

TOIMINTAOHJEISTUS

Toimintaohjeistuksissa mainittu ICT-hallinto tarkoittaa ICT-johtajaa ja/tai ICT-päällikköä.

Tietoturvaohjeet

Jokainen Puumerkin työntekijä on velvollinen huolehtimaan tietoturvasta. Yhtiön kokonaisturvallisuus muodostuu jokaisen henkilöstöön kuuluvan vastuullisen toiminnan kautta.

Noudata tietoturvaohjeita ja yleistä huolellisuutta tietoturva-asioissa. Vaikka tietoturva mielletään vahvasti tietotekniikkaan, kattaa se kaiken tiedonkäsittelyn osa-alueet: tulosteet, kopiot, arkistoinnin, hinnastot, suullisen viestinnän jne. Tietoturvallisuus on tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä. Tunnistamalla vaaratilanteet, osaat toimia oikein. Etätyön lisääntyessä yleisten ohjeiden lisäksi on jokaisen syytä huomioida myös etä- ja liikkuvan työn mukanaan tuomat erityispiirteet.

Työasema ja mobiili tietoturva

- Älä anna ulkopuolisten kurkkia olkasi yli, äläkä jaa ruutunäkymääsi, kun käsittelet arkaluonteisia tietoja tai syötät käyttäjätunnuksia ja salasanoja.
- Kirjaudu ulos työasemasta aina, kun poistut työasemalta ja kun lopetat työskentelyn, sulje myös ohjelmat ja sammuta työasema. Tällä varmistetaan samalla työasemasi eheys.
- Selvitä tiedon ja tiedoston alkuperä ennen käyttöä. Älä liitä koneeseen tallennusvälineitä (muistitikku, ulkoinen kiintolevy tai muita USB-laitteita), joiden sisällöstä et ole varma.
- Älä koskaan avaa tuntemattomasta lähteestä tullutta liitetiedostoa. Viesti, joka on tullut tuntemattomasta lähteestä voi sisältää myös viruksia.
- Suhtaudu ladattuihin tiedostoihin varovaisesti. Tietokoneille ei saa asentaa tai yrittää asentaa omia sovelluksia itse. Kaikki asennukset tapahtuvat IT-tuen toimesta.
- Vieraile vain sellaisilla verkkosivuilla, joiden turvallisuuteen voit luottaa.
- Säilytä käyttämäsi tallennusvälineet turallisessa paikassa. Tallenna tekemäsi työ käyttäen välitallennusta pitkissä työvaiheissa tai hyödynnä ohjelmien automaattista tallennusta. Älä jätä keskeneräistä työtä näytölle.
- Jos sinun ei tarvitse jakaa tiedostojasi ja/tai kansioitasi, älä jaa niitä.
- Huolehdi kannettavan tietokoneesi fyysisestä turvallisuudesta – älä jätä sitä esimerkiksi näkyviin auton takaistuimelle ja pidä huoli muutenkin laitteidesi fyysisestä sijainnista!

- Älä hätäile tai toimi hätiköidysti, kun huomaat jotain tietoturvaongelmiin viittaavia oireita. Tietoturvaan liittyvissä asioissa/ongelmissa voit aina ottaa yhteyttä IT-tukeen.

Etätyöhön liittyvät erityispiirteet ja niihin liittyvät tietoturvaohjeet

Jos olet ulkoverkossa (hotelli, lentokenttä, juna yms.) käytä aina VPN-yhteyttä tai muodosta yhteys omalla mobiililla.

Julkisilla paikoilla, käytä aina tietoturvasuojaa näytöllä.

Jos osallistut etäpalaveriin julkisissa paikoissa, huomioi ympäristö ja näkö- sekä kuuloetäisyydellä olevat ihmiset.

Myös kotona, mökillä työasema tulee lukita työpisteeltä poistuessa.

Yrityksen henkilökohtaiseen käyttöön luovutettuja käyttäjätunnuksia ja salasanoja ei saa käyttää julkisissa työasemissa tai laitteista. Esimerkiksi kirjaston tietokoneista ei saa kirjautua yrityksen tunnuksilla.

Käyttäjätunnukset ja salasanat

Käyttäjätunnukset ja salasanat ovat aina henkilökohtaisia. Niitä ei saa, tai niillä aktivoitua järjestelmää, luovuttaa toisen käyttöön, ei edes yhtiön henkilöstöön kuuluvalle.

Käytä hyvää salasanaa (riittävän pitkä, sisältää kirjaimia, numeroita ja erikoismerkkejä). Paras salasana on seipitetty merkkijono (esimerkiksi lyhennelmä lauseesta, jota et unohda, kuten "4Le4i4ct4est" sanoista "alea iacta est"). Älä käytä tätä esimerkki salasananä!

Käytä eri järjestelmissä eri salasanaa. Vaihda salasana riittävän usein (3 kk).

Syötä oma salasanasi vain koneelta, johon tai jonka omistajaan luotat. Koneessa käyttämäsi ohjelmat voivat tietämättäsi tallentaa salasanasi koneeseen, josta joku toinen voi myöhemmin saada kaivettua sen esille.

Tietoliikenneverkkojen käyttö

Yhtiön verkkoa voi käyttää langattoman lähiverkon, VPN:n tai tietoliikenneportin avulla. VPN- ja langattoman lähiverkon tunnuksina toimii henkilölle luovutettu tunnusyhdistelmä, jolla kirjaututaan myös tietokoneelle. Tietoliikenneporttia käytettäessä tunnistus tapahtuu automaattisesti. Yhtiön verkkoon saa kytkeä vain yhtiön käyttäjälle luovuttamia laitteita. Esimerkiksi omaa siviilipuhelinta ei saa kytkeä yhtiön langattomaan verkkoon, vaan siihen tulee käyttää vierasverkkoa.

Vieraille on toimistoilla käytössä langaton lähiverkko, joka ei ole yhteydessä yrityksen tietoliikennejärjestelmiin. Vierasverkkoon on omat tunnukset, jotka voi luovuttaa vierailun ajaksi käyttöön.

Tulostus ja sen ympäristö

Tulosteet, kopiot, skannatut asiakirjat on noudettava laitteelta välittömästi. Asiakirjojen tietoturvalliseen tuhoamiseen käytetään tietoturva-astioita, joita on yksi kappale jokaisessa toimipisteessä.

Monitoimilaitteet ovat tarkoitettu työhön liittyvään tulostamiseen. Laitteiden käyttö henkilökohtaisiin tarpeisiin on kielletty.

Yhteiskäyttölaitteet

Yhtiöllä on käytössä työn suorittamiseen liittyviä yhteiskäyttölaitteita, kuten trukkipäätteitä, matkapuhelimia, radiopuhelimia sekä työasemia. Näitä käytettäessä on noudatettava erityistä huolellisuutta, niin ICT-hallinnon kuin käyttäjien taholta. Ko. laitteiden käyttö on sallittu vain työtehtävien suorittamiseen. ICT-hallinto monitoroi laitteita ja varmistaa näin niiden asianmukaisen käytön.

Laitteiston sekä ohjelmistojen elinkaaren hallinta

ICT-hallinto vastaa työntekijöiden vakioituista työvälineistä ja niiden hankinnasta sekä rajaa käytettävän laitemalliston normaaliin työkäyttöön soveltuvaksi. Kaikki laitteet hankitaan IT-tuen kautta.

Työntekijöiden toimenkuvan mukainen henkilökohtainen peruslaitteisto kattaa: kannettavan tietokoneen (nykyiset kiinteät työasemat korvataan kannettavilla uusiutumisen yhteydessä), telakan, hiiren, näppäimistön, kuulokkeet ja näytön. Näyttöjen lukumäärä määräytyy toimenkuvan mukaan, kuitenkin maksimissaan 3 näyttöä per käyttäjä. Käyttäjällä ei voi olla kahta työkonetta.

Matkapuhelin ja tabletit: laitteiden käyttöjärjestelmä on Android, laitteissa on suojakuori ja panssarilasi. Lisävarusteet toimenkuvan mukaan: tarvittaessa matkalaturi ja handsfree-kuuloke. Puhelinmallit ovat vakioituja.

Laitteiden vähimmäiselinkaaret: kannettavat 48-60 kk ja matkapuhelimet 24-36 kk. Liittymissä on oletuksena dataliikenteen esto ulkomailta (ei EU) ja 50 € saldovahti. Yli 50 € puhelinlaskut käsitellään esimiehen kanssa, ja yli 150 € puhelinlaskut raportoidaan ICT-johtajalle sekä esimiehelle. Käyttäjällä voi olla vain yksi puhelinliittymä yhtiön puolesta. Langattoman verkon ulkopuolella verkko jaetaan ensisijaisesti matkapuhelimesta. Jos toimenkuva edellyttää, erillinen dataliittymä esimiehen suosituksesta ja ICT-hallinnon hyväksynnällä mahdollinen.

Puhelimien ja liittymien tarkemmat ohjeet on kuvattu omassa liitteessään ja voimassa olevat ohjeet löytyvät: [Intranet: henkilöstö – puhelin- ja liittymäohjeet](#).

Laitteiden uusiminen ja käytöstä poisto

Työlaitteet voidaan uusia lasketun elinkaaren päättyessä. Mikäli työlaite halutaan korvata ennen lasketun elinkaaren päättymistä, tulee tästä neuvotella ICT-hallinnon kanssa.

Käyttäjän rikkoessa työvälineensä on jäännösarvon korvausvelvollisuus käyttäjällä. Esihenkilö voi kuitenkin päättää laitteen korvaamisesta, ja päätöksessä otetaan huomioon ns. huolimattomuus-aspekti.

Käytetyistä ja poistettavista laitteista tulee aina raportoida heti ICT-hallinnolle sähköpostilla, joka hoitaa niiden hallitun poistamisen järjestelmistä ja fyysisen tietoturvallisen hävittämisen.

Laitteen uusimisen yhteydessä työntekijä vastaa vanhan laitteen palauttamisesta Keravalle. Koskee puhelimia, työasemia ja tallennusmedioita (kovalevyt, muistitikut, muistikortit).

Työsuhteen päättyessä:

- Esihenkilö täyttää työsuhteen päättymisilmoituksen intrassa HR-sivuilla.
- ICT-Hallinto sulkee hallinnassaan olevat käyttäjätilit sekä sulkee puhelin- ja dataliittymät kulloisenkin sopimusmallin mukaisesti.
- Käyttäjän esihenkilö vastaa työntekijöidensä laitteiden palauttamisesta Keravalle työntekijän työsuhteen päättyessä.

Käytöstä poistetut työasemat, puhelimet ja tallennusmediat tai niihin verrattavissa olevat laitteistot tietoturvataan ja uudelleen sijoitetaan tai hävitetään asianmukaisesti ICT-Hallinnon toimesta.

Ohjelmistot

Yhtiö tarjoaa toimenkuvan vaatimuksen mukaiset ohjelmistot työntekijöille. Perusohjelmiston rungon muodostavat ERP-järjestelmät, MS O365 -ohjelmistopaketti (Outlook, Excel, Powerpoint, Word, Teams, Power BI apps, Forms, OneDrive, OneNote, Yammer, Sharepoint). Mikäli työntekijän toimenkuva edellyttää muiden kuin edellä mainittujen ohjelmien käyttöä, esihenkilö lähettää hankintapyyntöön hyväksyttäväksi ICT-hallinnolle.

ICT-hallinto vastaa ohjelmistojen ajantasaisuudesta ja tietoturvasta.

Käytössä olevat partnereiden tarjoamat palvelut ja niiden ohjelmistot (M2, Exflow, Sympa, Atlantis, Kuljetus Velho) asennetaan käyttäjille käyttötarpeeseen perustuen.

Yleiset laitehankinnat

Yleisillä laitehankinoilla tarkoitetaan väliaikaisia, rakenteita vahvistavia ja nopean tarpeen hankintoja. Nämä toteutetaan aina ICT-hallinnon toimeksiannosta tarvelähtöisesti.

Muut turvajärjestelmät

Yhtiöllä on käytössään kulun-, työajan- ja kameravalvontajärjestelmät, palo- ja murtohälytysjärjestelmät sekä kiinteistöautomaatiojärjestelmiä. Näihin mahdollisesti liittyy henkilöstön velvoitteita.

Työntekijöille luovutetut näihin järjestelmiin liittyvät ohjaimet (ns. "lutikat"), käyttäjätunnukset, salasanaat ovat aina henkilökohtaisia. Ohjaimet, käyttäjätunnukset ja salasanaat tulee säilyttää siten, etteivät ne ole muiden käytettävissä.

Jos henkilö kadottaa?

Toimintaympäristöt

Ympäristöistä ICT-hallinto ylläpitää ajantasaisia arkkitehtuurikuvauksia.

Verkkoinfrastrukturi

Koostuu verkko-omaisuudesta, palvelimista, tietoliikenneyhteyksistä ja niiden oheislaitteista. ICT-hallinnolle kuuluu ylläpitää, päivittää ja valvoa näiden ajantasaisuutta ja huolehtia kokonaisuuden toimivuudesta sekä sen suojauksesta. Verkkoinfrastruktuuria päivitetään yhtiön liiketoimintatavoitteiden pohjalta.

Järjestelmäinfrastrukturi

ICT-hallinnon tehtävänä on huolehtia yhtiön tiedon eheydestä ja luotettavuudesta olemassa olevien järjestelmien puolelta ja edesauttaa henkilöstöä käyttämään niitä oikein. Yhtiön järjestelmäinfrastruktuurin rakenne toteutetaan mahdollisimman kustannustehokkaasti, synergiaedut huomioiden yhtiön liiketoimintatavoitteiden pohjalta.

Käyttöoikeuspolitiikka

Eri järjestelmien pääsy- ja käyttöoikeuspolitiikalla ohjataan tietoturvallisuutta toimenkuvaan perustuen työntekijöiden tarpeet huomioiden.

IT-palvelujen väärinkäytön seuraamukset

Tietotekniikkarikkomuksina pidetään yhtiön tietojärjestelmien käytöstä annettujen sääntöjen tai määräysten vastaista toimintaa tai tietojärjestelmien käyttöä Suomen lakien vastaisesti.

Tämä toimintaohje kuvaa toimenpiteitä, joita henkilöön voidaan kohdistaa, kun tietotekniikkarikkomus on havaittu tai sitä on perustellusti syytä epäillä. Toimenpiteet on jaettu käyttövaltuuksien rajoituksiin rikkomuksen selvitystyön ajaksi sekä mahdollisiin rikkomuksesta määriteltäviin seuraamuksiin.

Yhtiö voi rajoittaa IT-palveluiden käyttövaltuuksia selvitystyön ajaksi. Rajoituksista päätetään, kun tietotekniikkarikkomus on havaittu tai sitä epäillään. Valtuuksia rajoitetaan aina, kun perustelluista syistä epäillään, että käyttäjä on syyllistynyt väärinkäyttöön, ja on mahdollista, että käyttövaltuudesta on haittaa rikkomuksen selvittämiseksi tai vahinkojen minimoimiselle. Käyttäjälle

varataan mahdollisuus päästä kuultavaksi ja vakavammissa tapauksissa käyttäjä kutsutaan kuultavaksi.

Käyttövaltuuksien rajoittamisesta päättää ICT-hallinto. Rajoittamisen toteuttaa palvelun ylläpitäjä.

Kiireellisissä tapauksissa ylläpitäjä voi omalla päätöksellään rajoittaa käyttövaltuuksia enintään kolmeksi päiväksi, mistä tulee välittömästi ilmoittaa ICT-hallinnolle.

Tarvittaessa käyttäjän työasema voidaan kytkeä irti verkosta.

Rajoitukset puretaan selvitystyön päätyttyä, jos käyttövaltuuksien palauttamisesta ei ole ilmeistä haittaa.

Seuraamukset

Lievissä tapauksissa käyttäjälle huomautetaan asiattomasta toiminnasta.

Tietotekniikkarikkomuksen seurauksena käyttäjä voi olla korvausvastuussa väärinkäyttämistään resursseista (esim. palvelimet tai tietoverkko), välittömistä vahingoista ja väärinkäytön selvitystyön aiheuttamista kustannuksista.

Seuraamukset työntekijälle

Henkilökuntaa koskevia seuraamuksia voivat olla yhtiön työoikeudelliset toimet (kirjallinen varoitus, irtisanominen, työsuhteen purku) sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Käyttövaltuudet yksittäisiin järjestelmiin voidaan väärinkäytöksestä johtuvan luottamuspuolan synnyttyä evätä määräajaksi tai pysyvästi. Käyttövaltuuksiin kohdistuvista toimista päättää ICT-hallinto.

Seuraamukset muille käyttäjille

Yhtiöön kuulumattomia käyttäjiä (partnereille, asiakkaille, toimittajalle annetut rajapinnat) koskevat seuraamukset voivat olla käyttövaltuuksien poistaminen tai rajoittaminen sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Käyttövaltuudet yksittäisiin järjestelmiin voidaan väärinkäytöksestä johtuvan luottamuspuolan synnyttyä evätä määräajaksi tai pysyvästi. Käyttövaltuuksiin kohdistuvista toimista päättää ICT-hallinto.

Esimerkkejä IT-palvelujen väärinkäytöksistä

- Rikoslain ja tekijänoikeuslain alaisen materiaalin oikeudeton käsittely.



PUUMERKKI

TOIMINTAOHJE PUUMERKKI GROUP
Tieto- ja viestintätekniikka

**ICT (Information and Communication
Technology)**

4.3.2021

- Rikoslain alaista materiaalia ovat esimerkiksi lapsiporno, eläimiin sekaantuminen, raaka väkivalta, rasistinen aineisto ja kansankiihottamismateriaali, käsittelyä ovat mm. materiaalin levittäminen ja hallussapito.
- Tekijänoikeuslain alaista materiaalia ovat esimerkiksi musiikki, videot, sarjakuvat, elokuvat, pelit ja ohjelmistot.
- Tunnuksen luovuttamista on esimerkiksi: salasanan kertominen toiselle käyttäjälle, tietokoneen auki jättäminen niin, että toinen henkilö pääsee käyttämään toisen tunnusta.
- Tiedon luottamuksellisuuden vaarantamista on esimerkiksi: salassa pidettävän tai muutoin lain suojaa nauttivan tiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä (esimerkiksi palvelinten käyttäjätietojen luovutus), salassa pidettävän tiedon tietoturvan laiminlyönti (passiivista toimimattomuutta), tahalliset salassapitorikokset (aktiivista toimintaa), henkilötietolain rikkominen.
- Henkilökohtaisen tietoturvan laiminlyöntiä on esimerkiksi: salasanan jättäminen näkyviin, yhtiön varmuuskopiointikäytäntöjen laiminlyöminen.

Puumerkin johtoryhmälle raportoidaan 2 kertaa vuodessa

- Hankintarajan poikkeamat
- Ennen elinkaaren loppua tehdyt hankinnat
- Laiterikot
- Kaikki väärinkäytökset poikkeuksesta