KIRKON TIETOTURVAPOLITIIKKA

Suomen evankelis-luterilaisen kirkon tietojärjestelmien tietoturvapolitiikka

21.3.2019

KIRKON TIETOTURVAPOLITIIKKA

Suomen evankelis-luterilaisen kirkon tietojärjestelmien tietoturvapolitiikka

Sisällysluettelo

KIRKON TIETOTURVAPOLITIIKKA

Suomen evankelis-luterilaisen kirkon tietojärjestelmien tietoturvapolitiikka

1 JOHDANTO

Tietoturvapolitiikka määrittelee tietoturva- ja tietosuojatyön tavoitteet, vastuut ja organisoinnin Suomen evankelis-luterilaisessa kirkossa ja sen toimintayksiköissä. Tietoturvapolitiikka on annettu tiedoksi koko kirkon henkilöstölle ja yhteistyökumppaneille ja kaikkien kirkon työ- ja virkasuhteisten henkilökunnan samoin kuin vapaaehtoisten työntekijöiden ja luottamusasemassa olevien henkilöiden tulee toimia sen mukaisesti. Politiikkaa tarkennetaan kirkon tietoturvavaatimuksissa sekä muissa koko kirkon tai IT-alueen tasoisissa ohjeissa.

2 KESKEISET TERMIT

Tietoturvallisuuteen kuuluvat kaikki ne järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus[1]. Sanan tietoturvallisuus tilalla käytetään usein myös sanaa tietoturva. Ne tarkoittavat samaa asiaa.

Käytettävyys tarkoittaa tietoturvallisuuden yhteydessä sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Käytettävyyttä uhkaavat mm. ennakoimattomat tietokoneiden, tietoliikenneverkkojen ja tietokoneohjelmien rikkoutumiset. Ne voivat aiheutua esimerkiksi jonkin teknisen komponentin yllättävästä vikaantumisesta, tietokoneohjelman tekijän inhimillisestä virheestä tai rikollisen tahon tekemästä haittaohjelmasta tai jopa ns. verkkohyökkäyksestä.

Eheys tarkoittaa tietoturvallisuuden yhteydessä sitä, että tieto on yhtäpitävä alkuperäisen tiedon kanssa. Eheyttä uhkaavat mm. inhimilliset virheet tai väärinkäsitykset tietokoneohjelmien rakentamisessa tai tietojen tallennuksessa. Eheyttä uhkaavat myös rikollisten tahojen tarkoituksellisesti tekemät tietojen muuttamiset esimerkiksi rahaliikenteen käsittelyssä tai Internet-sivustojen sisällössä.

Luottamuksellisuus tarkoittaa sitä, että kukaan sivullinen ei saa tietoa tai ei voi käsitellä sitä. Luottamuksellisuutta uhkaavat samat seikat kuin eheyttäkin. Lisäksi luottamuksellisuus on uhattuna, jos tiedon käsittelyn käyttövaltuushallinnan prosessit tai niiden toteutus on hoidettu huonosti.

Tietoturvallisuudessa ei ole kyse vain tekniikasta, vaan ihmisten työskentelytavoista. Kaikkien tulee tietää, miten tietoturvallisuudesta voidaan huolehtia. Kyse ei ole myöskään vain yksittäisistä toimenpiteistä, vaan jatkuvasta ja suunnitelmallisesta toiminnasta, jonka kohteena ovat seuraavat kahdeksan tietoturvatyön osa-aluetta:

1. **Hallinnollinen tietoturvallisuus**: Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaatiossa käytettäviä tietoturvallisuuden toimintapolitiikkoja, toiminnan linjauksia, johtamista, organisointia, toimintojen sijoitusta organisaatioon, resursointia sekä vastuiden määrittelyä.

2. **Henkilöstöturvallisuus**: Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation tietojen ja tietojenkäsittelyn suojaamista ihmisten aiheuttamilta tahallisilta sekä tahattomilta uhkilta ja ihmisten toimista tietoturvallisuuden varmistajina.

3. **Fyysinen tietoturvallisuus**: Tietoturvallisuuden osa-alue, jossa tarkastellaan kaikkia organisaation tuotanto- ja toimitilojen fyysiseen suojaamiseen liittyviä asioita, joilla pyritään estämään organisaation tarvitsemien tietojen sekä fyysisen ja ei-fyysisen ominaisuuden tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin. Fyysinen turvallisuus on myös tietojen käytettävyyden ylläpitoa, siltä osin kuin tilaratkaisut voivat sitä palvella tai mahdollisesti olla esteenä.

4. **Tietojen ja tietojärjestelmien käytön turvallisuus**: Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation automaattisen ja manuaalisen tietojenkäsittelyn suojaamiseen liittyviä asioita.

5. **Laitteistoturvallisuus**: Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation käyttämien tietojenkäsittely- ja tietoliikennelaitteiden suojaamisasioita.

[1] Tietoturvallisuudelle on useita erilaisia määritelmiä. Tässä yhteydessä on käytetty valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hyväksymää sanastoa ja sen määritelmiä.

6. **Ohjelmistoturvallisuus**: Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation käyttämien tietokoneohjelmien suojaamista sekä ohjelmien lisensointia ja rekisteröintiä.

7. **Tietoaineistoturvallisuus**: Tietoturvallisuuden osa-alue, jossa tarkastellaan kaikissa eri talletusmuodoissa olevia organisaation päivittäessä toiminnassa tarvitsemia tietoja sekä niiden suojaamiseen liittyviä asioita.

8. **Tietoliikenneturvallisuus**: Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation käyttämien tietoverkkojen ja niissä tapahtuvien tietoliikenteen suojaamiseen liittyviä asioita.

Tietoturvatyö liittyy myös valmiussuunnitteluun ja varautumiseen yhteiskunnan häiriötilanteisiin ja poikkeusoloihin. Valtioneuvoston 23.11.2006 tekemä periaatepäätös yhteiskunnan elintärkeiden toimintojen turvaamisesta määrittelee uhkamalleja, joihin yhteiskunnan eri toimijoiden on valmiustoimissaan varauduttava. Ensimmäinen näistä uhkamalleista on sähköisen infrastruktuurin häiriintyminen.

Tietoturvallisuuden yhteydessä puhutaan usein myös tietosuojasta. Tietosuojassa on kyse oikeuksista ja velvollisuuksista sekä erityisesti yksityisyyden suojaan liittyvästä perusoikeudesta. Tietosuojassa on kyse siitä kuka saa käsitellä henkilötietoja, kenen henkilöiden ja mitä nimenomaisia tietoja hän saa käsitellä, ja missä tarkoituksessa.

EU:n yleinen tietosuoja-asetus tulee sovellettavaksi 25.5.2018 alkaen. Tietosuoja-asetus on suoraan sovellettavaa lainsäädäntöä aivan kuten mikä tahansa eduskunnan hyväksymä laki tai asetus. Lisäksi se on siten vahvemmassa asemassa, että mikään kansallinen laki tai asetus ei saa olla ristiriidassa EU:n tietosuoja-asetuksen kanssa. Tietosuoja-asetuksen säännöksiä täydennetään ja täsmennetään kansallisella lainsäädännöllä siltä osin kuin tietosuoja-asetuksessa on annettu kansallista harkintamarginaalia näin säätää.

3 KIRKON TIETOTURVATYÖN ORGANISOINTI

3.1 Yleistä

Seuraavissa kappaleissa on käsitelty tietoturvatyön organisointia, toimijoita ja niiden rooleja. Kuvaus on kirjoitettu seurakuntatalouden näkökulmasta. Samoja periaatteita noudatetaan soveltaen myös kirkon keskushallinnossa ja hiippakuntien tuomiokapituleissa.

3.2 Kirkolliskokous

Kirkolliskokous linjaa kokonaiskirkon ja seurakuntien tietoturva-asioita seuraavissa yhteyksissä:

- Kirkkolaki ja kirkkojärjestys: Kirkolliskokous tekee ehdotuksia eduskunnalle kirkkolain säätämisestä ja hyväksyy kirkkojärjestyksen. Näissä säädöksissä on myös tietoturvaa koskevia säännöksiä. Esimerkiksi kirkkolain 16 luvussa ja kirkkojärjestyksen 16 luvussa on kirkonkirjojenpitoon ja Kirjuri-jäsentietojärjestelmään liittyviä tietoturvaa koskevia säännöksiä.

- Yleinen lainsäädäntö: Tietoturva-asioiden hoitamisessa on otettava huomioon yleinen lainsäädäntö, joka sisältää tietoturvallisuutta koskevia säännöksiä ja joka kirkkolain perusteella tai muutoin välittömästi koskee myös kirkollishallintoa. Tällaisia säädöksiä ovat muun muassa henkilötietolaki, laki viranomaisten toiminnan julkisuudesta, sähköisen viestinnän tietosuojalaki, laki yksityisyyden suojasta työelämässä, hallintolaki, laki sähköisestä asioinnista viranomaistoiminnassa, laki uskontokuntien jäsenrekistereistä, laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista.

- Kirkon keskusrahaston talousarvio ja toiminta- ja taloussuunnitelma: Kirkolliskokous vahvistaa kirkon keskusrahaston talousarvion ja käsittelee toiminta- ja taloussuunnitelman. Nämä sisältävät myös tietoturvallisuuden kehittämiseen liittyviä asioita.

3.3 Kirkkohallituksen täysistunto

Tietoturva-asioihin liittyen kirkkohallituksen täysistunto:

- Asettaa kirkon tietoturvan johtoryhmän
- Antaa kirkon tietoturvamääräykset[2]

3.4 Kirkkohallituksen virastokollegio

Tietoturva-asioihin liittyen kirkkohallituksen virastokollegio:

[2] Kirkon tietoturvamääräys on kirkkolain tai kirkkojärjestyksen perusteella annettava seurakuntia sitova määräys.

- Nimittää kirkon tietoturvapäällikön
- Antaa yllättävän tietoturvauhan tai poikkeamatilanteen yhteydessä sellaisen kirkon tietoturvamääräyksen, joka on voimassa enintään neljä kuukautta
- Antaa kirkon tietoturvamääräyksiä täydentäviä yleisiä tietoturvaohjeita ja suosituksia sekä työalakohtaisiin tietojärjestelmiin ja perustietotekniikkaan liittyviä erityisiä tietoturvaohjeita

3.5 Kirkon tietoturvapäällikkö

Kirkon tietoturvapäällikkö:

- Vastaa KIRKKO-verkon ylläpidosta, verkon viestintäpalveluiden välisestä liikenteestä ja tietoturvasta sekä turvallisuudesta
- Toimii KIRKKO-verkon yhteisötilaajan vastuuhenkilönä, jolla on oikeus käsitellä tarpeellisia tunnistetietoja
- Oikeus ryhtyä välittömiin suojelutoimenpiteisiin Suomen lainsäädännön määrittelemissä puitteissa
- Nimeää yksittäistapauksessa tunnistamistietojen käsittelyssä mukana olevat henkilöt kirjallisesti etukäteen ja raportoi ilman aiheetonta viivytystä käsitellyistä tunnistetiedoista tietohallintojohtajalle
- Valmistelee yllättävän tietoturvauhan tai poikkeamatilanteen yhteydessä tilapäisen tietoturvamääräyksen Kirkkohallituksen virastokollegion päätettäväksi
- Vastaa tietoturva-asioiden tiedottamisesta tai sen järjestämisestä seurakunnille sekä tiedotusvälineille ja muille kirkon ulkopuolisille tahoille
- Järjestää seurakuntien toimittamien tietoturvaa koskevien arviointi- ja tapahtumaraporttien vastaanoton ja käsittelyn

Kirkon tietoturvapäällikön vastuulla ei kuitenkaan ole erilaisten tietojärjestelmien sisältöasioihin liittyvät tietoturvan tai tietosuojan asiat. Tietoturvapäällikön nimittää Kirkkohallituksen virastokollegio.

3.6 Kirkon tietoturvallisuuden johtoryhmä

Kirkon tietoturvallisuuden johtoryhmä:

- Seuraa tietoturvallisuuden tilannetta ja kehittämistarpeita koko kirkossa
- Valmistelee esityksen kirkon tietoturvapolitiikasta ja sen päivittämisestä
- Valmistelee esityksen kirkon yleisistä tietoturvamääräyksistä ja niiden päivittämisestä
- Valmistelee kirkon tietoturvapolitiikkaa ja yleisiä tietoturvamääräyksiä täydentäviä yleisiä ohjeita ja suosituksia
- Ohjaa ja tukee kirkon tietoturvapolitiikan, tietoturvamääräysten ja tietoturvaohjeiden koulutuksen järjestämistä ja muuta jalkautusta
- Tekee aloitteita työalakohtaisia tietojärjestelmiä ja niiden toimintoja tai perustietotekniikan eri osa-alueita koskettavien tarkempien tietoturvamääräysten ja -ohjeiden laatimisesta ja toimii yhteistyössä näiden laatimisprojektien kanssa

3.7 Kirkon yhteisten tietojärjestelmien tietoturvamääräykset ja -ohjeet

Kirkon yhteisten työalakohtaisten tietojärjestelmien sisällöllinen omistaja ja tekninen omistaja ovat yhdessä vastuussa tietojärjestelmän ja sen sisältämän tai sillä käsiteltävän tieto-omaisuuden turvallisuusvaatimusten laatimisesta ja noudattamisesta. Ratkaisut eivät saa olla ristiriidassa kirkon tietoturvapolitiikan ja yleisten tietoturvamääräysten kanssa.

Esimerkkeinä näistä kirkon yhteisistä tietojärjestelmistä ovat Kirjuri-jäsentietojärjestelmä, Kirkon palvelukeskuksen järjestelmät, seurakuntavaalien järjestelmät, evl.fi-sähköposti sekä verkossa tehtävän seurakuntatyön järjestelmät.

3.8 Kirkon yhteisen perustietotekniikan tietoturvamääräykset ja -ohjeet

Perustietotekniikan (it-infrastruktuurin) eri osa-alueiden omistajat ovat vastuussa näitä osa alueita koskevan tietoturvallisuuden suunnittelusta ja hoitamisesta. Ratkaisut eivät saa olla ristiriidassa kirkon tietoturvapolitiikan ja yleisten tietoturvamääräysten kanssa.

Esimerkkeinä näistä osa-alueista ovat KIRKKO-verkon keskitetty Internet-palomuuri, sekä KIRKKO-verkon yhteiset reitittimet ja kytkimet.

3.9 Seurakunnan kirkkoneuvosto tai seurakuntayhtymän yhteinen kirkkoneuvosto

Tietoturva-asioihin liittyen seurakunnan kirkkoneuvosto tai seurakuntayhtymän yhteinen kirkkoneuvosto:

- Vastaa seurakuntataloudelle annettujen tietoturvallisuutta koskevien määräysten ja ohjeiden noudattamisesta.
- Huolehtii siitä, että seurakuntataloudelle on asetettu tietoturvaryhmä. Ryhmän on järkevää olla yhteinen IT-yhteistyöalueen kaikkien seurakuntien kanssa.
- Huolehtii siitä, että seurakuntataloudelle on nimetty tietoturvavastaava. Sen on järkevää olla yhteinen IT-yhteistyöalueen kaikkien seurakuntien kanssa.
- Huolehtii siitä, että seurakuntataloudelle on nimetty yksi tai useampia tietoturvan yhdyshenkilöitä siten, että kukin seurakuntatalouden työntekijä tuntee oman yhdyshenkilönsä.
- Hyväksyy seurakuntatalouden oman tietoturvapolitiikan. Sen on järkevää olla yhteinen IT-yhteistyöalueen kaikkien seurakuntien kanssa. Siinä linjataan, miten seurakuntatalouden tietoturvallisuudesta tarkemmin huolehditaan ja mitkä ovat eri toimijoiden roolit, vastuut ja oikeudet. Siinä linjataan myös sisäisen valvonnan järjestäminen tietoturvallisuuden osalta.

3.10 IT-alueen / seurakuntatalouden tietoturvaryhmä

Tietoturvaryhmä:

- Ylläpitää IT-alueen seurakuntatalouksien tietoturvapolitiikan ja tietoturvallisuuteen liittyviä määräyksiä, ohjeita ja suosituksia siten, että ne ovat linjassa kirkon yhteisen tietoturvapolitiikan ja kirkon yhteisten tietoturvamääräysten kanssa.

- Valvoo tietoturvamääräysten, ohjeiden ja suositusten noudattamista.
- Käsittelee ajankohtaisia tietoturvallisuutta koskevia kysymyksiä.
- Suunnittelee ja järjestää tietoturvallisuuteen liittyvää koulutusta yhteistyössä tietoturvavastaavan ja tietoturvan yhdyshenkilöiden kanssa.

3.11 IT-alueen tietoturvavastaava

Tietoturvavastaava:

- Kehittää jatkuvasti ja aktiivisesti IT-alueen seurakuntien tietoturvallisuutta.
- Vastaa tietoturvallisuuteen liittyvien ohjeiden, suositusten ja määräysten tiedottamisesta tietoturvan yhdyshenkilöille, esimiehille ja kaikille työntekijöille.
- Ottaa vastaan havaintoja tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista ja raportoi ne säännöllisesti tietoturvaryhmälle ja kirkon tietoturvapäällikölle.
- Hyväksyy yllättävän tietoturvauhan tai poikkeamatilanteen yhteydessä sellaisen seurakuntatalouden tietoturvamääräyksen, joka on voimassa enintään kaksi kuukautta.

Tietoturvavastaavan tehtävät kuvataan ja ohjeistetaan tarkemmin IT-alueen / seurakuntatalouden tietoturvapolitiikassa, tietoturvamääräyksissä ja/tai tietoturvaohjeissa.

3.12 Seurakuntatalouden tietoturvan yhdyshenkilö

Tietoturvan yhdyshenkilö:

- Huolehtii saamiensa tietoturvallisuuteen liittyvien ohjeiden, suositusten ja määräysten tiedottamisesta kaikille työntekijöille.
- Osallistuu esimiesten tukena uusien työntekijöiden perehdyttämiseen tietoturvallisuutta koskevissa kysymyksissä.
- Ottaa vastaan ilmoituksia seurakunnassaan havaituista tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista ja raportoi niistä IT-alueen / seurakunnan tietoturvavastaavalle sekä oman seurakuntansa esimiehille. Menettelyt kuvataan tarkemmin IT-alueen / seurakuntatalouden tietoturvapolitiikassa ja/tai tietoturvamääräyksissä.

Tietoturvan yhdyshenkilön tehtävät kuvataan ja ohjeistetaan tarkemmin IT-alueen / seurakuntatalouden tietoturvapolitiikassa, tietoturvamääräyksissä ja/tai tietoturvaohjeissa. Joillakin IT-alueilla on sovittu, että jokaisessa seurakuntataloudessa on oma it-yhdyshenkilö. Tällöin it-yhdyshenkilö voi toimia myös tietoturvan yhdyshenkilönä.

3.13 Esimies

Esimies on velvollinen

- välittämään tietoa tietoturvallisuuteen liittyvistä määräyksistä, ohjeista ja suosituksista omille työntekijöilleen
- järjestämään uusien työntekijöiden perehdytyksen tietoturvallisuuden määräyksistä, ohjeista ja suosituksista ja on velvollinen huolehtimaan siitä, että työntekijät ovat tiedostaneet ja oppineet kyseiset asiat

- huolehtimaan siitä, että työntekijät noudattavat annettuja määräyksiä ja ohjeita
- vastaamaan omien työntekijöidensä osalta siitä, että tietojärjestelmien käyttöoikeudet vastaavat työtehtävien tarpeita
- järjestämään omaa toimialaansa koskevien tietoturvamääräysten ja -ohjeiden laatimisen, jos asioita ei ole vielä ohjeistettu
- puuttumaan kaikkiin tietoturvaa koskettaviin havaitsemiinsa epäkohtiin

Esimiehen tehtävät kuvataan ja ohjeistetaan tarkemmin IT-alueen / seurakuntatalouden tietoturvapolitiikassa, tietoturvamääräyksissä ja/tai tietoturvaohjeissa.

3.14 Työntekijä

Tässä yhteydessä työntekijällä tarkoitetaan virka- tai työsuhteessa olevaa työntekijää, luottamushenkilöä, vapaaehtoistyöntekijää tai ostopalveluna hankittua työntekijää. Työntekijä on velvollinen

- perehtymään häntä koskeviin tietoturvamääräyksiin ja ohjeisiin ja noudattamaan niitä päivittäisessä työssään
- ottamaan huomioon henkilötietolain mukainen huolellisuusvelvoite ja julkisuuslain mukainen hyvä tiedonhallintatapa
- raportoimaan esimiehelleen ja seurakunnan tietoturvan yhdyshenkilölle havaitsemansa tietoturvallisuuteen liittyvät epäkohdat ja poikkeamat

Työntekijän tehtävät kuvataan ja ohjeistetaan tarkemmin IT-alueen / seurakuntatalouden tietoturvapolitiikassa, tietoturvamääräyksissä ja/tai tietoturvaohjeissa.

3.15 Tilintarkastajat

Kirkkohallituksen yleiskirjeessä 35/2010, 19.10.2010 on käsitelty tilintarkastukseen tulevia muutoksia ja tilintarkastajien valintaa valtuustokaudelle 2011-2014. Siinä todetaan mm. seuraavaa:

"Tarkastuspalvelulla tarkoitetaan kirkkojärjestyksen 15 luvun 11-13 pykälien mukaista hallinnon ja talouden tarkastamista. Lakisääteisen tilintarkastuksen tekijä tarkastaa myös erikseen määriteltyjä kohteita, esimerkiksi EU-projektiin ja rakennusavustuksiin liittyvät tilitykset. Sopimuspohjaisten IT-yhteistyöalueiden isäntäseurakuntien tulee ottaa tarjouspyynnössään mukaan tietohallinnon ja tietoturvallisuuden tarkastustehtävän, kun ne pyytävät tarjousta tulevan valtuustokauden tilintarkastuksesta. IT-yhteistyöalueiden isäntäseurakuntien tulee hankkia tietohallinnon ja tietoturvallisuuden tilintarkastuksen vuonna 2011 hyvissä ajoin ennen Kirjurin käyttöönottoa ja sen jälkeen vuosittain vuodenvaihteen tienoilla, jotta tarkastuksen tulokset olisivat jäsenseurakuntien tilintarkastajien käytettävissä kevättalven ja kevään aikana. Isäntäseurakunta lähettää tiedot tietoturvallisuuden tarkastamisesta yhteistyöseurakunnille ja kirkkohallituksen tietohallintoyksikköön. Tarkastuksessa noudatetaan hyvää tilintarkastustapaa ja tilintarkastuslakia soveltuvin osin."

3.16 Rekisterinpitäjä

Rekisterinpitäjällä[3] tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisterinpitäjä on:

- Vastuussa henkilötietojen käsittelystä.
- Velvollinen toteuttamaan tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan voimassaolevaa lainsäädäntöä, ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille.
- Velvollinen toteuttamaan asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja.

Rekisterinpitäjä on kirkossa tyypillisesti seurakunta, keskusrekisteri tai molemmat. Keskusrekisteriin kuuluvalla seurakunnalla saattaa olla rekistereitä, joihin liittyvää henkilötietojen käsittelyn vastuuta ei ole ulkoistettu keskusrekisteriin.

3.17 Tietosuojavastaava

Seurakunta, seurakuntayhtymä, tuomiokapituli ja Kirkkohallitus ovat velvollisia nimittämään itselleen tietosuojavastaavan[4]. Yksi tietosuojavastaava voidaan nimittää useampaa seurakuntaa tai tuomiokapitulia varten.

Tietosuojavastaava:

- Antaa rekisterinpitäjälle ja sen työntekijöille tietoja ja neuvoja tietosuojasäännösten mukaisista velvollisuuksista.
- Seuraa että henkilötietojen käsittelyssä noudatetaan tietosuojasäännöksiä.
- Toimii yhteyshenkilönä valvontaviranomaiseen (tietosuojavaltuutettu) päin.
- On riippumaton, eikä hän saa ottaa vastaa ohjeita tehtäviensä hoitamisen yhteydessä. Hänellä tulee olla asiantuntemusta tietosuojalainsäädännöstä ja alan käytänteistä.

On huomioitava, että tietosuojavastaava ei ole vastuussa rekisterinpitäjän henkilötietojen käsittelyn lainmukaisuudesta tai velvollinen korjaamaan havaittuja teknisiä tai organisatorisia puutteita henkilötietojen käsittelyssä.

---

[3] Lisätietoa rekisterinpitäjän roolista ja velvollisuuksista Kirkon tietosuojasivustolta https://nuotta.evl.fi/Tietosuoja/SitePages/Kotisivu.aspx

[4] Lisätietoa tietosuojavastaavan roolista ja tehtävistä Kirkon tietosuojasivustolta https://nuotta.evl.fi/Tietosuoja/SitePages/Kotisivu.aspx

4 KIRKON TIETOTURVATYÖN KESKEISET LINJAUKSET

4.1 Tavoitteet ja periaatteet

Kirkon tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoaminen ja vääristäminen. Tavoitteena on myös pitää yllä suunnitelmallista ja jatkuvaa kehittämistoimintaa uhkien ja riskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi. Normaaliajan tietojen käsittelyn turvaamisen lisäksi kirkko varautuu myös häiriö- ja poikkeusoloihin siten, että toimintaa voidaan jatkaa mahdollisimman häiriöttömästi kaikissa olosuhteissa ja normaalitilanteeseen päästään palaamaan mahdollisimman nopeasti.

Tietojen luottamuksellisuudesta, eheydestä ja käytettävyydestä on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan.

4.2 Politiikan jalkauttaminen

Tietoturvallisuuteen liittyvistä ohjeista, suosituksista ja määräyksistä tiedottaminen tapahtuu luvussa 3 kuvatulla tavalla. Kirkon tietoturvapäällikkö välittää tietoa IT-alueiden tietoturvavastaaville ja he edelleen IT-alueensa seurakuntien tietoturvan yhdyshenkilöille. IT-alueen tietoturvavastaava ja tietoturvaryhmä organisoivat tietoturvallisuuteen liittyvää koulutusta alueellaan. Tiedottamisessa käytetään myös kirkkohallituksen yleiskirjeitä, kirkon yhteisiä verkkopalveluita sekä IT-alueiden omia verkkopalveluja.

Olemassa oleva tietoturvallisuusmateriaali jaetaan uusille työntekijöille ja sen läpikäyminen on osa uusien työntekijöiden perehdyttämistä. Tietoturvan yhdyshenkilöt osallistuvat perehdyttämiseen edistääkseen tietoturvallisuuteen liittyvistä asioista tiedottamista.

Kirkon tietoturvallisuuden johtoryhmä katselmoi ja ottaa kantaa tietoturvallisuutta koskeviin ohjeisiin ja määräyksiin. Ohjeet ja määräykset tallennetaan sähköisesti kaikkien työntekijöiden saataville.

4.3 Tarkastus ja arviointi

Tietoturvapolitiikan ja muiden tietoturvallisuusmääräysten ja -ohjeiden säännöllisestä tarkistamisesta ja arvioinnin järjestämisestä vastaa kirkon tietoturvallisuuden johtoryhmä koko kirkon tasolla ja IT-alueiden tietoturvaryhmät paikallisella tasolla. Arviointi suoritetaan aina, kun on tapahtunut sellaisia muutoksia, joilla on vaikutusta tietoturvallisuuteen. Tällaisia tilanteita ovat merkittävät poikkeustilanteet, uudenlaiset haavoittuvuudet (virukset yms.), organisaatiomuutokset tai muutokset teknisessä perusrakenteessa.

Seurakuntien tilintarkastajia ja etenkin IT-alueiden isäntäseurakuntien tilintarkastajia käytetään hyväksi tietoturvallisuuden toteutumisen arvioimisessa. Tilintarkastajat voivat riippumattomana kolmantena osapuolena arvioida, miten hyvin annetut ohjeet ja

määräykset on saatettu käytäntöön ja millä alueilla on tarvetta toiminnan tehostamiselle.

4.4 Väärinkäytösten seuraamukset

Mikäli epäillään tai on olemassa näyttöä tietoturvallisuutta vaarantavista tapahtumista tai on perusteltua syytä epäillä työntekijän syyllistyneen rikolliseen toimintaan tai väärinkäytöksiin, työnantajan pitää selvittää asia ja estää väärän toiminnan jatkaminen. Työnantajalla on käytettävissään työ- ja virkasuhdelainsäädännön mahdollistamia sanktioita. Työnantajan tulee tarvittaessa saattaa tieto lainvastaisesta menettelystä poliisille mahdollista rikostutkintaa varten.