Tietoturvapolitiikka

**Luokitus**: Julkinen

Tätä dokumenttia voidaan jakaa [Yrityksen] ulkopuolisille kiinnostuneille osapuolille.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Versio | Päivitetty | Muokkaaja | Asiakirjan muutokset | Hyväksyjä | Omistaja |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Sisällysluettelo

[Tämän asiakirjan tarkoitus 3](#_Toc194312034)

[Soveltamisala 3](#_Toc194312035)

[Toimitusjohtajan sitoumus 3](#_Toc194312036)

[Tietoturvan konteksti 3](#_Toc194312037)

[Tietoturvan tavoitteet 3](#_Toc194312038)

[Roolit ja vastuut 3](#_Toc194312039)

[Koulutus ja tietoisuuden lisääminen 4](#_Toc194312040)

[Fyysinen turvallisuus 4](#_Toc194312041)

[Suullinen viestintä 4](#_Toc194312042)

[Kolmansien osapuolten tietoturva 4](#_Toc194312043)

[Työntekijöiden taustaselvitykset 4](#_Toc194312044)

[Luvattoman pääsyn estäminen 5](#_Toc194312045)

[Tunnusten asianmukainen käyttö 5](#_Toc194312046)

[Salausmekanismit 5](#_Toc194312047)

[Tietojen luokittelu 5](#_Toc194312048)

[Luottamuksellinen tieto 5](#_Toc194312049)

[Luottamuksellisen tiedon käsittelyohjeet 5](#_Toc194312050)

[Sisäinen tieto 6](#_Toc194312051)

[Sisäisen tiedon käsittelyohjeet 6](#_Toc194312052)

[Julkinen tieto 6](#_Toc194312053)

[Julkisen tiedon käsittelyohjeet 7](#_Toc194312054)

[Tietoturvaloukkaukset 7](#_Toc194312055)

[Liittyvät politiikat ja asiakirjat 7](#_Toc194312056)

[Valvonta 8](#_Toc194312057)

[Riskien arviointi- ja käsittelymenetelmä 8](#_Toc194312058)

# Tämän asiakirjan tarkoitus

Tämä politiikka määrittelee [Yritykseen] sovellettavat tietoturvakäytännöt tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi.

# Soveltamisala

Tietoturvapolitiikka koskee kaikkia työntekijöitä ja kolmansia osapuolia.

# Toimitusjohtajan sitoumus

*”Tähän toimitusjohtajan lausunto sitoutumisesta tähän politiikkaan”*

[Toimitusjohtajan nimi, pvm ja allekirjoitus]

# Tietoturvan konteksti

Tietoturvan laajuus ja konteksti, mukaan lukien sisäiset ja ulkoiset tekijät, jotka vaikuttavat [Yrityksen] toimintaan, on dokumentoitu Tietoturvan hallintajärjestelmän (ISMS) laajuus -asiakirjassa, joka on saatavissa täällä: [lisää linkki dokumenttiin].

# Tietoturvan tavoitteet

* Varmistaa organisaation tietojen, mukaan lukien GDPR:n määrittelemien henkilötietojen luottamuksellisuus, eheys ja saatavuus.
* Tarjota tarvittavat resurssit tietoturvan hallintajärjestelmän kehittämiseen, toteuttamiseen ja jatkuvaan parantamiseen.
* Hallita tehokkaasti kolmansien osapuolien toimittajia, jotka käsittelevät, tallentavat tai siirtävät tietoja vähentääkseen ja hallitakseen tietoturvariskejä.
* Edistää tietoturvan ja tietosuojan kulttuuria tehokkaan koulutuksen ja tietoisuuden lisäämisen avulla.

# Roolit ja vastuut

**Tietoturvaryhmä:**

* Hyväksyy ja valvoo tietoturvapolitiikkaa.
* Hallinnoi tietoturvan hallintajärjestelmän (ISMS) viitekehystä.
* Ohjaa ja tukee [Yrityksen] tietoturvatehtävissä.

**Tietoturvapäällikkö:**

* Ylläpitää tietoturvan hallintajärjestelmää (ISMS).
* Varmistaa ISMS-vaatimusten noudattamisen
* Toteuttaa tietoturvariskien arviointeja.

**Järjestelmien omistajat:**

* Hallinnoivat tietoturvariskejä omalla vastuualueellaan.
* Tukevat tietoturvapäällikköä.
* Varmistavat prosessien ja politiikkojen noudattamisen.

**Esihenkilöt:**

* Myöntävät käyttöoikeuksia työroolien perusteella.
* Valvovat politiikkojen noudattamista omissa tiimeissään.
* Hallinnoivat [Yrityksen] laitteiden ja järjestelmien käyttöä ja palauttamista.

**Kaikki työntekijät:**

* Noudattavat tietoturvapolitiikkaa ja siihen liittyviä ohjeistuksia.
* Ilmoittavat politiikan rikkomuksista.
* Pyytävät poikkeuksia IT-tuen kautta.

# Koulutus ja tietoisuuden lisääminen

* Kaikkien työntekijöiden ja alihankkijoiden tulee suorittaa tietoturvakoulutus työtehtäviensä tueksi. Koulutuksen tulee vastata heidän rooliaan ja käsittelemiään tietoja.
* Uusien työntekijöiden perehdytykseen sisältyy pakollinen tietoturvatietoisuusosio.
* Työntekijöille tarjotaan säännöllisesti päivityksiä tietoturvauhkien kehittymisen huomioon ottamiseksi.

# Fyysinen turvallisuus

* Työntekijöiden tulee säilyttää kulkutunnisteensa huolellisesti ja ilmoittaa niiden katoamisesta.
* Fyysisiä pääsynhallintamenetelmiä, kuten avaimia tai kulkukortteja käytettävä rajoitetuille alueille ja laitteisiin pääsemiseksi.
* Vierailijoilla täytyy aina olla saattaja yrityksen tiloissa.

# Suullinen viestintä

* Ole varovainen keskustellessasi luottamuksellisista asioista julkisilla paikoilla, jotta tietoja ei voida salakuunnella.

# Kolmansien osapuolten tietoturva

* Kaikki organisaation puolesta tietoja käsittelevät kolmannet osapuolet käyvät läpi riskiarvioinnin.
* Kaikkien sisäisiä tai luottamuksellisia tietoja käsittelevien kolmansien osapuolten on allekirjoitettava salassapitosopimus.
* Organisaation tietoturvakäytännöt viestitään kolmansille osapuolille ja niiden noudattaminen sisällytetään sopimuksiin tarvittaessa.

# Työntekijöiden taustaselvitykset

* Organisaatio suorittaa taustaselvitykset osana rekrytointiprosessia.

# Luvattoman pääsyn estäminen

* Arkaluonteisen tiedon jakamiseen on saatava kirjallinen lupa.
* Käyttöoikeuksia hallinnoidaan *Pääsynhallintapolitiikan* mukaisesti.
* Käytössä on minimioikeuksien periaate (least privilege), eli työntekijät saavat vain heidän tehtäviinsä välttämättömät käyttöoikeudet.
* Tietoja auditoidaan säännöllisesti, jotta varmistutaan, että vain valtuutetuilla henkilöillä on pääsy niihin.

# Tunnusten asianmukainen käyttö

* Lisätietoja löytyy *Salasanapolitiikasta***.**
* Työntekijöiden ja alihankkijoiden tulee suojata henkilökohtaiset tunnuksensa eikä jakaa niitä kenellekään.
* Ota monivaiheinen tunnistautuminen (MFA) käyttöön aina, kun mahdollista.

# Salausmekanismit

* Salausavainten luontia, jakelua, kierrätystä ja tuhoamista koskevat prosessit dokumentoidaan.
* Salausavaimet säilytetään keskitetyssä ja rajoitetussa säilytyspaikassa.
* Hyväksyttyjen salaustekniikoiden- ja algoritmien luetteloa tarkastellaan ja päivitetään säännöllisesti, jotta se vastaa teknologian kehitystä ja uusia uhkia.

# Tietojen luokittelu

Tietojen luokittelun tarkoituksena on viestiä tiedon luottamuksellisuuden tasosta ja määrittää, kenelle sitä voidaan jakaa. Tätä varten [Yritys] on määritellyt kolme tietoluokkaa:

## Luottamuksellinen tieto

* Luvaton pääsy tai tietovuoto voi rikkoa lakeja ja säädöksiä tai aiheuttaa merkittäviä haittoja [Yritykselle], sen asiakkaille tai liikekumppaneille.
* Luottamuksellisen tiedon käyttö edellyttää tietojen omistajan tai asianmukaisen esihenkilön hyväksyntää.
* Esimerkkejä luottamuksellisesta tiedosta:
  + henkilötiedot
  + asiakastiedot
  + yrityksen taloudelliset tiedot
  + liiketoimintasuhteisiin liittyvät tiedot
  + järjestelmien tunnukset ja salasanat
  + tiedostojen salausavaimet

### Luottamuksellisen tiedon käsittelyohjeet

* **Salaus:** Kaikki luottamukselliset tiedot on salattava sekä siirron aikana että tallennettaessa, hyväksytyillä salausmenetelmillä.
* **Pääsynhallinta**: Käyttö on rajoitettava vain valtuutetuille henkilöille.
* **Tietojen säilytys**: Tiedot tulee säilyttää suojatuissa ympäristöissä (fyysisissä ja digitaalisissa).
* **Tietojen siirto**: Käytä turvallisia, salattuja kanavia luottamuksellisten tietojen siirtämiseen.
* **Hävittäminen**: Luottamukselliset tiedot tulee hävittää turvallisesti ja peruuttamattomasti, kun niitä ei enää tarvita. Tämä koskee paperidokumentteja, digitaalisia tiedostoja ja irrotettavia tallennusvälineitä.
* **Tietomurtoprotokolla:** Tietoturvaloukkauksille on oltava selkeä raportointi- ja reagointimenettely.

## Sisäinen tieto

* Tiedot, jotka on tarkoitettu vapaaseen käyttöön [Yrityksen] sisällä.
* Sisäisiä tietoja voidaan jakaa [Yrityksen] sisällä ilman erillistä tietojen omistajan hyväksyntää.
* Kaikki tiedot, joita ei ole erikseen luokiteltu *luottamuksellisiksi* tai *julkisiksi*, luokitellaan oletusarvoisesti *sisäisiksi*.
* Näiden tietojen luvaton luovuttaminen ulkopuolisille voi olla kiellettyä oikeudellisista tai sopimuksellisista syistä.
* Esimerkkejä sisäisistä tiedoista:
  + henkilöstöluettelot
  + sisäiset politiikat ja prosessit
  + sisäinen sähköpostiviestintä

### Sisäisen tiedon käsittelyohjeet

* **Salaus:** Sisäiset tiedot salataan siirron aikana ja tallennettaessa.
* **Pääsynhallinta**: Pääsy sisäisiin tietoihin on rajoitettava organisaation henkilöstölle ja sopimuskumppaneille. Niitä ei saa jakaa ulkopuolisille ilman kirjallista lupaa.
* **Tietojen säilytys**: Tiedot säilytetään suojatuissa ympäristöissä.
* **Tietojen siirto**: Huolellisuutta noudatettava, mutta salaus ei ole pakollista.
* **Hävittäminen**: Sisäiset tiedot on tuhottava turvallisesti ja peruuttamattomasti, kun niitä ei enää tarvita. Tämä koskee paperidokumentteja, digitaalisia tiedostoja ja irrotettavia tallennusvälineitä.
* **Tietomurtoprotokolla:** Luottamuksellisten tietojen tietomurroille on oltava selkeä raportointi- ja reagointimenettely.

## Julkinen tieto

* Julkiset tiedot ovat sellaisia, jotka organisaation määrittelemä vastuuhenkilö on hyväksynyt julkisesti jaettaviksi.
* Näitä tietoja voidaan jakaa myös organisaation ulkopuolelle.
* Esimerkkejä julkisista tiedoista:
  + markkinointiesitteet
  + [Yrityksen] verkkosivuilla julkaistut materiaalit
  + [Yrityksen] sosiaalisen median tilit

### Julkisen tiedon käsittelyohjeet

* **Salaus:** Julkisia tietoja ei salata.
* **Pääsynhallinta**: Julkisten tietojen kopioiden käyttöä ei rajoiteta ja niitä voidaan jakaa vapaasti. Kuitenkin alkuperäiset lähdetiedot, kuten markkinointiesitteet ja verkkosivujen sisältö, käsitellään sisäisinä tietoina.
* **Tietojen säilytys**: Julkisia tietoja voidaan säilyttää useilla eri alustoilla.
* **Tietojen siirto**: Huolellisuutta noudatettava, mutta salaus ei ole pakollista.
* **Hävittäminen**: Julkisten tietojen hävittämiseen ei tarvita erityistä suunnittelua tai valvontaa, mutta on suositeltavaa poistaa vanhentunut tieto, jotta virheellistä tai vanhentunutta tietoa ei jaeta edelleen.
* **Tietomurtoprotokolla:** Ei vaadita.

# Tietoturvaloukkaukset

* Järjestelmäturvallisuuteen liittyvät huolenaiheet on ilmoitettava heti IT-tukeen.
* Fyysiset tietoturvaloukkaukset on raportoitava toimistopäällikölle tai tietosuojavastaavalle.
* Henkilötietoihin liittyvät tietomurrot: Katso *Tietosuojapolitiikka*.
* Merkittäviä tietomurtoja koskevat ohjeet: Katso *Tietoturvapoikkeamien hallintaprosessi*.

# Liittyvät politiikat ja asiakirjat

Kattavan tietoturvahallinnan varmistamiseksi [Yritys] on laatinut useita yksityiskohtaisia käytäntöjä, jotka tukevat ja täydentävät tätä tietoturvapolitiikkaa ja antavat lisäkontekstia vastuualueisiin. Työntekijöiden, urakoitsijoiden ja muiden sidosryhmien on tutustuttava nähin politiikkoihin ja noudatettava niiden ohjeita:

|  |  |  |
| --- | --- | --- |
| Politiikka | Kuvaus | Sijainti |
| Hyväksyttävän käytön politiikka | Ohjeistaa henkilöstöä organisaation teknologian asianmukaisessa käytössä. | [linkki dokumenttiin] |
| Tietosuojapolitiikka | Kuvaa miten henkilötietoja käsitellään. | [linkki dokumenttiin] |
| Salasanapolitiikka | Määrittelee salasanavaatimukset ja niiden käytön periaatteet. | [linkki dokumenttiin] |
| Mobiililaitepolitiikka | Määrittelee organisaation tarjoamien mobiililaitteiden käytön säännöt. | [linkki dokumenttiin] |
| SaaS-politiikka | Kuvaa miten pilvipohjaisia ohjelmistoratkaisuja voidaan arvioida ja ottaa käyttöön organisaatiossa. | [linkki dokumenttiin] |
| Bring-Your-Own-Device Politiikka | Määrittelee miten henkilökohtaisia laitteita voidaan käyttää työtehtäviin. | [linkki dokumenttiin] |
| Pääsynhallintapolitiikka | Kuvaa miten järjestelmien käyttöoikeudet myönnetään ja hallitaan. | [linkki dokumenttiin] |
| Toimittajien tietoturvapolitiikka | Kuvaa miten kolmansien osapuolten organisaation tietoja käsittelevät toimijat tulee hallita. | [linkki dokumenttiin] |

# Valvonta

* [Yritys] valvoo IT-järjestelmiään varmistaakseen niiden lainmukaisuuden ja tietoturvavaatimusten täyttymisen.
* Lokitus ja tutkimusprosessit takaavat tietoturvan ja politiikkojen noudattamisen.

# Riskien arviointi- ja käsittelymenetelmä

Osana tietoturvan hallintajärjestelmäämme (ISMS) [Yritys] on sitoutunut tunnistamaan, arvioimaan ja hallitsemaan tietoturvariskejä. Tätä varten noudatamme erillisessä dokumentissa kuvattua jäsenneltyä riskiarviointi- ja käsittelymenetelmää.

Riskiarviointi- ja käsittelymenetelmä sisältää:

* **Riskien tunnistaminen:** Mahdollisten tietoturvauhkien ja haavoittuvuuksien järjestelmällinen tunnistaminen.
* **Riskien analysointi ja arviointi:** Arvioidaan tunnistettujen riskien todennäköisyys ja mahdollinen vaikutus, jotta ne voidaan priorisoida organisaation riskinsietokyvyn ja liiketoimintatavoitteiden mukaisesti.
* **Riskien käsittely:** Määritetään sopivimmat riskienhallintatoimenpiteet, jotka voivat sisältää riskin välttämisen, vähentämisen, jakamisen tai hyväksymisen.
* **Seuranta ja tarkastelu:** Riskien ja niiden käsittelytoimenpiteiden tehokkuuden säännöllinen seuranta ja arviointi ISMS-järjestelmän jatkuvan parantamisen varmistamiseksi.
* **Viestintä ja konsultointi:** Varmistetaan tehokas sisäinen ja ulkoinen viestintä sekä sidosryhmien osallistuminen riskienhallintaprosessiin.

Tämä menetelmä perustuu ISO 27001 –standardin periaatteisiin ja ohjeisiin ja tukee organisaation sitoutumista vahvaan tietoturvaan.

Lisätietoja riskiarvioinnin suorittamisesta ja sopivien käsittelyvaihtoehtojen valitsemisesta löytyy [lisää dokumentti], joka on saatavilla [lisää sijainti]. Dokumenttia ylläpitää Tietoturvaryhmä.

Kaikkien työntekijöiden ja asiaankuuluvien ulkoisten tahojen tulee perehtyä dokumentissa kuvattuun menetelmään ja osallistua aktiivisesti tietoturvariskien tunnistamiseen ja hallintaan omalla vastuualueellaan.