HAM

HAM Helsingin taidemuseosäätiö sr tietosuoja- ja tietoturvaohjeet 2024

Sisällys

1. Johdanto

Tämä tietosuoja- ja tietoturvaohje on tarkoitettu HAM Helsingin taidemuseosäätiö sr:n henkilöstön ja sen vastuulla olevia tietoja, tietojärjestelmiä tai toimitiloja käyttävien ulkopuolisten henkilöiden käyttöön.

Vastuu tietoturvallisuudesta ja siihen liittyvästä osaamisesta koskee jokaista. Kaikkien HAM Helsingin taidemuseosäätiön ylläpitämien ja hallinnoimien tilojen, laitteiden, tietoverkkojen ja palvelujen käyttäjien on noudatettava tässä dokumentissa esitettyjä ohjeita.

Nämä ohjeet täydentävät ja tarkentavat HAM Helsingin taidemuseosäätiön hallituksen hyväksymiä tietosuoja- ja tietoturvaperiaatteita. Tärkeimpinä tietoturvallisuustavoitteinamme on varmistaa toimintamme häiriöttömyys, meille uskottujen tietojen luottamuksellisuus ja oikeellisuus sekä lakien, asetusten ja määräysten toteutuminen.

Kaikki tietoturvallisuusohjeistukset löytyvät HAM Helsingin taidemuseosäätiön intranetistä

2. Tietoturvallisuuden tarkoitus

Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.

Tietoturvallisuus perustuu tiedon luottamuksellisuuteen, eheyteen, käytettävyyteen, kiistämättömyyteen ja tietosuojaan, jotka on turvattava järkevällä tasolla kaikissa olosuhteissa.

- Luottamuksellisuudella tarkoitetaan, että tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen käytettävissä. Sivullisille ei anneta mahdollisuutta muuttaa tai tuhota tietoja eikä muutoin käsitellä tietoja.
- Tietojen ja järjestelmien eheydellä tarkoitetaan, että ne ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena.
- Käytettävyydellä tarkoitetaan, että järjestelmien tiedot ja palvelut ovat aina niihin oikeutettujen käytettävissä ja saatavilla.
- Kiistämättömyydellä tarkoitetaan, että tietojen oikeellisuus on osoitettavissa.
- Tietosuojalla tarkoitetaan yksilön mahdollisuutta vaikuttaa hänestä kerättävään henkilökohtaiseen tietoon ja sen käyttöön.

3. Keskeiset tietoturvaohjeet, joita noudattamalla onnistut

1. Seuraa tietoturvallisuuteen ja tietosuojaan liittyviä tiedotteita, tutustu ohjeisiin ja osallistu mahdollisuuksien mukaan koulutuksiin. Toimi saamiesi ohjeiden mukaisesti.
2. Tue osaltasi kulunvalvontaa.
3. Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut sen luota. Lukitseminen onnistuu helposti painamalla Windows-lippupainiketta ja kirjainta L.
4. Työpäivän päättyessä kirjaudu tietojärjestelmistä ulos ja lukitse tai sammuta tietokoneesi.
5. Älä jätä vierasta valvomatta työhuoneeseesi tai muihin tiloihin.
6. Älä anna ulkopuolisen käyttää konettasi.

7. Noudata ns. puhtaan pöydän periaatetta. Älä säilytä työpöydällä luottamuksellista tai salassa pidettävää aineistoa.
8. Käsittele varsinkin salassa pidettäviä tietoja huolellisesti välineestä riippumatta, olipa tiedon välittäjänä sitten henkilö, tietokone, paperi, puhelin tai jokin muu.
9. Hävitä henkilö- ja asiakastietoja sisältävät paperit välittömästi käytön jälkeen tietosuojasäiliöön tai muulla tietoturvallisella tavalla. Suositeltavia ratkaisuja suojattavan paperijätteen hävittämiseksi on lukittavan tietosuojasäiliön lisäksi esimerkiksi: 1) tietoturvaluokan P4 (=salaiset asiakirjat) täyttävä tietoturvatuhoaja (silppuri), tai 2) paperijätteen hävittäminen polttamalla.
10. Älä luovuta henkilökohtaisia käyttäjätunnuksia ja salasanojasi toisen henkilön, edes kollegan, käyttöön.
11. Älä anna sivullisen nähdä tietokoneesi näyttöä tai näppäimistöä, kun käsittelet arkaluonteista tietoa tai kun syötät käyttäjätunnuksia ja salasanoja (käytä mahdollisuuksien mukaan näytönsuojakalvoa).
12. Vaihda salasanat heti, jos epäilet niiden paljastuneen.
13. Älä asenna ohjelmistoja tai tee järjestelmiin asetusmuutoksia, ellei tämä kuulu työtehtäviisi.
14. Tallenna tekemäsi työ mieluiten työtiloihin tai dokumentin hallintajärjestelmään. Siellä tiedot varmistetaan keskitetysti.
15. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen. Mikäli käytettävissä on ns. turvatulostus, käytä sitä tulostamiseen.
16. Muista, että käyttäessäsi HAM Helsingin taidemuseosäätiön laitetta, verkkoa tai sähköpostia näyt ja esiinnyt tietoverkossa aina tahtomattasikin edustajanamme.
17. Käytä aina asianmukaista salausta, mikäli sinun on siirrettävä internetin kautta luottamuksellista tai salassa pidettävää tietoa. Esim. sähköpostin osalta tulee käyttää salattua sähköpostia lähetettäessä henkilötietoa sisältävää postia järjestelmämme ulkopuolelle.
18. Älä surffaa arveluttavilla nettisivuilla.
19. Älä avaa outoja sähköpostiviestejä, niiden linkkejä tai liitteitä.
20. Työmatkalla ja etätöissä on käytettävä HAM Helsingin laitteita, eli tietokonetta ja mobiililaitteita, sekä niiden mukana tulevaa datayhteyttä. Jos koneen mukana tuleva datayhteys on huono, voidaan käyttää luotettavaa muuta datayhteyttä esim. kodin datayhteys. HAM Helsingin ulkopuolisilla laitteilla, jotka eivät ole HAM Helsingin IT-kumppanin laitehallinnan ja tietoturvan piirissä, ei tule kirjautua HAM Helsingin käytössä oleviin järjestelmiin.Ilmoita aina tietoturvallisuuteen liittyvistä ongelmatilanteista ja havaitsemistasi uhkista ja suojauspuutteista välittömästi HAMin ICT-vastaavalle.
21. Pyydä tarvittaessa neuvoa HAMin ICT-vastaavalta.

4. Tietoturvan toteuttaminen

4.1. Tietoturvallisuuden tärkeys

Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.

Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki, ei siis vain tekniikka, vaan myös jokapäiväiset toimintatapamme ja asenteemme.

4.2. Haastattelut, tiedustelut, tutkimukset ja tietojen luovutus

1. Ohjaa haastattelupyynnöt ja tiedustelut asian vastuuhenkilölle.
2. Varo antamasta viattomankin oloisten keskustelujen ja lomakkeiden yhteydessä tietoa luottamuksellisista, salassa pidettävistä tai yksityisyyden suojan piiriin kuuluvista tiedoista.
3. Ohjaa tietojen luovutus- ja tutkimuspyynnöt asiasta vastaavalle henkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista ja päättää luovutuksesta.
4. Jos olet epävarma, kenen vastuulle asia kuuluu, ole yhteydessä esihenkilöösi.

5. Henkilöstöturvallisuus

Tyypillisesti noin kaksi kolmannesta turvallisuusvahingoista on oman henkilökunnan tahallisesti tai tahattomasti aiheuttamia. Näitä vahinkoja ehkäistään seuraavilla toimenpiteillä:

- Jokainen tietoverkon käyttäjä perehdytetään tietoturvallisuuden perusteisiin, mm. tähän ohjeeseen.
- Tietoturvallisuuskoulutus on osa työhön opastusta.
- Työtehtävät pyritään rajaamaan siten, ettei niistä muodostu liian isoa tietoturvallisuusriskiä.
- Kriittiset työtehtävät eivät ole vain yhden henkilön varassa. Yksiköiden sisällä varmistetaan varahenkilöt tehtäviin ja huolehditaan heidän osaamisestaan.
- Pääsy- ja käyttöoikeudet annetaan tehtävän vaatimusten mukaan.
- Tehtävien vaihtuessa tai päättyessä tehtävään liittyvät avaimet, käyttö- ja kulkuoikeudet poistetaan käyttäjältä.
- Henkilöstön työsopimuksissa on salassapitolauseke.

6. Palvelutoimittajat ja alihankinta

Tietoturvallisuusperiaatteita ja ohjeita noudatetaan tietojenkäsittelypalveluita ja -kapasiteettia ostettaessa. Palvelun tuottajan tietoturvallisuustaso varmistetaan palvelun ulkoistus- ja alihankintatilanteissa. Palveluntarjoajat ja alihankkijat sitoutetaan tapauskohtaisesti soveltuvin ja järkevin osin tietoturvallisuusvaatimuksiimme sopimuksin.

Palvelutoimittajille asetetaan tietoturvallisuuden osalta saman tasoiset vaatimukset kuin omalle henkilöstölle.

7. Fyysinen turvallisuus

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

- Vierailijan isännän vastuulla on huolehtia, että ulkopuoliset henkilöt eivät pääse aiheettomasti liikkumaan tiloissamme. Ohjaa vieraat tai ”eksyneet” henkilöt oikeisiin paikkoihin. Älä päästä asiattomia henkilöitä toimitiloihin samalla oven avauksella esim. töistä lähtiessäsi.
- Älä jätä kulunvalvonnassa olevia tai muuten lukittuna pidettäväksi tarkoitettuja ovia auki eli varmista, että tällaiset ovet lukkiutuvat kuljettuasi niistä.
- Jos havaitset tiloissamme normaalin työajan ulkopuolella henkilöstöön kuulumattoman henkilön, on sinulla velvollisuus tarkistaa ulkopuolisen henkilöllisyys sekä selvittää hänen asiansa.

7.1. Avaimet ja kulkuluvat

Jokaiselle työntekijälle luovutetaan toimitiloihin pääsemiseksi tarvittavat avaimet ja kulkuluvat henkilökohtaisesti.

Käyttöön annetut avaimet ja kulkukoodit ovat tarkoitettu henkilökohtaiseen käyttöön, niitä ei saa luovuttaa tai lainata muille, eikä jättää näkyville esim. työpöydälle. Luovutetuista avaimista pidetään kirjaa. Avaimen ja kulkuoikeuden hyväksyy esihenkilö ja turvallisuusvastaava.

Jos fyysiset avaimet tai kulkukoodit katoavat tai ne varastetaan, on siitä välittömästi ilmoitettava HAM Helsingin taidemuseon päivystäjälle.

7.2. Ajoneuvot

Autoon ei ole turvallista jättää mitään luottamuksellista aineistoa tai arvokasta näkyville. Edes tavaratilassa ei pidä säilyttää pitkäaikaisesti (yli tunnin ajan) tärkeitä asiapapereita, tietokoneita, mobiililaitteita, muisteja tai muuta arvokasta.

7.3. Vieraat

Vierailijat ovat isännän vastuulla. Isännän tulee huolehtia, etteivät ulkopuoliset henkilöt pääse aiheettomasti liikkumaan tiloissamme. Vieraat tulee olla isännän ohjauksessa vierailun ajan.

Ketään asiatonta henkilöä ei tule päästää valvomatta liikkumaan toimitiloissa.

Jos neuvottelutilassa on muiden organisaatioiden kävijöitä, ei neuvottelutilaan tule jättää valvomatta omaa tietokonetta, ilman tietokoneen käyttöjärjestelmän lukitsemista.

8. Liikkuva työ, etätyö ja mobiililaitteet

Huomion kiinnittäminen tietoturvallisiin menettelytapoihin on erityisen tärkeää toimittaessa vakituisten toimistotilojen ulkopuolella. Etätyössä ja liikkuvassa työssä sinun tulee noudattaa soveltuvin osin kaikkia samoja turvallisuusperiaatteita kuin ollessasi HAM Helsingin varsinaisissa toimitiloissa. Kun välineitä kuljetetaan ja käytetään työpaikan toimitilojen tarjoamien turvatoimien ulkopuolella, tulee tietoturvallisiin menettelytapoihin kiinnittää erityistä huomiota ja huolellisuutta.

- Huolehdi työnteossa käyttämiesi koneiden, laitteiden ja älypuhelimien turvallisuudesta. Älä säilytä niissä luottamuksellista tietoa suojaamattomana.
- HAMin toiminnassa ei ole sallittua käyttää muistitikkuja tai muitakaan siihen rinnastettavia muistikortteja tai ulkoisia kova-/kiintolevyjä tietojen tallentamiseen, paitsi kun se on työtehtävän vuoksi välttämätöntä (esim. markkinointiaineiston toimitus ulkopuoliselle markkinointiyritykselle).
- Vältä vieraiden (esim. ulkopuolisten luennoitsijoiden) USB-tikkujen tai muistikorttien käyttöä, mikäli vain mahdollista.
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin (mm. lukitseminen, pääsykoodikyselyt, Bluetoothin näkyminen muille laitteille, sovellusten lataaminen, päivitykset). **Huom!** pääsykoodi on eri asia kuin SIM-kortin PIN-koodi.
- Huolehdi, että matkapuhelimessasi on päällä pääsykoodi-kysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat oletusarvoiset pääsykoodit.
- Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat ja pysyvät vain sinun käytössäsi.

- Kuljeta mukanasi vain välttämätön määrä tietoaineistoa ja varmistu aina aineiston asianmukaisesta suojauksesta.
- Etätyöpisteeseen ei ole suositeltavaa viedä luottamuksellisia henkilötietoja sisältäviä paperisia asiakirjoja. Mikäli näin joudut kuitenkin työn luonteen kannalta tekemään, olet vastuussa tietosuojattavan paperijätteen asianmukaisesta hävittämisestä asiakirjojen käyttötarkoituksen päättyessä, esim. polttamalla tai viemällä ne lukittuihin niihin tarkoitettuihin työpaikan tietosuojasäiliöihin.
- Etätyössä muista varmistaa, että sivulliset (esim. perheenjäsenet) eivät kuule luottamuksellisia tai salaisia puhelinkeskusteluita tai käytä työnantajan antamia töihin tarkoitettuja laitteita.
- Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä.
- Mikäli työskentelet julkisessa kulkuvälineessä, varmistu, etteivät kanssamatkustajat pysty näkemään käsittelemiäsi tietoja ja asiakirjoja. Käytä tarvittaessa laitteen näytön omaa tietoturvasuojaa tai erillistä kalvoa.
- Varo aiheettomien langattomien yhteyksien aktivoitumista koneeseesi.
- Säilytä tieto ja laitteet turvassa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa.
- Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin. Muista että päätelaiteturvallisuus pätee etenkin muissa paikoissa kuten hotelleissa, kahviloissa, kotimatkalla ja myös kotona. Erityisesti julkisiin WLAN-verkkoihin (esim. kahviloissa) yhdistämistä kannattaa välttää, sillä nämä voivat lähettää kaiken tietoliikenteen ei -salatussa muodossa palvelun tarjoajalle. Käytä ensisijaisesti puhelinta tai tietokonetta ja sen mobiilidataa verkkoyhteytenä. Jos päätelaitteella on saatavilla käyttöjärjestelmä-, tietosuoja-, selain- tai ohjelmistopäivitys, tulee nämä aina suorittaa mahdollisimman nopeasti, kun tilanne sen sallii.
- Vältä julkisten verkkojen käyttöä työasioissa, jos käsittelet luottamuksellisia tietoja.
- Liikkuvassa työssä ja etätöissä on käytettävä ensisijaisesti HAM Helsingin taidemuseon laitteita, eli tietokonetta ja mobiililaitteita, sekä niiden mukana tulevaa datayhteyttä. Jos koneen mukana tuleva datayhteys on huono, voidaan käyttää luotettavaa, muuta datayhteyttä esim. kodin datayhteys.
- Käytä aina salattua sähköpostia lähettäessäsi henkilötietoa sisältävää postia järjestelmämme ulkopuolelle. Salattua sähköpostia tulee käyttää aina sellaisessa viestinnässä, joka vaatii luottamuksellisuutta.

9. Tilaisuudet ja koulutukset - osallistumisluettelot

Koulutustilaisuuksiin tai muihin vastaaviin tilaisuuksiin ilmoittautumisen yhteydessä voidaan ilmoittautuneista kerätä vain sellaisia välttämättömiä henkilötietoja, joita tilaisuuden järjestäjä tarvitsee esimerkiksi seurannan, tilastoinnin tai laskutuksen järjestämiseksi. Tilaisuuden jälkeen henkilötiedot tulee poistaa, jos tietojen käytölle ei ole enää perustetta. Kerättyjä ilmoittautumistietoja ei saa käyttää muuhun tarkoitukseen.

Tilaisuuden järjestäjän vastuulla on arvioida, mitä tietoja ilmoittautumisen yhteydessä kerätään ja kuinka kauan tietoja säilytetään ennen niiden hävittämistä.

HAM Helsingin taidemuseo ei jaa, laita esille tai julkaise tilaisuuksiin ilmoittautuneiden tietoja (osallistujalistoja) edes tilaisuuksiin osallistujille.

10. Laitteistoturvallisuus

10.1. Kopiokoneet ja yhteiskäyttöiset tulostimet

Kopiokonetta ja yhteiskäyttöistä tulostinta käytettäessä tulee huolehtia siitä, että alkuperäiset ja kopioidut asiakirjat eivät jää laitteeseen tai sen lähettyville.

Jos laite mahdollistaa niin sanotun turvatulostamisen (tulostaminen alkaa vasta, kun olet kirjautunut laitteelle omilla tunnuksillasi), on tätä ominaisuutta käytettävä.

10.2. Työasemat

Kaikki hankinnat menevät HAMin ICT-vastaavan kautta.

Työasemissa on IT-tuen kanssa yhdessä määritelty vakiokokoonpano. Työasemiin saa tämän lisäksi asentaa ainoastaan HAM Helsingin taidemuseosäätiön hankkimia lisensoituja tai avoimen lähdekoodin ohjelmia. Ohjelmien luvaton kopiointi on ehdottomasti kielletty.

Jokainen työaseman käyttäjä vastaa osaltaan työasemansa turvallisuudesta. Työasemaa käytetään vain työtehtävien edellyttämiin tarkoituksiin.

Työntekijöille hankitut laitteet ovat HAM Helsingin omaisuutta tai vuokraamia. Ne on hankittu työntekijöille työntekoa tukeviin tarkoituksiin. Laitteiden antaminen ulkopuolisten käyttöön on ehdottomasti kielletty.

Poistuessasi työasemalta kirjaudu ulos työasemastasi tai lukitse työasemasi joko Windows-näppäin + L tai Ctrl-Alt-Delete + Enter -komennolla.

Työpaikalta poistuttaessa lukitse tai sammuta työasemasi sekä katkaise virta näytöstä ja henkilökohtaisesta tulostimesta.

- Tietokoneen käyttö sisältää sekä oman työaseman että tietoliikenneverkon kautta käytettävien palveluiden käytön.
- Vastaat käyttäjänä omasta koneestasi. Ole siis huolellinen. Vain työtehtävien hoitoon tarkoitettuja ja IT-tuen kanssa yhdessä sovittuja ohjelmia saa asentaa koneelle ja laitteita saa liittää verkkoon. Kirjaudu koneelle aina omilla käyttäjätunnuksillasi.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi (Windows-lippupainike ja kirjain L) aina kun poistut sen luota.
- Lisävarmistuksena voit myös käyttää salasanasuojattua näytönsäästäjää.
- Tallenna työsi käyttäen automaatti- tai välitallennuksia. Älä jätä työtä tallentamatta, kun poistut koneesi luota.
- Jos työaseman kiintolevy rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin, vaan se pitää hävittää tietoturvallisesti.
- Toimita hävitettävät laitteet HAMin ICT-vastaavalle hävitettäväksi.
- Kirjaudu ulos sekä ohjelmistoista että koneeltasi tai sammuta tietokoneesi työpäivän päättyessä.

10.3. Puhelimet

Puhelimet tulee suojata käynnistyksen yhteydessä kysyttävällä henkilökohtaisella tunnusluvulla eli pääsykoodilla (eri asia kuin SIM-kortin PIN-koodi).

Henkilökohtainen tunnusluku eli pääsykoodi:

- Kysytään laitetta käynnistettäessä.
- Kysytään, mikäli laitetta ei ole käytetty 1–5 minuuttiin.

Älypuhelimien sovellusten (esim. kalenteri ja sähköposti) käytössä täytyy noudattaa samoja turvallisuusohjeita kuin on annettu työaseman käytöstä. Varkaus- tai katoamistapauksessa tulee olla välittömästi

yhteydessä HAMin ICT-vastaavaan, joka auttaa puhelimen sisällön etätyhjentämisessä ja liittymän sulkemisessa.

Muista, että puhelinkeskustelua voidaan nauhoittaa tai sitä voidaan kuunnella.

Älä jätä soittamaasi puhelinvastaajaan viestiä, joka sisältää luottamuksellista tai salassa pidettäviä asioita. Jätä ainoastaan soittopyyntö.

Työsuhdepuhelimet ovat HAM Helsingin taidemuseosäätiön omaisuutta. Vanha puhelin tulee palauttaa HAMin ICT-vastaavalle

Palautuvista laitteista käyttäjän:

- on poistettava kaikki henkilökohtaiset tiedot, tiedostot, kuvat yms.
- Apple (iOS)-laitteista poistettava linkitys käyttäjän iCloud-tilille.
- kerrottava laitteen pääsykoodi palautuksen yhteydessä.

Vanhat puhelimet asetetaan tehdastilaan ja niiden sisältö tyhjennetään ennen kuin laitteet viedään kierrätykseen.

10.4. Siirrettävät tietovälineet

Siirrettävien tietovälineiden (esim. muistitikku/-kortti tai ulkoinen kova-/kiintolevy) käyttäminen on kielletty, paitsi tehtävissä, joissa se on välttämätöntä.

10.5. Salasanat, PIN- ja pääsykoodit

Salasanat, PIN- ja pääsykoodit suojaavat tietojärjestelmiä, käyttäjien tietoja sekä käyttäjiä. Käyttäjä vastaa tunnuksellaan tehdyistä toimista.

Järjestelmien salasanat, PIN- ja pääsykoodit ovat henkilökohtaisia. Pidä ne huolellisesti omana tietonasi.

Älypuhelimissa ja tableteissa on käytettävä pääsykoodia sekä käynnistyksessä että aikalukituksessa. Pääsykoodit on vaihdettava oletuksesta henkilökohtaiseksi.

Käytä riittävän pitkiä salasanoja ja pääsykoodeja.

Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanoja, PIN- tai pääsykoodejasi toisen henkilön käyttöön. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiisi.

Mikäli epäilet salasanasi, PIN- tai pääsykoodisi joutuneen jonkun ulkopuolisen tietoon, vaihda se välittömästi ja ilmoita asiasta HAMin ICT-vastaavalle.

Älä kirjoita salasanojasi, PIN- tai pääsykoodiasi paperille tai muistiin sellaiseen paikkaan, mistä ne ovat muiden löydettävissä.

Kun kirjoittaudut ensimmäistä kertaa sisään uuteen järjestelmään, vaihda käyttöösi annettu salasana, PIN- tai pääsykoodi välittömästi, ellei sinua ole ohjeistettu toisin.

Jos kirjaudut toimiston kokoushuoneen tietokoneelle, varmistu, ettei salasanasi tallennu laitteen muistiin.

Älä käytä järjestelmien käyttäjätunnusta, salasanaa, PIN- tai pääsykoodia Internetin tai muun vieraan verkon palveluissa.

Älä käytä työkäytössä olevaa käyttäjätunnusta tai salasanaa Internetin palveluihin rekisteröityessäsi.

Hyviä toimintatapoja salasanojen suhteen:

- Salasanan pituudeksi suositellaan vähintään 14 merkkiä.

- Käytä isoja- ja pieniä kirjaimia.
- Käytä numeroita ja erikoismerkkejä, paitsi järjestelmissä, jotka eivät tue niitä.
- Käytä ei -helposti arvattavia salasanoja.
- Vältä yleisiä salasanoja tai sanoja (password, qwerty, salasana123, kuukausia, viikonpäiviä, kutsumanimiä, syntymävuosia ja -päiviä).
- Helppo tapa turvallisiin salasanoihin on käyttää satunnaisiin sanoihin perustuva salasanalausekkeita; UP#(sJ2^74v0dX on toki erinomaisen hyvä salasana, mutta Valtamerilaiva-Kaksisataa-78-Selitys on vielä paljon parempi ja se on helpompi muistaa ja kirjoittaa.
- Vältä saman salasanan käyttöä. Käytä eri palveluihin/järjestelmiin eri salasanoja.
- Älä käytä samoja tunnuksia/salasanoja työssä, joita käytät yksityiselämässä ja päinvastoin.
- Käytä salasanojen hallintasovellusta (password manager). Nämä sovellukset luovat turvallisia salasanoja eikä käyttäjän tarvitse muistaa niitä ulkoa.
- Älä tallenna tunnuksia ja salasanoja selväkielisessä / ei -salatussa tiedostossa (esim. Word-, Excel tai Notepad -dokumentissa).

10.6. Käyttöoikeudet

Järjestelmän omistaja/pääkäyttäjä myöntää järjestelmiin käyttöoikeudet ja salasanat. Myönnetty tunnus ja salasana on työntekijän henkilökohtaiseksi tunnukseksi tarkoitettu ja niitä ei tule luovuttaa muille.

10.7. Tietoliikenne

HAM Helsingin taidemuseon toimiston tietoverkkoa ja sen palveluja saa käyttää ainoastaan museon henkilöstö.

Ulkopuolisille käyttäjille tarkoitettu vierailijaverkko on suojattu ja sijoitettu siten, ettei näillä ole pääsyä HAM Helsingin taidemuseon tietoverkkoon.

10.7.1. Sähköpostin ja Internetin käyttö

Kaikki suojaamaton sähköpostiviestintä kulkee julkisen internetin kautta salaamattomana, tämä pitää ottaa huomioon sähköpostiviestejä lähettäessä. Sisäiset sähköpostit eivät kuitenkaan liiku salaamattomana julkisen verkon kautta.

Jos viesti sisältää luottamuksellisia tietoja tai henkilötietoja, se on lähetettävä salattuna. Salatun postin lähettämiseen on HAMissa käytössä Securemail-palvelu.

Asiakkaille ja muille toimiston ulkopuolisille henkilöille on tarjotaan tarvittaessa mahdollisuus lähettää salattu viesti HAM Helsingin taidemuseolle.

Henkilöstön tulee käyttää HAM Helsingin taidemuseon omaa sähköpostijärjestelmää töihin liittyvissä sähköpostiviestinnöissä. Muiden sähköpostipalveluiden käyttäminen on ehdottomasti kielletty.

Muista tyhjentää sähköpostilaatikkosi säännöllisesti ja säilytä ainoastaan ne viestit, joita todella tarvitset. Viestien tarpeetonta säilyttämistä tulee välttää. Erityisesti henkilötietoja sisältävät viestit tulee poistaa, kun niitä ei enää tarvita.

Kirjoita tai valitse huolellisesti viestin vastaanottajan nimi ja sähköpostiosoite. Tarkista nämä kertaalleen vielä ennen viestin lähettämistä. Näin estät viestin joutumisen epähuomiossa väärälle vastaanottajalle.

Huolehdi siitä, että käyttämäsi sähköpostin jakelulistat ovat ajan tasalla. Poista tarpeettomat tai vanhentuneet osoitteet säännöllisesti.

Sähköpostilla vastaanotettaviin tuntemattomiin Internet-linkkeihin ja liitetiedostoihin tulee aina suhtautua varauksella. Älä avaa epäilyttäviä viestejä.

Sähköpostiosoitteesi on osa HAM Helsingin taidemuseosäätiön käyttämää sähköpostiosoitteistoa. Näitä sähköpostiosoitetta ei saa käyttää rekisteröintiä vaativissa palveluissa Internetissä, ellei rekisteröinti liity työtehtävien hoitoon. Tällöinkään ei saa käyttää samoja käyttäjätunnuksia ja salasanoja, joita käytetään sisäisissä järjestelmissä.

Myös lähettäjän tietojen väärentäminen on mahdollista. Varmista aina, että viestin sisältö on asianmukaista ennen liitetiedostojen tai linkkien avaamista.

- Opettele salatun sähköpostin käyttö, jotta tieto ei vahingossa lähde salaamattomana.
- Jos hätätapauksessa joudut pakottavasta syystä käyttämään julkisia päätteitä tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies).
- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Mikäli oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Jakelulista on henkilöluettelo, jonka jokainen vastaanottaja saa tietoonsa ja se voi olla henkilörekisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Käytä sähköpostin piilokopiotoimintoa, jos haluat estää jakelulistalla olevien osoitteiden näkymisen vastaanottajille.

10.7.2. Sähköpostin käyttö / Tietojen kalastelu

Saapuvaa sähköpostia skannataan myös pilven päässä Microsoftin tietoturvatuotteilla, mutta mikään tietoturvatuote ei koskaan ole täysin aukoton. Tämän vuoksi ei kannata koskaan olettaa, että jokainen saapunut sähköposti olisi varmuudella turvallinen.

On hyvä muistaa ja tarkistaa seuraavat asiat, kun saat tai olet lähettämässä sähköpostia / tekstiviestejä, jossa on linkkejä tai liitteitä mukana:

- Tarkista kuka lähettäjä on.
- Mistä sähköpostiosoitteesta viesti on tullut.
- Mikä on viestin sisältö.
- Miksi tämä viesti on lähetetty sinulle.
- Älä avaa linkkejä tai tiedostoja, mikäli ne vaikuttavat epäilyttäviltä tai epäilet niiden alkuperää.
- Pyri aina selvittämään viestin aitous, jos et ole siitä varma (esim. soittamalla lähettäjälle tai varmistamaan it-tuelta).
- Älä asenna ohjelmistoja mikäli niiden turvallisuudesta ei ole tietoa tai varmuutta.
- Sähköpostissa oleva linkki tai lähettäjä voi olla väärennetty, joten älä avaa epäilyttäviä viestejä ja poista ne / merkkaa roskapostiksi tai kalastusyritykseksi.
- Hiiren laittaminen URL-linkin päälle näyttää todellisen linkin, johon päädyt, mikäli linkkiä klikataan.
- Kalasteluviesteissä yritetään usein luoda kiireellisyyden tunnetta, joten mieti aina kahdesti, ennen kuin avaat tai klikkaat liiteitä/linkkejä.

- Älä vastaile tai välitä ketjukirjeen omaisia sähköpostiviestejä.
- Tarkista aina vastaanottajat, kun olet lähettämässä viestin, jotta oikeat henkilöt ovat mukana jakelussa.
- Tarkista aina viestin sisältö (esim. liitteet / tiedostot) ja että vastaanottajilla on oikeus näitä vastaanottaa.
- Jos välität viestin eteenpäin, tarkista ensin koko viestinketjun sisältö ja varmista, että et jaa asiaankuulumatonta tietoa vastaanottajalle.
- Jos käytät HAM Helsingin taidemuseosäätiön sähköpostia yksityisasioiden hoitamiseen, varmista, että sisältöä ei luulla tai tulkita HAM Helsingin taidemuseosäätiön toimintaan liittyväksi.
- Sähköpostin luokittelu on suositeltavaa (sisäinen, yksityinen, luottamuksellinen, salainen tms.).
- Esimerkiksi Word -dokumentit voivat olla muunneltavissa tai sisältää luonnosvaiheessa tehtyjä muutoksia, joten on suositeltavaa, että tiedostot lähetetään aina PDF -muodossa.
- Hyvämaineiset organisaatiot (esim. Microsoft) eivät lähetä koskaan salasanan vaihtoa vaativia sähköposteja.

10.7.3. Sähköpostin ja Internetin kielletyt tietosisällöt

Jokainen henkilökuntaan kuuluva edustaa järjestelmiä käyttäessään HAM Helsingin taidemuseosäätiötä, joten niitä tulee käyttää asiallisessa käyttötarkoituksessa ja hyvien tapojen mukaisesti.

Järjestelmien seuraavanlainen käyttö on kielletty:

- Tietokone ei saa olla kytkettynä yhtä aikaa HAM Helsingin lähiverkkoon ja ulkoiseen langattomaan verkkoon. Jos tietokoneesi on kytketty lähiverkkokaapelilla toimistolla, niin varmista, ettei laite ole saman aikaisesti yhteydessä langattomaan verkkoon.
- Järjestelmien kaupallinen hyödyntäminen esim. sivutoimissa tai omassa yritystoiminnassa.
- Tuntemattomien tai työtehtäviin kuulumattomien ohjelmien tai tiedostojen noutaminen/lataaminen Internetistä HAM Helsingin taidemuseon työasemaan.
- Sähköpostilaatikkoon saapuvien viestien automaattinen lähettäminen edelleen johonkin ulkoiseen sähköpostijärjestelmään.

10.8. Etätyö

Työmatkalla ja etätöissä on käytettävä ensisijaisesti HAM Helsingin laitteita, eli tietokonetta ja mobiililaitteita, ja niiden omaa datayhteyttä.

10.9. Tietojen varmistaminen ja palautus

Palvelimet varmistetaan ICT palveluntoimittajan toimesta. Tiedostopalvelimien muutokset varmistetaan kerran vuorokaudessa ja full backup tehdään kerran kuukaudessa. Varmistusten säilytysaika on yleensä 6 kuukautta.

Pilvipalveluista otetaan varmuuskopio päivittäin.

Työaseman varmuuskopioimisesta vastaa käyttäjä itse.

Sallittuja varmuuskopioinnin tallennuspaikkoja ovat: Teams / Sharepoint / Onedrive.

10.9.1. Luottamukselliset tiedot

Henkilötietoja ja muita luottamuksellisia tietoja saa käsitellä vain työhön liittyvässä tarkoituksessa. Henkilötietoja ja muita luottamuksellisia tietoja käsiteltäessä on kiinnitettävä erityistä huomiota tietoturvallisuuteen.

Asiakkaiden henkilötietoja säilytetään pääsääntöisesti vain asiakasrekistereissä ja henkilöstön tietoja Mepco-järjestelmässä. Em. järjestelmistä poimittuja henkilötietoja säilytetään vain niin kauan, kun tietojen käyttötarkoitus sitä edellyttää. Sen jälkeen tiedot hävitetään.

Esimerkiksi mikäli uutiskirjeen jakelulista ei ole saatavissa uutiskirjetyökalusta valmiina, tulee asiakasrekisteristä manuaalisesti haettu jakelulista hävittää käytön jälkeen.

10.10. Papereiden, paperiaineistojen ja esitysmateriaalien käsittely

Vältä turhaa paperille tulostamista.

Mikäli käytettävä tulostin sijaitsee muualla kuin työhuoneessa, nouda tulostettu aineisto välittömästi tulostamisen jälkeen.

Henkilötietoja tai muita arkaluontoisia tietoja sisältäviä paperisia tulosteita ei tule jättää pöydälle. Käyttötarkoituksen päätyttyä ne tulee joko arkistoida (kaappi/mappi) ja siirtää pois näkyviltä, tai hävittää tietoturvallisesti.

10.10.1. Papereiden, paperiaineistojen ja esitysmateriaalien hävittäminen

Jokainen on vastuussa omien tietosuojattavien paperijätteiden asianmukaisesta hävittämisestä käyttötarkoituksen päättyessä.

Luottamuksellinen paperimateriaali on käyttötarkoituksen päättyessä hävitettävä esim. polttamalla, silppuamalla tietoturvaluokan P4 (=salaiset asiakirjat) täyttävällä tietoturvatuhoajalla tai viemällä ne lukittuihin niihin tarkoitettuihin työpaikan tietosuojasäiliöihin.

Tietosuojasäiliöt tulee säilyttää sivullisten katseilta piilossa ja kulunvalvonnan piirissä.

Mikäli tarvitset toimintatavoista lisätietoa, ota yhteyttä HAMin ICT-vastaavaan.

10.11. Tietoteknisten laitteiden ja tietovälineiden tietoturvallinen tyhjennys

Jokaisen omalla vastuulla on huolehtia käytöstä poistuvien laitteiden sekä dataa sisältävien tietovälineiden tietoturvallisesta hävittämisestä. Tämä koskee myös ulkopuolisia henkilöitä, joille on luovutettu HAM Helsinki laitteita tai tietovälineitä työtehtävien suorittamista varten.

Monissa laitteissa ja tietovälineissä on tietosäilöjä, joissa olevia tietoja on hallittava turvallisesti. Tietokoneiden, kännyköiden, USB-muistitikkujen, muistikorttien ja CD/DVD-levyjen lisäksi niitä on esimerkiksi monissa tulostimissa ja monitoimilaitteissa.

Laitteen tai tietovälineen käytön lopettaminen on tärkeä vaihe laitteiden ja tiedon käsittelyn elinkaaressa, sillä hallinnan pettäminen elinkaaren lopussa voi mitätöidä aikaisemmat tietoturvan ja tietosuojan eteen tehdyt ponnistelut. Monet laitteet taltioivat tietämättämme automaattisesti erilaisia tietoja, jolloin ne saattavat sisältää paljon henkilötietoa.

Laitteissa ja tietovälineissä olevia tietoja tulee käsitellä huolellisesti myös siinä vaiheessa, kun niitä poistetaan käytöstä.

Jokaisen omalla vastuulla on huolehtia käytöstä poistuvien laitteiden sekä dataa sisältävien tietovälineiden tietoturvallisesta hävittämisestä.

Ennen laitteen tai tietovälineen antamista uudelle käyttäjälle, poistamista käytöstä tai leasing-laitteen vuokrasopimuksen päättymisen yhteydessä, ennen laitteen palautumista omistajalle, laitteet ja tietovälineet tulee tietoturvallisesti tyhjentää kaikesta henkilötiedosta. Laitteet tulee hävittää tietoturvallisesti.

Huom! CD/DVD-levyt on mahdollista hävittää myös tietoturvaluokan P4 (=salaiset asiakirjat) täyttävällä tietoturvatuhoajalla eli silppurilla, mikäli sellainen on käytettävissä.

Toimita käytöstä poistettavat tietotekniset laitteet ja tietovälineet HAMin ICT-vastaavalle. Mikäli tarvitset toimintatavoista lisätietoa, ota yhteyttä HAMin ICT-vastaavaan.

11. Tietoturvapoikkeamat ja niiden ilmoittaminen

11.1. Mikä on tietoturvapoikkeama?

Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena HAM Helsingin vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai käytettävyys on tai saattaa olla vaarantunut.

Tietoturvapoikkeamasta on kyse, jos esim.

- Tietojen salassapito tai luottamuksellisuus on vaarantunut.
- Ulkopuolinen on päässyt tietoihin.
- On havaittu haittaohjelma (esim. virukset, kiristyshaittaohjelmat, huijausviestit).
- Hallussasi oleva puhelin, tietokone, kulkulätkä, avain, dataa sisältävä tietoväline ym. on kadonnut.
- Henkilö- tai asiakastietoja on joutunut ulkopuolisen henkilön käsiin.

Esimerkkejä tietoturvapoikkeamasta:

- Mobiilipuhelin tai muu tallenteita sisältävä laite katoaa.
- Ulkopuolinen on saanut haltuunsa tunnukset sisäverkkoon tai sähköpostiin.
- Asiakkaalle on vahingossa lähetetty tai annettu toisen henkilön jäsentietoja.
- Asiakastä koskevia papereita on pöydällä tai avoimissa tietosuojasäiliöissä siten, että muu ulkopuolinen voi ne nähdä.
- Asiakaille lähetettäviä asiakirjoja katoaa tai varastetaan.

Tietoturvapoikkeamia voivat myös olla tietomurtojen, odottamattomien ja merkittävien käyttökatkosten tai www-sivujen luvattomien muutosten aiheuttamat häiriötilanteet.

11.2. Ilmoitusvelvollisuus ja toiminta ongelmatilanteessa

Ilmoita tietosuojaan liittyvistä epäilyistä, ongelmatilanteista ja havaitsemistasi uhkista ja suojauspuutteista HAMin ICT-vastaavalle. Muista ilmoittaa havaitsemasi ongelmatilanteet aina mahdollisimman pian! Tietoturvapoikkeamista, joihin liittyy henkilötietojen luottamuksellisuuden vaarantuminen, on HAMin ICT-vastaavaan. tehtävä ilmoitus valvontaviranomaisille ja rekisteröidyille **72 tunnin sisällä**. Siksi on erityisen tärkeää, että ilmoitat poikkeamatilanteet välittömästi, jotta asia ehditään selvittää riittävän varhaisessa vaiheessa.

11.3. Tietoturvapoikkeamien ilmoittaminen

Kaikki henkilötietojen tietoturvaloukkaukset, niiden vaikutukset ja korjaavat toimenpiteet dokumentoidaan reaaliaikaisesti. HAMin ICT-vastaava vastaa dokumentoinnista.

Jos henkilötietojen tietoturvaloukkaus on tapahtunut ja HAM on näiden tietojen osalta rekisterinpitäjänä, HAMin ICT-vastaava ilmoittaa siitä EU Tietosuoja-asetuksen artiklan 33 mukaisesti ilman aiheetonta viivytystä ja mahdollisuuksien mukaan **72 tunnin kuluessa** sen ilmitulosta toimivaltaiselle valvontaviranomaiselle (https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta), paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot toimitetaan vaiheittain ilman aiheetonta viivytystä.

Jos HAM toimii henkilötietojen käsittelijän ominaisuudessa, se ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.

Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille ja HAM Helsingin taidemuseo toimii näiden tietojen osalta rekisterinpitäjänä, HAMin ICT-vastaava ilmoittaa tietoturvaloukkauksesta rekisteröidylle EU Tietosuoja-asetuksen artiklan 34 mukaisesti ilman aiheetonta viivytystä.

HAMin ICT-vastaava vastaa yhdessä hallintojohtajan kanssa tietoturvapoikkeamien sisäisestä ja ulkoisesta viestinnästä. Tietoturvaloukkauksen tapahduttua HAMin ICT-vastaava yhdessä ICT palveluntoimittajan kanssa varmistaa tarvittavin lisätoimenpitein, että rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia loukkauksia ei todennäköisesti jatkossa tapahdu.

11.4. Epäilty haittaohjelmatartunta

Jos epäilet haittaohjelmatartuntaa, havaitsemalla esim.:

- Tietokoneen ja/tai tietoliikenneyhteyden selittämätöntä hidastumista tai toimintaa.
- Ylimääräisiä ääniefektejä.
- Näytölle ilmestyviä tunnistamattomia viestejä.
- Työaseman/palvelimen levytilan loppuvan yllättäen.
- Tiedostojen ja/tai viestien muuttumista tai katoamista.

Kirjaa mahdollisimman tarkasti havaintosi ja ongelman syntyä edeltävät toimenpiteesi. Ota yhteys HAMin ICT-vastaavaan.

Mikäli saat näytöllesi ilmoituksen/varoituksen tietokoneviruksesta (kun käsittelet jotain tiedostoa tai sähköpostiviestiä), kirjaa mahdollisimman tarkasti havaintosi ja em. ilmoituksen/varoituksen ilmestymistä edeltävät toimenpiteesi. Älä yritä korjata asiaa yksin, vaan ota yhteys HAMin ICT-vastaava

Jos joku (esim. työkaverisi tai ystäväsi) ottaa sinuun yhteyttä ja kertoo saaneensa sinulta (oudon) sähköpostiviestin ja mielestäsi et itse ole sitä lähettänyt, on todennäköistä, että työasemaasi on tarttunut jokin tietokonevirus tai on tehty osoitteen väärennys, jolloin lähettäjän kohdalla on sinun sähköpostiosoitteesi. Ota heti yhteys HAMin ICT-vastaavaan.

Jos koneellesi tulee virusvaroitus, älä lähetä saamaasi varoitusta muille HAM Helsingin taidemuseon henkilöstöön kuuluville, vaan ota yhteys HAMin ICT-vastaavaan.

Poista aina epäilyttävä sähköposti avaamatta sitä.

Siirrettävien tietovälineiden (esim. muistitikku/-kortti tai ulkoinen kova-/kiintolevy) käyttäminen on HAM Helsinginssa kielletty, mutta jos erillisellä luvalla työtehtäviin liittyen joudut niitä käyttämään, niin tarkista aina ulkoiset tietovälineet haittaohjelmien varalta ennen kuin avaat tiedostoja niiltä. Tarkastuksen voi tehdä Windowsin omalla Windows Defender-tuotteella tai F-securen antiviruksella.

Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa:

- Tietokonetta ei tarvitse sulkea, mutta irrota lähiverkkokaapeli työasemastasi ja sulje langaton verkkoyhteys (WLAN/ WI-FI).
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki.

- Ota yhteyttä HAMin ICT-vastaavaan.
- Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

11.5. Luvaton käyttö tai tietomurto (ns. hakkerointi)

Mahdollisissa tietomurtotilanteissa on tärkeää säilyttää maltti, toimia johdonmukaisesti ja pitää tieto aluksi suppean ryhmän piirissä (HAMin ICT-vastaava ja lähin esihenkilö). Tärkeää on myös pitää kirjaa tapahtumista ja tehdyistä toimenpiteistä (mitä havaitsi, missä ja milloin, mitä teki seuraavaksi ja keneen otti yhteyttä, yms.).

Alla on lueteltu muutama suuntaa antava tapahtuma, jotka voivat viitata tietomurtoon. Ilmoita heti havainnoista lähimmälle esihenkilöllesi ja HAMin ICT-vastaavalle.

- Työasemasi sisäänkirjautumisikkunassa on tuntematon käyttäjätunnus ja asiasta ei ole ilmoitettu etukäteen.
- Sisäänkirjautumisvaiheessa tulee ilmoitus, että käyttäjätunnus on lukittu ja mielestäsi et ole tehnyt epäonnistuneita kirjautumisyrityksiä itse.
- Kotihakemistoon/muuhun hakemistoon on ilmestynyt uusia tiedostoja, kadonnut tiedostoja tai joitain tiedostoja on muutettu ja mielestäsi et ole niitä itse tehnyt.
- Sähköpostilaatikossa on tiettyjä sähköpostiviestejä kadonnut.
- Havaitset järjestelmissä/sovelluksissa jotain muuta outoa tai epäilyttävää.

11.6. Uudet tietoturvauhat ja trendit

Tekoalyn (tukiälyn) käyttö työnteossa on aina mahdollinen tietoturvauhka. Esimerkiksi chattibotit ja virtuaaliavustajat kuten ChatGPT, Grok yms. ovat nousseet suuren suosioon viime aikoina. Suositus on, että näille palveluille ei syötetä organisaatioon tai asiakkaisiin liittyvää tietoa tai varsinkaan mitään luottamuksellista, arkaluonteista tai salassapidettävää tietoa. Turvallisinta on käyttää näitä palveluita API rajapinnan kautta, jotta tieto pysyy organisaation hallussa. Tämä koskee AI-ympäristöjä yleisesti.

Chat GPT:n sijaan suositellaan käytettäväksi joko Copilot M365 sovellusta tai jotakin muuta Ms Copilot sovellusta, kunhan sovellukseen ollaan kirjautuneena omilla Microsoftin käyttäjätunnuksilla. Sovellukseen tulee silloin käyttäjän kuvan yhteyteen vihreä teksti ”suojattu” tai vastaava merkintä.

Toinen uudentyyppinen tekoälyuhka on ns. syvävääreennös (deepfake). Tekoälyn avulla voidaan luoda kuvaa tai ääntä joka vaikutta aidolta. Esimerkiksi syvävääreennetyt puhelut, jossa pyydetään rahaa tai pankkitietoja, ovat yleistyneet. Tämän tyyppiset uhat ovat harvinaisia, mutta tietoisuus näistä auttaa olemaan varuillaan.

Lista HAM Helsingissä hyväksytyistä työkaluista (muiden käyttö johtoryhmän luvalla):

1. **Microsoft M365 Copilot**, jota voi käyttää sisäisenä tukiälynä, kunhan varmistaa, että on aina kirjautuneena palvelun tai apin sisään omilla Microsoft tunnuksilla tietoturvan varmistamiseksi.

Minkään muun teköälysovelluksen käyttö työasioihin ilman HAM Helsingin taidemuseon lupaa on kielletty. Sovellukset evaluoidaan ja niiden turvallisuus varmistetaan ennen käytön sallimista. Käytön sallimisen jälkeenkään ei ohjelmiin tule syöttää mitään HAM Helsingin taidemuseoon tai asiakkaisiin liittyvää tietoa.

Loppukäyttäjillä on aina vastuu tekoälyn tuottaman sisällön oikeellisuuden arvioimisesta ja sen hyödyntämisestä.

12. Lisätietoja

Tämän ohjeen lisäksi tietoa tietoturvallisuudesta on saatavissa mm. HAM Helsingin intranetistä.