NÄRPES STAD
NÄRPIÖN KAUPUNKI

NÄRPIÖN KAUPUNGIN TIETOTURVAPOLITIIKKA

Luotu: 29.10.2020
Asiakirjan vastuutaho: Tietoturvaryhmä
Kaupunginhallituksen hyväksymä 16.12.2020

Sisällysluettelo

1. Johdanto ja tausta

Närpiön kaupungin tietoturva perustuu tälle tietoturvapolitiikalle, joka täydentää kaupungin muita esimerkiksi tietotekniikkaa, laatua, viestintää ja muuta riskienhallintaa koskevia ohjausasiakirjoja. Tämä politiikka koskee kaikkia työntekijöitä, viranhaltijoita, luottamushenkilöitä ja sidosryhmien edustajia, jotka työnsä tai tehtävänsä puitteissa käsittelevät Närpiön kaupungin omistamia tai hallinnoimia tietoja.

Tieto on erittäin tärkeä resurssi ja edellytys Närpiön kaupungin asianmukaisen toiminnan harjoittamiselle. Tieto voi olla arkaluonteista tai salassa pidettävää ja tietoa voidaan pahimmillaan väärinkäyttää yhteiskunnan toimivuuden häiritsemiseksi tai taloudellisten hyötyjen saavuttamiseksi.

2. Tarkoitus

Tämän politiikan tarkoituksena on selkeyttää turvallisen tiedonhallinnan vaatimuksia Närpiön kaupungin lautakunnissa ja yhtiöissä. Jatkuva tietoturvatyö on tarpeellista kaupungin tehtävien suorittamisen ja tavoitteiden saavuttamisen kannalta. Tietoturvatyön tarkoituksena on suojella kaupungin toimintaa häiriöiltä ja vähentää vahinkoja estämällä ja ehkäisemällä ei-toivottujen tapahtumien vaikutuksia.

3. Tietoturva

Teknisen kehityksen myötä yhä enemmän tietoa tallennetaan myös pilvipalveluihin, eikä ainoastaan paikallisille palvelimille tai fyysisessä paperimuodossa. Tämä kehitys merkitsee, että tiedon käsittelyä ja suojaamista koskevat vaatimukset lisääntyvät. Närpiön kaupunki pyrkii aktiivisesti ylläpitämään
tarpeellisia turvallisuusvaatimuksia ja varmistamaan tietojen turvallisen käsittelyn toiminnassaan.

Tietoturvapolitiikka kattaa kaikenlaisen tiedon riippumatta siitä, sijaitsevatko tiedot pilvipalveluissa, tietokoneilla, puheluissa / tekstiviesteissä, fyysisissä keskusteluissa tai paperilla. Seuraavat käsittelyohjeet koskevat kaikkea tietoa.

Tietoturvalla tarkoitetaan tietojen käsittelyä koskevien asianmukaisten rutiinien ja suojausten luomista ja ylläpitämistä neljään näkökohtaan perustuen:

- **Luottamuksellisuus:** tieto ei ole sivullisten saatavilla sivullisille tai sitä ei paljasteta sivullisille
- **Eheys:** tieto on oikeaa, ajan tasalla ja täydellistä
- **Saatavuus:** tieto on asianomaisen saatavilla ja käytettävissä
- **Jäljitettävyys:** tietoja muokattaessa tekijä ja ajankohta voidaan selvittää.

Eri tietoja koskevat erilaiset vaatimukset näiden neljän näkökohdan suhteen. Vaatimukset voivat perustua oikeudellisiin vaatimuksiin tai Närpiön kaupungin asettamiin tavoitteisiin. Lisäksi tietysti asukkailla, yrityksillä ja muilla läheisillä toimijoilla on tarpeita ja odotuksia, jotka asettavat vaatimuksia tietoturvallemme.

Närpiön kaupungin tietoturva sisältää myös kyberturvallisuuden, tietosuojan ja muut turvallisuuden osa-alueet. Näistä kaupungille keskeisimmät ovat seuraavat:

- Luottamuksellisuuden, yksilönsuojan, saatavuuden ja jatkuvuuden varmistaminen kyberava-

ruudessa.

- Yksilönsuojan ja sitä turvaavien oikeuksien toteutumisen lakisääteinen varmistaminen henkilötietojen käsittelyssä.
- Kaupungin tilojen ja niissä olevien ihmisten, tietojen ja muun omaisuuden suojaaminen erilaisilta vahingoilta, ilkivallalta ja sivullisilta.
- Henkilöstöprosessin toimenpiteet ennen työsuhteen alkamista, sen aikana ja päättyessä.

4. Tavoitteet

Tietoturvalla ei ole itseisarvoa, vaan sen tarkoitus on edistää Närpiön kaupungin laajempien visioiden, strategioiden ja tavoitteiden saavuttamista. Närpiön kaupungin on saavutettava ja ylläpidettävä tietoturvan taso, joka

- takaa vahvan, varman ja luotettavan tietojen käsittelyn,
- mahdollistaa aktiivisen osallistumisen digitaaliseen yhteiskuntaan,
- edistää esimerkiksi laatua, tehokkuutta ja yksilönsuojaa koskevien tavoitteiden saavuttamista,
- vastaa asukkaiden ja ulkoisten toimintojen tarpeita ja odotuksia,
- ilmaistaan ajanmukaisissa ohjausasiakirjoissa kuten politiikassa ja ohjeistuksissa,
- enoudattaa lakien, asetusten, säännösten ja sopimusten asettamia vaatimuksia.

5. Järjestäminen, asemat ja vastuut

Jokainen, joka jossain määrin hallinnoi tietovaroja, on vastuussa tietoturvan ylläpitämisestä. Vastuu toiminnasta määrittää vastuuta kyseisen toiminnan tietoturvasta. Närpiön kaupungin tietoturvaa koskeva politiikka hyväksytään kaupunginhallituksessa.

Tietohallintoyksikkö (kaupunginhallitus) seuraa kaupungin tietoturvaa. Kaupunginhallitus hyväksyy koko kaupunkia koskevan tietoturvapolitiikan, ohjeistukset ja linjaukset. Kaupunginhallitus järjestää sisäisen valvonnan ja riskienhallinnan.

Tietoturvavastaava (kaupunginjohtaja) on kokonaisvastuussa tietoturvasta ja sitä koskevasta raportoimisesta kaupunginvaltuustolle. Tietoturvavastaava vastaa tietoturvapolitiikasta ja esittelee sitä koskevat muutokset kaupunginvaltuustolle. Kaupungin johtoryhmä ja tietoturvaryhmä avustavat kaupunginjohtajaa tietoturvaa koskevissa asioissa

Tietoturvaryhmä seuraa tietoturvan yleistä kehitystä ja uhkakuvia sekä seuraa kaupungin tietoturvatyötä. Ryhmä analysoi ja arvioi edellä mainittua kokonaisuutta ja tekee arvioinnin perusteella ehdotuksia tietoturvan parantamiseksi. Lisäksi ryhmä avustaa koko kaupungin hallintoa tietoturvaa koskevissa asioissa.

Toimialajohtajat vastaavat riskienhallinnasta ja valmiudesta sekä toimialojensa tietoturvasta ja tietosuojasta.

Kaupungin konserniyhtiöiden hallitukset ja toimitusjohtajat vastaavat organisaatioidensa tietoturvasta ja tietosuojasta.

Aluepäälliköt ja esimiehet vastaavat omien vastuualueidensa tietoturvasta. Heidän tärkeimmät tehtävänsä ovat huolehtia seuraavista asioista:

- työntekijät perehdytetään kaupungin tietoturva- ja tietosuojaohjeisiin sekä jokaiselle

työntekijälle kuuluvaan vastuuseen,

- työntekijän työsuhteen päättyessä tai henkilön siirtyessä muihin tehtäviin kaupungin tiedot ja muu omaisuus palautetaan ja asiasta tiedotetaan IT-henkilöstölle / Dynamo Netille valtuuksien poistamiseksi.

Henkilökunta vastaa ohjeiden noudattamisesta. Lisäksi jokaisen on välittömästi ilmoitettava havaitsemansa poikkeamat, uhat ja riskit tietoturvavastaavalle ja tietosuojavastaavalle tai esimiehelleen.

Tietojen ”omistaja” vastaa tietojen luokittelusta (julkisuus ja luottamuksellisuus) ja sen yksilönsuojan varmistamisesta ja tietojen luokittelun mukaisesta tallentamisesta.

Tietokoneohjelmiston ”omistaja” vastaa ohjelmiston häiriöiden ja niihin liittyvien tietojen riskienhallinnasta ja valmiudesta sekä tietoturvasta. Tietokoneohjelmiston omistaja tai tämän valtuuttama henkilö myöntää valtuudet työntekijän esimiehen tekemän hakemuksen perusteella.

Prosessin ”omistaja”vastaa riskienhallinnasta ja valmiudesta prosessin häiriöihin liittyen, sekä tietoturvasta. Hän vastaa myös prosessin riippuvuussuhteiden tunnistamisesta ja niiden kriittisyyden arvioimisesta.

IT-turvallisuudesta vastaava on vastuussa tietotekniikan tietoturvasta, sitä tukevien ohjeiden valmistelusta sekä It-turvallisuutta koskevien vaatimusten noudattamisesta. IT-turvallisuudesta vastaava valvoo kaupungin tietoturvaa raportoiden tehtävän hoitamisesta tietoturvavastaavalle ja tietosuojaryhmälle.

Tietosuojasta vastaava vastaa tietosuojasta, sitä tukevien ohjeiden valmistelusta sekä tietosuojaa koskevien vaatimusten ja lakien noudattamisesta. Tietosuojasta vastaava seuraa kaupungin tietosuojaa raportoiden tehtävän hoitamisesta tietoturvavastaavalle ja tietosuojaryhmälle.

Tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa koko organisaatiota ja konserniyhtiöitä tietosuojasäännösten noudattamisessa. Hän toimii myös asukkaiden, henkilökunnan ja tietosuojavaltuutetun toimiston yhteyshenkilönä henkilötietojen käsittelyä ja tietosuojaa koskevissa asioissa.

Tietosuojaryhmä koostuu tietosuoja-asioihin liittyvistä yhteyshenkilöistä. Ryhmä kokoontuu säännöllisesti ja aina tarvittaessa tietosuoja-asioiden käsittelemiseksi. Tietosuojaryhmän tehtävänä on varmistaa osoitusvelvollisuuden täyttyminen, valmistella tietosuojapolitiikka, koordinoida henkilöstön koulutus ja seurata tietosuojan toteutumista kokonaisuudessaan.

Asiakirjahallinto vastaa asiakirjahallinnosta ja siihen liittyvistä ohjeista. Sisäinen tarkastus vastaa tietoturvan asianmukaisuuden ja riittävyyden varmistamisesta sekä tarkastuksesta.

Henkilöstöhallinto vastaa henkilöstöprosessin tietoturvasta ja tietosuojasta.
Tämä vastuu sisältää:

- ohjeistuksen ja tuen henkilökunnalle
- tietoturvaan ja tietosuojaan liittyvän koulutuksen ja perehdyttämisen järjestämisen
- taustatietojen tarkistamisen tarvittaessa.

Kaupunginarkistolla on valvontavastuu tietojen käsittelemisestä kuntalain, hallintolain, arkistolain ja viranomaisten toiminnan julkisuutta koskevan lain määräämällä tavalla, sekä

kunnan sisäisten tietojen pitkäaikaista käsittelyä ja säilyttämistä koskevien ohjausasiakirjojen mukaisesti.

Rekisterinpitäjiä ovat kaupunginhallitus ja muut kaupungin lautakunnat.
Kyseiset tahot vastaavat henkilötietojen käsittelystä ja huolehtivat henkilötietojen asianmukaisesta käsittelyssä toiminnassa.

6. Tietoaineistojen luokittelu

Kaupungin tietovarat on luokiteltava luottamuksellisuutta, eheyttä, jäljitettävyyttä ja saatavuutta koskevien vaatimusten perusteella. Siten kullekin tietovaralle voidaan asettaa sopivat suojaus-vaatimukset. Erityisen tärkeiksi katsotuille tietovaroille on tehtävä riskianalyysit ja vaikutusten arvioinnit.

Tietoluokituksessa toiminnan kannalta kriittisiksi havaituille toimintajärjestelmille on laadittava järjestelmän turvallisuussuunnitelma ja pidettävä se ajan tasalla. Niiden tietovarojen kohdalla, joilla on korkeat saatavuusvaatimukset, sisältyy myös jatkuvuussuunnitelma.

7. Työn periaatteet

Närpiön kaupungin on tietoturva-asioissa työskenneltävä siten, että edellä mainitut tavoitteet saavutetaan. Tietoturvatyön on luotava normit, tuettava ja valvottava kaupungin toimintaa. Työssä on tärkeää pystyä tunnistamaan Närpiön kaupungin tietovaroja koskevat uhat, haavoittuvuudet ja riskit ja pystyä luomaan ja ottamaan käyttöön turvallisuustoimenpiteitä, jotka vähentävät kyseiset riskit hyväksyttävälle tasolle.

Närpiön kaupungin tietoturvaa koskevan työn on:

- bpohjauduttava kokonaiskuvaan, joka perustuu tietoon, mutta sisältää myös prosessit, ihmiset ja tekniikan,
- oltava jatkuvan tarkastelun ja parantelun alaisena, koska Närpiön kaupunki ympäristöineen, uhkakuvat mukaan lukien, on jatkuvassa muutoksessa,
- oltava ennaltaehkäisevää ja ennakoivaa, mutta myös kyettävä käsittelemään tapahtumia, vakavia häiriöitä ja kriisejä, joita voi silti sattua,
- pohjauduttava Närpiön kaupungin arvoille ja otettava huomioon toiminnan tarpeet, ulkoiset vaatimukset ja vallitsevat uhkakuvat,
- oltava hyvin viestitty toiminnalle; koko henkilöstölle on saatava ajan tasalla olevaa tietoa ja koulutusta korkean turvallisuustietoisuuden saavuttamiseksi ja ylläpitämiseksi sekä tämän politiikan ja sen perustana olevien tietoturvaohjeiden noudattamiseksi,
- tapahduttava aktiivisessa yhteistyössä ympäröivän yhteiskunnan, kuten viranomaisten, yritysten ja verkostojen kanssa,
- tultava huomioiduksi tietojärjestelmien hankinnassa, kehittämisessä ja poistamisessa.

8. Uudistaminen, seuranta ja raportointi

Tietoturvapolitiikkaa uudistetaan tarvittaessa ja siitä vastaa kaupungin tietoturvaryhmä. Tietoturvapolitiikan ja tietoturvaohjeiden noudattamista on seurattava säännöllisesti.

IT-turvallisuudesta vastaavan on pyynnöstä ilmoitettava IT-turvallisuuden tilanne ja tila tietoturvasta vastaavalle ja tietoturvaryhmälle. Erityiset syyt, kuten vakavat vaaratilanteet, puutteet tai tarpeet on aina raportoitava.

Tietosuojasta vastaavan on pyynnöstä ilmoitettava tietosuojan tilasta ja tilasta tietoturvavastaavalle ja tietoturvaryhmälle. Erityiset syyt, kuten vakavat vaaratilanteet, puutteet tai tarpeet on aina raportoitava.