Tietoturvatoimet tilitoimistossa
Tilitoimiston toimeksiantosopimuksen Liite nro 1B
Tilitoimisto: Tili Johanna

Tämä seloste kertoo tietoturvaa ja henkilötietojen lainmukaista käsittelyä varmentavista toimista, joita noudatetaan tilitoimistossa Tili Johannalla. Nämä tietoturvatoimet koskevat Tili Johannan toimintaa henkilötietojen käsittelijänä ja rekisterinpitäjänä sekä muiden luottamuksellisten aineistojen käsitelijänä.

Hallinto

- Tietoturva sekä henkilötietojen lainmukainen käsittely ovat keskeinen osa tilitoimiston toimintaperiaatteita.
- Tietoturvaan ja henkilötietojen käsittelyyn liittyvät roolit ja vastuut on nimetty henkilötasolla.
- Tietoturvapolitiikka ja siihen liittyvät käytännöt on määritelty.

Henkilösto

- Henkilöstön roolit, työtehtävät ja vastuut on määritetty selkeästi.
- Työntekijöiden kanssa on laadittu sopimus liike- ja ammattisalaisuuksien salassapidosta.
- Ty6suhteiden päättymisen varalle on luotu toimintamalli, jossa on huomioitu käyttöoikeuksien poistaminen ja työntekijän hallussa mahdollisesti olevien aineistojen palauttaminen.
- Henkilöstö on perehdytetty tietoturvapolitiikkaan ja -käytäntöihin ja perehdytys kuuluu osana uusien työntekijöiden koulutusohjelmaa.
- Olennaisten tietoturvaan liittyvien vaaratilanteiden raportointiin ja käsittelyyn on toimintamalli.

Toimintamallit

- Suojattavan tiedon käsittely erilaisissa viestintäjärjestelmissä, kuten sähkököpostissa 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 hyväksymillä palveluntarjoajilla.
- Etätyöskentelylle on luotu tietoturvaan liittyvät ohjeet.

Toimitilaturvallisuus

- Tilitoimiston tiloissa on turvalukitus.
- 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. Tunnistetiedot tallennetaan rahanpesulain edellyttämällä tavalla.
- Asiakkaan aineistojen luovutustilanteessa noudatetaan hyvän tilitoimistotavan edellyttämiä sekä asiakkaan kanssa sovittuja tunnistus- ja luovutus kuittauskäytäntöjä.
- Jos tilitoimisto hallinnoi sopimuksen mukaan asiakkaan puolesta asiakkaan käyttäjien pääsyä tietojärjestelmiin, käyttäjähallinnointi tapahtuu asiakkaan nimettyjen henkilöiden kanssa, sovittuja tunnustamistapoja hyödyntäen sekä huolehtien tunnusten ja salasanojen tietoturvallisista toimitustavoista.

Käyttävaltuushallinta ja salasanapolitiikka

- Tietojärjestelmissä käytetään vain yksilöityjä nimetyille henkilöille osoitettuja käyttäjätunnus- tai salasanapareja. Poikkeuksena ovat tilanteet, joissa tilitoimisto johto on arvioinut riskin epäolennaiseksi.
- 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.
- Tietojärjestelmien pääkäyttäjätunnusten oletussalasanat on vaihdettu ja tietojärjestelmien salasanat vaihdetaan säännöllisesti.

Ulkopuoliset toimijat

- 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

- Ulkopuolisista ICT-palveluista on laadittu kirjalliset palvelusopimukset sekä kirjallinen sopimus luottamuksellisen tiedon salassapidosta.
- Tilitoimiston ja palveluntarjoajan välinen vastuunjako on dokumentoitu kirjallisesti ja palveluntarjoaja on tietoinen tilitoimiston tietoturvakäytännöistä ja suojattavista kohteista.

Suojattavien kohteiden ja tiedon hallinta

Suojattavia kohteita ovat esimerkiksi työasemat, kannettavat tietokoneet, palvelimet ja mobiililaitteet.

- Suojattaville kohteille on maaritelty hyväksyttävän käytön pelisäännöt.
- Asiakkaan kirjanpitoaineistolle, henkilötiedoille ja muille tiedoille on laadittu käsittelyohjeet.
- Sekä digitaalisen tiedon että tulosteiden tuhoamiselle on laadittu tietoturvallisen tuhoamisen menettely ohjeet.
- Käytössä on asianmukaiset tietosuojaroskasäiliöt tai asiakirjasilppuri luokitellun tiedon tuhoamista varten.

Tietokoneiden ja mobiililaitteiden tietoturva

- Tilitoimiston käytössä olevat työasemat, kannettavat tietokoneet, mobiililaitteet ja muut päätelaitteet on rekisterbity ja dokumentoitu asianmukaisesti.
- Koneiden säännöllisistä tietoturvapäivityksistä huolehditaan asianmukaisesti ja päivityksiä valvotaan. Työntekijöiden oikeutta asentaa ohjelmistoja työasemille on rajattu ja asennuksia valvotaan.
- Asianmukainen virus- ja haittaohjelmien torjuntaohjelmisto on käytössä.
- Tietoverkko ja tietokoneet on suojattu palomuurilla.
- Työntekijöiden 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 kytked 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.
- Käytettäessä siirrettäviä tietovälineitä edellä mainittuihin tarkoituksiin on niiden sisältö suojattu salasanalla.

Palvelin- ja tietoliikenneturvallisuus

- Toimitilojen palvelintilat ja tietoliikenneyhteyksien edellyttämät tilat pidetään lukittuina.
- Langattomien verkkojen tietoliikenne on salattu.
- Vierasverkot on eriytetty tilitoimiston sisäisestä tietoverkosta luotettavalla menetelmällä.
- Palvelinkäyttöjärjestelmät päivitetään säännöllisesti.
- Palvelinjärjestelmä on rakennettu vikasietoiseksi tai kahdennetuksi siten, että tietojärjestelmien toiminta ei keskeydy yksittäisestä laiterikosta.

Taloushallinnon pilvipalvelut

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

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