Yrityksen tietoturvapolitiikka

Ohje

Oy Yritys Ab

**Yrityksen tietoturvapolitiikka**

Tässä politiikassa tietoturvalla tarkoitetaan tiedon luottamuksellisuuden, eheyden ja käytettävyyden varmistamista sen esitys- tai käyttötavasta riippumatta. Tämä politiikka määrittelee tietoturvan perusvaatimukset ja luo pohjan politiikan mukaisen toiminnan suunnittelulle ja jalkauttamiselle. Politiikan läpiviennin tukemiseksi on lisäksi laadittu tarkempaa ohjeistusta tietoturvan ja -suojan eri osa-alueille allaolevan taulukon mukaisesti Tietoturvapolitiikka velvoittaa yrityksen koko henkilökuntaa kaikissa toimintamaissa.

Tietoturvallisuutta toteutetaan ja kehitetään riskiperusteisesti käyttäen tarkoituksen-mukaisia, laadukkaita ja kustannustehokkaita ratkaisuja. Tietoturvapolitiikan tarkoituksenmukaisuutta arvioidaan riskienhallinnan ohjausryhmässä vuosittain. Tietoturvapolitiikka on keskeinen osa hyvää hallinnointitapaa (Corporate Governance).  Tämä ohje on osa yrityksemme hallinnollista tietoturvaa.

**Tavoite**

Tietoturvan ensisijaisena tavoitteena on yrityksen toimintojen jatkuvuuden turvaaminen kaikissa olosuhteissa. Tarkoituksenmukainen ja tehokas tietoturva yhdessä henkilöstöosaamisen kanssa mahdollistavat yrityksen toimintoihin liittyvien ICT-ratkaisujen käytettävyyden sekä prosesseissa, rekistereissä ja palveluissa käytettävien tietojen eheyden ja luottamuksellisuuden kaikissa olosuhteissa. Tietoturva mahdollistaa tietosuojan toteutumisen.

Yrityksessämme henkilötietojen turvaaminen on olennainen osa vastuullista toimintaa, jota sekä asiakkaamme että yhteistyökumppanimme odottavat meiltä. Digitaalisuuden kasvun myötä tietoturvallisuutta säännellään enenevässä määrin myös lainsäädännöillä.

**Osiot**

Olemme jakaneet tämän tietoturvapolitiikan kymmeneen eri osa-alueeseen, jotka ovat:

1. Fyysinen tietoturva 6. Luottamuksellista tietoa sisältävät laitteet

2. Vierailijakäytännöt 7. Sosiaalinen media

3. Etätyö 8. Tietoturvarikkomukset

4. B.Y.O.D. -käytännöt 9. Salasanapolitiikka

5. Sähköpostikäytännöt 10. Sidosryhmäkäytännöt

# Fyysinen tietoturva

Yrityksen toimitilojen sekä niissä sijaitsevien laitteiden suojaamista kutsutaan yleisesti nimellä fyysinen turvallisuus. Esimerkiksi tärkeitä tietoja sisältävän palvelimen eheyttä, luottamuksellisuutta ja saatavuutta ei voida varmistaa, mikäli se ei ole fyysisesti turvattu.

Fyysinen uhka, kuten tulipalo, saattaa tuhota tietokoneita tai varmuuskopioita. Palo-, vesi- tai sähkövahingoilta suojautuminen on tärkeässä osassa kokonaisvaltaisen tietoturvan hallintaa. Myös inhimilliset uhat, kuten varkaudet ja ilkivalta, tulee ottaa huomioon.

Fyysisen turvallisuuden tarkistuslista

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Toimitilojen kulunvalvonta |  |
| Vartiointi ja hälytysjärjestelmä |  |
| Työasemien murtosuojaus |  |
| Palvelintilojen ja laitekaappien fyysinen suojaus |  |
| Turvamerkintä |  |

Fyysinen turvallisuus muodostaa tietoturvallisuuden kivijalan ja ilman sitä hallinnolliset ja tekniset turvaratkaisut menettävät tehojaan.

# Vierailijakäytännöt

Oman henkilöstön lisäksi yrityksen toimitiloihin voi tulla vieraita kaupallisessa tarkoituksessa tai erilaisissa huolto- ja korjaustehtävissä. Tällaisissa tapauksissa vierailulla pitää aina olla yrityksemme edustajana "vierailun isäntä", joka vastaa siitä että vieras ei pääse näkemään salassa pidettävää tietoa, johon tällä ei ole oikeutta. Arkinen esimerkki tällaisesta on mikä tahansa yrityksemme hallussa oleva henkilötieto.

## Asiakirjaturvallisuus

Jokainen yrityksen toimihenkilö vastaa omalta osaltaan hyvästä asiakirjakäsittelytavasta. Lähtökohta asiakirjaturvallisuuden järjestämisessä on se, että turvallisuusluokitellun aineiston määrä minimoidaan. Erityisiä henkilötietoja sisältävien asiakirjojen kanssa on noudatettava huolellisuutta.

Asiakirjaturvallisuuden merkitys kohoaa erityisesti silloin, kun asiakirjoja jostain syystä käsitellään yrityksen toimitilojen ulkopuolella. Lähtökohta turvallisuusluokitellun tiedon suhteen on aina se, että henkilölle annetaan pääsy vain siihen tietoon, jota hän tarvitsee työtehtäviensä suorittamiseksi ja vain siksi aikaa, kun hän suorittaa tätä työtehtävää.

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Vierailijakäytännöt ohjeistus |  |
| Asiakirjaturvallisuus ja menettelyohjeetohjeet |  |

# Etätyöt

Tyoimihenkilöiden tulee noudattaa etätyössä yrityksen tietoturvasta ja tietosuojasta antamia ohjeita sekä raportoida mahdollista tietoturvaa vaarantavista seikoista esimiehelleen ja/tai ICT-asi-antuntijalle. Etätyötä tekevän tulee kiinnittää huomiota tietoturvallisiin menettelytapoihin toimiessaan työpaikan toimitilojen ulkopuolella.

Tietojärjestelmien etäkäytön osalta noudatetaan tietohallinnon antamia ohjeita. Työntekijän on sitouduttava noudattamaan etätyössä samaa salassapitovelvollisuutta, jota häneltä työssä ollessa normaalistikin edellytetään.

On vältettävä viemästä etätyöpisteeseen yrityksen liiketoiminnan kannalta arkaluontoista tietoa tai henkilötietoja sisältäviä asiakirjoja. Varsinkin manuaalista aineistoa käsiteltäessä on noudatettava erityistä huolellisuutta, jotta tietoja ei pääse sellaisten tahojen käsiin, joilla ei ole tietojen käsittelyoikeutta.

**Etätyön 10 tietoturvaohjetta:**

1. Käytä työtehtävien tekemiseen työantajan tarjoamia laitteita.
2. Suojaa laitteiden fyysistä turvallisuutta etätyöpisteessä.
3. Hyödynnä suojattuja verkkoyhteyksiä ja -laitteita.
4. Tiedosta kodin muista älylaitteista aiheutuvat riskit.
5. Asenna tietoturvapäivitykset ajallaan.
6. Tiedosta IT-palveluiden normaali toiminta etätyöympäristössä.
7. Tallenna työtiedostot sovittuun paikkaan, erikseen yksityisistä.
8. Jaa tietoa järkevästi ja turvallisesti.
9. Käytä etätöissä työnantajan tarjoamia ja ohjeistamia IT-palveluita.
10. Ota selvää, miten varmuuskopiointi toimii. Ja käytä sitä.

# BYOD -käytännöt

Bring Your Own Device eli BYOD on toimintatapa, jossa organisaatio sallii työntekijän itsekustantamansa päätelaiteen käytön jokapäiväisessä työnteossa. Kun organisaatiolla ei ole enää omat laitteet käytössä, on vaikea tasapainoilla täsmällisen tietoturvan ja henkilökohtaisen datan välillä.

BYOD tuo mukanaan monenlaisia riskejä. Kadonneisiin tai varastettuihin laitteisiin ei kiinnitetä niin paljon huomioita, kun ne eivät ole enää organisaation omistuksessa. Yritys ei saa tapauksista edes tietoa, jos käyttäjä itse ei tee ilmoitusta. Luottamuksellista tietoa saattaa olla turvattomilla kanavilla, jotka on helposti kaapattavissa. Lisäksi mobiililaitteet ovat yleensä aina yhdistettynä verkkoon, ja niistä voidaan tehdä myös tukiasemia.

**BYOD tarkistuslista, jos omien laitteiden käyttö on sallittua**

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Laitteet ovat pääsykoodattuja. |  |
| Päivitykset ovat ajan tasalla. |  |
| Määritellään palvelut, joita omalla laitteella tai sen kautta voi käyttää. |  |
| Ohjeistetaan käyttäjiä sammuttamaan tarpeettomat aplikaatiot. |  |
| Määritellään, kenelle ja miten tietoturvapoik-keamasta ilmoitetaan. |  |

# Sähköpostikäytännöt

Sähköposti on yksi yritysten tärkeimmistä työvälineistä, kun ne kommunikoivat asiakkaidensa kanssa. Sähköpostin välityksellä siirretään päivittäin viestintäosapuolten kesken paitsi liikesalaisuuksia usein myös henkilötietoja.

Liikesalaisuuksia voivat olla esimerkiksi tuotekehitysprojekteihin liittyvät tiedot, hinnoitteluperiaatteet tai vaikkapa yritysjärjestelyihin liittyvä tiedonvaihto. Arkaluonteisia henkilötietoja voivat olla henkilöstöhallintoon liittyvät tiedot, kuten henkilötunnus tai tieto työntekijän jäsenyydestä ammattiliittoon. EU:n uuden tietosuoja-asetuksen myötä sähköpostin käyttöä erityisesti arkaluonteisten henkilötietojen välittämiseen on syytä tarkastella vakavasti.

## Sähköpostin tietoturva

EU on antanut myös uuden liikesalaisuusdirektiivin, jonka tarkoitus on tehostaa yritysten liikesalaisuuksien suojaamista. ”Sähköposti on kuin postikortti” on usein käytetty ja varsin osuva fraasi. Kuka tahansa joka saa postikortin käteensä, voi lukea kortista lähettäjän, vastaanottajan ja viestin sisällön.

Käytännössä asia ei kuitenkaan ole aivan niin yksinkertaista ja normaalin sähköpostin turvaksi on kehitetty erilaisia luottamuksellisuutta parantavia mekanismeja, kuten TLS (transport layer security).

Kun TLS on kytkettynä läpi koko viestin välitysketjun lähettäjältä vastaanottajalle, kulkee itsessään selkokielinen sähköpostiviesti TLS-salattuna aina vastaanottajan omaan sähköpostipalveluun ja päätelaitteeseen saakka. Myös yrityksen sisäinen sähköpostiliikenne kulkee palveluntarjoajan verkossa samalla tavalla turvallisesti.

## Sähköpostin tietoturvauhat

Sähköposti on helppokäyttöisyytensä vuoksi yksi keskeisimpiä yrityksen kyberuhkaväyliä. Sen kautta on edelleen helppo välittää viruksia, haittaohjelmia ja huijausviestejä, joiden suhteen loppukäyttäjien on oltava tarkkana: mikään tekninen ratkaisu kun ei täysin poista loppukäyttäjien osaamista.

**Sähköpostikäytäntöjen tarkistuslista**

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Ainoastaan oikeaksi tunnistettujen lähettäjien viesteissä olevat linkit tai liitteet avataan. |  |
| Yrityksen sähköpostipalvelu käyttää TLS -protokollaa. |  |
| Luottamukselliseen viestitään käytetään turvapostia tai vastaavaa. |  |
| Sähköpostin salasana on turvallinen. |  |
| Käyttäjät osaavat tarkistaa otsikkotiedoista viestin todellisen lähettäjän, ohje:  <https://d-fence.fi/headerit> |  |
| Sähköpostilla tulleet laskut tarkistetaan aina erikseen. |  |
| Muistutetaan säännöllisesti kalasteluviesteistä ja niihin reagoimisesta. |  |

# Luottamuksellista tietoa sisältävien laitteiden käsittely

Yrityksessä käsitellään säännöllisesti luottamuksellisia ja salassa pidettäviä tietoja, lähtökohtana tulee olla tietokoneiden kaikkien tallennusvälineiden (kuten kiintolevyn) tietojen salaus.

Kannettavien tietokoneiden osalta riski joutua mm. anastusrikoksen kohteeksi on suurempi kuin pöytätietokoneiden, joten erityisesti kannettavien tietokoneiden ja tallennusvälineiden tiedot tulee aina salata. Salaaminen vaikeuttaa tai jopa estää tallennettuun tietoon pääsyä, jos laite joutuu vääriin käsiin.

Tietokoneiden tulee lyhyen ajan kuluessa lukittua automaattisesti, mikäli niitä ei käytetä. Tietokone tulee lukita myös aina, jos tietokone jää valvomatta esimerkiksi tauon ajaksi. Erityisesti vastaanotto- ja vierastiloissa sijaitsevat tietokoneet on lukittava heti poistuttaessa paikalta lyhyeksikin aikaa.

Käytettäessä tietokoneita tai muita laitteita toimiston ulkopuolella tulee huolehtia siitä, että sivulliset eivät voi nähdä ruudulla näkyviä tietoja. Hyvä käytäntö on asentaa laitteidensa näyttöön suojakalvo, joka estää näytöllä olevien tietojen näkymisen muille kuin laitteen käyttäjälle.

Yrityksen omat päätelaitteet ovat aina ensisijaisesti tarkoitettu työkäyttöön. Tietoturvaan ja salassa-pitoon liittyvistä syistä muiden henkilöiden, myös perheenjäsenten, ei tule sallia käyttää tietokonetta.

Tietokoneelle tulee asentaa ainoastaan työn kannalta tarpeellisia ja turvallisia ohjelmistoja. Samoin tietokoneella tulee käyttää ainoastaan työn kannalta tarpeellisia ja turvallisia verkkosivustoja.

**Siirrettävät tallennusvälineet**

Siirrettäviin tallennusvälineisiin liittyy vakavia tietoturvariskejä, jotka toimihenkilön tulee huomioida. Tallennusväline voi kadota tai joutua varkauden kohteeksi. Tallennusvälineiden käytöstä ja säilytyksestä on huolehdittava siten, että niissä olevat luottamukselliset tiedot ovat suojassa.

Siirrettävät tallennusvälineet voivat myös olla riskialttiita virusten ja haittaohjelmien kannalta. Ulkopuolisen tahon omistamaa tai käyttämää tallennusvälinettä (kuten USB tikku) ei tule kytkeä yrityksessä käytettäviin laitteisiin varmistumatta ensin huolellisesti, että se on turvallista tehdä.

**Mobiilit päätelaitteet**

Puhelimeen ja tablettiin tallennetuu usein yrityksessä käytettävää tietoa tai puhelimella voi olla pääsy verkkoyhteyden kautta erilaisiin yrityksessä käytettäviin palveluihin, jotka voivat sisältää luottamuksellista ja salassa pidettävää tietoa.

Mobiililaite voi myös sisältää kalenterimerkintöjä, asiakastietoja, tuote- tai palvelutietoja hintoineen sekä muuta liikesalaisuuden piiriin kuuluvaa tietoa.

Mobiililaitteen lukituksen (pin koodi tms.) lisäksi myös siihen tallennettava sisältö on hyvä salata. Laitteessa tulee olla aktivoituna myös mahdollisuus tietojen poistamiseen, puhelimen paikantamiseen ja sen lukitsemiseen etänä, jos puhelin tarjoaa tällaisen mahdollisuuden.

**Luottamuksellista tietoa sisältävien laitteiden turvatarkistuslista**

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Päivitykset ovat ajan tasalla. |  |
| Laitteissa on asiaankuuluvat virustorjuntaohjelmistot. |  |
| Laitteisiin on määritelty käyttöoikeudet erikseen (salasana). |  |
| Laitteissa on automaattilukitukset |  |

# Saosiaalinen media

Sosiaalisen median tietoturvaongelmat syntyvät pääosin perinteisten tietoturvauhkien ja uusien toimintamallien ja palveluiden yhdistelmänä. Sosiaalinen media ei toistaiseksi ole tuonut varsinaisesti uusia tietoturvauhkia, mutta sosiaalisen median toimintaperiaatteen luonteesta johtuen ilmenevät tietoturvauhat eri tavalla kuin perinteisessä mediassa. Toimintaperiaatteisiin kohdistuvat tietoturvauhat korostuvat erityisesti yhteisöpalveluissa.

Keskeisimmät tietoturvauhat perustuvat sekä käyttäjän omaan toimintaan että ammattimaiseen ja suunniteltuun toimintaan, jossa rikolliset, ääriryhmät tai valtiot pyrkivät esim. saamaan haltuunsa tietoa (luottokortti- ja henkilötietoja, yrityssalaisuuksia, valtiosalaisuuksia), vaikuttamaan päätöksentekoon (kuluttajien, yritysjohdon, valtionjohdon) tai tahraamaan organisaatioiden tai ihmisten mainetta.

Ammattirikolliset hakevat taloudellista etua hyödyntämällä sosiaalisen median palveluita ja niiden kautta levitettäviä haittaohjelmia, jotka mahdollistavat esim. käyttäjän tietokoneen etähallinnan ja käyttämisen rikollisjärjestön haluamaan käyttötarkoitukseen

Sosiaalisen median palveluiden käyttö tulee arvioida niiden kautta saatujen hyötyjen perusteella tasapainotettuna mahdollisiin riskeihin. Riskienhallinnan tulisi toimia keskeisenä osana palveluiden käyttöä suunniteltaessa. Lähtökohta on, että organisaatiolla on selkeä tavoite sosiaalisen median hyödyntämisessä sekä riittävästi resursseja tavoitteen saavuttamiseksi. Sosiaalisen median palveluiden ohjeistaminen tulee olla linjassa organisaation tietoturvapolitiikan kanssa.

Palveluita käytettäessä tulee määrittää palveluissa sallitut verkkoidentiteetit.

**Verkkoidentiteettejä on kolmenlaisia:**

1. **Organisaatiotunnus:** palveluun kirjaudutaan roolipohjaisella (sähköposti)tunnuksella tai organisaation tarjoamalla, henkilökohtaisella (sähköposti)tunnuksella. Palvelun käyttäjä edustaa organisaatiotaan. Muista resursointi organisaatiotunnuksella.

*Organisaation sosiaalisen median palvelua päivittävät henkilöt kirjautuvat palveluun organisaation henkilökohtaista sähköpostitunnusta ([etu.suku@organisaatio.fi](mailto:etu.suku@organisaatio.fi)) tai roolipohjaista tunnusta ([tiedottaja@organisaatio.fi](mailto:tiedottaja@organisaatio.fi)) käyttäen. Tällöin työnantajalla on täysi oikeus määrätä, mitä tällaisella tunnuksella voidaan tehdä ja millaisiin keskusteluihin sillä voidaan osallistua.*

1. **Hybridi:** palveluun kirjaudutaan joko organisaation tarjoamalla henkilökohtaisella (sähköposti)tunnuksella tai omalla yksityisellä (sähköposti)tunnuksella. Palvelun käyttäjä mainitsee työnantajansa, mutta toimii palvelussa asiantuntijaroolissa yksityishenkilönä.

*Esim. LinkedIn on ammattimaiseen verkostoitumiseen tarkoitettu yhteisöpalvelu, jota verkostoitumisen lisäksi hyödynnetään oman osaamisen kehittämiseen seuraamalla omien verkostojensa ja ryhmiensä viestejä ja keskusteluja. Käyttö perustuu kuitenkin harvoin organisaation suositukseen hyödyntää palvelua*; *tunnuksen luominen ja ylläpito on perustunut henkilön omatoimiseen päätökseen ottaa palvelu käyttöön. Osa palvelua käyttävistä kirjautuu palveluun organisaation sähköpostitunnuksella ja osa vapaa-ajan tunnuksella. Työnantajan mahdollisuus ohjeistaa hybridinomainen osallistuminen on hyvin rajattu. Organisaation tarjoaman sähköpostitunnuksen käyttö voidaan halutessaan kieltää ja työntekijää sitoo edelleen työntekijään liittyvät velvoitteet, mutta muilta osin henkilön toiminta sosiaalisen median palvelussa on henkilön itse päätettävissä oleva asia.*

1. **Täysin yksityinen identiteetti:** palveluun kirjaudutaan omalla henkilökohtaisella (sähköposti)tunnuksella. Palvelun käyttäjä toimii täysin yksityishenkilönä.

**Sosiaalisen median käyttämisen turvatarkistuslista**

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Verkkoidentiteetti- ja käyttöohjeistus |  |
| Yksityisyysasetusohjeistus |  |
| Salasanaohjeistus |  |
| Haitta-ja kalasteluviestiohjeet sekä kehotus varoa lyhyitä URL:eja |  |
| Määritellään, mitä yritykseen liittyviä teemoja saa kertoa ja mitä ei? |  |
| Luodaan malli mahdolliseen maineen hallintaan tai häirintäkommentointiin. |  |

# Tietoturvarikkomukset

Tietoturvarikkomus on yrityksen tulkinnan mukaan mikä tahansa tietoturvapolitiikan, tietoturva- tai tietosuojaohjeistuksen tai EU -tietosuoja-asetuksen vastainen toiminta. Kaikki rikkomusepäilyt tutkitaan.Tietoturvallisuutta seurataan hallinnollisesti ja teknisesti.

Seurannassa noudatetaan lakeja, sopimuksia ja hyviä valvontaperiaatteita. Rikkomustilanteet käsitellään lojaliteettirikkomuksina ja työnantajan ohjeiden vastaisina toimina. Tahallisista rikkomuksista saattaa seurata kurinpidollisia sekä rikosoikeudellisia toimenpiteitä. Yrityksellä on erillinen kirjallinen ohje tietoturvaloukkaustilanteiden varalle

**Ilmoitusvelvollisuus ja toiminta poikkeamatilanteissa**

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

* Jos hallussasi oleva laite, kulkukortti, tunniste tms. katoaa tai varastetaan, ilmoita siitä välittömästi ko. asian vastuuhenkilölle tai päätelaitteen tukipalvelusta vastaavalla toimittajalle mahdollisen vahingon pienentämiseksi.
* Ilmoita aina haittaohjelmista (esim. virushälytys päätelaitteella) ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi tietoturvavastaavalle, tietohallinto-organisaatiolle tai omalle esimiehellesi.
* 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 puhelimellasi.
* Ota yhteyttä tietoturvavastaavaan. Auta tutkinnassa. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

**Muista:** Millään teknisellä toimella ei voida kokonaan eliminoida loppukäyttäjän osaamistarvetta.

**Tietoturvarikkomukset turvatarkistuslista**

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Henkilöstön ohjeet poikkeamien havaitsemiseksi ja ilmoitusprosessi |  |
| Tietosuojaan liittyviin poikkeamiin toimintaprosessin suunnittelu ja malli |  |
| Tiedotus siitä, kenelle yrityksessä poikkeamasta ilmoitetaan |  |
| Ohjeet vahinkojen minimoimiseksi |  |

Viranomaisen sivulta löytyvät lomakkeet osoitteessa <https://tietosuoja.fi/lomakkeet>

# Salasanapolitiikka

Salasanojen merkitys tietoturvan ja -suojan toteutumisen kannalta on keskeinen. Useat tietomurrot ja onnistuneet huijaukset käynnistyvät kohdistettuna hyökkäyksenä tai osana kalastelukampanjaa, jossa urkitaan käyttäjien tunnuksia ja salasanoja. Mitä paremmin salasanaohjeistusta noudatetaan, sitä pienemmän hyökkäyspinnan rikolliset saavat käyttöönsä.

**Millainen on hyvä salasana?**

Netti on pullollaan erilaisia ohjeita salasanojen murtamiseksi. Salasana on käytännössä sitä helpompi murtaa, mitä vähemmän siinä on merkkejä. Alle 8 merkkiset salasanat ovat nykyään (2020) liian helppoja murtaa, eli on käytettävä pidempiä. Vähintään 12 merkkisiä, mieluiten 16 merkkisiä. Ei sellaisia, jotka ovat suoraan luettavassa muodossa ja niiden on hyvä sisältää isoja ja pieniä kirjaimia sekä numeroita (tai niiden korvaavuuksia) ja erikoismerkkejä.

**Salasanapolitiikka turvatarkistuslista**

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Salasanaohjeistus |  |
| Eri salasana jokaiseen järjestelmään |  |
| Yrityksen järjestelmäsalasanoja ei saa tallentaa selaimeen. |  |
| Pohtikaa salasanaholvin käyttöä |  |

# Sidosryhmävaatimukset

Lähes kaikilla yrityksillä on sidosryhmiä, alihankkijoita, kumppaneita tai päämiehiä. Riskienhallinnan ytimessä on ennaltaehkäisy. Huonosti valituista kumppaneista voi aiheutua monenlaisia kassavirtaan tai yrityksen maineeseen vaikuttavia riskejä.

Yritysten taustoista kertovat tiedot kannattaa siis aina tarkistaa toimiessasi uuden yhteistyökumppanin tai asiakkaan kanssa. Taustatiedoista selviää muun muassa, miten kannattava ja vakavarainen yritys on. Lisäksi tiedot kertovat, onko yritys kasvamassa vai onko toiminta hiipumassa?

Selvittämällä liikekumppanin taustat, kuten luottotiedot, voidaan arvioida paremmin myös kumppanin maksukykyä. Samalla yrityksen positiiviset luottotiedot viestivät vastuullisesta liiketoiminnasta sekä kyvystä ja halusta hoitaa taloudelliset velvoitteet.

**Ennakkoperintärekisteri, epr**

Palveluita ostettaessa on aina tarkistettava epr ennen laskun maksamista. Todella varovainen tulostaa vielä kirjanpitoon joka kerta saamansa tuloksen.

Jos suorituksen saaja on merkitty ennakkoperintärekisteriin, maksaja voi maksaa korvauksen ilman ennakonpidätystä. Jos rekisterimerkintää ei ole, ennakonpidätys on toimitettava. Rekisteröinnin tarkistusvelvollisuus ei koske tavaran kauppaa tai vuokraustoimintaa.

**GDPR kelpoisuus**

Tilaaja - toimittaja (rekisterinpitäjä - henkilötietojen käsittelijä) välistä suhdetta ja vastuuta säädellään erikseen tietosuoja-asetuksessa (artikla 28), joka sanoo näin:

*Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tämän asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu.*

Rekisterinpitäjä on vastuussa henkilötietojen käsitelystä. Myös ulkoistustapauksissa.

Rekisterinpitäjän ja henkilötietojen käsittelijän kesken on myös tehtävä kirjallinen sopimus sekä rekisterinpitäjän on annettava käsittelijälle ohjeistus.

Koska rikkomuksista seuraavat sanktiot voivat olla tuntuviakin, on yrityksen toiminnan kannalta välttämätöntä varmistua myös kumppanin GDPR -kelpoisuudesta.

**Sidosryhmävaatimukset turvatarkistuslista**

|  |  |
| --- | --- |
| **Teema** | **Vastuuhenkilö** |
| Tarkista taustat  <https://www.asiakastieto.fi/web/fi/palvelut-yrityksille/tarkista-ennen-kaupantekoa/luottotiedot-ja-luokitukset.html> |  |
| Tarkista epr  <https://www.ytj.fi/> |  |
| Ulkoistustapauksissa sopimukset ja ohjeistus tehtynä |  |
| Tilaajavastuu  <https://www.vastuugroup.fi/fi-fi/palvelut/luotettava-kumppani> |  |
| GDPR -kelpoisuus  <https://tietosuojavastuu.fi/> |  |

**Lopuksi**

Tietosuoja lähtee rekisteröidyn henkilötiedosta ja sen käsittelystä. Tietoturva mahdollistaa tietosuojan toteutumisen, eli vaikka ne ovatkin eri asioita, liittyvät ne toisiinsa saumattomasti.

Digitaalisaatio on tullut jäädäkseen. Se tarjoaa meille aivan uusia liiketoimintamahdollisuuksia, mutta toisaalta organisaatioihimme kohdistuvat kyberriskit ovat myös saaneet aivan uusia muotoja. Tämä kehitys näyttää jatkuvan.

Onneksi kyberturva ei ole rakettitiedettä vaan pieniä oikeita tekoja jokapäiväisessä elämässämme. Maalaisjärjen käyttöä kiireettömässä arjessa. Kun varmistamme, että tässä dokumentissa kuvatut asiat ovat kunnossa, useimmat organisaatiot pääsevät sillä jo pitkälle.