

Lapinlahden kunta

Henkilöstön tietoturvaohje

Johdanto

Vastuu tietoturvallisuudesta ja siihen liittyvästä osaamisesta kuuluu omalta osaltaan jokaiselle työntekijälle. Tätä tietoturvaohjetta tulee noudattaa koko kuntaorganisaatiossa. Osassa työyksiköitä on omia tarkempia ammattialakohtaisia ohjeita, joita noudatetaan rinnan tämän ohjeen kanssa. Osassa yksiköitä on toiminnan luonteesta johtuen tarve noudattaa tiukempaa ohjeistusta. Tässä ohjeessa on asetettu kuntaorganisaation minimitaso tietoturvassa, jota voidaan yksiköiden omissa ohjeissa tiukentaa. Oman toiminnan ohella tätä ohjetta tulee noudattaa kunnan toimeksiannosta tehtävässä työssä (esim. palvelutoimittajat). Ohjetta tulee noudattaa myös esim. harjoittelijoiden ja opiskelijoiden osalta.

Tiedottaminen ja koulutus

- Seuraa tietoturvallisuuteen liittyviä organisaatiosi tiedotteita, tutustu ohjeisiin ja osallistu tietoturvakoulutukseen.
- Noudata organisaatiosi tietoturvaohjeita.

Toimitilaturvallisuus

- Noudata organisaatiosi kulunvalvontaohjetta.
- Mikäli epäilet, että ulkopuolinen henkilö oleskelee kunnan tiloissa ilman asiallista syytä, tarkista henkilön kulkuoikeus kyseiseen tilaan ja huolehdi, että henkilö poistuu tarvittaessa tilasta.
- Älä jätä työvälineitä valvomatta neuvottelutiloihin.
- Älä jätä vieraita yksin neuvottelu- tai työtiloihin. Saata vieraat aulaan tai ulos kokouksen jälkeen.
- Asiakaspalvelupisteessä tai -tilanteessa päätelaitteen näyttö ei saa näkyä asioijalle.
- Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseen tai henkilökunnan tiloihin.
- Huolehdi, ettei neuvottelutiloissa ole esillä asiaan liittymätöntä materiaalia. Huolehdi neuvottelun päättyessä, ettei pöydille, tauluihin, roskakoreihin tai muualle jää käsiteltyjä salassa pidettäviä aineistoja tai muistiinpanoja.
- Säilytä tieto ja laitteet turvallisessa paikassa, tarpeen mukaan lukitussa kaapissa ja huoneessa.
- Älä jätä kannettavaa päätelaitetta ilman valvontaa. Huolehdi myös muistitikkujen, CD-/DVD-levyjen, paperitulosteiden ym. asianmukaisesta säilyttämisestä.
- Noudata "puhtaan pöydän" periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi. Huolehdi myös siitä, että toimitilan ulko-ovi lukittuu poistuessasi.
- Ohjaa vieraat tai "eksyneet" henkilöt oikeisiin paikkoihin, tarvittaessa saata henkilö aulaan tai ulos. Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä auki kulunvalvonnassa olevia tai ovia, jotka on muuten tarkoitettu pidettäväksi suljettuina.

Päätelaitteet

- Päätelaitetta (kannettava tietokone, pöytäkone, älypuhelin, tabletti jne.) käytetään yhä useammin maksu- ja tunnistautumisvälineenä. Suojele sitä kuten lompakkoasi.
- Älä anna ulkopuolisen henkilön, edes tutun, käyttää päätelaitettasi.

- Estä päätelaitteesi, esimerkiksi puhelimen, luvaton käyttö asettamalla siihen laitteen käyttöohjeen mukaiset automaattiset lukitukset.

Tietoaineistojen käsittely

- Merkitse salassa pidettäviin asiakirjoihin sen salassapidosta kertova tunniste. Laatiessasi salassa pidettävää asiakirjaa, vastaat sen luokittelusta ja luokittelun merkitsemisestä.
- Käsittele (mm. tallenna, siirrä, tulosta, lähetä, kopioi, kuljeta, säilytä, arkistoi, hävitä) salassa pidettäviä tietoja annettujen ohjeiden mukaan.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi henkilökirjaston tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Telekopiota (faxia) voi poikkeustapauksissa käyttää salassa pidettävän aineiston lähettämiseen. Varmistu tällöin, että vastaanottaja on paikalla.
- Salassa pidettävää tietoa voidaan tallentaa, siirtää ja arkistoida usealla eri tallennusvälineellä ja tavalla. Noudata tietoaineistojen ja tallennusvälineiden hävittämisessä annettuja ohjeita. Selvitä, missä sijaitsevat lähimmät salassa pidettävän materiaalin hävittämiseen tarkoitetut tietoturvalliset säiliöt tai tuhoajat.
- Noudata tulostamisessa ja tulosteiden noutamisessa huolellisuutta ja annettuja ohjeita, jotta tulosteet eivät joudu muiden tahojen luettaviksi.
- Ole erityisen varovainen työskennellessäsi julkisissa tiloissa ja huomioi, että joku voi nähdä syöttämiäsi tunnuksia tai muita tietoja huomaamattasi tai salakuunnella keskusteluitasi.
- Julkista tietoa voi välittää internetin kautta tavallisella salaamattomalla sähköpostilla. Salassa pidettävän tiedon välittämisessä internetin kautta on käytettävä turvasähköpostia.
- Älä anna ulkopuolisten nähdä tietokoneesi näyttöruutua, kun käsittelet salassa pidettävää tietoa, tai näppäimistöä, kun syötät käyttäjätunnuksia ja salasanoja. Pyri käyttämään päätelaitteissasi tietoturvakalvoa.

Tunnukset ja salasanat

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi tai salasanojasi toisen henkilön käyttöön. Älä edes tietohallintohenkilöstölle, koska he eivät tarvitse niitä työtehtäviensä hoitamiseen.
- Käytä eri salasanaa eri palveluissa – työkäyttöön liittyviä tunnuksia tai salasanoja ei saa koskaan käyttää vapaa-ajan palveluissa.
- Huolehdi salasanasi laadusta käyttämällä vain vahvoja salasanoja, jotka ovat mahdollisimman pitkiä. Vaihda salasanasi silloin kun sitä edellytetään tai kun epäilet sen paljastuneen. Vahvassa salasanassa on pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Se on helppo muistaa, mutta vaikea arvata.
- Älä kirjoita salasanoja muistiin tai säilytä sellaisessa paikassa, mistä ne ovat helposti löydettävissä.

Työvälineiden ja internetin käyttö

- Käytä työhösi liittyviä tietoaineistoja ja organisaatiosi antamia työvälineitä vain työtehtäviesi hoitamiseen.
- Kunnan internet yhteys on tarkoitettu työasioiden hoitamiseen. Omia yksityisasiaita voi hoitaa vain vähäisessä määrin (esim. pankin sivujen kautta tapahtuva laskujen maksaminen). Älä selaa sellaisia epäilyttäviä www-sivustoja, jotka eivät liity työtehtäviisi. Sivujen kautta saatetaan yrittää siirtää päätelaitteeseesi haitta- tai vakoiluohjelmia.

- Ole varovainen – valitse tarvittaessa ”Peruuta”, jos www-sivu ei vaikuta luotettavalta ja sivusto ehdottaa tai edellyttää tiedoston lataamista tietokoneellasi.
- Älä asenna ohjelmistoja tai tee niiden asetusmuutoksia, ellei se kuulu työtehtäviisi. Peruskäyttäjänä sinulla näitä oikeuksia ei tulisi olla. Jos huomaat, että sinulla on johonkin palveluun tai toimintoon liikaa oikeuksia, velvollisuutesi on pyytää niiden korjaamista.
- Salaamaton muistitikku soveltuu vain julkisen tiedon siirtämiseen. Salatulla muistitikulla voit siirtää salassa pidettäviä tietoaineistoja.
- Lahjaksi saatuja tai löydettyjä muistitikkuja ei saa liittää päätelaitteeseen.
- Huolehdi käytöstä poistetun muistitikun asianmukaisesta hävittämisestä.
- Tallenna laatimasi asiakirjat N tai K-asemalle, josta tiedot varmistetaan keskitetysti. Tietokoneen paikallista muistia (C asema) ei tule käyttää asiakirjojen tallennukseen.
- Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työnantajan päätelaitteisiin tai palvelimille.
- Jos käytät julkisia päätelaitteita tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies).
- Säilytä tieto ja laitteet turvallisessa paikassa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen. Kannettavia tietokoneita tai puhelimia ei saa jättää autoon näkyvälle paikalle, eikä niitä saa säilyttää autossa yön yli.
- Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulla ei myöskään ole mahdollisuutta poistaa näitä tietoja laitteelta.

Sosiaalinen media ja sähköposti

- Muista, että aina kun käytät oman työorganisaatiosi laitteita, verkkoa tai sähköpostia, esiinnyt tietoverkossa organisaatiosi edustajana.
- Huomioi, että palvelun ylläpitäjät pääsevät käsiksi kaikkeen palvelussa käsiteltävään tietoon, myös kahdenvälisiin keskusteluihin. Internetverkkoon päätynyttä tietoa voi olla mahdotonta poistaa jälkikäteen.
- Käsittele palveluissa vain sellaista tietoa, jonka käyttöön palvelu on hyväksytty (huomioi mikä tieto on julkista, mikä salassa pidettävää).
- Älä keskustele työasioista tai jaa työhön liittyviä kuvia muissa kuin työtehtäviin hyväksytyissä palveluissa tai järjestelmissä. Tämä koskee myös sosiaalisen median käyttöä.
- Käytä työ sähköpostia vain työtehtäviesi hoitamiseen. Käytä muuhun kuin työtehtävien hoitamiseen vapaa-ajan sähköpostiasi. Työnantajan sähköpostiosoitteen saa luovuttaa vain sellaiseen internetpalveluun rekisteröidyttyessä, jolla on selkeä yhteys työtehtäviin.
- Ole erityisen varovainen, jos saat vieraskielisen tai huonolla suomen kielellä kirjoitetun sähköpostiviestin, jonka mukana on liitetiedosto tai linkki ulkoiselle www-sivustolle, vaikka lähettäjä olisi hyvin tuntemasi henkilö, vaikka viestin asiasisältö vaikuttaa tai liitetiedoston nimi ja tyyppi vaikuttavat työtehtäviisi liittyviltä
- Pyydä tarvittaessa kunnan tietohallintoa tutkimaan saamasi epäilyttävä liitetiedosto ennen sen avaamista.
- Poista epäilyttävät sähköpostit, älä avaa niitä.
- Kunnan sähköpostijärjestelmä ei lähetä automaattisesti kuittausta viestin lähettäjälle. Huolehdi sähköisen asiakirjan vastaanottamisesta ilmoittamisesta.
- Työtehtävien keskeytymättömän hoitamisen vuoksi työntekijällä on velvollisuus käyttää sähköpostijärjestelmän automaattista vastaustoimintoa ilmoittaakseen poissaolostaan, sen kestosta ja siitä kuka hoitaa hänen tehtäviään poissaolon aikana.

- Jos saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Jos oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Jakelulista on henkilöluettelo (sähköpostiosoitteita), jonka jokainen vastaanottaja saa tietoonsa. Se voi olla henkilörekisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Voit käyttää sähköpostin piilokopioimintaa, jos haluat estää sähköpostin jakelussa olevien osoitteiden näkymisen vastaanottajille.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin, myös valmiita jakelulistoja käyttäessäsi. Vältä turhien sähköpostien lähettämistä jakelulistojen kautta.
- Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä käsittelyä edellyttävä virkapostisi työnantajan käyttöön.

Haastattelut, kyselyt, tutkimukset ja tietojen luovutus

- Ohjaa haastattelu- ja kyselypyynnöt asian vastuuhenkilölle ja toimi organisaation viestintäpolitiikan mukaisesti. Pyydä tarvittaessa apua esimieheltäsi.
- Varo antamasta viattomankin oloisten keskustelujen yhteydessä tietoa salassa pidettävistä tai yksityisyyden suojan piiriin kuuluvista tiedoista. Ole tarkka etenkin erilaisissa internetissä toimivissa sosiaalisen median palveluissa.
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista ja mahdollisesta korvattavuudesta sekä päättää luovutuksesta. Ellet tiedä oikeaa tahoja, ota yhteys esimiehesi.

Havaitsitko ongelman?

- Jos huomaat tietoturvaongelman, velvollisuutesi on tarttua asiaan ja ilmoittaa siitä välittömästi esimiehelle ellet itse pysty korjaamaan ongelmaa.
- Ilmoita tietoturvallisuuden liittyvistä ongelmista, uhkista tai suojauspuutteista organisaatiosi tietosuojavastaavalle tai esimiehellesi.