MEIDÄN KIRKON TIETOTURVAPOLITIIKKA 2011

Suomen evankelis-luterilaisen kirkon tietojärjestelmien tietoturvapolitiikka vuodelle 2011

10.2.2011

MEIDÄN KIRKON TIETOTURVAPOLITIIKKA 2011

Suomen evankelis-luterilaisen kirkon tietojärjestelmien tietoturvapolitiikka vuodelle 2011

Sisällysluettelo

1. JOHDANTO 2

2. TIETOTURVALLISUUS - MITÄ SE ON 3

3. KIRKON TIETOTURVATYÖN ORGANISOINTI 5

3.1 Yleistä 5
3.2 Kirkolliskokous 5
3.3 Kirkkohallituksen täysistunto 5
3.4 Kirkkohallituksen virastokollegio 6
3.5 Kirkon tietoturvapäällikkö 6
3.6 Kirkon tietoturvallisuuden johtoryhmä 6
3.7 Kirkon yhteisten tietojärjestelmien tietoturvamääräykset ja ohjeet 7
3.8 Kirkon yhteisen perustietotekniikan tietoturvamääräykset ja ohjeet 7
3.9 Seurakunnan kirkkoneuvosto tai seurakuntayhtymän yhteinen kirkkoneuvosto 7
3.10 IT-alueen / seurakuntatalouden tietoturvaryhmä 8
3.11 IT-alueen tietoturvavastaava 8
3.12 Seurakuntatalouden tietoturvan yhdyshenkilö 9
3.13 Esimies 9
3.14 Työntekijä 9
3.15 Tilintarkastajat 10

4. KIRKON TIETOTURVATYÖN KESKEISET LINJAUKSET 11

4.1 Tavoitteet ja periaatteet 11
4.2 Politiikan jalkauttaminen 11
4.3 Tarkastus ja arviointi 12
4.4 Väärinkäytösten seuraamukset 12

5. KIRKKOHALLITUKSEN PÄÄTÖS 12

MEIDÄN KIRKON TIETOTURVAPOLITIIKKA 2011

Suomen evankelis-luterilaisen kirkon tietojärjestelmien tietoturvapolitiikka vuodelle 2011

1. JOHDANTO

Meidän kirkko tietoverkoissa -nimisen kirkon tietohallintostrategian linjausten mukaisesti kirkkohallituksen täysistunto asetti 22.9.2009 kirkon tietoturvallisuuden johtoryhmän. Sen yhdeksi tehtäväksi annettiin laatia ensimmäinen versio kirkon tietoturvapolitiikasta[1]. Työryhmä on nimennyt lopputuloksen Meidän kirkon tietoturvapolitiikaksi.

Käsillä oleva kirkon tietoturvapolitiikan ensimmäinen versio on tehty vuotta 2011 ajatellen. Tarkoitus on tehdä uusi ja 1.12.2011 voimaan tuleva versio mm. seurakunnilta saadun palautteen pohjalta.

Kirkon tietoturvallisuuden kehittäminen on lähivuosina tärkeää ja ajankohtaista mm. KITKE-hankkeen, HeTa-hankkeen ja HEV-hankkeen vuoksi:

- KITKE-hankkeessa rakennettava kirkon yhteinen Kirjuri-järjestelmä vaatii tietoturvan kehittämistä etenkin henkilötietojen turvallisen käsittelyn vuoksi. Keskeiset Kirjuri-järjestelmän tietoturva-asiat on säädetty kirkkolaissa. Kirkolliskokous hyväksyi kirkkolain 16 luvun ja 25 luvun muutosesityksen marraskuussa 2008. Eduskunta hyväksyi 26.5.2010 sitä koskevan hallituksen esityksen HE 19/2010. Lakimuutokset tulevat voimaan 1.12.2011.

- HeTa-hankkeessa rakennettava HeTa-palvelukeskus ja sen yhteiset tietojärjestelmät vaativat tietoturvan kehittämistä etenkin maksuaineiston ja henkilötietojen turvallisen hoitamisen vuoksi.

- HEV-hankkeessa eli Hengellinen elämä verkossa -hankkeessa kehitetään seurakuntatyötä avoimessa Internet-verkossa ja sen sosiaalisissa medioissa. Avoimen Internetin tietoturvallinen työkäyttö vaatii tietoturvauhat huomioivien työtapojen ja teknisten ratkaisujen kehittämistä. Hyvänä esimerkkinä on Facebookin turvallinen käyttö. Verkossa tehdään myös verkkoauttamistyötä, jolloin viestinnän luottamuksellisuuden varmistaminen on tärkeää.

Edellä mainittujen hankkeiden tarpeet ovat olleet erityisesti esillä kirkon tietoturvapolitiikan laatimisessa. Niitä koskevat tietoturvatyön keinot ovat samanlaiset ja ratkaisut toisiaan tukevia. Lisäksi samat ratkaisut kehittävät kokonaiskirkon ja seurakuntien tietoturvaa myös muiden työalojen toimintatapojen ja tietojärjestelmien osalta.

[1] Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) tietoturvasanaston mukaan "tietoturvapolitiikka on johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta". Voidaan puhua myös tietoturvaperiaatteista. Tietoturvastrategia on suunnitelma tietoturvapolitiikan jalkauttamiselle.

2. TIETOTURVALLISUUS - MITÄ SE ON

Tietoturvallisuuteen kuuluvat kaikki ne järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus[2]. 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.

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

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

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.

Tietoturvallisuuden yhteydessä puhutaan usein myös tietosuojasta. Tietosuoja[3] on "ihmisen yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä. Näitä ovat muun muassa tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen sekä henkilötietojen suojaaminen valtuudettomalta tai henkilöä vahingoittavalta käytöltä". - Voidaan todeta, että tietoturvan hallintaan liittyvät tehtävät ovat monilta osin päällekkäiset tietosuojan hallintaan liittyvien tehtävien kanssa.

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.

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

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: Kirkolliskokouksen asiana on mm. tehdä ehdotuksia Suomen eduskunnan hyväksymän kirkkolain säätämisestä ja hyväksyä kirkkojärjestys. 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 yleistä lainsäädäntöä, joka sisältää tietoturvaa 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: Kirkolliskokouksen asiana on myös vahvistaa kirkon keskusrahaston talousarvio ja käsitellä kirkon keskusrahaston toiminta- ja taloussuunnitelma. Nämä sisältävät myös tietoturvan kehittämiseen liittyviä asioita. Esimerkiksi kirkon tietokoneiden tietoturvaohjelmien käyttöoikeuslisenssit on viime vuosina ostettu keskitetysti Kirkkohallituksen toimesta.

3.3 Kirkkohallituksen täysistunto

Tietoturva-asioihin liittyen kirkkohallituksen täysistunto:

- Asettaa kirkon tietoturvan johtoryhmän
- Antaa kirkon tietoturvamääräykset[4]

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

3.4 Kirkkohallituksen virastokollegio

Tietoturva-asioihin liittyen kirkkohallituksen virastokollegio:

- 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:

- Antaa yllättävän tietoturvauhan tai poikkeamatilanteen yhteydessä sellaisen tietoturvamääräyksen, joka on voimassa enintään kaksi kuukautta
- 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 työalakohtaisten tietojärjestelmien sisältöasioihin liittyvät tietoturvan tai tietosuojan asiat. Esimerkiksi kirkonkirjojenpitoon ja Kirjuri-järjestelmään, HeTa-järjestelmään tai Palvelevan netti -nimisen verkkoauttamispalvelun liittyvät tietosuojakysymykset kuuluvat Kirkkohallituksessa asianomaisille viranhaltijoille.

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 työalakohtaisen tietojärjestelmän sisällöllinen omistaja ja tekninen omistaja[5] 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-järjestelmä, HeTa-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 ohjeiden ja määräysten noudattamisesta.
- Huolehtii siitä, että seurakuntataloudelle on asetettu tietoturvaryhmä. Se kannattaa olla yhteinen IT-yhteistyöalueen kaikkien seurakuntien kanssa.
- Huolehtii siitä, että seurakuntataloudelle on nimetty tietoturvavastaava. Se kannattaa 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. Se kannattaa 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.

Käytännön ohjeita em. tehtävien osalta vuoden 2011 alkuun:

[5] Tietojärjestelmän sisällöllinen omistaja on se yksikkö, jonka toimintaa ja tietojenkäsittelyä varten järjestelmä on hankittu ja joka määrittelee mm. järjestelmän käyttöön oikeutetut. Tekninen omistaja on Kirkkohallituksessa joko tietohallintoyksikkö tai KT:n verkkoviestintäyksikkö.

- Kirkkohallitus asettaa kirkon tietoturvan johtoryhmän ohjauksessa toimivan työryhmän, joka laatii mallit IT-alueen (seurakuntatalouden) paikallisesta tietoturvapolitiikasta ja paikallisista tietoturvamääräyksistä.
- IT-alueen johtokunta asettaa työryhmän laatimaan ehdotuksen IT-alueen seurakuntatalouksien paikallisesta tietoturvapolitiikasta ja paikallisista tietoturvamääräyksistä. Samassa yhteydessä kyseinen työryhmä tekee ehdotuksen IT-alueen seurakuntatalouksien yhteisen tietoturvaryhmän asettamisesta ja yhteisen tietoturvavastaavan nimittämisestä sekä seurakuntatalouksien omien tietoturvan yhdyshenkilöiden nimittämisestä.

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.

Käytännön ohjeita em. tehtävien osalta vuodelle 2011:

- Tietoturvaryhmän ja tietoturvavastaavan ensimmäisiä tehtäviä ovat tietoturvakoulutuksen suunnittelu ja järjestäminen tietoturvan yhdyshenkilöille ja sen jälkeen kaikille työntekijöille.
- Kirkkohallitus asettaa kirkon tietoturvan johtoryhmän ohjauksessa toimivan työryhmän suunnittelemaan po. tietoturvakoulutusta yhteistyössä IT-alueiden / seurakuntien asiantuntijoiden 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.

Tietoturvavavastaavan 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."

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.

Kirkon tietoturvatyön erityistavoitteet vuodelle 2011 ovat seuraavat:

- IT-alueiden tietoturvaryhmien asettaminen ja tietoturvavastaavien nimeäminen
- seurakuntatalouksien tietoturvan yhdyshenkilöiden nimeäminen
- IT-alueiden tietoturvapolitiikan ja tietoturvamääräysten laatiminen
- tietoturvallisuuden koulutussuunnitelman laatiminen koko kirkon tasolla ja IT-alueilla
- työntekijöiden tietoturvakoulutuksen aloittaminen
- työalakohtaisten ja hankekohtaisten tietoturvamääräysten ja -ohjeiden laatiminen

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. IT-alueet voivat myös laatia ohjevideoita osana koulutusta ja tiedotusta. Tiedottamisessa käytetään myös kirkkohallituksen yleiskirjeitä, sakasti.evl.fi -verkkopalvelua sekä IT-alueiden omia verkkopalveluja.

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

Kirkon tietoturvallisuuden johtoryhmä laatii mallipohjia eri dokumenteista, joiden perusteella IT-alueet voivat helpommin suunnitella ja toteuttaa oman alueensa tarkentavia alueellisia dokumentteja esimerkiksi koko kirkon tason tietoturvapolitiikasta sekä valmistella koulutusmateriaalia alueensa seurakuntien työntekijöille.

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.

Tietoturvapolitiikan toimivuutta arvioidaan joka toinen vuosi tarkastelemalla raportteja rekisteröityjen turvallisuuspoikkeamatilanteiden lukumäärästä ja vaikutuksista.

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 työnantajaansa tai muita työntekijöitä kohtaan, 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.

5. KIRKKOHALLITUKSEN PÄÄTÖS

Kirkkohallituksen virastokollegio päätti 10.2.2011:

1. Merkitä tiedoksi kirkon tietoturvallisuuden johtoryhmän laatiman Meidän kirkon tietoturvapolitiikka 2011 -nimisen asiakirjan sekä Kirkon yleiset tietoturvamääräykset 2011 -nimisen asiakirjan.

2. Kehottaa IT-yhteistyöalueita ja niiden seurakuntia järjestämään tietoturvallisuutensa em. asiakirjoissa kuvatuilla tavoilla.

3. Merkitä tiedoksi, että kirkon tietoturvallisuuden johtoryhmä valmistelee em. asiakirjoissa kuvattuja asioita siten, että ne annettaisiin kirkon säädöskokoelman määräyksenä 1.12.2011 lähtien, jolloin kirkkolain 16 luvun muutos tulee voimaan.