HENKILÖTIETOJEN TIETOTURVA TILITOIMISTOSSA
Liite 1-B

Päivitetty lokakuu 2026

Hallinto

Tietoturva ja henkilötietojen asianmukainen käsittely ovat kiinteä osa tilitoimiston toimintaa ja johtamista. Tietojen suojaamisesta huolehditaan sekä teknisin että organisatorisin toimenpitein. Tietoturvan hallinta perustuu määriteltyihin toimintaperiaatteisiin, vastuisiin ja säännölliseen arviointiin.

Tietoturvan ja henkilötietojen käsittelyn asianmukaisuus varmistetaan muun muassa seuraavilla toimenpiteillä:

- Tietoturva ja henkilötietojen lainmukainen käsittely on huomioitu osana organisaation toimintaperiaatteita ja käytäntöjä.
- Tietoturvaan ja henkilötietojen käsittelyyn liittyvät roolit ja vastuut on määritelty ja nimetty.
- Organisaatiolla on määritelty tietoturvapolitiikka sekä sitä tukevat ohjeet ja toimintakäytännöt.
- Tietoturvapolitiikan ja tietoturvakäytäntöjen toimivuutta arvioidaan ja katselmoidaan säännöllisesti.
- Tietoturvan hallintaa ja siihen liittyviä käytäntöjä arvioidaan myös riippumattoman ulkopuolisen asiantuntijan toimesta.

Henkilöstö

Tietoturvan ja tietosuojan toteutuminen varmistetaan henkilöstöä koskevilla sopimuksilla, selkeästi määritellyillä vastuilla, sisäisillä ohjeistuksilla, koulutuksella sekä tietoturvapoikkeamien hallintaan liittyvillä toimintamalleilla.

- Henkilöstön roolit, työtehtävät ja vastuut on määritelty selkeästi.
- Työntekijöiden kanssa on sovittu liike- ja ammattisalaisuuksien sekä muiden luottamuksellisten tietojen salassapidosta.
- Henkilöstö on sitoutettu henkilötietojen asianmukaiseen ja tietosuoja-asetuksen mukaiseen käsittelyyn.

- Henkilöstö perehdytetään tietoturva- ja tietosuojapolitiikkoihin, ohjeisiin ja toimintakäytäntöihin osana uusien työntekijöiden perehdytystä.
- Henkilöstön tietoteknistä ja ammatillista osaamista ylläpidetään ja kehitetään säännöllisellä koulutuksella. Koulutuksissa käsitellään myös tietosuojaa ja tietoturvaa sekä tietojen asianmukaista ja turvallista käsittelyä.
- Henkilötietojen käsittelyä varten on laadittu sisäinen tietosuojapolitiikka ja sitä tukevat ohjeistukset.
- Tietoturvapoikkeamien ja henkilötietojen tietoturvaloukkausten ilmoittamista, käsittelyä ja tarvittavia jatkotoimenpiteitä varten on määritelty toimintamallit ja henkilöstölle on annettu niitä koskevat ohjeet.
- Työsuhteen muutostilanteita ja päättymistä varten on määritelty toimintamalli, jolla varmistetaan käyttöoikeuksien asianmukainen muuttaminen tai poistaminen sekä työntekijän hallussa olevien aineistojen palauttaminen.

Toimintamallit

- Suojattavan tiedon käsittely erilaisissa viestintäjärjestelmissä, kuten sähköpostissa tai pikaviestimissä on määritelty ja internetin ja sosiaalisen median käytölle tilitoimiston tietoverkossa luotu hyväksyttävän käytön pelisäännöt.
- Ulkopuolisten pilvitallennuspalveluiden käyttö tapahtuu ainoastaan yrityksen johdon määrittämissä tilanteissa ja hyväksymillä palveluntarjoajilla.
- Etätyöskentelylle on luotu tietoturvaan liittyvät ohjeet.

Toimitilaturvallisuus

- Tilitoimistolla on ajantasainen rekisteri toimitilojen ja muiden suojattavien kohteiden avaimista sekä kulkutunnisteista.
- Asiakkaiden ja kolmansien osapuolten pääsy työpisteisiin sekä suojattaviin kohteisiin ja tietoihin on estetty

Asiakkaan tunnistaminen ja aineistojen luovutukset

- Asiakkaiden edustajat tunnistetaan ennen asiakassuhteen alkamista ja tunnistetiedot tallennetaan rahanpesulain edellyttämällä tavalla.
- Asiakkaan aineistojen luovutustilanteessa noudatetaan hyvän tilitoimistotavan edellyttämiä sekä asiakkaan kanssa sovittuja tunnistus- ja luovutuskuittauskäytäntöjä. Paperisia aineistoja luovutettaessa tunnistamme henkilön ja laadimme aineistojen luovutuksesta luovutusdokumentin.
- Jos tilitoimisto hallinnoi sopimuksen mukaan asiakkaan puolesta asiakkaan käyttäjien pääsyä tietojärjestelmiin, käyttäjähallinnointi tapahtuu asiakkaan nimettyjen henkilöiden kanssa, sovittuja tunnistamistapoja hyödyntäen sekä käyttöoikeuksiin liittyvät tiedot toimitetaan tietoturvallisia menetelmiä käyttäen.

Käyttövaltuushallinta ja salasanapolitiikka

Käyttäjäoikeuksia hallinnoidaan keskitetysti ja järjestelmäkohtaisesti. Kaikilla työntekijöillä on henkilökohtaiset käyttäjätunnukset eri järjestelmiin ja pääsy luottamukselliseen tietoon tapahtuu aina kirjautumisen kautta. Mahdollisuuksien mukaan käytetään monivaiheisia tunnistautumismenetelmiä. Henkilökohtaisilla käyttäjätunnuksilla varmistetaan myös asianmukaiset lokitiedot tehdyistä muutoksista.

Lisäksi työntekijöiden käyttäjäoikeuksien tarpeellisuutta tarkastellaan työtehtävien olennaisesti muuttuessa.

- Tietojärjestelmissä käytetään vain yksilöityjä nimetyille henkilöille osoitettuja käyttäjätunnuksia.
- Henkilöstön käyttäjätunnuksista ja käyttöoikeuksista tilitoimiston ulkopuolisiin tietojärjestelmiin pidetään kirjaa.
- Työntekijöiden käyttöoikeuksien tarpeellisuutta tarkastellaan työtehtävien olennaisesti muuttuessa.
- Salasanat, PIN-koodit ja käyttäjähallintaan tarkoitetut koodit säilytetään tarkoitukseen soveltuvassa turvallisessa tietojärjestelmässä/tiedostossa.
- Kaikissa luottamuksellista tietoa sisältävissä tietojärjestelmissä on käytössä salasanaan tai vastaavaan menettelyyn perustuva pääsynhallinta.

Ulkopuoliset toimijat

Ulkopuolisia toimijoita ovat esimerkiksi siivousliikkeet, vartiointiliikkeet, kiinteistönhoitoyritykset, isännöintiliikkeet ja muut yhteistyökumppanit, joilla on pääsy organisaatioin toimitiloihin tai suojattaviin tietoihin.

- Tilitoimiston yhteistyökumppaneiden kanssa on laadittu kirjallinen sopimus luottamuksellisen tiedon salassapidosta ja yhteistyökumppanit ovat tietoisia tilitoimiston tietoturvakäytännöistä ja suojattavista kohteista sekä tietosuoja-asetuksen vaatimuksista.
- Toimitiloissa säännöllisesti työskentelevät ulkopuolisten toimijoiden työntekijät perehdytetään tarvittavissa määrin tilitoimiston tietoturvakäytäntöihin

Ulkoistetut ICT-palvelut

Ulkoistetuilla ICT-palveluilla tarkoitetaan VIEW Groupin käyttämiä ulkopuolisia palveluntarjoajia, jotka tuottavat esimerkiksi ICT-ympäristön, palvelimien ja työasemien ylläpitoon, tallennukseen ja varmistukseen, tietoturvaan tai tietoliikenneyhteyksiin liittyviä palveluita.

- Ulkoistetuista ICT-palveluista on laadittu kirjalliset palvelusopimukset, joissa määritellään palvelun tuottamiseen liittyvät keskeiset ehdot ja vastuut.
- Palveluntarjoajien kanssa on sovittu luottamuksellisten tietojen salassapidosta.
- VIEW Groupin ja palveluntarjoajan välinen vastuunjako on määritelty ja dokumentoitu.
- Palveluntarjoajille asetetaan palvelun edellyttämät tietoturvaa ja suojattavien tietojen käsittelyä koskevat vaatimukset.
- Ulkoistettujen ICT-palveluiden toimintaa, tietoturvaa ja kehittämistarpeita käsitellään säännöllisesti yhteistyössä palveluntarjoajien kanssa.

Suojattavien kohteiden ja tiedon hallinta

Asiakastietojen ja muiden suojattavien tietojen turvallisesta käsittelystä huolehditaan niiden koko elinkaaren ajan. Suojattavia kohteita ovat

tietojen lisäksi esimerkiksi työasemat, palvelimet, mobiililaitteet sekä muut tietojen käsittelyyn käytettävät laitteet ja välineet.

- Sähköisiin järjestelmiin ja asiakastietoihin myönnetään käyttöoikeudet työtehtävien ja käsittelytarpeen perusteella.
- Asiakkaiden kirjanpitoaineistojen, henkilötietojen ja muiden luottamuksellisten tietojen käsittelyä varten on laadittu sisäiset käsittely- ja prosessiohjeet.
- Suojattaville kohteille ja tietojärjestelmille on määritelty hyväksyttävän käytön periaatteet.
- Paperimuotoisen aineiston turvallista käsittelyä tuetaan turvatulostusratkaisulla, jolla ehkäistään luottamuksellisen aineiston joutumista asiattomien henkilöiden haltuun.
- Sähköisen ja paperimuotoisen aineiston turvalliseen hävittämiseen on määritelty asianmukaiset menettelytavat. Paperiaineiston hävittämiseen käytetään lukittuja tietosuojasäiliöitä tai muita tietoturvallisia hävitysmenetelmiä.
- Siirrettävien tietovälineiden, kuten USB-massamuistien, käyttöä asiakastietojen käsittelyssä vältetään.

Tietokoneiden ja mobiililaitteiden tietoturva

Tietokoneiden, mobiililaitteiden ja muiden päätelaitteiden tietoturvasta huolehditaan keskitetyn laitehallinnan, teknisten suojausratkaisujen sekä määriteltyjen käyttö- ja hallintakäytäntöjen avulla.

- Organisaation käytössä olevat työasemat, mobiililaitteet ja muut päätelaitteet rekisteröidään ja niitä hallitaan keskitetysti.
- Päätelaitteiden käyttöjärjestelmien ja ohjelmistojen tietoturvapäivityksistä huolehditaan keskitetysti ja niiden ajantasaisuutta valvotaan.
- Työntekijöillä ei ole oikeuksia asentaa muita kuin organisaation hyväksymiä ohjelmistoja omille työasemilleen.
- Päätelaitteilla käytetään keskitetysti hallittuja virus- ja haittaohjelmien torjunta- sekä muita tietoturvaratkaisuja.
- Tietoverkkoja ja päätelaitteita suojataan palomuuriratkaisuilla.
- Työasemien tallennuslevyt on suojattu salauksella.

- Työasemien ja palvelimien haavoittuvuuksia tunnistetaan ja arvioidaan tarkoitukseen soveltuvilla skannaus- ja analysointityökaluilla.
- Henkilökohtaisten tietokoneiden ja mobiililaitteiden käyttö henkilötietojen käsittelyyn on kielletty.

Siirrettävät tietovälineet

Siirrettäviä tietovälineitä ovat esimerkiksi USB-muistitikut, USB-massamuistit, CD/DVD-levyt ja muut vastaavat muistilla tai tallennustilalla varustetut laitteet, jotka voidaan kytkeä tietokoneeseen.

- Tilitoimistossa ei käytetä siirrettäviä tietovälineitä työtehtävien hoitamiseen tai suojattavan tiedon käsittelyyn lukuun ottamatta erikseen sovittuja tilanteita kuten aineiston luovutus tilintarkastajalle tai aineiston luovutus tai vastaanotto asiakkaan nimetyn yhteyshenkilön kanssa, mikäli se ei ole muilla keinoilla mahdollista.
- Käytettäessä siirrettäviä tietovälineitä edellä mainittuihin tarkoitukseen on niiden sisältö suojattu salasanalla.

Palvelin- ja tietoliikenneturvallisuus

Verkon ajantasaisuudesta vastaa VIEW Groupin keskitetty ICT-hallinto yhdessä ICT palveluntarjoajan kanssa. Verkkolaitteet päivitetään säännöllisesti ja niissä esiin tulleet haavoittuvuudet paikataan. Käytössä on ainoastaan yrityskäyttöön tarkoitettuja verkkolaitteita, joiden toimintaa ja tietoturvaa valvotaan keskitetysti. VIEW Group Oy:n oma palvelinympäristö sijaitsee Ruotsissa, Microsoftin konesalissa. Kaikki tietoliikenne työasemien ja palvelimen välillä on salattua.

- Langattomien verkkojen tietoliikenne on salattu.
- Vierasverkot on eriytetty tilitoimiston sisäisestä tietoverkosta luotettavalla menetelmällä.
- Palvelinkäyttöjärjestelmät päivitetään säännöllisesti.
- Palvelinjärjestelmä on rakennettu vikasietoiseksi tai kahdennettuksi siten, että tietojärjestelmien toiminta ei keskeydy yksittäisestä laiterikosta.

Taloushallinnon pilvipalvelut

Taloushallinnon pilvipalvelulla tarkoitetaan SaaS- tai ASP-palveluna toimitettavia taloushallinnon tietojärjestelmiä, joita organisaatio käyttää taloushallinnon palveluidensa tuottamiseen omille asiakkailleen.

- Sopimuksiimme taloushallinnon pilvipalvelun käytöstä sisältyy kirjallinen palvelutasosopimus.
- Tilitoimiston ja palveluntarjoajan välinen vastuunjako on dokumentoitu kirjallisesti.
- Tilitoimisto on saanut palveluntarjoajalta selvitykset, jotka todentavat että palvelua tuotetaan tietosuoja-asetuksen sekä kirjanpitolain asettamat aineiston säilytysvaatimukset huomioiden.

Henkilötietojen tietoturva tilitoimistossa (Liite 1-B) versio

Tilitoimistolla on velvollisuus päivittää tähän henkilötietojen tietoturvaan koskevaan dokumenttiin tulevat muutokset vastaamaan kulloistakin käytäntöä.

Kulloinkin voimassa oleva versio tästä dokumentista on asiakkaan saatavilla osoitteessa https://viewgroup.fi/sopimusehdot