KÄRKÖLÄ

KÄRKÖLÄN KUNTA

TIETOTURVAPOLITIIKKA

Kunnanhallitus 15.4.2024 § 78

Kärkölän kunta 044 770 2200 kirjaamo@karkola.fi
Opintie 2

SISÄLLYS

1. Kärkölän kunnan tietoturvapolitiikka

1.1. Johdanto

Tietoturvapolitiikka on Kärkölän kunnanhallituksen hyväksymä strateginen asiakirja tietoturvallisen toiminnan toteuttamiseksi ja kehittämiseksi. Kunnan tietoturvapolitiikan tavoitteena on varmistaa yhdenmukaiset toimintaperiaatteet, käytännöt ja vastuut hyvän tietoturvatason toteuttamiseksi.

Tätä politiikkaa sovelletaan kaikkeen tietoon riippumatta esitystavasta, muodosta tai elinkaaren vaiheesta.

1.2 Tietoturvan määritelmä

Tietoturvalla tarkoitetaan eri muodoissa olevien tietojen suojaamista uhkatekijöiltä siten, että toimintojen ja palvelutuotannon laatu, luotettavuus ja jatkuvuus varmistuvat ja että toiminnassa käsiteltäviin tietoihin kohdentuvat riskitekijät minimoidaan.

Digitaalisen turvallisuuden tavoitteena osana tietoturvaa on toimintaympäristön turvallinen hallinta ja luotettava toiminta myös häiriötilanteissa. Digitaalinen turvallisuus koostuu tietoturvallisuudesta, tietosuojasta, kyberturvallisuudesta, riskienhallinnasta sekä toiminnan jatkuvuudenhallinnasta ja varautumisesta.

Tietoturva koostuu tiedon *luottamuksellisuuden, eheyden, saatavuuden, käytettävyyden* ja tarvittaessa *kiistämättömyyden* varmistamisesta hallinnollisin ja teknisin toimin. Tarvittaessa tiedon käyttö *todennetaan*.

Tietojen luottamuksellisuus:

- Tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Luottamuksellisuus saavutetaan estämällä valtuudeton käyttö sekä luokittelemalla ja tarvittaessa salaamalla käsiteltävä tietosisältö.

Tietojen eheys:

- Tiedon oikeellisuus ja suojaus on järjestetty niin, että tietoa ei voi tahallisesti tai tahattomasti muuttaa vaarantaen toiminnan luotettavuutta. Eheys varmistetaan niin, että tietoa ei voida muuttaa ilman asianmukaisia valtuuksia ja että yritykset käsitellä tietoa tai järjestelmiä ilman valtuuksia havaitaan. Eheyden varmistaminen sisältää myös

varotoimet tiedon tahattoman vääristymisen estämiseksi inhimillisen tai teknisen häiriön seurauksena.

Tiedon saatavuus ja käytettävyys:

- Tieto on saatavissa ja käytettävissä silloin, kun sitä tarvitaan. Saatavuuden varmistamiseksi tulee ylläpitää riittävää kapasiteettia, vikasietoisia toteutuksia, varmuuskopiokäytäntöjä sekä käyttää luotettavaksi todettuja teknisiä ratkaisuja.

Tiedon kiistämättömyys:

- Tiedonkäsittelyyn liittyvät toimenpiteet suoritetaan niin, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa toimenpiteiden aikana ja jälkikäteen. Kiistämättömyyden toteutumista tuetaan kattavilla ja keskitetyillä tapahtumien kirjaus- ja lokienhallinta-käytännöillä.

Todentaminen:

- Tiedon kohteen todenmukaisuus, oikeellisuus, alkuperä tai käyttäjän aitous varmistetaan määritellyllä luottamustasolla.

1.3 Toimintaympäristö

Kärkölän kunnan toiminta ja palvelutuotanto perustuvat merkittäviltä osin tietoon ja sen käsittelyyn, koulutetun ja tietoturvatietoisen henkilöstön osaamiseen sekä hyvän hallinnon periaatteiden noudattamiseen. Kaikissa muodoissa olevan tiedon ja tietojen käsittelyn turvaaminen on osa kunnan toimintaa ja kokonaisturvallisuuden ylläpitämistä.

Tietoturvaan liittyvät toiminnan tavoitteet, vastuut ja periaatteet määritellään tietoturvapolitiikassa Kärkölän kunnan johdon linjausten mukaisesti.

Tämä politiikka toimii perustana yksityiskohtaisemmille määräyksille, ohjeille sekä käytännöille, joiden avulla tietoturvatyö on osa kunnan toimintaa. Tietoturvapolitiikka koskee jokaista Kärkölän kunnan työntekijää, viranhaltijaa, luottamushenkilöä ja kunnan lukuun toimivaa, joka työnsä tai toimeksiantonsa perusteella käsittelee kunnan omistamaa tai hallinnoimaa tietoa.

1.4 Tietoturvan vaatimuksenmukaisuus

Lainsäädäntö edellyttää tietoturvan ja tietosuojan vaatimusten huomioimista kunnan toimintojen ja palvelutuotannon toteuttamisessa. Kärkölän kunnassa tietoturvallisuutta, tietosuojaa, tiedonhallintaa ja -käsittelyä ohjaavat mm. seuraavat säädökset ja ohjeet:

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

Yleinen tietoturvatilanne maailmassa on luonteeltaan muuttuvaa. Tietoon ja sen käsittelyyn liittyvät teknologiat, mm. tekoäly, kehittyvät nopeasti. Kärkölän kunnassa seurataan ja huomioidaan ennakoivasti myös valmisteilla olevaa lainsäädäntöä:

EU:n ehdottama tekoälysäädös

Tietoturvan ja tietosuojan vaatimusten osalta huomioidaan myös sisäiset ja ulkoiset riskit, sopimusvelvoitteet, soveltuvat kansalliset tietoturvaa koskevat standardit ja kriteeristöt, julkishallintoa koskevat suositukset ja hyvät käytännöt.

2. Tietoturvatyön vastuut ja periaatteet

Kärkölän kunnan tietoturvan omistajuus ja ylätason vastuut määritellään hallintosäännössä. Tietoturvan käytännön vastuut ja velvollisuudet määritellään tietoturvapolitiikassa seuraavasti:

Kunnanhallitus:

- Tietoturvallisuusjärjestelyt, tietojärjestelmien toiminta ja yhteen toimivuus sekä tietovarantojen toiminta ja yhteen toimivuus
- Tietoturvallisuustoimenpiteet sekä poikkeusoloihin varautuminen
- Luokittelu julkiseen ja ei-julkiseen varautumisen dokumentaatioon
- Julkisen ja ei-julkisen tietoturvaan ja varautumiseen liittyvän dokumentaation tallentamistavoista ja -sijainneista päättäminen
- Tietoturvapolitiikan hyväksyminen

Johtoryhmä:

- Tietoturvan toteutumisen asianmukaisuuden ja riittävyyden seuranta

Kansliapäällikkö:

- Tietoturvan järjestäminen ja toteutumisen raportointi kunnanhallitukselle
- Tietoaineistojen ja tietojärjestelmien tietoturvallisuus
- Tietojen siirtäminen tietoverkossa
- Tietoaineistojen turvallisuuden varmistaminen
- Tietojärjestelmien käyttöoikeuksien hallinta
- Lokitietojen kerääminen tietojärjestelmien käytöstä ja luovutuksesta
- Tietoturvapolitiikasta johdettavien tietoturva-asiakirjojen valmistelu
- Tekoäly, tekoälyn käytön käytänteiden ja tekoälyä käyttävien sovellusten sekä ohjelmistojen tietoturvallisuuden varmistaminen

Toimialajohtaja:

- Tietoturvan toteutumisen valvonta ja raportointi omalla toimialallaan
- Tietoturvan toimeenpano, ylläpito ja kehittäminen toimialallaan
- Operatiivisten tietojärjestelmien tietoturvallisen käytön ohjeistaminen yhteistyössä tietojärjestelmän vastuuhenkilön kanssa

Henkilöstöpäällikkö:

- Tietoturvan ja tietosuojan toteuttaminen henkilöstöprosessin kaikissa vaiheissa: työsuhteen alkaessa, työsuhteen aikana ja sen päättyessä

Esihenkilö:

- Ohjauksessaan olevien tietoturva- ja tietosuojaperehdytys, omaisuuden hallinta, avainten ja työvälineiden luovutus ja palautus sekä käyttö- ja pääsyoikeuksien hallinnan toteuttaminen

Henkilöstö:

- Määräysten ja ohjeiden noudattaminen
- Tietoturvapoikkeamien ja ei-toivottujen tapahtumien ilmoittaminen välittömästi omalle esihenkilölle tai kansliapäällikölle sekä WPro-työturvallisuusjärjestelmään

Tietosuojavastaava:

- Henkilötietojen käsittelyn valvonta ja yhteistyö valvontaviranomaisen kanssa
- Henkilökunnan ja johdon tukeminen tietosuoja-asioissa
- Tietosuojaan liittyvä sisäinen viestintä

Tietojärjestelmän pääkäyttäjä:

- Tietoturvan, tietosuojan ja käyttöoikeuksien hallinta tietojärjestelmässä
- Tietojärjestelmän käytön seuranta ja tietosuojaselosteen edellyttämien tietojen toimittaminen tietohallintoon koottua ilmoitusmenettelyä varten

Tiedon omistaja:

- Tiedon, tietokokonaisuuden tai tietosisällön tuottaminen ja käsittely
- Päävastuu tiedosta riippumatta siitä, missä tai kenen toimesta tietoa käsitellään
- Informointi tietoja edelleen luovutettaessa tietoon mahdollisesti liittyvistä suojaus- ja muista velvoitteista

Ulkoinen ICT-palveluntuottaja:

- Sopimuksenmukaisen tietoturvatason toteuttaminen
- Palvelun tietoturvallisuuteen liittyvien teknisten riskien tai poikkeamien hallinta ja raportointi

3. Tietoturvatyön tavoitteet

Tietoturvatyön tavoitteena on kehittää kunnan toimintaympäristön digitaalisen turvallisuuden hallintaa ja varmistaa toimintojen ja palvelutuotannon luotettavuus ja jatkuvuus. Tietoturvatyö on kiinteä osa kunnan johtamista ja riskienhallintaa, ja sillä luodaan yhdenmukaiset tietoturvakäytänteet hallintosäännöstä johdettujen periaatteiden mukaisesti.

Tietoturvan kehittämisen tavoitteita ovat kokonaisvaltainen tietoturvatyön kehittäminen, uhkatekijöiden tunnistaminen ja ennaltaehkäisy sekä tiedon ja sen arvon suojaaminen.

Kunnan tietoturvatyötä tehdään kunnan johdon ohjauksessa, ja se perustuu jatkuvan kehittämiseen malliin. Kehitysprosesseissa arvioidaan kunnan toimintaympäristöön kohdistuvia tekijöitä, asetetaan tavoitteet ja laaditaan suunnitelmat niiden saavuttamiseksi. Suunnitelmat johdetaan työkäytännöiksi, ja tavoitteiden toteutumista seurataan säännöllisesti. Käytäntöjä tarkistetaan ja muutetaan tarvittaessa seurannan ja tulosten perustella.

Kärkölän kunnan tietoturvatyön tavoitteena on

- luoda ja ylläpitää luotettava ja turvallinen ympäristö kunnassa tapahtuvalle tiedon käsittelylle
- toteuttaa palvelut ja niiden edellyttämät järjestelmät niin toimintavarmoiksi ja hyvin suojatuiksi, että ne sellaisinaan kestävät kohtuudella odotettavissa olevat tietoturva- ja kyberuhkat
- varmistaa mahdollisimman häiriötön ja turvallinen toiminta sekä palvelutuotanto
- huolehtia vaatimusten mukaisesta tietojen, ja erityisesti henkilötietojen käsittelystä kaikissa tilanteissa
- tukea kunnan turvallisuuskulttuurin kehittämistä

3.1 Tietoturvan uhkatekijöiden tunnistaminen ja hallinta

Kärkölän kunta muodostaa tiedonhallintayksikön. Tiedonhallintayksikön tulee tiedonhallintalain mukaisesti tunnistaa merkittävät tietoon ja tietojenkäsittelyyn kohdentuvat riskitekijät ja hallita niihin liittyviä tietoturvatoimenpiteitä. Digitaalisessa

toimintaympäristössä pyritään tunnistamaan tietoturvaan kohdistuvat uhkatekijät ja reagoimaan poikkeamiin ennakoivasti.

3.2 Tietojen ja palveluiden jatkuvuuden turvaaminen

Tietojärjestelmien, tietoverkkojen ja tietojenkäsittelyn keskeytymätön toiminta tulee turvata.

Tiedon luvaton käyttö tai tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen on havaittava ja estettävä, ja näistä mahdollisesti aiheutuvat vahingot on minimoitava.

Kriittisten toimintojen saatavuus pyritään varmistamaan normaalioloissa sekä poikkeusolojen häiriötilanteissa mahdollisimman lyhyellä toipumisajalla.

3.3 Tiedon, tietojärjestelmien ja päätelaitteiden turvallinen käyttö

Kärkölän kunnan tietojärjestelmäympäristössä käytetään kunnan tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten.

Kärkölän kunta tarjoaa tarvittavat päätelaitteet henkilökunnan ja luottamushenkilöiden käyttöön työ- tai luottamustehtävien hoitamista varten. Kunnan osoittamilla laitteilla ei tule käsitellä henkilökohtaista aineistoa. Henkilökohtaisilla päätelaitteilla ei tule kirjautua työ- tai luottamustehtävien edellyttämiin järjestelmiin tai käsitellä näihin liittyviä aineistoja tai dokumentteja tietoturvasyistä.

3.4 Henkilökunnan ja luottamushenkilöiden tietoturvatietouden ja osaamisen kehittäminen

Tietoturvapolitiikka ja siihen liittyvät muut ohjeistukset ja käytännöt ovat kunnan johtamista ja käytännön toimintaa. Tämä edellyttää sekä henkilökunnalta että luottamushenkilöiltä tietoturvakäytänteiden tuntemista ja ohjeistusten noudattamista. Tietoturva- ja tietosuojaymmärryksen osaamisen lisääminen on osa kehittämis- ja perehdyttämistoimintaa.

Tavoitteena on parantaa kyvykkyyttä vastata tietoturvan uhkakuviin sekä varmistaa tietoturvan, tietosuojan ja yksityisyydensuojan toteutuminen parantamalla tietoturvaymmärrystä läpi organisaation.

3.5 Hankintoihin liittyvät tietoturvaedellytykset

Tietoturva- ja tietosuojanäkökulmat on huomioitava myös hankinnoissa. Hankinnan vastuutaho varmistuu siitä, että hankinnoissa noudatetaan näiltä osin Kärkölän kunnan Hankintaohjetta.

3.6 Toimintaketjujen tietoturvan varmistaminen

Tietoturvallisen toimintaympäristön hallintaan kuuluu myös toimintaketjujen tietoturvan varmistaminen. Palvelutuottajat, yhteistyökumppanit ja alihankintaketjut sitoutetaan ja velvoitetaan noudattamaan Kärkölän kunnan tietoturvakäytänteitä.

3.7 Tietosuojan varmistaminen

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

Henkilötietoja käsiteltäessä määritellään rekisterinpitäjä. Rekisterinpitäjällä on vastuu henkilötietojen käsittelyn lainmukaisuudesta. Rekisterinpitäjä määrittää, mihin käyttötarkoitukseen ja miten henkilötietoja käsitellään.

Kärkölän kunta käsittelee henkilötietoja rekisterinpitäjänä tietosuojan toimintaperiaatteiden ja voimassa olevan lainsäädännön mukaisesti:

- Henkilötietoja kerätään ennalta määriteltyjen käyttötarkoitusten kannalta vain niiltä osin, kuin se palvelujen tuottamisen ja tehtävien suorittamisen kannalta on välttämätöntä
- Henkilötietojen suojaamisesta ja elinkaarihallinnasta huolehditaan suunnitelmallisesti ja läpinäkyvästi
- Henkilöstön riittävä tietosuojaosaaminen varmistetaan tehtävänkuvan edellytysten perusteella
- Henkilötietojen käsittelyn periaatteista informoidaan asiakkaita kattavasti
- Henkilötietojen käsittelyyn liittyviä riskejä arvioidaan säännöllisesti
- Sopimuskumppaneilta edellytetään lainsäädännön edellyttämien tietosuojaperiaatteiden noudattamista.

Tietosuoja-asetuksessa säädetään henkilötietojen käsittelyn periaatteista:

- Henkilötietoja tulee käsitellä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- Käsiteltävien henkilötietojen laatu varmistetaan. Tietojen tulee olla täsmällisiä ja virheettömiä. Virheelliset tiedot korjataan.
- Henkilötietojen luottamuksellisuus ja turvallisuus varmistetaan. Tiedot suojataan luvattomalta pääsyltä, vahingossa tapatuvilta häviämisiltä, tuhoutumiselta ja vahingoittumiselta.
- Käsiteltävät henkilötiedot ovat olennaisia, asianmukaisia ja riittäviä palvelun tarjoamiseksi. Tietoja kerätään vain määriteltyä käyttötarkoitusta varten.
- Henkilötietoja säilytetään vain niin kauan, kuin se käyttötarkoituksen osalta on tarpeellista, arkistointivaatimukset huomioiden.
- Henkilötietoja käsitellään käyttötarkoitussidonnaisuuden periaatteen mukaan vain siinä tarkoituksessa, mihin ne on alun perin kerätty, eikä niitä voi jakaa käsiteltäviksi muissa tarkoituksissa.

3.8 Lokitietojen hallinta

Lokitieto tarkoittaa suojattavan tiedon tai tietojärjestelmän käsittelystä tai luovuttamisesta tai tietoliikenneverkon käytöstä kerättävää käyttäjäkohtaista tietoa. Lokimerkinnöistä selviää tapahtumien toteutuminen ja ajankohta. Lokitiedoilla voidaan valvoa tietoturvan ja tietosuojan toteutumista ja jäljitettävyyttä, ja niitä kerätään aina, kun tietojärjestelmän tai palvelun käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen avulla voidaan muodostaa aukoton tapahtumaketju tiedonkäsittelyn ja tapahtumien todentamiseen. Lokitiedoilla voidaan tarvittaessa vahvistaa ja toteuttaa työ- tai virkasuhteessa olevan oikeusturvaa tietojen käsittelyn osalta varmistamalla tapahtumien kiistämättömyys.

Lokitiedot suojataan, ja niitä voivat käsitellä vain siihen oikeutetut henkilöt. Lokitietojen käsittelyssä on huomioitava toiminnan oikeellisuus, tiedonhallinnan elinkaari ja säilyttämisen lakisääteiset velvoitteet.

3.9 Käyttövaltuushallinta

Tietojärjestelmän tai tiedon omistajan, rekisterinpitäjän tai muun vastuutahon tulee määrittää tietojärjestelmän tai palvelun käyttövaltuuksien hallinnan ja käsittelyn myöntämisen periaatteet. Käyttövaltuuksien myöntämisessä huomioidaan tietojenkäsittelyn oikeuksiin liittyvät lakisääteiset velvoitteet. Pääkäyttäjät määrittelevät ja myöntävät käyttövaltuudet käyttäjän työtehtävien edellyttämässä laajuudessa. Käyttövaltuushallinnan avulla tietojen luvallinen käyttö on mahdollista ja luvaton käyttö estetään. Käyttäjälle annetaan tarvittavaan toimintaympäristöön vain sellaiset käyttövaltuudet, jotka ovat työn suorittamisen kannalta välttämättömiä.

Käyttövaltuushallinnan on oltava ajantasaista, ja sen avulla huolehditaan käyttäjätunnusten ja pääsyoikeuksien elinkaarihallinnasta työsuhteen ajan. Pääsyoikeus perustuu käyttäjän allekirjoittamaan Salassapito-, vaitiolo- ja käyttäjäsopimukseen.

Käyttöoikeudet ja käyttäjätunnukset ovat henkilökohtaisia, eikä niitä saa luovuttaa toiselle henkilölle.

3.10 Kokonaisturvallisuuden hallinta

Kokonaisturvallisuuden hallinta edellyttää kunnan toimintaympäristön kattavaa tuntemusta, toiminnan suunnittelua, osaamisen ylläpitoa, viestintää sekä jatkuvaa seurantaa ja muutosten hallintaa.

Kärkölän kunnassa kokonaisturvallisuudella tarkoitetaan niitä osa-alueita, jotka yhdessä tietoturvakäytäntöjen kanssa muodostavat eheän kokonaisuuden kunnan tiedon, tietojärjestelmien ja - verkkojen sekä henkilöstön, kunnan kiinteistöjen ja muun omaisuuden suojaksi:

Kyberturvallisuus:

- Kybertoimintaympäristön turvaamisen toimenpiteet

Fyysinen turvallisuus:

- Toimenpiteet, järjestelmät ja rakenteet, joiden avulla kunnan tiloja ja siellä olevia ihmisiä, kuljetuksia, matkatyötä sekä tietoa ja muuta omaisuutta suojataan fyysisiltä ja kiinteistö- ja ympäristövahingoilta, vahingoittamisyrityksiltä ja oikeudettomilta henkilöiltä.

Henkilöstöturvallisuus:

- Tietoturvatoimenpiteet, joita suoritetaan henkilöstöprosessin kaikissa vaiheissa: ennen palvelussuhdetta, sen aikana ja palvelussuhteen päättyessä.

Riskienhallinta:

- Kaikki kunnan toiminnot ja organisaatiotasot kattava järjestelmällinen toiminta kunnan sisäisten ja ulkoisten riskien hallitsemiseksi kunnan kannalta tarkoituksenmukaisia ja kustannustehokkaita ratkaisuja käyttämällä. Riskienhallinnassa pyritään ennakointiin jälkikäteisen reagoinnin sijaan, ja tavoitteena on laatia riskienhallintasuunnitelma kaikille kriittisiksi luokitelluille palveluille ja järjestelmille. Tietoturvan ja kokonaisturvallisuuden kehittäminen liitetään riskienhallinnan kautta kunnan johtamisjärjestelmään ja tätä kautta koko kunnan toiminnan kehittämiseen.

Varautuminen ja jatkuvuudenhallinta:

- Hallinnolliset ja tekniset toteutukset (esim. valmius-, jatkuvuus-, toipumis- ja pelastussuunnitelmat sekä niihin liittyvät prosessit), joilla kunnan toimintojen ja palveluiden jatkuvuus turvataan normaalioloissa, häiriötilanteissa sekä poikkeusoloissa. Jatkuvuudesta huolehditaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia jatkuvuus- ja muita suunnitelmia. Lisäksi toimintaympäristön tilaa seurataan aktiivisesti ja mahdollisiin poikkeamiin ja häiriöihin reagoidaan tietoturvapoikkeamien hallintaprosessin mukaisesti.
- Varautumisen dokumentointi tulee arvioida julkisen ja ei-julkisen tiedon osalta tietoturvasyistä. Ei-julkisen dokumentaation tallentamistavoista ja -sijainneista on päätettävä erikseen.

Tietosuoja:

- Velvoittavien tietosuojasäädösten mukaiset toimenpiteet, joilla varmistetaan henkilön riittävä yksityisyydensuoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.

Mainitut vaatimukset saatetaan tarvittavilta osin koskemaan myös kunnan sidosryhmiä sopimushallinnan keinoin.

4. Tietoturvan järjestämisen periaatteet ja tietoturvallisuuden toteuttaminen

Tietoturvallisuustyötä toteutetaan kunnassa suunnitelmallisesti. Keskeistä on, että kunnalla on riittävät kyvykkyydet kehittää ja ylläpitää turvallisuuskulttuuria.

Kärkölän kunnan tietoturvatyössä noudatetaan seuraavia periaatteita:

- Tietoturvallisuutta ja tietosuojaa johdetaan järjestelmällisesti
- Henkilötietojen käsittelyyn kiinnitetään erityistä huomiota huolehtimalla tietosuojasäädösten vaatimusten täyttymisestä
- Henkilöstön osaamisesta huolehditaan koulutussuunnitelman mukaisilla jatkuvilla koulutuskäytännöillä
- Toimintaympäristön tilaa seurataan aktiivisesti
- Uhka- ja riskiympäristöä arvioidaan säännöllisesti kaikilla toimialoilla, ja siihen reagoidaan tilanteen edellyttämällä tavalla
- Toiminnan jatkuvuutta uhkaaviin poikkeamiin ja häiriöihin varaudutaan ennakolta ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia jatkuvuus- ja muita suunnitelmia
- Kunnan määrittelemät tietoturvavaatimukset huomioidaan mahdollisimman varhaisessa vaiheessa liittyen toimintojen, hankintojen ja teknisten järjestelmien suunnitteluun, ja edellytetyt tietoturvavaatimukset sisällytetään kaikkiin sopimuksiin
- Tietoturvadokumentaatiota prosesseineen pidetään ajan tasalla
- Tietoturvan toteutumista tuetaan sisäisellä ja ulkoisella viestinnällä
- Tietojärjestelmät ja tietojenkäsittely toteutetaan hyvän tiedonhallintatavan mukaisesti, joka mahdollistaa tarvittavien asiakirjojen julkisuuden, tiedon asianmukaisen arkistoinnin ja hävittämisen.

5. Digitaalisen turvallisuuden tilannekuva, seuranta ja uudet teknologiat

5.1 Tilannekuva ja seuranta

Digitaalisen turvallisuuden tilannekuva muuttuu jatkuvasti. Uhkat ovat todellisia, ja niitä tulee tarkastella realistisesti. Organisaatioihin kohdistuu lisääntyvästi mm. palvelunestohyökkäyksiä, tietojenkalasteluita, huijauspuheluita ja murtautumisyrityksiä käyttäjätileille. Vaikutukset voivat olla hetkellisiä häiriötilanteita tai ne voivat edellyttää vakavia, kalliita ja pitkäkestoisia jatko- ja korjaustoimenpiteitä. Pienenkään organisaation ei tule pitää olettamana sitä, että se tai sen käsittelemä tieto ei olisi hyökkääjän näkökulmasta kiinnostavaa, vaan digitaalisen turvallisuuden tilanteen heikkenemiseen ja mahdollisiin uhkiin tulee suhtautua vakavasti.

Kärkölän kunnassa huomioidaan tilannekuvan ajantasainen kehitys mm. seuraamalla muuttuvaa lainsäädäntöä, kansallisia suosituksia, standardeja ja kriteeristöjä, julkishallintoa koskevia suosituksia sekä Kyberturvallisuuskeskuksen julkaisemaa säännöllistä viikkokatsausta, joka käsittelee uusimpia tietoturva- ja kyberturvatapauksia ja ilmiöitä.

5.2 Kehittyvät teknologiat

Teknologian ja tekoälyn kehittymisen myötä näiden käytön vaikutukset on tunnistettava kunnan toiminnoissa ja palvelutuotannossa. Uusia sovelluksia kehitetään jatkuvasti, ja myös kuntaorganisaatioiden käyttömahdollisuudet monipuolistuvat ja lisääntyvät.

Uusia teknologioita ja tekoälyä sekä näiden soveltamista on tarkasteltava tietoturvan ja tietosuojan näkökulmista. Tekoälyä käytetään myös haitallisiin ja rikollisiin tarkoituksiin.

6. Tietoturvadokumentaation ylläpito

Tämän tietoturvapolitiikan säännöllisestä katselmoinnista vastaa sen omistajana kansliapäällikkö tai hänen nimeämänsä taho.

Tästä politiikasta johdettu muu tietoturvadokumentaatio katselmoidaan ja päivitetään sekä hyväksytään kansliapäällikön ohjaamalla tavalla.

Kärkölän kunnan tietoturvadokumentaatio on henkilöstön saatavilla kunnan sisäisissä informaatiokanavissa henkilön työtehtävien edellyttämässä laajuudessa.

7. Ohjeen voimaantulo ja ajantasaisuus

Tämä ohje tulee voimaan 15.4.2024.

Kunnanhallitus valtuuttaa kansliapäällikön hyväksymään tietoturvapolitiikkaan sellaiset vähäiset korjaukset ja täsmennykset, jotka ovat tarpeellisia sen ajan tasalla pitämiseksi. Tietoturvapolitiikka tuodaan kunnanhallituksen käsittelyyn, kun toiminnassa tai lainsäädännössä tapahtuu sellaisia merkittäviä muutoksia, jotka edellyttävät tietoturvapolitiikan laajaa päivittämistä.