SIVUKADUN AVOPALVELU OY

Yrityksen Tietoturvasäännöt ja ohjeistus

Sisällys

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
- Sivukadun avopalvelu Oy:n toimeksiannosta työskenteleville alihankkijoille
- Sivukadun avopalvelu Oy:n tietojärjestelmiä tai toimitiloja säännönmukaisesti käyttäville henkilöille (esim. harjoittelijat, opiskelijat, siivoojat).

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 Sivukadun avopalvelu Oy:n Teamsissa tietoturvallisuuden kanavalla!

Yrityksemme tietoturvavastaava on Jyrki Jalassuo. Tietoturvaan liittyvissä kysymyksissä voit aina kääntyä suoraan hänen puoleensa.

2. Toimitilojen turvallisuus

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.

- Asiakasohjaustilanteessa päätelaitteen näyttö ei saa näkyä asiakkaalle, jos on vaarana että näkyy muiden kuin asiakkaan omia tietoja.
- Huolehdi, ettei neuvottelutiloissa, toimiston pöydällä tai yleisissä tiloissa ole esillä asiaan liittymätöntä materiaalia.
- Huolehdi neuvottelun tai asiakastapaamisen 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 tai pöytäkonetta ilman valvontaa. Huolehdi myös muistitikkujen, CD-/ DVD-levyjen, paperitulosteiden ym. asianmukaisesta säilyttämisestä.
- Noudata “puhtaan pöydän” periaatetta. Työ- pöydällä ei saa säilyttää salassa pidettävää tietoa, kun tietoa ei tarvita työtehtävien suorittamisessa.
- Kuvaaminen organisaation tiloissa vierailijoiden ja asiakkaiden toimesta kiellettyä. Valvo vieraidesi ja asiakkaidesi toimintaa (esimerkiksi kameroiden käyttöä). Poikkeuksena kuvat joihin on pyydetty erikseen lupa ja kuvat on otettu yleistä turvallisuutta noudattaen
- Lukitse toimiston 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 ulos. Älä päästä asiattomia henkilöitä lukittuihin toimitiloihin ilman valvontaasi.
- Ilmoita kadonneista avaimista Teamsissa, tee myös poikkeamailmoitus

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.
- Estä asiaton pääsy tietojärjestelmiin sammuttamalla tai lukitsemalla päätelaitteesi aina kun poistut se ei ole käytössäsi.
- Jos työaseman kiintolevy tai muu tallennus- väline, kuten esimerkiksi muistitikku tai CD-/DVD-levy, puhelin tai tietokone rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin. Tiedot täytyy tuhota ja poistaa laitteelta huolellisesti.
- Siirrä tietokone virranhallintatilaan tai sammuta se työpäivän päättyessä
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin, joita ovat mm. PIN- tai salasanakyselyt, laitteen automaattinen lukitus ja suojakoodi- kyselyt, tietoliikenneyhteyksien käyttäminen ja salaaminen.
- Huolehdi, että matkapuhelimessasi on päällä PIN- ja suojakoodikysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat oletuskoodit.
- Jos kadotat kannettavan päätelaitteen, tee välittömästi ilmoitus kadonneesta laitteesta poikkeamailmoituksena Teamsiin, jotta sen väärinkäyttö voidaan estää sekä ilmoita esimiehellesi puhelimitse.
- 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 tai PIN-koodejasi toisen henkilön käyttöön – älä edes lomien aikana.
- Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiin. Vaihda salasanasi riittävän usein ja heti, jos epäilet niiden paljastuneen.
- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä. Hyvässä salasanassa on pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Hyvä salasana on helppo muistaa, mutta vaikea arvata.
- Älä kirjoita salasanoja muistiin tai säilytä sellaisessa paikassa, mistä ne ovat helposti löydettävissä.
- Älä käytä samaa käyttäjätunnusta ja salasanaa internet-palveluihin rekisteröityessäsi tai niitä käyttäessäsi

4. Tietojen ja asiakirjojen käsittely

Asiakastietoja sisältävät dokumentit käsitellään ja säilytetään aina ensisijaisesti Domacaressa

Työsuhdetta koskevat tiedot säilytetään ja käsitellään aina ensisijaisesti Netvisorissa

Yrityksen sisäinen viestintä ja yritystä koskevat tiedot käsitellään säilytetään Teams: sovelluksessa / yrityksen Office 365 verkkopalvelimella.

Huom! Olet vaitiolovelvollinen myös yrityksen toiminnasta ja yritystä koskevista tiedoista.

Vältä tiedostojen tallentamista muualle kuin sille osoitettuun turvalliseen palvelin tilaan

- Ole erityisen huolellinen salassa pidettävän tiedon, kuten asiakastiedon, henkilökunnan henkilötietojen ja yritystä koskevien tietojen käsittelyssä.
- Muista, että voit käyttää ja käsitellä asiakas/potilastietoja tai muita salassa pidettäviä tietoja vain työtehtäviesi hoitamisessa.
- Esimerkiksi asiakas- ja potilasrekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Käyttötarkoitus on kuvattu rekisteriselosteessa.
- Huomioi myös, että tietojärjestelmien käyttöä valvotaan ja tietojen käsittelystäsi kirjataan tunniste- ja lokitiedot Domacaressa.
- Kun käsittelet salassa pidettävää tietoa, huolehdi, etteivät sivulliset näe tietoja asia- kirjoistasi tai tietokoneesi näytöltä. Varo syöttämästä salasanojasi siten, että joku ”näkee” salasanan sormiesi liikkeistä.
- Varo antamasta viattomankin oloisten keskustelujen yhteydessä sivulliselle potilastietoja tai muuta salassa pidettävää tietoa. Ole tarkka etenkin erilaisissa internetissä toimivissa sosiaalisen median palveluissa. Muista, että myös tieto sosiaali- ja terveyspalveluiden käytöstä on salassa pidettävä tieto. Samoin yritystä koskevat tiedot, joita ei ole määrätty julkisiksi (esim. kilpailutiedot)
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista sekä päättää luovutuksesta. Ellet tiedä oikeaa tahoa, ota yhteys esimieheesi. Pääsääntöisesti kaikesta asiakastietojen luovutuksesta vastaa kunnan sosiaalitoimi. Me emme luovuta tietoja asiakkaille suoraan. Yritystietojen luovutuksesta vastaa yrityksen omistajat.
- Tarkista aina 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) ulkopuolelle tai siirtäessäsi niitä tietovälineellä (muistitikku) Domacareen tai Office 365 palvelimelle. Alusta käytetyt muistitikut huolellisesti.
- 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!
- Varmistu vastaanottajan oikeudesta lukea aineistoa sekä sen perille menosta.
- Vältä ylimääräistä 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.
- 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 esimiehesi on sallinut.
- Ohjelmien lataaminen internetin kautta ja asentaminen päätelaitteille on kiellettyä lukuun ottamatta Domacarea, Netvisoria, Office 365 ohjelmistoa, 112 sovellusta ja yleisesti tunnettuja ja turvallisia sovelluksia.
- 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 tietoturvavastaavalle
- 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. ”kalasteluviestejä”, 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 (sähköposti- osoitteita), 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. Hyvinvointitoimialan virallinen sähköposti- osoite on:
- hyvinvointitoimiala@kirjaamo.fi
- Muista, että aina kun käytät työnantajan laitteita, verkkoa tai sähköpostia, esiinnyt tietoverkossa työnantajan edustajana.

5.1. Teamsin ja WhatsUp:in käyttö

WhatsUp viestintä sopii lähinnä arkisiin kysymyksiin ja mukavan arkea piristävän keskustelun ylläpitoon. Alustalla voit keskustella arjen iloista ja pitää hyvää henkeä yllä. Jakaa kuvia, joissa ei näy kuvissa ihmisiä tai korkeintaan yhteisesti sovitusti kuvia henkilökunnasta. Asiakkaan kuvia tai asiakkaan auton (esim) kuvia ei alustalla julkaista. Teksti, jonka laitat WhatsUp ryhmään tulee olla sellaista, että se kestää julkisen tarkastelun kaikissa tilanteissa. Tiesithän, että Facebook ja WhatsUp ovat saman yrityksen omistuksessa.

Teamsin tietoturva on WhatsUpia parempi mutta ei ohjelmisto ei ole täysin tietoturvallinen. Ammatillinen keskustelu, jota Teamsissa käydään, voidaan käydä suoraan ja puhuen asioista niiden oikealla nimellä. Asiakkaista käytämme kuitenkin nimikirjaimia lempinimiä, joita ei voida yhdistää suoraan asiakkaaseen. Teamsissä ei julkaista kenenkään henkilötietoja tai asiakastietoja. Ei henkilökuntaan kuuluvan eikä asiakkaiden. Keskustelu ohjataan Teamsissä oikeille kanaville ja vain asianosaisten kommentoitavaksi. Samat ohjeet koskevat myös Teams videoneuvotteluita.

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.

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 yrityksen 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.

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.
- 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.

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 Sivukadun avopalvelu Oy:n epävirallisena edustajana. Yrityksen virallisena edustajana somessa toimivat 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, kiristyksen, vakoiluyrityksen tai muun hyökkäyksen kohteeksi, älä epäröi pyytää apua esimieheltä, työsuojeluvaltuutetuilta tai liitostasi.

Toimintaohjeita

Ajantasaiset ohjeet ja yhteystiedot löydät Teamsista

Jos hallussasi olevat päätelaitteesi, avaimet, puhelin tai laite katoaa tai varastetaan, ilmoita siitä välittömästi tietosuojavastaavalle.

Jos polttoaine kortti katoaa tai varastetaan, ilmoita siitä välittömästi esihenkilölle ja Fleat innovationille.

Ilmoita aina haittaohjelmista (esim. virushälytys päätelaitteella) ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi omalle esimiehellesi.

Tee jälkikäteen tietoturva/ poikkeamailmoitus Teamsin kautta tilanteista, joissa tietoturvallisuus tai tietosuoja on vaarantunut.

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/3/4G) yhteys työasemastasi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki tai ota siitä kuva kännykälläsi.
- Ota yhteyttä Jyrkiin. 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. Vakavissa tapauksissa väärinkäyttö voi johtaa myös vahingonkorvausvaatimuksiin tai rikosoikeudellisiin seuraamuksiin. Seurauksena voi olla myös työsuhteen päättäminen.

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

Yrityksessämme 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:

“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 18 §, Hyvä tiedonhallintatapa)

“Henkilötietojen suojaamiseksi rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset 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

Suomen kyberturvallisuusstrategia julkaistiin tammikuussa 2013. 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 (= kybertoimintaympäristö). 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. Kyberturvallisuu- teen 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 tietoverk- kojen kautta tulevien uhkakuvien pienentämisessä ja torjumisessa. Lisätietoa löydät esimerkiksi yhteiskunnan turvallisuusstrategiasta ja Suomen kyberturvallisuusstrategiasta.

9.5 Kohdistetut hyökkäykset

Viestintävirasto on tiedottanut kohdistetuista hyökkäyksistä 5.8.2011 Tietoturva nyt -artikkelissa seuraavaa:

”Kohdistettu hyökkäys on tiettyyn toimijaan tai toimijajoukkoon suunnattu kohteen erityispiirteet huomioiva tietoturvaloukkaus. Hyökkääjä valikoi kohteensa tarkasti tämän hallussa olevien tietoaineistojen tai muiden vastaavien seikkojen perusteella. Hyökkääjän motiivina voi olla esimerkiksi yritysten tai valtioiden 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 web-sivustolle. Jos käyttäjä avaa liitetiedoton tai seuraa linkkiä, voi haittaohjelma saastuttaa hänen koneensa. Asennuttuaan haittaohjelma ottaa yhteyden hyökkääjän ylläpitämään haittaohjelman ohjaamiseen käytettävään komentopalvelimeen. Tämän jälkeen hyökkääjällä on käytännössä suora tietoliikenneyhteys hyökkäyksen kohteena olevaan tietokoneeseen. Hyökkääjä voi kerätä tietoja kohteen tietokoneelta ja mahdollisesti laajentaa hyökkäystä kohteen 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 osapuolelta. Joissakin hyökkäyksissä on myös hyödynnetty 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 uusimmat kohdistetut hyökkäykset tapahtuvat 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 kunnallisesta 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 viranomaistoi-minnassa (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 § 1. kohta: Henkilötietorikos
- Tietosuojalaki (1050/2018) 26 §: Tietosuojarikos
- Vahingonkorvauslaki (41/1974)

Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategiasta

Uudistuvat säädöstekstit löytyvät ajantasaisina mm. Valtion säädöstietopankki –sivustolta (www.finlex.fi)