HENKILÖTIETOJEN TIETOTURVA TILITOIMISTOSSA

Liite 1-B
Versio 31.5.2018

Tietoturva tilitoimistossa varmistetaan sekä teknisin että organisatorisin toimenpitein. Henkilötietojen käsittely toteutetaan asianmukaisesti ja tietoturvallisesti. Asianmukainen käsittely varmistetaan alla listatuilla toimenpiteillä.

Henkilöstö

Rantalaisen työntekijöiden kanssa on laadittu sopimus liike- ja ammattisalaisuuksien salassapidosta. Lisäksi koko henkilöstö on allekirjoittanut tietosuojasopimuksen, jonka tarkoituksena on varmistaa käsittelemiemme rekisteröityjen yksityisten ihmisten tietosuoja-asetuksen mukaisten oikeuksien toteutuminen. Rantalainen panostaa henkilöstönsä tietotekniseen- sekä substanssiosaamiseen säännöllisillä koulutuksilla. Tietosuoja ja tietoturva-asioita käsitellään koulutuksissa, joissa painopisteenä on tietojen laadukas ja asianmukainen käsittely. Lisäksi on luotu sisäinen tietosuojapolitiikka ja -ohjeistus, jonka mukaisesti henkilötietoihin pohjautuvaa materiaalia käsitellään. Asiakasmateriaaleja säilytetään lukituissa tiloissa.

Työsuhteiden muutostilanteiden varalle on luotu toimintamallit, joilla varmistetaan, että käyttöoikeudet poistetaan viimeistään työsuhteen päättyessä. Mahdollisten olennaisten tietoturvaan liittyvien poikkeamien varalle on kehitetty toimintamalli osana sisäistä toiminnan ohjausta.

Etätyön tekemisestä on määritetty sisäinen ohjeistus, jossa on huomioitu tietosuojasäännökset.

Asiakkaan tunnistaminen ja aineistojen luovutus

Asiakas pyritään aina tunnistamaan sähköisin menetelmin ja siten aineistot pyritään luovuttamaan sähköisessä muodossa ja salattuna. Paperisia aineistoja luovutettaessa tunnistamme henkilön ja laadimme aineistojen luovutuksesta luovutusdokumentin.

Käyttöoikeuksien hallinnointi ja salasanapolitiikka

Käyttäjäoikeuksia hallinnoidaan keskitetysti ja järjestelmäkohtaisesti. Kaikilla työntekijöillä on henkilökohtaiset käyttäjätunnukset eri järjestelmiin, ja pääsy luottamukselliseen tietoon tapahtuu aina salasanan avulla. Soveltuvin osin käytetään monivaiheisia tunnistautumismenetelmiä. Henkilökohtaisilla käyttäjätunnuksilla varmistetaan myös asianmukaiset lokitiedot tehdyistä muutoksista. Salasanat vaihdetaan säännöllisesti yrityksen kulloinkin voimassa olevan salasanapolitiikan mukaisesti, ja salasanan kompleksisuus on varmistettu teknisillä menetelmillä. Eri järjestelmien oletussalasanat on vaihdettu käyttöönoton yhteydessä. Lisäksi työntekijöiden käyttäjäoikeuksien tarpeellisuutta tarkastellaan työtehtävien olennaisesti muuttuessa.

Ulkoistetut ICT-palvelut ja ohjelmistot

Ulkopuolisista ICT-palveluista on laadittu kirjalliset palvelusopimukset sekä kirjalliset sopimukset luottamuksellisten tietojen salassapidosta. Rantalaisen ja palveluntarjoajan välinen vastuunjako on dokumentoitu kirjallisesti. Rantalainen toimii läheisessä yhteistyössä ICT-palveluntarjoajansa kanssa ja kehittää säännöllisesti sekä sisäisen ICT-ympäristön että ulkoisten palveluidensa tietoturvaa.

Tiedon hallinta ja suojattavat kohteet

Rantalainen pyrkii käsittelemään kaikkea asiakastietoa sähköisin menetelmin. Sähköisissä järjestelmissä pääsy on rajattu tietoja käsitteleville henkilöille ja heidän varahenkilöilleen. Asiakasmateriaalin käsittelylle on laadittu sisäiset käsittely- ja prosessiohjeet, jolla varmistetaan asianmukainen käsittely. Paperisen asiakasmateriaalin tuhoamista varten on käytössä lukitut tietosuojaroskasäilöt. Käytössä on turvatulostusratkaisu, jolla vältetään paperisen asiakasmateriaalin joutuminen vääriin käsiin. Siirrettäviä tietovälineitä, kuten USB-massamuisteja ja niiden käyttöä pyritään välttämään asiakasmateriaalin käsittelyssä.

Tietokoneiden ja mobiililaitteiden tietoturva

Rantalaisella on käytössä keskitetty työasemahallinta, jonka kautta työasemiin jaellaan säännöllisesti ajantasaiset tietoturvapäivitykset. Työntekijöillä ei ole oikeuksia asentaa muita kuin Rantalaisen ICT-hallinnon hyväksymiä ohjelmistoja omille työasemilleen. Käytössä ovat keskitetyt virustorjunta- ja palomuurisovellukset, joiden ajantasaisuutta valvotaan. Yhteydet sähköisiin järjestelmiin toteutetaan salattujen yhteyksien kautta. Työasemien levyjärjestelmät ovat kryptattuja, sekä työasemien ja palvelimien haavoittuvuuksia tutkitaan skannaus- ja analysointityökalujen avulla.

Verkon ja muun ICT-ympäristön tietoturva

Verkon ajantasaisuudesta vastaa Rantalaisen keskitetty ICT-hallinto yhdessä ICT-palveluntarjoajan kanssa. Verkkolaitteet päivitetään säännöllisesti ja niissä esiin tulleet haavoittuvuudet paikataan. Käytössä on vain yrityskäyttöön tarkoitettuja verkkolaitteita. Rantalaisen oma palvelinympäristö sijaitsee Suomessa ICT-palveluntarjoajan konesalissa ja ympäristö on kahdennettu. Kaikki tietoliikenne toimipisteiden ja konesalin välillä on salattua. Asiakasverkot (mukaan lukien langaton vierasverkko) on eriytetty Rantalaisen omasta verkosta.

Taloushallinnon ohjelmistot ja pilvipalvelut

Sisäisessä käytössä ja asiakaskäytössä on useita erilaisia taloushallinnon ohjelmistoja ja pilvipalveluita. Tietoturvaa eri ohjelmistoissa on kuvattu henkilötietojen käsittelyä koskevan sopimuksen liitteessä 2-B.