Kuntalain 54 §:n mukainen sopimus viranomaistehtävän hoitamisesta

1. OSAPUOLET

1.1. Ylivieskan kaupunki (”vastuukunta”)

Sopimusyhteyshenkilö: Sopimusyhteyshenkilö: Työllisyysaluejohtaja Mervi Mäkihonka, mervi.makihonka@ylivieska.fi, 044 429 4205

1.2. Nivalan kaupunki (”tuottajakunta”)

Sopimusyhteyshenkilö: Kaupunginjohtaja Päivi Karikumpu, paivi.karikumpu@nivala.fi, 040 344 7200

Jäljempänä erikseen ”Osapuoli” tai yhdessä ”Osapuolet”

Yhteyshenkilöiden tehtävänä on seurata ja valvoa tämän Sopimuksen toteutumista sekä tiedottaa siitä oman organisaationsa sisällä ja toiselle sopimusosapuolelle. Sopimusta koskevat tiedonannot ja yhteydenpito tapahtuvat pääsääntöisesti kirjallisesti joko postitse tai sähköpostitse.

2. SOPIMUKSEN TAUSTA JA TARKOITUS

Sopimuksen tausta

Sopimuksen osapuolet ovat osapuolina yhteistoiminta-alueessa, josta ne ovat sopineet kuntalain 52 §:n mukaisella sopimuksella kuntien yhteisestä toimielimestä. Osapuolet ovat muodostaneet yhteistoiminta-alueen eli työllisyysalueen työvoimapalveluiden järjestämisestä annetussa laissa säädettyjen työvoimapalveluiden järjestämiseksi yhteistoiminnassa. Ylivieska, Kalajoki, Nivala -työllisyysalueeseen kuuluvat Ylivieskan, Kalajoen ja Nivalan kaupungit sekä Sievin, Alavieskan ja Merijärven kunnat.

Kuntalain 51 §:n mukaisena vastuukuntana toimii Ylivieskan kaupunki. Osapuolten muodostama yhteinen toimielin toimii lain edellyttämänä työvoimaviranomaisena. Järjestämisvastuussa oleva vastuukunta vastaa kuntalain 8 §:n 2. momentin mukaisesti palvelujen ja muiden toimenpiteiden yhdenvertaisesta saatavuudesta, tarpeen, määrän ja laadun määrittelemisestä, tuottamistavasta, tuottamisen valvonnasta ja viranomaiselle kuuluvan toimivallan käyttämisestä.

Sen estämättä, mitä kuntalain 8 §:n 2. momentin 5 kohdassa säädetään, järjestämisvastuussa oleva kunta voi sopia laissa tarkoitetun työvoimaviranomaiselle kuuluvan toimivallan siirtämisestä kuntalain 54 §:n mukaisesti.

Sopimuksen tarkoitus

Tämän sopimuksen (jäljempänä ”Sopimus”) tarkoituksena on sopia työvoimaviranomaiselle (Vastuukunnalle) työvoimapalveluiden järjestämislain mukaan kuuluvan tehtävän antamisesta virkavastuulla työllisyysalueen osapuolena olevan Nivalan kaupungin (Tuottajakunnan) viranhaltijan hoidettavaksi.

3. **SOPIMUKSEN KOHDE**

Sopimuksen sisältö koskee työvoimaviranomaiselle laissa säädettyjä tehtäviä, joissa toimivaltaa voidaan siirtää viranhaltijalle.

Tällä sopimuksella Vastuukunta antaa työvoimapalveluiden järjestämislain mukaiset alla luetellut tehtävät hoidettavaksi Nivalan kaupungin **TE-asiantuntijan** virassa toimivalle viranhaltijalle.

Siirrettävät tehtävät ovat seuraavat:

1) **Työvoimapalveluiden järjestämisestä annetun lain (380/2023) lukujen 4, 5, 6, 10, 13, 14, 16 ja 17 mukaiset, sopimuksen liitteenä olevan (Liite 1) tehtävänkuvan kannalta tarpeelliset työnantaja-asiakkaita koskevat palveluprosessiin liittyvät tehtävät.**

Viranhaltija hoitaa tehtäväänsä siten kuin siitä on määrätty kulloinkin voimassa olevassa lainsäädännössä, asetuksissa ja toimintaa valvovien viranomaisten määräyksissä sekä tämän Sopimuksen liitteenä olevassa tarkemmassa Tehtäväkuvauksessa (liite 1).

4. VIRANHALTIJAN ASEMA

Tämän Sopimuksen mukaisia tehtäviä hoitaessaan palvelua tuottava viranhaltija toimii palvelun Tuottajakunnan työn johdon ja valvonnan alaisuudessa ja noudattaa sen antamia virkasuhteeseen liittyviä ohjeita ja sääntöjä. Selvyyden vuoksi todetaan, että Tuottajakunta vastaa myös tarvittavista sijaistusjärjestelyistä.

Muutoksenhaku viranhaltijan päätöksiin tapahtuu siten kuin haettaisiin muutosta Vastuukunnan päätökseen.

Otto-oikeus määräytyy Vastuukunnan hallintosäännön mukaan työvoimapalveluiden järjestämisvastuun alaisten päätösten osalta.

Vastuukunta antaa järjestämisvastuuseensa perustuen palvelun tuottamiseen liittyvää ohjeistusta kohdassa 5 sovitun mukaisesti.

5. TEHTÄVÄN HOIDON VALVONTA

Vastuukunta valvoo ja ohjaa viranhaltijan tehtävän toteuttamista. Valvonnalla varmistetaan, että siirrettyä tehtävää tuotetaan laadukkaasti, kustannustehokkaasti ja lainmukaisesti. Vastuukunnan valvonta- ja seurantaoikeus sekä Tuottajakunnan raportointivelvollisuus voi sisältää esimerkiksi seuraavia menettelyitä:

— Lisäselvitysten pyytäminen
— Säännöllisten raporttien toimittaminen [kuten asiakasmäärät ja käsittelyajat]
— Seurantapalaverit
— Laadun toteutumisen arviointimenettelyt ja mittaukset.

Tämän sopimuksen tavoitteiden ja tehtävän hoidon seurantaa toteutetaan puolivuosittain tehtävällä raportoinnilla ja katselmoinnilla osapuolten yhteistoimintaa johtavassa työllisyyslautakunnassa. Seurantakatselmoinnissa tulee käydä läpi ainakin seuraavat asiakokonaisuudet:

— Menettelytavat asiakasohjauksessa
— Tehtävän hoitamiseen liittyvä laadun arviointi
— Keskeiset raportoitavat luvut, kuten asiakasmäärät ja käsittelyajat
— Valvonnassa esille tulleet huomiot
— Mahdolliset viranhaltijan toimintaan tai päätöksentekoon kohdistuneet muutoksenhaut, reklamaatiot, muistutukset ja kantelut
— Talousarvion seuranta
— Muut ajankohtaiset asiat

Mikäli siirrettyä tehtävää ei hoideta tämän Sopimuksen ja sen tavoitteiden mukaisesti, voi Vastuukunta irtisanoa sopimuksen päättymään tämän Sopimuksen kohdan 10 mukaisesti.

6. KUSTANNUSTEN JAKO

Työllisyysalueen talouden ohjauksesta ja kustannustenjaosta on sovittu osapuolten välisessä kuntalain 52 §:n mukaisessa sopimuksessa yhteisestä toimielimestä.

Tässä sopimuksessa tarkoitettujen tehtävien hoitamista koskevien kustannusten laskutusperusteena käytetään Tuottajakunnan tarvitsemaa työmäärää 5 päivää/viikko. Vastuukunnan kustannus on siten 3079,07 €/kuukausi lisättynä sivukuluilla ja mahdollisilla KVTES:n mukaisilla lisillä, sisältäen työaikaa yleistyöajan mukaisesti 38h 15min/viikko. Hintoihin lisätään voimassa oleva arvonlisävero.

Tuottajakunta laskuttaa vastuukuntaa kuukausittain.

Palvelun hintaa tarkastetaan kalenterivuosittain kunta-alan virkaehtosopimuksen (KVTES) mahdollisten yleiskorotusten mukaisesti.

Muiden mahdollisten kustannusten osalta sovelletaan, mitä osapuolten välisessä sopimuksessa yhteisestä toimielimestä on sovittu.

7. VAHINGONKORVAUS

Viranhaltijan viranomaistehtävää hoitaessaan aiheuttamasta vahingosta vastaa Tuottajakunta tai viranhaltija isännänvastuuta ja henkilökohtaista vastuuta koskevien vahingonkorvauslain (412/1974) säännösten mukaisesti. Myös mahdollinen takautumisvastuu suhteessa viranhaltijaan määräytyy vahingonkorvauslain perusteella.

Vahingonkorvausta koskevien kustannusten jakoon sovelletaan, mitä Osapuolet ovat sopineet yhteistä toimielintä koskevan sopimuksen kohdassa 13.

8. SALASSAPITO JA HENKILÖTIETOJEN KÄSITTELY

EU:n yleisessä tietosuoja-asetuksessa tarkoitettuna rekisterinpitäjänä toimii Vastuukunta. Tuottajakunnan viranhaltija käsittelee henkilötietoja Järjestäjäkunnan lukuun. Tuottajakunnan tulee noudattaa voimassa olevaa tietosuojalainsäädännön edellyttämää hyvää tietojenkäsittelytapaa ja henkilötietojen suojaamista koskevia säännöksiä sekä tämän

Sopimuksen liitteitä 2 A ja B (A) Ylivieskan kaupungin tietoturva- ja tietosuojapolitiikka 2023–2027 ja (B) Tietoturvaohje henkilöstölle, sekä rekisterinpitäjän antamia ohjeita ottaen erityisesti huomioon, mitä on säädetty sisäänrakennetusta ja oletusarvoisesta tietosuojasta.

9. ARKISTOINTI

Osapuolet vastaavat omalta osaltaan käytössään olevan ohjeistuksen mukaan toiminnassa kertyvien asiakirjojen ja tiedostojen arkistoinnista, salassapidosta ja tietojen annosta.

10. SOPIMUKSEN VOIMASSAOLO JA PÄÄTTÄMINEN

Tämä Sopimus tulee voimaan 1.1.2025. Sopimus on voimassa toistaiseksi.

Osapuoli voi irtisanoa Sopimuksen kuuden (6) kuukauden irtisanomisaikaa noudattaen. Irtisanominen on tehtävä kirjallisesti. Kirjalliseksi irtisanomisilmoitukseksi katsotaan myös sähköisessä muodossa (esim. sähköposti) tehdyn ilmoitukset. Irtisanomisaika lasketaan alkavaksi kirjallisen irtisanomisilmoituksen lähettämistä seuraavan kalenterikuukauden alusta.

Vastuukunnalla on järjestämisvastuu työvoimapalveluista. Vastuukunnalla on oikeus irtisanoa Sopimus päättymään välittömästi, mikäli Tuottajakunta ei pysty hoitamaan tehtävää lainkaan tai Vastuukunta muutoin perustellusti katsoo, että Tuottajakunnan toiminnan vuoksi työvoimapalvelujen yhdenvertainen saatavuus tai laatu olennaisesti vaarantuu, ja jos Tuottajakunta ei ole kohtuullisessa ajassa kirjallisen päättämisuhan sisältävän huomautuksen saatuaan ryhtynyt riittäviin toimenpiteisiin tilanteen korjaamiseksi.

Selvyyden vuoksi todetaan, että tämän Sopimuksen irtisanominen tarkoittaa, että siirretty toimivalta palautuu Vastuukunnalle. Osapuolet huolehtivat tarvittavat muutokset hallintosääntöön.

11. SOPIMUKSEN MUUTTAMINEN

Kaikki muutokset tähän Sopimukseen on tehtävä molempien Osapuolien allekirjoittamalla kirjallisella sopimusmuutoksella. Sopimusmuutokset tulee käsitellä ja hyväksyä osapuolen toimivaltaisessa toimielimessä.

12. ERIMIELISYYKSIEN RATKAISEMINEN

Mikäli Osapuolten välille syntyy erimielisyyksiä tämän sopimuksen soveltamisesta, pyrkivät osapuolet ratkaisemaan erimielisyydet ensisijaisesti keskinäisin neuvotteluin. Mikäli neuvottelut eivät johda sovintoon, riita sopimusvelvoitteista ratkaistaan hallintoriita-asiana lain mukaan toimivaltaisessa hallinto-oikeudessa.

13. MUUT TARVITTAVAT EHDOT

Ei ole.

14. SOPIMUSASIAKIRJAT JA NIIDEN PÄTEVYYS

Sopimus muodostuu tästä sopimuksesta ja sen seuraavista liitteistä:

Liite 1 Tehtävänkuvaus

Liite 2 A Ylivieskan kaupungin tietoturva- ja tietosuojapolitiikka 2023–2027
B Tietoturvaohje henkilöstölle

Sopimus ja sen liitteet muodostavat sopimusasiakirjat ja ne täydentävät toisiaan. Jos sopimusasiakirjat ovat keskenään ristiriidassa, noudatetaan yllä kuvattua pätevyysjärjestystä, kuitenkin niin, että henkilötietojen käsittelyyn liittyvissä kysymyksissä noudatetaan aina ensisijaisesti sitä koskevaa liitettä (Liite 2).

15. ALLEKIRJOITUKSET JA PÄIVÄYS

Tämä sopimus on allekirjoitettu sähköisesti, osapuolilla on oikeus ottaa sopimuksesta tarpeelliseksi katsomansa määrä kopioita.

Mervi Mäkihonka, työllisyysaluejohtaja
Ylivieskan kaupunki

Päivi Karikumpu, kaupunginjohtaja
Nivalan kaupunki

TE-asiantuntija, työnantajapalvelut

Yritysasiantuntijan tehtäviin kuuluvat aktiivinen yhteydenpito alueen työnantajiin, työmahdollisuuksien ja työkokeilumahdollisuuksien kartoittaminen ja työnantajien palvelu- ja koulutustarpeiden selvittäminen yhdessä kuntien elinkeinopalveluiden ja muiden sidosryhmien kanssa. Tehtävänä on tuottaa tietoa työllisyysalueelle työvoima- ja osaamistarpeista säännöllisesti. Asiantuntija ohjaa ja neuvoo alueen työnantajia työllistämiseen ja yrittäjyyteen liittyvissä asioissa yhdessä kuntien yritysasiantuntijoiden kanssa.

Asiantuntijan tehtäviin kuuluvat avoimia työpaikkoja koskevien tietojen julkaiseminen ja välittäminen työllisyysalueen te-asiantuntijoille, avoimeen työpaikkaan sopivien työnhakijoiden etsiminen ja esittely, työnhakijalle sopivien työpaikkojen tarjoaminen ja rekrytointitilaisuuksien ja kampanjoiden järjestäminen yhdessä kuntien elinkeinopalveluiden ja yhteistyöverkostojen kanssa.

Asiantuntija toimii myös alueellisen työnantajapalveluiden verkoston kehittämisessä ja toiminnan suunnittelussa yhdessä kuntien elinkeinopalvelujen ja yhteistyöverkoston kanssa. Tehtäviin kuuluvat myös muutosturvan viranomaistehtävät sekä äkillisten rakennemuutosten viranomaistyö yhdessä alueellisten ja paikallisten toimijoiden kanssa.

Asiantuntija osallistuu valmennuspalveluiden kehittämiseen ja toteuttamiseen työllisyysalueen työnhakija- ja työnantaja-asiakkaille. Asiantuntijan tehtäviin kuuluvat myös muiden asiakaskohderyhmien palvelu tarpeen mukaan sekä muita mahdollisia työllisyysalueen tehtäviä.

YLIVIESKAN KAUPUNGIN TIETOTURVA- JA TIETOSUOJAPOLITIIKKA 2023–2027

Kaupunginhallitus 22.1.2024 § 18

YLIVIESKA
kasvun ihmeitä

YLIVIESKA

Sisällys

Ylivieskan kaupungin tietoturva- ja tietosuojapolitiikka

Johdanto

Tämä tietoturva- ja tietosuojapolitikkaa kuvaa ne Ylivieskan kaupungin tietoturvallisuuden ja tietosuojan tavoitteet, vastuut ja toteuttamiskeinot, jotka Ylivieskan kaupungin johto on hyväksynyt. Johto sitoutuu noudattamaan tietoturvaan ja tietosuojaan liittyvää lainsäädäntöä ja uusimpia viranomaisvaatimuksia. Ylivieskan kaupunki ottaa tietoturvan huomioon kaikessa toiminnassaan ja edellyttää samaa myös henkilökunnaltaan ja sidosryhmiltään.

Tietoturvan ensisijainen tarkoitus on varmistaa tietojen asianmukainen ja luotettava käsittely organisaatiossa. Päivittäisessä työssä tämä tarkoittaa pääasiassa sitä, että tietoja voivat käyttää ainoastaan niitä virka- ja työtehtävissään tarvitsevat henkilöt. Järjestelmähankintoja ja käyttöönottoja suunniteltaessa otetaan huomioon järjestelmille asetettavat käytettävyys-, tietosuoja- ja tietoturvavaatimukset kaupungin hankintaohjeen ja -prosessien mukaisesti.

Tämä tietoturva- ja tietosuojapolitiikka on julkinen asiakirja. Johto sitoutuu parantamaan tietoturvaa ja tietosuojaa jatkuvasti ja asettaa vuosittain tietoturvan ja tietosuojan kehittämistavoitteet. Mahdolliset tietoturva- ja tietosuojapolitiikkaan liittyvät huomautukset ja kehittämiskohteet pyydetään toimittamaan tietoturvapäällikölle ja tietosuojavastaavalle.

1. Tietoturva- ja tietosuojapolitiikan tavoitteet

1.1. Tietoturvallisuuden käsite ja merkitys

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä tunnistettavuudesta eli pääsynvalvonnasta sekä kiistämättömyydestä. Tietoturvatoimet koskevat tiedon käsittelyä, kuten tallennusta, luovutusta ja siirtoa.

Tietoturvatoimilla suojataan manuaaliset ja automaattiset tietojärjestelmät ja niiden toiminta ja sisältö. Päämääränä on turvata Ylivieskan kaupungin keskeytymätön ja luotettava toiminta. Tietoturvan osalta tätä päämäärää tavoitellaan siten, että estetään tietojen ja tietojärjestelmien valtuudeton käyttö sekä tiedon tahaton tai tahallinen tuhoaminen ja vääristyminen. Ylivieskan kaupungin kriittiset tiedot, tietojenkäsittelyjärjestelmät ja palvelut pidetään asianmukaisesti suojattuna sekä normaali- että poikkeustilanteissa. Luettelo kriittisistä kohteista ja niiden suojauksista on salassa pidettävä. Uhka- ja poikkeustilanteisiin varaudutaan etukäteen riskianalyysillä ja toipumissuunnitelmalla, jotta mahdolliset vahingot saadaan minimoitua.

1.2. Tavoitteet

Tavoitteena on turvata tietojenkäsittelyn turvallisuus siten, että sekä Ylivieskan kaupungin henkilökunta että sidosryhmät voivat luottaa tietojenkäsittelyn asianmukaisuuteen ja että koko henkilökunta on sitoutunut huolehtimaan omalta osaltaan turvallisuudesta. Samalla turvataan ensisijaisen toiminnan mahdollisimman sujuva ja häiriötön toiminta.

Näiden päämäärien saavuttamiseksi:
Kaikkien tietoa käsittelevien henkilöiden on ymmärrettävä tietojenkäsittelyn periaatteet: mitä tietoa saa käsitellä, missä tarkoituksessa tietoa saa käsitellä ja milloin tietoa saa käsitellä.
Organisaation kaikkien työntekijöiden tietoturvatietoisuus on oltava

riittävä. Kaikki ymmärtävät oman merkityksensä sekä tehtävänsä ja velvollisuutensa tietoturvallisuuden ylläpidossa.

Tietoturvaa toteutetaan kaikilla tasoilla siten, että tietoturva on mukana kaikessa toiminnassa. Tällä toimintatavalla varmistetaan tietoturvallisen työkulttuurin toteutuminen.
Tietojen luottamuksellisuuden, eheyden ja saatavuuden vaatimus toteutuu kaikessa tietojenkäsittelyssä ja se mahdollistaa tietoturvallisen asioinnin ja tietojen käytön.

Tietoturvallisuuden vaatimukset otetaan huomioon kaikessa kehittämistoiminnassa sekä hankinnoissa. Tietoturvallinen toimintatapa on mukana jokapäiväisessä toiminnassa sekä toimintaprosesseissa ja tietojärjestelmissä niin, että helpoin ja luontevin tapa tehdä jokin asia on myös tietoturvallisuuden kannalta paras. Tietoturvallisuuteen sekä tietosuojaan liittyvissä kysymyksissä voi kääntyä tietosuoja- ja tietoturvavastaavien puoleen.

1.3. Tietosuoja

Tietosuojalla turvataan henkilötietojen käsittelyä. Se on perusoikeus, joka turvaa henkilön oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä.
Vaatimukset tietosuojan toteuttamiselle tulevat yleisestä EU:n tietosuoja-asetuksesta. Tietosuoja-asetuksen tavoitteena on turvata henkilötietojen käsittelyn läpinäkyvyys ja oikeasuhtaisuus sekä varmistaa rekisteröityjen oikeudet ja tietosuojan toteutuminen.
Kansallinen lainsäädäntö ja EU:n tietosuoja-asetus velvoittavat rekisterinpitäjän suunnittelemaan henkilötietojen käsittelyn ja osoittamaan käsittelyn lainmukaisuuden. Rekisterinpitäjän on suojattava rekisteröidyn tiedot asiattomalta käsittelyltä. Suojaustoimet on ulotettava kaikkeen tiedon käsittelyyn, siirtoon ja säilytykseen tallennusmuodosta

riippumatta.

Tietosuojan toteutumista seurataan aktiivisesti ja kaikkeen asiattomaan käyttöön puututaan. Jokaisen työntekijän on ilmoitettava esimiehelleen havaitsemistaan tietosuojaan liittyvistä ongelmista.

Tietojen oikeudettoman käytön seurauksena saattaa olla työnantajan antama huomautus, varoitus tai oikeudellisia seurauksia teon vakavuuden mukaan.

1.4. Henkilötietojen käsittely

Henkilötietoja käsittelevät Ylivieskan virkamiehet ja työntekijät, joiden virka- tai työtehtäviin ko. henkilötietojen käsittely kuuluu. Henkilötietoja voivat käsitellä myös esim. sopimuskumppanit tai järjestelmien ylläpitäjät, siinä laajuudessa kuin se on tarpeen käsittelyn tarkoituksen kannalta henkilötietojen käsittelyä koskevan sopimuksen perusteella. Käsittelytoimet suunnitellaan ja määritellään tiedon elinkaari huomioiden. Henkilötietojen käyttö on sallittua vain lainsäädännön nojalla tai henkilön suostumuksen perusteella. Tietojen säilytys ja käyttö tapahtuu tietoturvaperiaatteita noudattaen.

Henkilötietojen tulee säilyä virheettöminä ja niiden tulee olla saatavilla tarpeen mukaisesti. Henkilötietoihin pääsy on rajattu työtehtävän mukaiseksi. Mikäli henkilötietoja luovutetaan, tulee siirron olla tietoturvallinen ja perustua lakiin tai suostumukseen. Tietoja voidaan luovuttaa lakien ja asetusten nojalla tai rekisteröidyn suostumuksella.

2. Tietoturvan ja tietosuojan organisointi ja vastuut

Tietoturvan ja tietosuojan vastuiden ylätasot kuvataan tässä tietoturvapolitiikassa. Tarkemmat vastuiden kuvaukset ja sisällöt löytyvät "Tietoturvavastuut" dokumentista.

2.1. Organisaatio

Tietoturvallisuus on osa Ylivieskan kaupungin kokonaisturvallisuutta ja tietoturvan eri osa-alueille määritellään vastuuhenkilöt. Tietoturvallisuusorganisaation keskeisimmät toimijat ja roolit sekä heidän vastuunsa ja velvollisuutensa on kerrottu erillisessä Ylivieskan kaupungin tietoturvavastuu-dokumentissa.
Luettelon vastuuhenkilöistä voi pyytää kirjaamosta.

2.2. Johdon vastuut

Kaupungin johto on vastuussa tietoturvan linjauksista ja johtamisesta. Se määrittelee tietoturvan tavoitetason ja ne hyödyt, joita tieto-omaisuuden turvaavalla toiminnalla saavutetaan. Kaupunginhallitus nimeää ne vastuuhenkilöt, joiden tehtävänä on toteuttaa turvallisuusjohtamiseen liittyviä tehtäviä. Johto hyväksyy ulkopuoliset palvelutahot, mikäli tietoturvatyössä tarvitaan ulkoisia asiantuntijoita ja ammattilaisia.
Johto on vastuussa siitä, että kaikki kaupungin työntekijät ovat tietoisia kaupungin tietoturva- ja tietosuojapolitiikasta ja periaatteista. Johto on vastuussa myös siitä, että tietoturvavastuut ovat sidosryhmien tiedossa ja tietoturvaohjeita noudatetaan siten, että myös asiakkaiden ja yhteistyökumppaneiden tietoturva ei vaarannu. Johdon tehtävä on integroida tietoturvallisuus osaksi organisaation johtamisjärjestelmää siten, että tietoturva otetaan huomioon kaikessa toiminnassa.

2.3. Tietoturvaorganisaatio

Ylivieskan kaupungin tietoturvaorganisaatioon kuuluvat tietoturva- ja tietosuojaryhmä, tietoturvapäällikkö, tietosuojavastaava ja toimialojen

tietoturvavastaavat.

Tietoturvapäällikkö toimii tietoturva- ja tietosuojaryhmän puheenjohtajana ja ryhmä valitsee keskuudestaan sihteerin. Tietoturva- ja tietosuojaryhmä kokoontuu vähintään neljä kertaa vuodessa ja tarvittaessa useammin.
Tietoturva- ja tietosuojaryhmä vastaa kaupungin keskeisten toimintojen tietoturvan ja tietosuojan kehittämisestä, tietoturva- ja tietosuojatyön koordinoinnista ja toimenpiteistä tietoturva- ja tietosuojaloukkauksien osalta.

2.4. Työntekijöiden vastuut

Jokaisella kaupungin työntekijällä on vastuu toimia siten, että kaupungin tietoturva säilyy loukkaamattomana. Jokainen työntekijä on velvollinen raportoimaan havaituista poikkeamatilanteista esimiehelleen, joka vie asian eteenpäin tietoturvapäällikölle ja tietosuojavastaavalle. Myös työtehtävissä havaitut tietoturvallisuuteen liittyvät puutteet raportoidaan.

2.5. Organisaation yhteistyökumppaneiden vastuut

Sidosryhmät ja yhteistyökumppanit sitoutuvat omalta osaltaan turvalliseen tiedonkäsittelyyn asioidessaan Ylivieskan kaupungin kanssa. Tilaajaan velvollisuus on huolehtia, että kaikkiin tarjouspyyntöihin ja palvelusopimuksiin sisällytetään tietohallinnon ylläpitämät yleiset tietoturvavaatimukset täydennettynä kyseisen palvelun erityisvaatimuksilla sekä häiriötilanteiden toimintamallit ja selkeä vastuunjako läpi koko palveluketjun. Tietotekniikan käyttöohjeiden ja tietoturva- ja tietosuojapolitiikan noudattamisesta tehdään tarvittaessa kirjallinen sopimus.

3. Tietoturvallisuuden laajuus ja periaatteet

3.1. Tietoturvan perustason määrittely

Perustasolla häiriöitä voivat aiheuttaa mm. ihmisten huolimattomuus, tahallisen ilkivallan tekijät, järjestäytyneet rikolliset, laiteviat, onnettomuudet, valtiolliset toimijat tai luonnonmullistukset. Tietoturvaa hallitaan arvioimalla näiden riskien esiintymisen todennäköisyyttä ja tiheyttä ja valitsemalla sopivia menetelmiä, joilla tietoturvauhkia voidaan hallita.

Tietoturvasuunnitelmia pidetään yllä ja suunnitelmiin liittyviä käytäntöjä harjoitellaan, jotta niistä tulee osa organisaation toimintaa. Jatkuvuussuunnitelmia tulee kehittää ja toteuttaa käytännössä, jotta voidaan varmistua siitä, että toimintaprosessit saadaan palautettua toimintaan vaaditussa ajassa.

Ylivieskan kaupunki osallistuu tietoturvan perustason määrittämiseen kansallisilla ja alueellisilla yhteistyöalustoilla. Yhteistyöllä varmistamme tietoturvallisuuteen liittyvien hyvien käytänteiden käyttöönoton ja läpiviennin.

3.2. Tietoturvan periaatteet

Hallinnollista tietoturvaa toteutetaan luomalla periaatteet kaupungin tietoturvatyölle. Johto arvioi riskit ja luo puitteet tietoturvan hallinnan muiden osa-alueiden menettelytavoille. Hallinnollisen tietoturvan toimenpiteitä ovat resurssien nimeämiset, vastuiden jakamiset, salassapito- ja turvallisuussopimusten tekeminen. Tietoturvallinen ajattelutapa pyritään sisällyttämään kaupungin jokapäiväisiin toimiin.

Henkilöturvallisuus pyritään pitämään korkealla tasolla valitsemalla oikeat henkilöt työtehtäviin, perehdyttämällä ja kouluttamalla henkilöt

toimimaan oikein prosessien mukaan sekä noudattamalla sovittuja menettelyjä irtisanomistilanteissa. Näitä periaatteita sovelletaan sekä vakituisiin että tilapäisiin työntekijöihin.

Tietotekniikan käyttöympäristö laitteineen ja tiedonsiirtovälineineen suojataan fyysisin turvallisuustoimenpitein. Kiinteistöt, toimitilat, laitteet ja tietovarastot suojataan asiaankuulumattomilta henkilöiltä sekä erilaisilta vahingoilta ja onnettomuuksilta. Jotta toiminnan jatkuminen voidaan taata ajan kuluessa, riskien havaitsemiseen ja vähentämiseen tähtääviä toimenpiteitä kehitetään siten, että ne muodostuvat arkirutiineiksi.

Laitteistoturvallisuudessa otetaan huomioon laitteiden koko elinkaari, takuut, sopimukset ja tukipalvelut. Laitteistoturvallisuus taataan laitteiston suojauksella ja asianmukaisilla asennus-, ylläpito- ja poistotoimenpiteillä. Lisäksi laitteille määritellään omistaja ja laitteen turvaluokka sekä suunnitellaan laitteiden valvonta ja kapasiteetit.
Ohjelmistoturvallisuus taataan oikeanlaisilla ohjelmistoihin kohdistuvilla toimilla. Tähän kuuluvat ohjelmistojen päivitykset, pääsynvalvonta- ja lokimenettelyt sekä varmuuskopiot. Ohjelmistoja saa asentaa vain tietohallinnon luvalla. Tämä koskee erityisesti ilmaisohjelmia. Ohjelmistopäivitysten julkaisuja seurataan aktiivisesti ja päivitysten kriittisyys arvioidaan ennakolta, jos mahdollista. Kriittiset päivitykset asennetaan välittömästi viivytyksettä. Kriittisten komponenttien, palvelinten, työasemien, käyttöjärjestelmien sekä ohjelmistojen turvatoimet ja -päivitykset on kuvattu tietoturvasuunnitelmassa.

Tietoliikenneturvallisuus suojataan tarvittavilla toimenpiteillä siten, että tietojen siirto järjestelmästä toiseen on turvallista. Kriittiset viestit ja dokumentit välitetään luokitusten vaatimin salausmenettelyin. Viestinvälityksen tietosuojaa koskevat vaatimukset ja vastuut on määritelty

kaupungin ja viestinvälitysoperaattorin välisissä sopimuksissa.

Tietoaineistoturvallisuutta pidetään yllä luokittelemalla tietoja niiden kriittisyyden perusteella ja antamalla käsittelyoikeudet luokittelujen perusteella sekä valvomalla tiedonkäsittelyä. Käyttöturvallisuutta parannetaan luomalla ja ylläpitämällä turvalliset toimintaolosuhteet huolehtimalla käytön ja tekniikan toimivuuden valvonnasta, käyttöoikeuksista, sekä ohjelmistotuesta ja varmuus- ja suojakopioinnista sekä häiriöraportoinnista. Käyttöturvallisuus otetaan myös huomioon ylläpito-, huolto- ja kehittämistoimintoihin liittyvissä toimenpiteissä.

Tietoturvapoikkeamista, haitallisista ja toimintaa vaarantavista tapahtumista raportoidaan kaikilla tasoilla viivytyksettä poikkeamien hallintaprosessin mukaisesti.

Palveluja ulkoistettaessa huolehditaan Suomen ja EU:n lainsäädännön mukaisesta luottamuksellisen aineiston käsittelystä.

3.3. Tietoturvallisuuden toteutumista tukevia käytäntöjä

Ylivieskan kaupungin tietoturvallisuuden toteutumista varmistetaan käyttämällä seuraavia toimenpiteitä:

- Tietojen merkityksen arviointi
- kriittisen tiedon tunnistaminen
- Tiedon käytettävyys, eheys ja luottamuksellisuus
- Tiedon luokittelua ja käsittely
- luokittelutavat
- käsittelyohjeet
- Hallinnollisen tietoturvallisuuden käytäntöjen omaksuminen
- Käyttö- ja pääsyoikeuksien hallinta
- Turvallisuusselvitykset
- Turvallisuussopimukset

- Salassapitosopimukset
- Henkilöstön osaaminen (tietoturva- ja sovellusosaaminen)
- Tieto- ja yksityisyydensuojan noudattaminen
- Henkilötietojen käsittely
- Yksityisyydensuoja työelämässä
- Viestinnän suoja
- Teknisen tietoturvallisuuden toteuttaminen ja ylläpito
- Palomuurit yms. ratkaisut
- Haittaohjelmien torjunta
- Tiedonsiirron suojaaminen
- Päätelaitteiden suojaus
- Salaustekniikan hyödyntäminen
- Laitteisto- ja ohjelmistoturvallisuus
- Varmuuskopiointi ja muut varmistukset
- Käyttöturvallisuus (ohjeet ja tuki)
- Järjestelmien ja prosessien toiminnan jatkuvuuden varmistaminen
- Havainnointikyvyn kehittäminen
- Sieto- ja palautumiskyvyn kehittäminen
- Ympäristön fyysinen turvallisuus
- Jatkuva havainnointi, lokiseuranta Muutoksenhallinta
- Vaikutuksenarviointi
- Tiedonhallintamallin kehittäminen
- Varautuminen häiriöihin

4. Suojattavat kohteet ja niiden turvatoimien priorisointi

Suojattavat kohteet tunnistetaan ja tietoturvakriittisyys arvioidaan ja perustellaan. Kriittiset kohteet luetteloidaan ja priorisoidaan ja kohteille tehdään riski- ja vaikutustenarviointi kriittisyysjärjestyksessä. Riskien kontrollit arvioidaan ja valitaan toimintaympäristöön parhaiten soveltuvat tietoturvakontrollit. Tietoturvakontrollien toteuttamiseen osoitetaan vastuutahot.

Riskien hallinta ja tietoturvakontrollien käyttöönotto ja vastuut kuvataan riskienhallintasuunnitelmassa.

5. Tietoturvallisuuden hallintajärjestelmä

Ylivieskan kaupungin tietoturvan hallintaan liittyvä dokumentaatio säilytetään dokumenttien hallintajärjestelmässä ja tulostettu kopio arkistossa.

Tietoturvallisuuden toteuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten, fyysisten ja teknisten ratkaisujen avulla. Tietoturvallisuusmääritykset tarkistetaan ja arvioidaan vähintään vuosittain tai merkittävien muutosten yhteydessä. Tietoturvan hallintajärjestelmän ja kehittämissuunnitelman hyödyllisyys ja toimivuus käsitellään johdon katselmoinnissa ja johto päättää tarvittavista laajavaikutteisista muutoksista. Tietoturvallisuuskuvausten teknisestä ylläpidosta tietosuojan osalta vastaa tietosuojavastaava yhdessä tietoturvapäällikön johdon kanssa.

5.1. Tietoturvan kehittämisvisio

Ylivieskan kaupungilla on vuonna 2027 käytössä kokonaisvaltainen tietoturvan hallintajärjestelmä. Henkilöstö on tietoturvatietoista, motivoitunutta ja sitoutunutta yhteistoiminnassa asetettuihin tietoturvatavoitteisiin.

6. Tietoturvakoulutus ja -ohjeet

Ylivieskan kaupunki kouluttaa johtoa ja henkilökuntaa säännöllisesti tietoturvaan ja tietosuojaan liittyvissä asioissa. Henkilökunta osallistuu säännöllisesti verkkokoulutuksiin ja tarpeen mukaan luokkahuonekoulutuksiin sekä seminaareihin tai työpajoihin. Koulutukset kuvataan tarkemmin koulutussuunnitelmassa. Uusien työntekijöiden perehdytyskoulutuksiin sisältyy tietoturvakoulutus. Tietoturvakoulutuksien toteutumista seurataan. Mikäli tietojärjestelmiin tai organisaatiorakenteisiin tehdään merkittäviä uudistuksia

tai hankintaan uusia tietojärjestelmiä, arvioidaan tietoturvakoulutuksen tarve erikseen näissä tilanteissa.

7. Tietoturvallisuudesta tiedottaminen

Kaupungin johto tiedottaa ja ohjeistaa henkilökuntaa, mikäli organisaatiossa esiintyy tietoturvapoikkeamia. Johto varoittaa ja ohjeistaa henkilökuntaa myös varautumaan, mikäli tietyt tietoturvaloukkauksen lisääntyvät ajoittain.

8. Tietoturvallisuuden ja tietosuojan seuranta

Jokainen työntekijä on velvollinen ilmoittamaan havaitsemistaan tietoturvapuutteista. Toimialojen vastuuhenkilöiden tehtävänä on valvoa, että tietoturva toteutuu käytännössä ja ryhtyä toimiin, mikäli henkilökunta ilmoittaa tietoturvaan liittyvästä epäilystä tai epäkohdasta. Tietoturvaohjeistukseen liittyvien laiminlyöntien sattuessa seurauksena voi olla teon vakavuudesta ja tahallisuudesta johtuen huomautus tai kirjallinen varoitus, rikosilmoitus tai jopa palvelussuhteen purkaminen. Tietoturva- ja tietosuojarikkomuksista on yksityiskohtaisempaa tietoa kohdassa ”Tietojärjestelmien valvonta ja seuraamukset”.

Tietoturvavastuista tehdään laite- ja sovellustoimittajien sekä palveluntarjoajien kanssa erilliset sopimukset.

Tietoturvakäytännöille tehdään vertaisarviointeja saman toimialueen toimijoiden kanssa ja/tai niitä katselmoidaan erillisissä auditointitilaisuuksissa.

9. Poikkeamien hallintaprosessi

Poikkeamien käsittely on kuvattu jatkuvuus- ja toipumissuunnitelmassa. Kun havaitaan poikkeamaepäily, noudatetaan suunnitelman mukaisia toimia. Mikäli poikkeamaa ei ole riskikartoituksessa osattu ennakoida, toimitaan nopeasti tilanteen edellyttämällä tavalla vahinkojen minimoimiseksi. Jokainen poikkeamatilanteeseen osallistuva dokumentoi tilannetta vaihe

vaiheelta kirjaamalla päiväyksen, kelloajan ja tehtävän, jonka tehnyt poikkeamaepäilyyn liittyen. Tilanteen mentyä ohi, tietoturvan kokonaiskuva dokumentoidaan ja tallennetaan poikkeamien hallintaan.

Kaikki merkittävät haitalliset tapahtumat kirjataan tulevien kehittämistoimien perustaksi. Myös ns. ”läheltä piti” –tapaukset rekisteröidään. Onnettomuuksien, turvallisuusrikkomusten ja palvelujen keskeytysten seuraukset analysoidaan. Haitallisista tietoturvatapahtumista kerätään jatkuvasti ajan tasalla olevaa tilannekuvaa yhdyshenkilöverkoston ja teknisten valvontatietojen avulla. Tilannekuva havainnollistaa tietoturva-poikkeamatilanteen ja niiden aiheuttamat vaikutukset. Kerättyä dataa käytetään tulevissa arvioinneissa apuna tietoturvatoimien suunnittelussa ja priorisoinnissa.

Tietoturvaloukkauksesta ilmoitetaan tarpeen vaatiessa myös Traficomin Kyberturvallisuuskeskukseen nettilomakkeella. Tarvittaessa tietoturvarikoksesta tehdään rikosilmoitus poliisille. Tietosuojaan kohdistuvista loukkauksista tehdään ilmoitus tietosuojavaltuutetun toimistolle.

10. Tietojärjestelmien valvonta ja seuraamukset

Tietojen ja tietojärjestelmien käyttöä valvotaan olemassa olevien lakien ja asetusten mukaisesti huomioiden yksityisyyden suoja työelämässä. Tietojärjestelmien lokivalvontaa suoritetaan tietosuojavastaavan laatiman ja tietoturva- ja tietosuojaryhmän hyväksymän lokivalvontasuunnitelman mukaisesti.

Kaikki tietoturvarikkomukset käsitellään asianmukaisesti. Tietoturvarikkomusta lieventää merkittävästi, mikäli rikkomuksen tehnyt henkilö on välittömästi rikkomuksen huomattuaan ottanut yhteyttä esimieheensä sekä tietoturva- tai tietosuojavastaavaan, eikä käytä missään olosuhteissa väärin saamaansa tietoa. Tietoturvarikkomuksesta seuraa varoitus tai sen perusteella on mahdollista

päättää työ- tai virkasuhde. Tieto- turvarikkomuksesta voi seurata myös rikosoikeudellinen vastuu. Yksityiskohtaisempaa tietoa tieto-turva- ja tietosuojarikkomuksesta seuraamustaulukosta.

TAHALLISUUDEN ASTE RIKKOMUKSEN VAKAVUUS	**Tietämättömyys, osaamattomuus, erehdys, vahinko, huolimattomuus**	**Piittaamattomuus, tahallisuus, toistuvuus**	**Rikoksentekotarkoitus (vahingonteko, luvaton käyttö, vakoilu, salassapitorikos, aseman/väärinkäyttö hyötymistarkoitus)**
Vakava rikkomus **(lain mukaan rikkomuksena tai rikoksena tuomittava teko)**	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään	- tehdään rikosilmoitus - työnantaja käynnistää palvelussuhteen päättämismenettelyn	– tutkintapyyntö poliisille – työnantaja käynnistää palvelussuhteen päättämismenettelyn
Rikkomus **(vakava väärinkäyttö tai turvallisuuden rikkominen)**	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus	- kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään - työnantaja käynnistää palvelussuhteen päättämismenettelyn	- tutkintapyyntö poliisille - työnantaja käynnistää palvelussuhteen päättämismenettelyn
Lievä rikkomus **(asiaton toiminta tai väärinkäytös)**	- puheeksi ottaminen ja opastus - suullinen huomautus	- suullinen huomautus - kirjallinen varoitus - työnantaja käynnistää palvelussuhteen päättämismenettelyn	– tutkintapyyntöä poliisille harkitaan – kirjallinen varoitus – työnantaja käynnistää palvelussuhteen päättämismenettelyn

Toiminnan oikeellisuus on varmistettava ensisijaisesti lähiesimieheltä tai tietoturva- ja tietosuojavastaavilta.

Tietoturva- ja tietosuojarikkomusten seuraamustaulukko

- **Vakava rikkomus (lain mukaan rikkomuksena tai rikoksena tuomittava teko)**

- Salassa pidettävien tietojen oikeudeton käsittely ja luovuttaminen
- Tietojen luvaton käyttö (esim. tekijänoikeuden loukkaus tai rikoslain alaisen materiaalin oikeudeton käsittely ja hallussapito, kuten mm. rasistinen aineisto tai lapsiporno)
- Hakkerointi ja tunkeutuminen tietojärjestelmiin
- Vahingonteko (esim. haittaohjelmien tahallinen levittäminen tai palvelun tahallinen estäminen)
- Vakoilu
- Virka-aseman väärinkäyttö
- Hyötymistarkoitus

- **Rikkomus (vakava väärinkäyttö tai turvallisuuden rikkominen)**
  - Ohjeiden vastainen laitteistojen tai ohjelmien käyttö
  - Tunnuksen luovuttaminen (esim. salasanan kertominen toiselle käyttäjälle tai avoimen työaseman luovuttaminen niin, että toinen pääsee valvomatta käyttämään luovuttajan tunnusta)
  - Tiedon luottamuksellisuuden vaarantaminen (esim. työaseman jättäminen auki valvomatta)
  - Ylläpito-oikeuksien luvaton hallussapito
  - Ohjelmien ja pelien luvaton kopiointi

- **Lievä rikkomus (asiaton toiminta tai väärinkäytös)**
  - Henkilökohtaisen tietoturvan/tietosuojan laiminlyönti (esim. käyttäjätunnuksen huolimaton käyttö, salasanan jättäminen näkyviin, salassa pidettävien asiakirjojen jättäminen näkyviin)
  - Haitan aiheuttaminen (esim. laitteiden/ohjelmien lukitseminen ja toisten oikeutetun pääsyn estäminen)
  - Resurssien tuhlaus (esim. työajan väärinkäyttö, kuten asiaton surffailu internetissä)

- Luvaton kaupallinen tai poliittinen toiminta (esim. sähköpostin käyttäminen henkilökohtaiseen markkinointiin)
- Kulunvalvontaohjeiden rikkominen (esim. avainten luovuttaminen toisen käyttöön)

Tietoturvaohje henkilöstölle

1. Johdanto

Tietoturvallisuus perustuu lainsäädäntöön, normiohjaukseen sekä sopimuksiin. Vastuu tietoturvallisuudesta ja siihen liittyvästä osaamisesta kuuluu omalta osaltaan jokaiselle, myös sinulle. Turvallisuus ja tietoturvallisuus kokonaisturvallisuuden osana muodostuvat suurelta osin yksilöiden tekemistä valinnoista erilaisissa arkipäivän tilanteissa.

Tämä tietoturvaohje on tarkoitettu:

- koko henkilöstölle noudatettavaksi niin työvälineiden kuin palveluiden käytössä,
- Ylivieskan kaupungin toimeksiannosta työskenteleville (esim. tietotekniikkatoimittajamme ja muut palvelutoimittajat),
- Ylivieskan kaupungin tietojärjestelmiä tai toimitiloja säännönmukaisesti käyttäville henkilöille (esim. harjoittelijat, opiskelijat).

Ohjeeseen on koottu keskeisimmät tietoturvallisuuden perusasiat. Se antaa neuvoja tietoturvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tilanteissa.

Kun saat hyvän idean tietoturvallisuuden parantamisesta, tee siitä aloite Ylivieskan kaupungin tietoturvavastaavalle tai omalle esimiehellesi!

2. Toimitilaturvallisuus

Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja ICT-laitteita säilytetään turvallisissa tiloissa. Toimitilojen turvallisuus sisältää mm. kulunvalvonnan, teknisen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä lähettipalvelujen ja tietoaineistoja sisältävien lähetysten turvallisuuden.

- Asiakaspalvelupisteessä tai -tilanteessa päätelaitteen näyttö ei saa näkyä asioijalle.
- Noudata kulunvalvonnasta annettuja ohjeita.
- 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, kun tietoa ei tarvita työtehtävien suorittamisessa.
- Kuvaaminen organisaation tiloissa voi olla kiellettyä – noudata ohjeistusta. Valvo myös vieraidesi toimintaa ja esimerkiksi kameroiden käyttöä.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi. Huolehdi tarvittaessa 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 lukittuihin toimitiloihin esim. töistä lähtiessäsi.

- Älä jätä auki kulunvalvonnassa olevia ovia tai ovia, jotka on muuten tarkoitettu pidettäväksi suljettuina.

3. Päätelaitteet ja käyttöoikeudet

Päätelaitteella tarkoitetaan tässä ohjeessa työtehtävien hoitoon tarkoitettua elektronista laitetta, joka voi olla esimerkiksi puhelin, älypuhelin, kannettava-, tabletti-, pöytätietokone tai jokin vastaava laite. Käyttö sisältää sekä päätelaitteen että verkon kautta käytettävät palvelut.

3.1. Päätelaitteet

- Vastaat käyttäjänä omasta päätelaitteestasi. Ole siis huolellinen.
- Vain asennusoikeudet saanut henkilö saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää ohjelmia laitteisiin.
- Kirjaudu laitteelle aina omilla käyttöoikeuksillasi.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteestäsi.
- Jos työaseman kiintolevy tai muu tallennus- väline, kuten esimerkiksi muistitikku tai CD- /DVD-levy rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin.
- Siirrä tietokone virranhallintatilaan tai sammuta se työpäivän päättyessä, ellei muuta ole ohjeistettu työyksikössä tai esimerkiksi tietoturvapäivitysten johdosta.
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin, joita ovat mm. PIN- tai salasanakyselyt, laitteen automaattinen lukitus ja suojakoodikyselyt, tietoliikenneyhteyksien käyttäminen ja salaaminen.
- Huolehdi, että matkapuhelimessasi on päällä PIN- ja suojakoodikysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat oletuskoodit.
- Omien päätelaitteiden käyttö työtehtävissä ei ole sallittua.

Jos kadotat kannettavan päätelaitteen, tee välittömästi ilmoitus kadonneesta laitteesta Ylivieskan kaupungin tietohallintoon tai Joki ICT:lle, jotta sen väärinkäyttö voidaan estää sekä ilmoita esimiehellesi. Kannettavat päätelaitteet muodostavat suuremman riskin kuin perinteiset pöytäkoneet niin vahingossa tapahtuvan kadottamisen kuin varastamisen näkökulmasta. Huolehdi tämän takia laitteiden automaattisesta lukittumisesta.

3.2. Salasanat ja käyttäjätunnukset

Tietojärjestelmien käyttöön tarvitaan käyttöoikeus. Käyttöoikeus on henkilökohtainen ja se on yhdistetty sinun henkilöllisyyteesi ja työtehtävääsi. Käsittele käyttäjätunnusta ja salasanaa samalla tavalla kuin pankkikorttiasi ja tunnuslukuasi.

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, toimikorttiasi tai PIN-koodejasi toisen henkilön käyttöön – älä edes lomien aikana. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiin. Myöskään tietohallintohenkilöstö ei tarvitse tehtäviensä hoitamiseksi salasanaasi.
- Vaihda salasanasi riittävän usein ja heti, jos epäilet niiden paljastuneen.

- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä. Ohjeita salasanan laadintaan saat organisaation salasanaohjeesta.
- Älä kirjoita salasanoja muistiin tai säilytä sellaisessa paikassa, mistä ne ovat helposti löydettävissä.
- Älä käytä työnantajan antamaa käyttäjätunnusta ja salasanaa internetpalveluihin rekisteröityessäsi tai niitä käyttäessäsi.

4. Tietojen ja asiakirjojen käsittely

- Ole erityisen huolellinen salassa pidettävän tiedon, kuten henkilötietojen käsittelyssä.
- Muista, että voit käyttää ja käsitellä salassa pidettäviä tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi asiakasrekisterin tietojen käyttötarkoituksen vastainen käyttö on lain vastaista. Käyttötarkoitus on kuvattu rekisteriselosteessa. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Kun käsittelet salassa pidettävää tietoa, huolehdi, etteivät sivulliset näe tietoja asiakirjoistasi tai tietokoneesi näytöltä. Varo syöttämästä salasanojasi siten, että joku ”näkee” salasanan sormiesi liikkeistä.
- Varo antamasta viattomankin oloisten keskustelujen yhteydessä sivulliselle asiakastietoja tai muuta salassa pidettävää tietoa. Ole tarkka etenkin erilaisissa internetissä toimivissa sosiaalisen median palveluissa.
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista sekä päättää luovutuksesta. Ellet tiedä oikeaa tahoa, ota yhteys esimieheesi.
- Tarkista aina Ylivieskan kaupungin ulkopuolelta tuotu muistitikku, CD-/DVD-levy tai muu tietoväline haittaohjelmien torjuntaohjelmalla ennen käyttöä, ellei torjuntaohjelma suorita sitä automaattisesti.
- Varo toimisto-ohjelmilla (esim. tekstinkäsittely, esitysgrafiikka, taulukkolaskenta, PDF) tehtyjen tiedostojen piiloon jääviä tietoja (ns. meta-, jäännös- ja piilotiedot). Tiedosto voi sisältää siinä aiemmin ollutta tietoa tai muuta järjestelmässä olevaa tietoa, vaikka se ei näytöllä näkyisikään.
- Jos joudut lähettämään salassa pidettävää aineistoa sähköpostilla, käytä turvapostia. Ellei sinulla ole turvapostin käyttömahdollisuutta mutta koet, että työssäsi tarvitset sitä, ota yhteys esimieheesi, joka harkintansa mukaan tilaa sinulle tunnuksen. Varmistu vastaanottajan oikeudesta lukea aineistoa sekä sen perille menosta.
- Vältä tulostamista ja kopiointia. Käytä aina, mikäli mahdollista ”Turvatulostinta”. Ylimääräiset kopiot, väliversiot ja epäkelvot kappaleet (kustannus- ja ympäristövaikutusten ohella) lisäävät tiedon vääriin käsiin joutumisen vaaraa. Varmista, mihin tulostimeen tulostat ja missä tulostin sijaitsee. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen.
- Kun hävität salassa pidettäviä tietoja, käytä aina tietosuojajätesäiliöitä. Tietosuojajätesäiliön voi tarvittaessa tilata teknisestä huollosta. Noudata jäteohjeita!
- Selvitä itsellesi tietojen ja asiakirjojen käyttöä, luovutusta, käsittelyä ja

arkistointia koskevat säännöt ja rajoitukset.

5. Internetin ja sähköpostin käyttö

Internet ja viestintäratkaisut (sähköposti, kalenteri, pikaviestintä, sähköiset kokouspalvelut) ovat hyviä työvälineitä tiedon hakuun ja työskentelyyn ajasta ja paikasta riippumatta. On kuitenkin muistettava, että sähköpostissa tai internetissä ei itsessään ole mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa. Internetin ja viestintäratkaisuiden käyttö vaativatkin käyttäjältä huolellisuutta.

- Internet ja viestintäratkaisut ovat työpaikalla tarkoitettu työkäyttöön. Käytä henkilökohtaiseen viestintään yksityistä vapaa-ajan sähköpostia.
- Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työnantajan päätelaitteisiin tai palvelimille.
- Käytä vain sellaisia palveluita, jotka tiedät turvallisiksi ja joiden käytön Ylivieskan kaupunki on sallinut.
- Ohjelmien lataaminen internetin kautta ja asentaminen on kiellettyä. Jos tarvitset tiettyä ohjelmaa työtehtäviesi hoitamiseen, ota yhteyttä kaupungin tietohallintoon tai Joki ICT:lle.
- Työsähköpostia saa käsitellä vain kaupungin omistamilla laitteilla tai kaupungin etäkäyttöyhteyden kautta.
- Työhön liittyvä sähköposti vastaanotetaan ja ohjataan kaupungin sähköpostijärjestelmään. Sitä ei saa ohjata tai jatko lähettää automaattisesti kaupungin sähköpostijärjestelmän ulkopuolelle.
- Sähköinen kirjeenvaihto asiakkaan-/potilaan kanssa ei ole sallittua muutoin kuin turvapostin välityksellä. Tällöinkin viestittelyn tulee olla vain ”yleisluontoista”.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia. Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä. Tarvittaessa voit ilmoittaa asiasta kaupungin tietohallintoon tai Joki ICT:lle.
- Roskapostia voivat olla esim. sähköpostiin tilaamatta tulleet mainokset. Roskapostiin ei kannata vastata, vaan se pitää poistaa.
- Suhtaudu terveen epäluuloisesti sähköpostiviestin luotettavuuteen. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Varo ns. ”kalastelu-viestejä”, joissa sinua pyydetään syöttämään tunnuksia ja salasanoja aidontuntuisiin palveluihin. Vältä myös napauttamasta sähköpostiviesteissä olevia linkkejä, jos et tiedä minne kyseinen linkki johtaa tai jos viesti ei liity työtehtäviisi.
- Älä välitä ketjukirjeitä eteenpäin.
- 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 piilokopiotoimintoa, 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. Ennen kuin napautat Lähetä– painiketta, varmista että Vastaanottaja ja mahdollisissa Kopio sekä Piilokopio– kentissä olevat vastaanottajat ovat juuri ne henkilöt, joille tarkoituksesi on viesti lähettää.
- Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä käsittelyä edellyttävä työpostisi työnantajan käyttöön ja poista mahdolliset henkilökohtaiset viestit – noudata annettua ohjeistusta.
- Huomioi, että tietojärjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä, sähköpostiliikenteestä ja internet-selauksesta. Tietoja käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Väärinkäytöksiin voidaan puuttua.
- Olet vaitiolovelvollinen myös vahingossa saamistasi viesteistä tai kuulemistasi asioista.
- Ohjaa sähköisesti asioivat asiakkaat lähettämään käsittelyyn tulevat ja vireille saatetut asiat organisaation määrittelemään sähköpostiin, asiointipalveluun tai muuhun vastaavaan sähköiseen palveluun.

Muista, että aina kun käytät työnantajan laitteita, verkkoa tai sähköpostia, esiinnyt tietoverkossa työnantajan edustajana.

6. Etätyöskentely, liikkuva työ ja matkatyö

Etätyöllä tarkoitetaan muualla kuin organisaation vakituisessa toimipisteessä tehtävää työtä, jolloin käyttöympäristöt vaihtelevat eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Etätyöntekijän omilla toimenpiteillä ja menettelytavoilla on tällöin suuri merkitys. Etäyhteys on tietoliikenneyhteys organisaation sisäverkon ulkopuolelta ja etäkäyttö tietoteknisten palvelujen käyttöä etäyhteyden avulla. Etätyöntekijän on kyettävä tekemään itsenäiset arviot etätyöympäristön turvallisuudesta.

- Käytä etätyössä vain tietohallinnon hyväksymiä päätelaitteita.
- Kiinnitä kaikessa toiminnassasi huomiota tietoturvallisiin menettelytapoihin. Erityisen tärkeää tämä on silloin, kun toimit vakituisen työpisteen ulkopuolella. Etätyössä sinun tulee noudattaa soveltuvin osin kaikkia samoja turvallisuusperiaatteita kuin ollessasi Ylivieskan kaupungin varsinaisissa toimitiloissa.
- Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat ja pysyvät vain sinun käytössäsi.
- Huolehdi, että käyttämäsi käyttäjätunnukset, salasanat, toimikortit, PIN-koodit ja muut tunnistusvälineet ovat vain sinun hallussasi ja tiedossasi.
- Kuljeta mukanasi vain välttämätön määrä tietoaineistoa ja varmistu aina aineiston asianmukaisesta suojauksesta.
- Älä lataa tai asenna laitteisiin mitään työhön kuulumatonta.
- Käytä tietojen salausta silloin kun sitä edellytetään.

Matkoilla, julkisissa kulkuneuvoissa, nettikahviloissa…

- Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä ml. henkilötiedot.
- Säilytä tieto ja laitteet turvallisessa paikassa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen.
- Jos työskentelet julkisissa tiloissa, varmistu, etteivät muut henkilöt pysty kurkistamaan ja näkemään käsittelemiäsi tietoja ja asiakirjoja. Voit käyttää tarvittaessa näyttösuojaa.
- Älä käytä julkisia päätteitä (esim. nettikahvilat, kirjastot) työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulla ei myöskään ole mahdollisuutta poistaa näitä tietoja laitteelta.

Lisätietoa etätyön ja liikkuvan työn tietosuojasta ja tietoturvallisuudesta löydät erillisestä ohjeesta.

7. Sosiaalinen media

Sosiaalisen median palvelut sisältävät samanlaisia uhkia ja riskejä kuin muutkin perinteiset internetin kautta käytettävät palvelut, mutta erityisesti tietosuojaan, henkilön yksilöivään tietoon liittyvät asiat nousevat näissä palveluissa esille.

Somessa sisältö leviää ilman viivettä ja ennakkovalvontaa. Sosiaalinen media on ensisijaisesti tarkoitettu julkisten asioiden käsittelyyn ja keskusteluun. Älä siis jaa tai kerro siellä mitään sellaista, mitä et kertoisi sadan henkilön edessä auditoriossa. Kaikki someen laitettu materiaali on jollain tasolla julkista, myös täysin kahdenväliseksi tarkoitettu viestintä.

Työntekijä ei saa aiheuttaa vahinkoa työnantajalle, joten muistathan lojaliteetti- ja vaitiolovelvollisuuden. Jos mainitset sosiaalisen median palvelun henkilöprofiilissasi työnantajasi, esiinnyt tällöin Ylivieskan kaupungin epävirallisena edustajana. Ylivieskan kaupungin virallisena edustajana somessa voivat toimia johdon kanssa erikseen sovitut henkilöt.

Tarkista käyttäjäprofiilin yksityisyyden suojaa koskevat asetukset ja muuta niitä tarvittaessa siten, että tietosi eivät leviä laajemmalle kuin haluamallesi käyttäjäjoukolle. Älä hyväksy tuntemattomia yhteydenottoyrityksiä verkostoosi, äläkä napsauta vieraita, hämäräperäisiä linkkejä.

Jos epäilet, että olet joutunut kiusaamisen, huijauksen tai muun hyökkäyksen kohteeksi, älä epäröi pyytää apua kaupungin tietohallinnosta, työsuojeluvaltuutetuilta tai hallintopalveluista.

8. Tietoturvallisuuspoikkeamat

Sinulla on aina velvollisuus kertoa, jos sinulla on ongelmia tietoturvallisuusasioissa.

- Jos hallussasi oleva kulkuavain, muut avaimet tai henkilökortti katoaa tai varastetaan, ilmoita siitä välittömästi tekniseen huoltoon.

- Jos päätelaitteesi katoaa tai varastetaan, ilmoita siitä välittömästi kaupungin tietohallintoon tai Joki ICT:lle.
- Jos henkilökorttisi katoaa, ota välittömästi yhteys hallintopalveluihin.
- Ilmoita aina haittaohjelmista (esim. virushälytys päätelaitteella) ja muista tietoturvallisuuteen liittyvistä ongelmista **välittömästi** omalle esimiehellesi. Tämän velvollisuutena on saattaa asia tietoturvapäällikön ja tietosuojavastaavan tietoon.
- Ilmoita aina myös muista turvallisuuteen liittyvistä epäilyistä, suojauspuutteista tai ongelmista ja kehitysideoista turvallisuudesta vastaaville tai omalle esimiehellesi.

Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa:

- Älä hätiköi.
- Älä sulje päätelaitetta, mutta irrota lähiverkkokaapeli tai katkaise langaton (wlan/3/4/5G) yhteys työasemastasi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki tai ota siitä kuva kännykälläsi.
- Ota yhteyttä kaupungin tietohallintoon tai Joki ICT:lle. Auta tutkinnassa. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

Lakien, määräysten ja ohjeiden rikkomisen seurauksena käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehellesi. Vakavissa tapauksissa väärinkäyttö voi johtaa myös vahingonkorvausvaatimuksiin tai rikosoikeudellisiin seuraamuksiin. Seurauksena voi olla myös työsuhteen päättäminen.

9. Tietoturvallisuus osana toiminnan laatua

9.1 Mitä tietoturvallisuudella tarkoitetaan?

Tietoturvallisuus on osa organisaation toiminnan laatua. Tietoturvajärjestelyjen tarkoituksena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit otetaan huomioon. Käytännössä tämä merkitsee mm. sitä, että tiedot ja tietojärjestelmät pidetään vain niiden käyttöön oikeutettujen saatavilla. Sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja. Tietojen käsittelyyn oikeutetutkin saavat käyttää tietoja ja järjestelmiä vain asianmukaisesti työtehtävissään. Tietojen, järjestelmien ja palveluiden on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muiden vahinkojen, tapahtumien tai häiriötilanteiden vuoksi. Tietojen, järjestelmien ja palveluiden on myös pysyttävä toiminnassa ja oltava saatavilla silloin kun niitä tarvitaan. Etenkin sähköisissä asiointipalveluissa tarve käyttää palveluita ympärivuorokautisesti ja paikasta riippumatta on lisääntynyt, kun virkamiesten ja kansalaisten käyttötavat ovat muuttuneet. Palveluiden täytyy kyetä tunnistamaan käyttäjät luotettavasti sekä tuottamaan tarvittavaa lokia, josta tapahtumat voidaan tarvittaessa jälkikäteen selvittää.

9.2 Miksi tietoturvallisuus on tärkeää?

Tietoturvatoimenpiteillä turvataan yksilön, yhteisön ja yhteiskunnan etuja. Siksi tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys. Yhteiskunnan toiminnot ovat suurelta osin riippuvaisia tietojen käsittelystä ja siirrosta. Verkottuneessa

toimintaympäristössä harva organisaatio on enää vastuussa yksinomaan omasta tietoturvallisuudestaan. Tietoturvallisuudesta huolehtiminen on jokaisen organisaatiossa työskentelevän velvollisuus. Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen sekä muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki. Tämä ei koske vain tekniikkaa, vaan myös jokapäiväiset toimintatapamme ja asenteemme vaikuttavat – vahvin lenkki on oikealla tavalla toimiva yksilö! Puutteellinen tietoturvallisuus vaarantaa valtion, kansalaisten, yhteisöjen ja asiakkaiden etuja sekä aiheuttaa lisätyötä ja -kustannuksia. Tietoturvallisuutta kehittämällä parannetaan toimintojen luotettavuutta ja jatkuvuutta. Mitä paremmin häiriötilanteiden hallinta on otettu huomioon organisaation toiminnassa, sitä nopeammin toiminta saadaan palautettua vakiotasolle ja tiedotettua häiriöstä asiakkaille.

9.3 Lainsäädäntö tietoturvallisuuden perustana

Ylivieskan kaupungissa käsitellään runsaasti sekä julkista että salassa pidettävää tietoa. Julkisuuslainsäädännön mukaan tieto on julkista, ellei se julkisuuslain tai muiden säädösten perusteella ole erikseen määrätty salassa pidettäväksi. Suomen lainsäädännössä on paljon tietoturvavelvoitteita – toisin sanoen myös lainsäädäntö lähtee siitä, että tietoturvallisuus on hoidettava asianmukaisesti. Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain (621/1999) ja asetuksen (1030/1999) lisäksi useisiin muihin lakeihin. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. Tietojen lainmukaisesta käsittelystä on aina huolehdittava.

Joitakin keskeisiä laeissa asetettuja tietoturvavelvoitteita ovat:

- "Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti." (Laki julkisen hallinnon tiedonhallinnasta 906/2019, 13 §)
- ”Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä.” (Laki viranomaisten toiminnan julkisuudesta 621/1999, 18 §, Hyvä tiedonhallintatapa)
- ”Henkilötietojen suojaamiseksi rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asian mukaiset tekniset ja organisatoriset toimenpiteet.” (Tietosuoja-asetus 679/2016/EU, 24 artikla).
- ”Rekisterinpitäjän on määritellessään ja käyttäessään henkilötietoja otettava huomioon uusimmat tekniset mahdollisuudet rekisteröityjen oikeuksien suojaamisessa.” ja ”Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain tarkoituksen kannalta olennaisia tietoja” (Tietosuoja-asetus 679/2016/EU, 25 artikla, Käsittelyn turvallisuus artiklassa 32).

Tietoturvallisuuteen keskeisesti liittyvien säädösten luettelo on listattu luvussa 9.6.

9.4 Kyberturvallisuus keskittyy yhteiskunnan toimivuuden takaamiseen

Kansallista kyberturvallisuustyötä ohjaa lokakuussa 2019 julkaistu Suomen kyberturvallisuusstrategia. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa sähköisessä muodossa olevaan tiedonkäsittelyyn

tarkoitettuun, yhdestä tai useammasta tietojärjestelmästä koostuvaan, palveluun tai ICT-järjestelmään voidaan luottaa ja jossa sen toiminta turvataan. Tämä edellyttää myös sitä, että tiedonkäsittelyyn liittyvät fyysiset rakenteet suojataan tarkoituksenmukaisesti. Kyberturvallisuus keskittyy ensisijaisesti yhteiskunnan toimivuuden kannalta elintärkeiden toimintojen kokonaisvaltaiseen suojaamiseen (esimerkiksi sähkönjakelu, kriittisten tietoliikenneyhteyksien ylläpito), kun tietoturvallisuus keskittyy tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen. Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on hallita ennakoivasti ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia. Kyberuhkien toteutuminen voi aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle. Kyberturvallisuuteen liittyy myös sotilaallista tiedustelu- ja vaikuttamiskykyä, joka tarkoittaa kyberpuolustuksen kehittämistä osana muun sotilaallisen voimankäytön kehittämistä. Tästä päävastuu on puolustusvoimilla.

Siinä missä tietoturvallisuus keskittyy tietoaineistojen suojaamiseen, kyberturvallisuus kattaa kaiken infrastruktuurin tuottamisessa tarvittavat osa-alueet. Pääpaino kyberturvallisuuden puolella on tietoverkkojen kautta tulevien uhkakuvien pienentämisessä ja torjumisessa. Lisätietoa löydät esimerkiksi yhteiskunnan turvallisuusstrategiasta ja Suomen kyberturvallisuusstrategiasta.

9.5 Kohdistetut hyökkäykset

Kohdistettu hyökkäys on tiettyyn toimijaan tai toimijajoukkoon suunnattu tietoturvaloukkaus, joka huomioi kohteen erityispiirteet. Hyökkääjä valikoi kohteensa tämän hallussa olevien tietoaineistojen tai muiden vastaavien seikkojen perusteella. Hyökkäyksen motiivina voi olla esimerkiksi organisaation hallussa olevien arkaluontoisten tietojen varastaminen.

Kohteiden valikoimisen takia hyökkäyksestä voi aiheutua merkittäviä vahinkoja. Kohdistettu hyökkäys käynnistyy usein lähettämällä kohteelle räätälöity sähköpostiviesti. Sähköpostissa on haitallista koodia sisältävä liitetiedosto tai linkki haittaohjelmaa levittävälle verkkosivulle. Jos käyttäjä avaa liitetiedoton tai seuraa linkkiä, voi haittaohjelma saastuttaa avaamiseen käytetyn laitteen. Asennuttuaan laitteeseen haittaohjelma ottaa yhteyden hyökkääjän ylläpitämään komentopalvelimeen, jolla tämä voi ohjata haittaohjelmaa. Tämän jälkeen hyökkääjällä on käytännössä suora tietoliikenneyhteys hyökkäyksen kohteena olevaan laitteeseen. Hyökkääjä voi kerätä tietoja kohteen laitteelta ja mahdollisesti laajentaa hyökkäystä kohdeorganisaation sisäverkon muihin osiin. Joissain tapauksissa hyökkäyksiä on yritetty ulottaa julkisesta verkosta irrallisiin tietokoneisiin saastuttamalla tiedonsiirtoon käytettyjä USB-tikkuja.

Hyökkääjä pyrkii räätälöimään sähköpostiviestin sellaiseksi, että vastaanottaja pitää viestiä mahdollisimman luotettavana ja päivittäiseen toimintaan liittyvänä. Usein sähköpostin lähettäjätiedot on väärennetty siten, että viesti näyttäisi tulevan kohteen kollegalta tai muulta luotetulta taholta. Hyökkäyksissä voidaan myös hyödyntää luotetuilta tahoilta kaapattuja sähköpostitilejä. Hyökkääjä voi myös yrittää huijata vastaanottaja avaamaan liite lähettämällä ensin vaarattoman tiedoston liitteenä ja heti perään ”korjatun”, esim. haittaohjelmaa sisältävän PDF-tiedoston.

Miten kohdistetun hyökkäyksen voi välttää?

- ole erityisen varovainen, jos saat vieraskielisen 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

- kohdistettuja hyökkäyksiä tehdään myös suomen kielellä, joten ole huolellinen aina avatessasi organisaation ulkopuolelta saapuvia myös suomenkielisiä liitetiedostoja
- pyydä tarvittaessa organisaatiosi tietohallintoa tutkimaan saamasi epäilyttävä liitetiedosto ennen sen avaamista – noudata tässä organisaatiosi ohjeistusta

9.6 Tietoturvallisuuteen keskeisesti liittyvät säädökset

Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat:

- Suomen perustuslaki (731/1999) 2.luku 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki kunnan ja hyvinvointialueen viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004): Arkaluonteiset kansainväliset asiakirjat
- EU:n tietosuoja-asetus (679/2016/EU): Henkilötietojen käsittelyn periaatteet
- Turvallisuusselvityslaki (726/2014): Henkilöturvallisuusselvitys
- Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
- Laki sähköisen viestinnän palveluista (917/2014): Sähköisen viestinnän tietosuojarikkomus
- Rikoslaki (39/1889) 34.luku 9a §: Vaaran aiheuttaminen tietojenkäsittelylle
- Rikoslaki (39/1889) 38.luku 8 §: Tietomurto
- Rikoslaki (39/1889) 38.luku 9 §: Tietosuojarikos
- Vahingonkorvauslaki (412/1974)
- Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategiasta
- Uudistuvat säädöstekstit löytyvät ajantasaisina mm. Valtion säädöstietopankki –sivustolta (www.finlex.fi)

Lisää tietoa tietoturvasta:

- Lainsäädäntö – Valtion säädöstietopankki (finlex.fi)
- Tietosuojavaltuutetun toimiston ohjeet (tietosuoja.fi)
- Tietoyhteiskunnan kehittämiskeskuksen ohjeet (tieke.fi)
- Kyberturvallisuuskeskuksen materiaalit (kyberturvallisuuskeskus.fi)

Tietoturvan ja tietosuojan huoneentaulu

1. Noudata annettuja tietoturvaohjeita ja -käytäntöjä.
2. Lukitse tietokoneesi/ohjelmistot tai kirjaudu niistä ulos aina kun poistut sen läheisyydestä. Pyri käyttämään eri salasanaa eri järjestelmissä. Säilytä salasanat ja muut kirjautumisessa käytettävät tunnisteet, kuten toimikorttisi ja PIN-koodit huolellisesti.
3. Varo paljastamasta luottamuksellisia tietoja sivullisille työpaikalla tai sen ulkopuolella esim. sosiaalisessa mediassa.

4. Älä surffaa arveluttavilla nettisivuilla. Älä avaa outoja sähköpostiviestejä tai niiden liitteitä.
5. Huolehdi papereiden, muistitikkujen, CD-/DVD-levyjen, puhelinten, salasanojen, avainten, kulkunappien, toimikorttien ym. asianmukaisesta käsittelystä ja säilyttämisestä.
6. Hävitä tietosuojattava jäte asianmukaisesti.
7. Huolehdi erityisesti etätyössä kannettavan tietokoneen ja sen tietojen suojaamisesta. Hanki kannettavaan tietokoneeseen suojakalvo, joka estää sivulta tapahtuvan salakatselun.
8. Muista kunnioittaa asiakkaiden ja työkavereiden yksityisyyttä. Näin ylläpidät luottamusta.
9. Kerro esimiehellesi, mikäli havaitset tietoturva- tai tietosuojarikkomuksia.
10. Älä hätäänny, jos jotain poikkeavaa tapahtuu. Soita rohkeasti kaupungin tietohallintoon tai Joki ICT:lle.

SIGNATURES **ALLEKIRJOITUKSET** **UNDERSKRIFTER** **SIGNATURER** **UNDERSKRIFTER**

This documents contains 36 pages before this page
Tämä asiakirja sisältää 36 sivua ennen tätä sivua
Detta dokument innehåller 36 sidor före denna sida
Dokumentet inneholder 36 sider før denne siden
Dette dokument indeholder 36 sider før denne side

MERVI JOHANNA MÄKIHONKA
Company - Yritys - Företag - Selskap - Virksomhed: Ylivieskan kaupunki
cc264980-01d4-4d59-907c-194c9b2845c9 - 2025-01-08 16:25:42 UTC +02:00
BankID / MobileID - 830fcf30-c1d1-4185-93cd-c8ec0a9c1ef7 - FI
Authority to sign - Asemavaltuutus - Ställningsfullmakt - Autoritet til å signere - Myndighed til at underskrive

Päivi Eliisa Karikumpu
Company - Yritys - Företag - Selskap - Virksomhed: Nivalan kaupunki
cae0c69b-196e-44b1-94f0-a32b2e9cda45 - 2025-01-10 14:39:15 UTC +02:00
BankID / MobileID - ed3d4680-8e06-482e-bd35-4e97fef8bcaa - FI
Authority to sign - Asemavaltuutus - Ställningsfullmakt - Autoritet til å signere - Myndighed til at underskrive

authority to sign	asemavaltuutus	ställningsfullmakt	autoritet til å signere	myndighed til at underskrive
representative	nimenkirjoitusoikeus	firmateckningsrätt	representant	repræsentant
custodial	huoltaja/edunvalvoja	förvaltare	foresatte/verge	frihedsberøvende