesti. Toiminnassa noudatetaan valtionhallinnon, kuntaliiton ja tietosuojavaltuutetun antamia ohjeita ja suosituksia. Tietoturvapolitiikka pohjautuu useaan lakiin ja asetukseen. Näitä ovat muun muassa:

- EU:n yleinen tietosuoja-asetus (EU 2016/679)
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- Tietosuojalaki (1050/2018)

4. Tavoitteet

Tietoturvapolitiikan tavoitteena on:

1. Turvata toiminnalle tärkeiden tietojen, palveluiden, tietojärjestelmien ja tietoverkkojen toiminta normaaleissa ja poikkeusoloissa.

2. Luoda ja kehittää hyvät tietoturvakäytännöt, jotka mahdollistavat hyvän käytännön tietoturvatason.

3. Kehittää tietoturvaa jatkuvasti ja pitkäjänteisesti.

4. Ennalta ehkäistä tietojen käsittelyyn ja tietoon kohdistuvat uhat tai rajoittamaan vaikutukset hyväksyttävälle tasolle.

5. Varmistaa kaikkien osapuolten työskentelevän tietoturvallisesti joka päivä. Tietoturvallisuus on luonnollinen osa kaikkea toimintaa. Se on sisällytetty ja suhteutettu kattavasti kaikkeen toimintaan joka päivä.

Haapaveden kaupungilla käsitellään julkista, luottamuksellista ja salassa pidettävää tietoa. Tietoturvapolitiikalla pyritään estämään tietojen valtuudeton käyttö, tahaton tai tahallinen tietojen tuhoaminen ja tietojen päätyminen vääriin käsiin. Tietojen turvallisesta luomisesta, käytöstä, luovuttamisesta, tallentamisesta, arkistoinnista ja tuhoamisesta huolehditaan koko tiedon elinkaaren ajan. Turvallinen tietojenkäsittely käsittää tiedon sen kaikissa muodoissa, kuten paperinen, puhuttu ja sähköinen muoto. Erityistä huomioita kiinnitetään kolmannelta osapuolelta hankittavien palveluiden tietoturvaan.

Onnistuneen tietoturvapolitiikan edellytys on ylimmän johdon, esihenkilöiden, luottamushenkilöiden ja käyttäjien sitoutuminen tietoturvapolitiikkaan ja käytännön tietoturvatyöhön. Organisaatiolle laaditaan tietotilinpäätös, joka on osa tietojohtamista, riskienhallintaa ja sisäistä valvontaa.

Tietoturva kuuluu kaikille. Tietoturva näkyy jokaisen arjessa annettujen ohjeiden ja käytäntöjen noudattamisena. Tavoitteena on matalan ilmoittamisen malli, jossa pienetkin epäilykset tietoturvan vaarantumisesta tai rikkomisesta ilmoitetaan. Tietoturvatyöryhmä käsittelee ilmoitukset. Toiminnassa ei etsitä syyllisiä. Tietoturvatyössä etsitään ja korjataan ongelmia sekä minimoidaan riskejä.

5. Vastuut

Jokainen käyttäjä on organisaation tärkein tietoturvasta vastaava henkilö. Tietoturva ja tietoturvallisen työtavan noudattaminen kuuluvat kaikille. Jokainen vastaa omalta osaltaan omasta tietoturvallisesta toiminnasta, annettujen ohjeiden ja tietoturvapolitiikan noudattamisesta sekä järjestettyihin koulutuksiin osallistumisesta. Jokainen on velvollinen ilmoittamaan havaitsemastaan tietoturvapoikkeamasta esihenkilölleen ja tietoturvavastaavalle.

Esihenkilöt vastaavat oman alueensa tietoturvasta ja tietoturvapolitiikan noudattamisesta. Esihenkilöt huolehtivat, että käyttäjien kanssa on tehty asianmukaiset ja voimassa olevat vaitiolo- ja salassapitosopimukset. Käyttäjien tarvitsemien käyttöoikeuksien ja käyttäjätunnusten anominen ja organisaation palveluksesta poistuvien käyttäjien ilmoittaminen ylläpidolle kuuluu esihenkilöiden vastuulle.

Pääkäyttäjät nimetään jokaiselle käytettävälle tietojärjestelmälle. Tietojärjestelmien pääkäyttäjien vastuulla on sovellusten käytettävyydestä, kehittämisestä, käyttöoikeuksista ja järjestelmän tietoturvasta huolehtiminen. Muutoksista ja päivityksistä tiedottaminen on myös pääkäyttäjän vastuulla.

Tietoturvavastaava vastaa yleisesti tietoturvasta, sen seurannasta sekä tietoturvan ja tietoturvakäytäntöjen kehittämisestä yhdessä tietoturvatyöryhmän kanssa. Tietoturvavastaavana toimii tietohallintojohtaja.

Tietosuojavastaava on organisaation erityisasiantuntija, joka auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja lakien edellyttämän tietoturvatason. Asiakirjojen hallintaan ja laatuun liittyvät vaatimukset ovat osa tietoturvaa. EU:n tietosuoja-asetus velvoittaa nimeämään tietosuojavastaavan. Tietosuojavastaavan nimeää kaupunginhallitus.

Arkistonhoitaja vastaa arkistoitavien asiakirjojen käytettävyydestä, säilymisestä ja lainmukaisesta säilytyksestä. Arkistonmuodostamissuunnitelmassa huomioidaan arkistotoimen ja tietoturvan vaatimukset.

Rekisterinpitäjänä kaupunki on vastuussa siitä, ettei henkilötietoja käsitellä ilman laillista perustetta. Rekisterinpitäjä huolehtii henkilötietojen asianmukaisesta ja tietoturvallisesta

käsittelystä. Henkilötietojen käsittely on aina tarkoitussidonnaista, joka on määritelty etukäteen. Rekisterinpitäjän tietosuojavelvollisuudet koskevat kaikkia organisaation käsittelemiä henkilötietoja. Rekisterinpitäjällä on velvollisuus ilmoittaa ilman aiheetonta viivästystä valvontaviranomaisille havaituista henkilötietojen tietoturvaloukkauksista.

Luottamushenkilöt sitoutuvat noudattamaan kaupungin tietoturvapolitiikkaa, noudattamaan salassapitoa tarpeellisin osin sekä vastaavat omalta osaltaan tietoturvallisesta tavasta toimia sekä annettujen tietoturvaohjeiden noudattamisesta.

Toimialajohtajat huolehtivat ja vastaavat oman toimialansa tietoturvasta, ohjeiden ja tietoturvapolitiikan noudattamisesta. Lisäksi toimialajohtajat vastaavat siitä, että heidän toimialansa käytössä olevista ohjelmistoista on tehty tarvittavat rekisteriselosteet. Rekisteriselosteet toimitetaan arkistonhoitajalle. Toimialajohtajat huolehtivat myös, että rekisteriselosteet ovat ajan tasalla.

Tietoturvatyöryhmä vastaa tietoturvapolitiikan ajan tasalla pitämisestä sekä tietoturvapoikkeamien käsittelystä. Tarvittaessa tietoturvatyöryhmä laatii esiin tulleiden tapausten perusteella vaadittavat korjaustoimenpiteet. Tietoturvatyöryhmän jäseniksi kuuluvat kaupungin johtoryhmän jäsenet. Tarvittaessa työryhmää voidaan täydentää tarpeelliseksi katsotuilla henkilöillä.

Kaupunginjohtaja ja kaupunginhallitus johtavat ja valvovat tietoturvaa. Ylin johto määrittelee turvallisuuden keskeiset periaatteet osana toiminta- ja tietoturvaohjelmaa. Kaupunginhallitus hyväksyy Haapaveden kaupungin tietoturvapolitiikan ja tietoturvaperiaatteet. Kaupunginhallitus ohjaa ja ohjeistaa tietoturvatyöryhmän toimintaa tarvittaessa. Tietoturvan tarvitsemat resurssit varataan vuosittain talousarvioon. Kaupunginhallitus ja tietoturvatyöryhmä valvovat ja seuraavat tietoturvapolitiikan toteutumista ja kehittävät tietoturvapolitiikkaa pitkäjänteisesti.

6. Ulkoistukset ja kolmannet osapuolet

Haapaveden kaupungin tietoturvapolitiikkaa sovelletaan myös sidosryhmiin, kuten vuokratyövoimaan, harjoittelijoihin, alihankkijoihin ja konsultteihin. Hankintoja tehdessä tietosuojan vaatimukset asetetaan jo tarjouspyynnössä ja liitetään osaksi tarjouspyynnön perusteella tehtävää sopimusta. Tarvittaessa toimijoilta vaaditaan salassapitosopimus.

7. Toteutus

Tietoturvaa ylläpidetään hallinnollisin, fyysisin ja teknisin menetelmin. Jatkuva kehitys varmistetaan riittävällä resursoinnilla ja taloudellisella panostuksella. Tietoturvakartoitusten avulla tunnistetaan tietoaineistot ja tietojärjestelmät, arvioidaan tietoaineistoon ja tietojen käsittelyyn liittyvät riskit. Kartoituksen tulosten pohjalta kehitetään menetelmät ja toimintatavat riskien poistamiseksi tai minimoimiseksi.

Tarvittaessa kaupungin tietojenkäsittelyä ja tietojärjestelmien tietoturvan tasoa arvioidaan ulkoisen tarkastuksen kautta. Tietoturvaa kehitetään aktiivisesti. Kehitystyössä otetaan huomioon erilaiset sidosryhmät, kuten palvelujen toimittajat.

Tietojärjestelmälistaus sisältää tarkemman kuvauksen käytössä olevista tietojärjestelmistä. Listauksesta ilmenee, käsitelläänkö järjestelmässä henkilötietoja ja kuka on kyseisen järjestelmän pääkäyttäjä.

Pääsyn valvonnalla huolehditaan, ettei järjestelmää tai toimintoa voida käyttää ilman lupaa. Luotettava pääsynvalvonta edellyttää, että jokainen käyttäjä voidaan tunnistaa. Tämä edellyttää henkilökohtaisia käyttäjätunnuksia. Käyttäjälle myönnetyt pääsy- ja käyttöoikeudet tulee olla dokumentoituna niin, että käyttäjän työsuhteen päättyessä kaikki tunnukset tulevat lukittua ja poistettua.

Henkilökunnalle ja luottamushenkilöille kohdennetulla ohjeistuksella, koulutuksella ja tiedottamisella varmistetaan käyttäjien riittävät valmiudet tietoturvalliseen työskentelytapaan. Tarvittaessa voidaan tehdä sisäisiä tarkastuksia tietoturvakäytäntöjen käyttöönotosta ja niiden ymmärtämisestä toiminnassa.

8. Seuranta

Seurantaa toteutetaan sekä teknisin että hallinnollisin menetelmin. Tietoturvapolitiikan toteutumista seurataan kaupunginhallitukselle toimitettavalla tietotilinpäätöksellä. Tietotilinpäätös sisältää vuoden aikana henkilökunnalle järjestetyt koulutukset, koulutukseen osallistuneiden määrän, tietoturvatyöryhmän kokoontumiset, ilmoitetut ja havaitut tietoturvapoikkeama-ilmoitukset sekä tietosuojaan vaikuttavat hankkeet ja niiden sen hetkiset tilanteet. Teknisenä seurantamenetelmänä on kattava tietojärjestelmien lokilistaus.

Haapaveden kaupungin tietojärjestelmiä ja toimintatapoja arvioidaan omavalvonnan ja sisäisen tarkastuksen keinoin. Tarvittaessa käytetään ulkopuolisia toimijoita.

Ilmoitetut ja havaitut tietoturvapoikkeamat kirjataan ylös ja käsitellään tietoturvatyöryhmässä.