HENKILÖTIETOJEN TIETOTURVA TILITOIMISTOSSA

Tietoturvaa ja henkilötietojen lainmukaista käsittelyä varmentavat toimet.	
Tilitoimisto: Tili- ja yrityskonsultointi EiVi Ky	
Laatija, päivittäjä: **Ville Hiltunen**	
Päiväys, muutospäiväys: 04.12.2018	
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
Henkilöstö	
✓	Henkilöstön roolit, työtehtävät ja vastuut on määritetty selkeästi.
✓	Työntekijöiden kanssa on laadittu sopimus liike- ja ammattisalaisuuksien salassapidosta
✓	Työsuhteiden 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 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.
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

✓	Tilitoimiston tiloissa on murtohälytysjärjestelmä
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.
✓	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
Käyttövaltuushallinta ja salasanapolitiikka	
✓	Tietojärjestelmissä käytetään vain yksilöityjä nimetyille henkilöille osoitettuja käyttäjätunnus/salasanapareja. Poikkeuksena ovat tilanteet, joissa tilitoimiston johto on arvioinut riskin epäolennaiseksi.
✓	Henkilöstön käyttäjätunnuksista ja käyttöoikeuksista tilitoimiston ulkopuolisiin tietojärjestelmiin pidetään kirjaa.
✓	Työntekijöiden käyttöoikeuksien tarpeellisuutta tarkastellaan työtehtävien olennaisesti muuttuessa.
✓	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	
Ulkopuolisia toimijoita ovat esimerkiksi siivousliikkeet, vartiointiliikkeet, kiinteistönhoitoyritykset, isännöintiliikkeet ja muut yhteistyökumppanit, joilla on pääsy organisaatioin toimitiloihin tai suojattaviin tietoihin.	
Ulkoistetut ICT-palvelut	
Ulkoistetuilla ICT-palveluilla tarkoitetaan tässä kohdassa tilitoimiston ulkopuolisia yrityksiä, jotka tuottavat tilitoimistolle esimerkiksi palvelimien ja työasemien ylläpitopalvelua, tallennus- sekä varmistuspalveluita, tietoturvan ylläpitopalvelua tai tietoliikenneyhteyksien ylläpitopalvelua.	
✓	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 määritelty hyväksyttävän käytön pelisäännöt.

	Asiakaan kirjanpitoaineistolle, henkilötiedoille ja muille tiedoille on laadittu käsittelyohjeet.
✓	Sekä digitaalisen tiedon, että tulosteiden tuhoamiselle on laadittu tietoturvallisen tuhoamisen menettelyohjeet.
✓	Käytössä on asianmukaiset tietosuojaroskasäiliöt tai asiakirjasilppuri luokitellun tiedon tuhoamista varten.
Tietokoneiden ja mobiililaitteiden tietoturva	
✓	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 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.
Palvelin- ja tietoliikenneturvallisuus	
✓	Toimitilojen palvelintilat ja tietoliikenneyhteyksien edellyttämät tilat pidetään lukittuina.
✓	Langattomien verkkojen tietoliikenne on salattu.
✓	Palvelinjärjestelmä on rakennettu vikasietoiseksi tai kahdennettuksi 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 palvelutasosopimus.
✓	Tilitoimiston ja palveluntarjoajan välinen vastuunjako on dokumentoitu kirjallisesti.
✓	Tilitoimisto on saanut palveluntarjoajalta selvitykset, jotka todentavat että palvelua tuotetaan tietosuojaasetuksen sekä kirjanpitolain asettamat aineiston säilytysvaatimukset huomioiden.