

PK-yrityksen tietoturvallisuustarkastus

Tietokoneet ja muut tietojenkäsittelyyn tarkoitetut laitteet sisältävät yleensä yrityksen toiminnan kannalta erittäin kriittistä tietoa. Tämän tiedon oikeellisuus, käytettävyys tarvittaessa ja luottamuksellisuus voi olla yrityksen toiminnan kannalta sen elinehto. Tiedot ja järjestelmät tulee suojata monelta eri uhkatekijältä, varmistaa toiminnan lainmukaisuus sekä varautua siihen, että kaikesta huolimatta jotain voi sattua. Oheisessa tarkastuslistassa on lueteltu pienen ja keskisuuren yrityksen tärkeimpiä tietoturvallisuustarkastuskohteita:

TOIMENPIDE	Kunnossa	Parannettavaa
Vastuut ja ilmoitukset		
Tietoturvallisuuden kehittäminen ja koordinointi on vastuutettu yrityksessä. Myös laitteilla ja järjestelmillä on nimetyt vastuuhenkilöt.	☐	☐
Kaikkien yrityksessä työskentelevien kanssa on käyty lävitse organisaation tietoturvallisuusohjeet ja korostettu niiden noudattamista.	☐	☐
Työntekijöitä on ohjeistettu henkilötietojen keräämisestä: Henkilötietojen tietolähteenä on pääsääntöisesti oltava henkilö itse. Muualta tietoja saa kerätä / tarkastaa vain henkilön suostumuksella.	☐	☐
Henkilötietolain edellyttämät rekisteriselosteet ovat saatavilla toimipisteessä. Jos tiloissa on (tallentava) kameravalvonta, on siitä ilmoitettu näkyvästi ja myös tästä on laadittu henkilörekisteriseloste.	☐	☐
Luottamuksellisen tiedon käsittely		
Luottamuksellista tietoa (paperista tai sähköistä) saavat käsitellä vain ne, jotka tietoa tarvitsevat ja joilla on siihen oikeus.	☐	☐
Luottamuksellisen tiedon käsittelyyn, säilytykseen ja luovutukseen on laadittu ohjeet.	☐	☐
Henkilötietoja ja muuta luottamuksellista paperimuodossa olevaa aineistoa säilytetään lukituissa tiloissa (lukituissa kaapeissa tai työhuoneissa).	☐	☐
Luottamuksellista sähköistä tietoa säilytetään käyttöoikeuksiltaan rajatussa verkon hakemistossa, tunnistautumisen vaativassa järjestelmässä tai <u>salakirjoitetulla</u> muistivälineellä (USB-tikku, kannettava tietokone, ulkoinen kiintolevy).	☐	☐
Asiakastilanteissa nähtävillä pidetään vain asiakasta itseään koskeva aineisto.	☐	☐
Henkilöstöä on ohjeistettu välttämään työasioista keskustelemista sekä puhumasta työpuheluja julkisilla paikoilla tai ulkopuolisten läsnä ollessa.	☐	☐

TOIMENPIDE	Kunnossa	Parannettavaa
Puhelimitse tai sähköisesti asioitaessa pyritään varmistamaan vastapuolen henkilöllisyys.	☐	☐
Arkaluonteisia tai luottamuksellisia tietoja, kuten henkilötunnusta ja terveystietoja ei välitetä puhelimitse varmistumatta kysyjän oikeudesta tietoihin. Sähköpostitse näitä tietoja ei lähetetä lainkaan.	☐	☐
Henkilötietoja tai muuta luottamuksellista aineistoa siirretään toimitilojen ulkopuolelle vain salattuna ja vain välttämätön määrä.	☐	☐
Poistettavia, luottamuksellisia tietoja sisältävät tietovälineet tuhoetaan turvallisesti. Paperit ja kalvot silputaan; kiintolevyt, nauhat ja muistitikut murskataan fyysisesti tai ylikirjoitetaan luotettavilla ohjelmilla.	☐	☐
Tietojen varmistaminen		
Henkilökohtaisilta tietokoneilta varmistetaan tärkeät tiedot mahdollisimman pian verkkopalvelimille.	☐	☐
Kriittisestä ja toiminnan kannalta olennaisista tiedoista otetaan täysvarmistukset säännöllisesti vähintään kerran viikossa. Muuttuneet tiedot varmistetaan vähintään kerran päivässä. Ohjelmat aina muutosten jälkeen.	☐	☐
Varmistaminen on vastuutettu henkilöille, joilla on riittävä osaaminen asiaan. Varmistajalla on varahenkilö poissaolojen tai lomien ajaksi.	☐	☐
Tietojärjestelmien lokerista tai tallenteista varmistetaan, että varmistettu tieto on todella siirtynyt varmistusvälineelle (nauhat, USB-kiintolevyt).	☐	☐
Varmistusvälineitä vaihdetaan viikoittain siten, että koko ajan on tallessa useamman ajanhetken aineisto. Esimerkiksi tämän viikon, edellisen viikon ja edellisen kuun vaihteen tilanne..	☐	☐
Varmistetun aineiston palauttamista varmistusvälineeltä tietojärjestelmiin testataan ainakin osalla aineistoa säännöllisesti, esimerkiksi kerran kuukaudessa.	☐	☐
Varmistetut tiedot siirretään vähintään kerran viikossa lukittuun tilaan toiseen rakennukseen tai samassa rakennuksessa vähintään DIS 60 - luokiteltuun dataturvakaappiin.	☐	☐
ATK-laitteiden käyttö ja suojaus		
Toimipaikan laitteita (myös asiakaspisteiden laitteet) käytetään vain työtehtävien hoitoon. ATK- ja tietoliikennelaitteisiin ei saa kytkeä kuin yrityksen omia tai yrityksen käyttöönsä hyväksymiä oheis- ja lisälaitteita.	☐	☐
Kriittisten laitteiden rikkoontumisen varalta on olemassa tai nopeasti saatavissa nopeasti käyttöön saatava varalaitte tai toimintaa voi muuten jatkaa varamenettelyillä (esimerkiksi manuaalisesti).	☐	☐
Toimipaikan kaikissa tietokoneissa on ajantasainen virustorjunta, vakoojaohjelmien torjunta sekä viimeisimmät toimivat tietoturvapäivitykset.	☐	☐
Yrityksen sisäverkko on erotettu julkisista verkoista (mm. internet) asian tuntijan asentamalla palomuurilla. Tarpeeton liikenne estetään. Palomuuriasetukset tarkastetaan vähintään kerran vuodessa.	☐	☐
Langattomat yhteydet (WLAN) on salakirjoitettu riittävän vahvasti (esim. WEP128 tai WPA-/WPA2 –suojausella).	☐	☐
Työasemat lukitaan tai ne lukittuvat automaattisesti 15 minuutin sisällä, kun niillä ei työskennellä.	☐	☐
Työaseman ja järjestelmien salasana ovat henkilökohtaisia ja vaikeasti arvattavia. Pituus on mieluummin yli 8 merkkiä. Salasanoja ei saa paljastaa muille ja ne on vaihdettava säännöllisesti vähintään 3 kk välein.	☐	☐

TOIMENPIDE	Kunnossa	Parannettavaa
Asiakaspalvelutiloissa olevat tai muuten helposti mukaan siepattavat (esim. kannettavat) ATK-laitteet lukitaan kiinni rakenteisiin esimerkiksi tarkoituksiin varatuilla kaapeleilla.	☐	☐
Tärkeimmät ATK-laitteet (esim. palvelimet, tietoliikennelaitteet) on varustettu riittävän akustokapasiteetin omaavilla, katkemattoman virransyötön takaavilla UPS-laitteilla tai varavoimalla.	☐	☐
Kriittiset laitteet osaavat ajaa itsensä turvallisesti alas sähkönsaannin estyessä.	☐	☐
Tietotekniset laitetilat on varustettu riittävällä jäähdytyksellä, ilmanvaihdolla sekä lämpötilan muutoksesta varoittavalla etähälytyksellä laiterikkojen varalta.	☐	☐
Toimitilojen fyysinen suojaus		
Toimitilat pidetään lukittuina ja ikkunat suljettuina, kun tiloissa ei oleskella.	☐	☐
Takaovet ja valvomattomat ulko-ovet (muut kuin asiakaspalvelutilan ovet) pidetään jatkuvasti lukittuina.	☐	☐
Toimitilan kaikissa ulko-ovissa on käyttölukko sekä varmuuslukko, jotka pidetään lukossa, kun tiloissa ei oleskella.	☐	☐
Toimitilan avaimista pidetään kirjaa. Katoamistapauksessa ulko-ovien ja kriittisten tilojen lukot vaihdetaan välittömästi. Muut lukot tarvittaessa.	☐	☐
Toimitiloissa on käytössä rikosilmoitinlaitteisto, jonka kytkemisestä on sovittu henkilöstön kanssa tai joka kytkeytyy automaattisesti tiettyinä kellonaikana. Hälytinalaite hälyttää 24 h päivystävään vartiointiliikkeeseen.	☐	☐
Rikosilmoitinlaitteiston valvonta-alue kattaa tärkeimmät kulkureitit ja arvoomaisuuden. Laite hälyttää ovien avauksesta ja tiloissa liikkumisesta.	☐	☐
Tiloissa kulkeminen on valvottua. Asiakkaat, vieraat ja muut kävijät pääsevät liikkumaan tiloissa vain rajatusti ja valvotusti. Kriittisissä tiloissa vieraat liikkuvat saatettuna.	☐	☐
Palvelimet ja muut tärkeät tietotekniset laitteet (kytkimet, reitittimet, palomuurilaitteet, mahdolliset varmistuslaitteet) on sijoitettu omaan, tarkoitusta varten varattuun ja lukittuun tilaan.	☐	☐
Erityisesti tietoteknisiä laitteita sisältävien tilojen kaapeli- ja putkiläpiviennit on tiivistetty luokitelluilla palokatkotuotteilla (esimerkiksi massat) mahdollisessa palotilanteessa savukaasujen ja noen leviämisen estämiseksi.	☐	☐
Kaikki tietotekniset laitteet sähkö- ja datakaapelointineen on nostettu vähintään 10 cm korkeuteen lattiatasolta vuotovahinkojen välttämiseksi.	☐	☐
Tietoteknisissä tiloissa on lattialla päivystäjälle hälyttävä vuotoilmaisin.	☐	☐
Toimitiloissa on paloilmoinninalaiteeseen tai rikosilmoitinjärjestelmään kytketyt savuilmaisimet palon havaitsemiseksi.	☐	☐
Toimitiloihin on varattu riittävästi esteettömästi sijoitettua ja merkittyä, määrääjain huollettua alkusammutuskalustoa. (Vähintään yksi 6 kg sammutin / kerros sekä sammutuspeite keittiötiloihin). Atk- ja sähkölaitteiden läheisyydessä oleva sammutin tulisi olla 5 kg hiilidioksidisammutin (CO2).	☐	☐
Henkilöstölle on opastettu hälyttimien ja sammutusvälineiden sijoitus ja oikea käyttö.	☐	☐