Sisällys

Yleisesti tietoturvasta ja tietosuojasta

Tietosuoja tarkoittaa sitä, että tietojen käsittelyssä suojataan yksityisyyttä tarkoituksenmukaisesti. Tietosuojalla viitataan esimerkiksi henkilötietojen tai muiden salassa pidettävien tietojen käsittelyyn siten, että niitä käsitellään laillisesti, luottamuksellisesti, asianmukaisesti ja huolellisesti sekä tarkoituksenmukaisesti. Tietosuojan tarkoituksena on turvata rekisteröidyn oikeuksien toteutuminen henkilötietojen käsittelyssä.

Tietoturvalla tarkoitetaan tietojen, tietojärjestelmien, palveluiden ja verkkoliikenteen suojaamista. Julkisessa toiminnassa tulee huomioida sekä tietoturva että tietosuoja.

Usein tietosuojan loukkaukset tapahtuvat vahingossa, esimerkiksi siten että salassa pidettävää tietoa sisältäviä keskusteluja käydään huolimattomasti ja sivullinen henkilö kuulee keskustelun. Tietosuojan ja tietoturvan suhteen onkin pyrittävä huolellisuuteen. Tietokonetta käytettäessä on huomioitava tietosuoja siten, etteivät sivulliset näe näyttöruudulta mahdollisia luottamuksellisia tietoja. Tietokoneen sijoittelun lisäksi tietosuojaa voidaan parantaa erillisellä tietoturvasuojalla, joka estää näkemästä näytön sisältöä sivusta katsottaessa.

Kaikki kunnan palveluksessa olevat henkilöt ovat velvollisia edistämään tietoturvaa ja tietosuojaa:

- noudattamalla tietojen käsittelystä annettuja ohjeita
- estämällä luottamuksellisen tiedon päätymisen sivullisille
- estämällä tiedon tai tietojärjestelmien luvattoman käytön
- estämällä tiedon tahallisen tai tahattoman tuhoutumisen tai vääristymisen
- varautumalla riskeihin ja vähentämällä tietoturva- ja tietosuojariskejä

Fyysinen tietoturva ja tietosuoja

Poistuttaessa huoneesta tai muuten jätettäessä työasema kirjauduttava työasemalta ulos ja näin varmistuttava, ettei työasemalle pääse ulkopuolista henkilöä. Lukitse työasema painamalla Ctrl+Alt+Del – yhdistelmää ja valitse Lukitse.

Työaseman käyttö

• Kirjaudu työasemallesi sekä käytössäsi olevaan järjestelmään aina omalla käyttäjätunnuksellasi.
• Vältä tallentamista työaseman kiintolevylle tai muistitikulle. Tallenna tiedot verkkopalvelimen levylle (esim. U-levy).
• Pilvitallennustilaa kuten Microsoft Teams, Onedrive tai Google Drive ei saa käyttää luottamuksellisen tiedon tallentamiseen.
• Nouda tulostamasi asiakirjat tulostimelta välittömästi ja huolehdi, etteivät ne joudu vääriin käsiin. (Pyri kuitenkin välttämään tulostamista.)
• Kirjaudu ulos järjestelmästä, kun lopetat sen käytön.
• Sammuta virta työasemasta, näytöstä ja tulostimesta työpäivän päätteeksi.

Toimitilat

• Noudata kulunvalvonnasta annettuja ohjeita.

• Älä säilytä työpöydällä salassa pidettävää aineistoa.
• Älä anna ulkopuolisen käyttää tietokonettasi äläkä jätä ulkopuolista yksin tai valvomatta työhuoneeseesi.
• Asiakaspalvelupisteessä/ työhuoneessa oleva tietokoneen näyttö ei saa näkyä asiakkaalle.

Matkatyö ja mobiilikäyttö

• Säilytä kannettava tietokone, tabletti ja puhelin huolellisesti.
• Jos kannettava tietokone, tabletti tai puhelin häviää, ilmoita siitä heti esimiehellesi.
• Huolehdi, että käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat vain sinun käytössäsi ja tiedossasi. Huolehdi, ettei kukaan ulkopuolinen näe käsittelemiäsi tietoja.
• Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin.
• Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä.
• Käytä mobiililaitteesi suojakoodia estääksesi laitteen luvaton käyttö. Suojakoodin käyttöönotto-ohjeet löydät laitteen käyttöohjeista.

Käyttöoikeudet ja salasanat

Kunnan tietojärjestelmät suojataan salasanoilla ja käyttäjäkohtaisilla käyttöoikeuksilla. Kunnan käyttämien erillisohjelmien käyttäjätunnusten myöntämisestä tai käyttöoikeuksista päättää ohjelmasta vastaavan toimialajohtaja tai hänen valtuuttamansa henkilö. Sähköisten asiakirjojen suojaamisesta vastaa jokainen viranhaltija/työntekijä itse.

• Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, tai PIN-koodejasi toisen henkilön käyttöön.
• Älä käytä organisaation antamaa käyttäjätunnusta ja salasanaa muita palveluita käyttäessäsi.
• Vaihda salasanat säännöllisesti tai aina, jos epäilet niiden paljastuneen.
• Käytä riittävän vahvaa salasanaa sisältäen numeroita, isoja ja pieniä kirjaimia sekä erikoismerkkejä.

Vaitiolovelvollisuus

Julkisuuslain 23 §:ssä määrätään, ettei viranomaisen palveluksessa oleva tai luottamustehtävää hoitava saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, eikä muutakaan viranomaisessa toimiessaan tietoonsa saamaa seikkaa, josta lailla on säädetty vaitiolovelvollisuus. Vaitiolovelvollisuuden piiriin kuuluvaa tietoa ei saa paljastaa

senkään jälkeen, kun toiminta viranomaisessa tai tehtävän hoitaminen viranomaisen lukuun on päättynyt. Tämä lainkohta koskee myös harjoittelijoita ja määräaikaisessa työsuhteessa olevia.

Toiminta henkilöstö- ja luottamushenkilömuutoksissa

Esimiehen tehtävänä on ilmoittaa kunnan tietohallintoon sähköpostitunnusten lakkauttamisesta henkilön jäädessä pois kunnan palveluksesta. Sähköpostin haltijan on välitettävä tarpeelliset viestit niitä tarvitseville, jotta henkilöstömuutokset eivät vaaranna kunnan toiminnan jatkuvuutta.

Virka- tai työsuhteen päättyessä esimiehen ja palveluksesta poistuvan henkilön tulee varmistaa henkilön käytössä olleiden tiedostojen luotettava arkistointi. Palveluksesta poistuva henkilö huolehtii työpisteensä tyhjentämisestä ja tarpeettomien papereiden hävittämisestä. Esimies huolehtii siitä, että työntekijän käytössä ollut kunnan omaisuus palautuu kunnalle. Esimies huolehtii ja vastaa sähköisten laitteiden palautumisesta tietohallintoon, joka puhdistaa tiedot sisäisiltä ja ulkoisilta tallennusvälineiltä. Hallintojohtaja vastaa luottamushenkilöiden käytössä olleiden sähköisten laitteiden palautumisesta kunnan haltuun luottamushenkilöiden jäädessä pois luottamustoimestaan.

Sopimushallinta

Kunnanhallitus vastaa hallintosäännön mukaan sopimusten hallinnan järjestämisestä ja antaa tarkemmat ohjeet sopimusten hallinnasta. Lautakunnat puolestaan määräävät sopimusten vastuuhenkilöt omilla toimialoillaan.

Sopimusten hallinnassa on varmistuttava siitä, että sopimuksien teon ja hallinnan prosessi on selkeä ja kaikki osapuolet tietävät vastuunsa ja toimivaltansa prosessissa. Sopimuksia voivat allekirjoittaa vain henkilöt, joille on annettu siihen valtuudet ja sopimuksilla on oltava omistaja, joka vastaa sopimusten seurannasta.

Sähköposti

Jokaisella kunnan työntekijällä on oltava henkilökohtainen kunnan työsähköposti ja yksityisiä asioita varten jokaisella on oltava oma yksityinen sähköposti. Työnantajalla on oltava pääsy työntekijän

työsähköpostiin hätätapauksissa. Käyttämällä yksityisasioihin yksityistä sähköpostia, vahvistetaan myös yksityisyydensuojaa.

Lomalle tai virkavapaalle jäädessä on asetettava työsähköpostiin poissaoloviesti ja asetettava työpuhelimeen vastaajaviesti tai soitonsiirto.

- Älä anna työsähköpostiosoitettasi ulkopuolisille muissa kuin työhön liittyvissä yhteyksissä.
- Käy säännöllisesti katsomassa myös roskapostikansiota, siltä varalta, että sinne on joutunut tärkeitä sähköpostiviestejä.
- Suhtaudu varauksella epätavallisiin sähköposteja ja liitetiedostoihin. Älä avaa niitä. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta.
- Asiakkaan salassa pidettäviä asiakastietoja sisältäviä viestejä ei saa asiakkaan suostumuksellakaan lähettää suojaamattomassa sähköpostissa.
- Kalenterivarauksen Aihe- ja Sijainti-kohtiin ei pidä merkitä salassa pidettäviä tai arkaluonteisia tietoja.
- Mikäli saat sähköpostin, jonka asia kuuluu toiselle henkilölle, ohjaa viesti viivytyksettä oikealle vastaanottajalle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Sähköpostiviestit kuuluvat kirjesalaisuuden piiriin.

Käytä henkilötietoja välitettäessä erityistä suojattua sähköpostiyhteyttä. Suojatun sähköpostiyhteydenkäyttö opetetaan uudelle työntekijälle perehdytyksen yhteydessä.

Sähköpostin käytöstä

- Jos sähköpostiviestin otsikko näyttää epäilyttävältä, älä avaa viestiä.
- Suhtaudu varauksella viesteihin, jotka on kirjoitettu kielellä, jota lähettäjä ei yleensä käyttäisi. Tarvittaessa varmista viestin alkuperä sen lähettäjältä.
- Älä avaa epäilyttäviä sähköpostin liitetiedostoja.

Verkkoselaimen käyttö

• Työpaikalla verkkoselain on tarkoitettu työtehtävissä tarvittavaan tiedonhakuun.

Henkilötietojen kerääminen ja luovuttaminen

Henkilötietojen keräämisestä ja luovuttamisesta säädetään Euroopan unionin perusoikeuksien artiklassa 8, jonka mukaan jokaisella on oikeus henkilötietojen suojaan. Lisäksi henkilötietojen keräämisestä ja luovuttamisesta säädetään Euroopan Unionin Tietosuoja-asetuksen 5 artiklassa.

Rekisteröidyn oikeuksiin kuuluu se, että rekisterinpitäjän on informoitava rekisteröityä henkilötietojen käsittelystä. Henkilötietojen kerääminen vaatii aina perusteen. Peruste voi olla esimerkiksi laki, suostumus tai sopimus. Rekisteröidyllä on myös oikeus tutustua omiin tietoihinsa ja oikeus tarkastaa omat tiedot. Lisäksi hänellä on oikeus vaatia tietojen oikaisua, poistamista tai käsittelyn rajoittamista tai kieltää niiden käsittely.

Rekisterinpitäjän oikeus käsitellä henkilötietoja edellyttää, että henkilötietojen suojaa koskevat vaatimukset on otettu huomioon suunniteltaessa käsittelytoimia ja käsiteltäessä henkilötietoja. Periaatteet ovat lainmukaisuus, asianmukaisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointivaatimus, täsmällisyysvaatimus, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus. Rekisterinpitäjällä on osoitusvelvollisuus näiden periaatteiden noudattamisesta.

Sosiaalinen media

Jos sosiaalisen median palvelun käyttö on osa virallisia työtehtäviäsi, voit käyttää palvelussa kunnan sähköpostiosoitetta. Muussa tapauksessa sosiaalisen median palveluihin kannattaa ilmoittaa yksityinen sähköpostiosoite.
Käytä sosiaalisen median palveluissa ja muissa ulkoisissa palveluissa eri tunnusta ja salasanaa kuin kunnan omissa palveluissa.

- Tarkista käyttäjäprofiilisi yksityisyyden suojaan vaikuttavat asetukset ja päivitä ne tarvittaessa asianmukaisiksi.
- Älä laita palveluun liian henkilökohtaisia tietoja. Kunnioita myös muiden tietosuojaa: älä laita perheesi, ystävien tai muiden henkilöiden kuvia tai tietoja palveluun ilman heidän suostumustaan.

- Harkitse tarkoin, mitä itseesi, tuttaviisi tai työpaikkaasi liittyviä asioita käsittelet sosiaalisessa mediassa. Kerran sosiaaliseen mediaan vietyä tietoa voi olla mahdotonta saada poistettua kokonaan.
- Varo paljastamasta itsestäsi tai työyhteisöstäsi sellaisia seikkoja, joita ulkopuolinen taho voi hyödyntää kalastelu- tai huijausyrityksissä (tietosuojaloukkaus). Esimerkiksi tiedot poissaoloista tai liian tarkat henkilö-, yhteys- tai tehtävätiedot voivat olla tällaisia.

Mainitessasi työnantajasi esimerkiksi sosiaalisen median profiilissa olisi mediakäyttäytymisesi on oltava työnantajan edun mukaista.

Tietoturvaloukkaus & häiriöilmoitus

Tietoturvaloukkauksista tai muista häiriötilanteista tietosuojan suhteen on toimitettava kunnan tietosuojavastaavalle ilmoitus.

Tietoliikennehäiriöistä on toimitettava häiriöilmoitus tietoliikenneyhteyksien palveluntarjoajalle sekä kunnan ICT-asioista vastaavalle.

Tietosuojaselosteet

Tietosuojaseloste laaditaan kaikista henkilötietoja sisältävistä rekistereistä.
Yksittäisiä rekistereitä ylläpitävät käytännön vastuuhenkilöt vastaavat tietosuojaselosteiden tekemisestä ylläpitämistään henkilötietorekistereistä.

Tietoturva- ja tietosuojaohjeen käyttö osana perehdytystä

Lakien, määräysten ja ohjeiden rikkomisesta käyttöoikeudet voidaan tietojärjestelmiin peruuttaa. Rikkomuksista tiedotetaan aina esimiehille. Esimiehen vastuulla on käydä tämä tietoturvaohje läpi uuden työntekijän kanssa samalla, kun työntekijälle annetaan verkon käyttäjätunnus.