Itä-Suomen it-aluekeskus	**IITAN TIETOTURVAPOLITTIIKKA 2012 ja tietoturvamääräykset**

Versio 1	**13.1.2012**
Versio 2	**7.2.2012**

1. 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 osaalue, 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.

2. IT-ALUEKESKUS IITAN TIETOTURVATYÖN ORGANISOINTI

Seuraavissa kappaleissa on käsitelty tietoturvatyön organisointia, toimijoita ja niiden rooleja. Kuvaus on kirjoitettu seurakuntatalouden näkökulmasta. Tietoturvan organisointi perustuu koko kirkon tietoturvapolitiikkaan, joka asettaa pakotteita myös alueelliselle tietoturvapolitiikalle.

2.1 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.

2.2 IT-alueen 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.

2.3 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.

2.4 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. Toimenkuvassa selvennetään myös sitä mitä, kenelle ja miten yhdyshenkilö raportoi. Toimenkuvassa painotetaan tarkkailijan ja tiedonvälittäjän roolia, jolloin vastuualueet ovat selkeästi erillään esim. esimieheen verrattuna. Joillakin IT-alueilla on sovittu, että jokaisessa seurakuntataloudessa on oma it-yhdyshenkilö. Tällöin it-yhdyshenkilö voi toimia myös tietoturvan yhdyshenkilönä.

2.5 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 tietoturvapolitiikassa, tietoturvamääräyksissä ja/tai tietoturvaohjeissa. Toimenkuvaan sisällytetään ilmoitusvelvollisuus poikkeamista IT-alueen tietoturvavastavalle, joka raportoi/käsittelee asiat eteenpäin tapauskohtaisesti.

2.6 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 / tietoturvapolitiikassa, tietoturvamääräyksissä ja/tai tietoturvaohjeissa.

2.7 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. ITyhteistyöalueiden 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. IT-ALUEEN TIETOTURVATYÖN KESKEISET LINJAUKSET
3.1 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 seurakunta 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.

IT-alueen tietoturvatyön erityistavoitteet vuodelle 2012 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 ITalueilla
- työntekijöiden tietoturvakoulutuksen aloittaminen
- työalakohtaisten ja hankekohtaisten tietoturvamääräysten ja -ohjeiden laatiminen

3.2 Politiikan jalkauttaminen

Tietoturvallisuuteen liittyvistä ohjeista, suosituksista ja määräyksistä tiedottaminen tapahtuu luvussa 3 kuvatulla tavalla. Kirkon tietoturvapäällikkö välittää tietoa ITalueiden 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.

Perehdyttäminen hoidetaan IITAn alueella käyttäen seuraavia menetelmiä:
- kirkkoneuvostojen puheenjohtajille ja esittelijöille järjestetään perehdyttämistilaisuuksia rovastikunnittain tietoturvapolitiikan ja tietoturvamääräysten hyväksymiseksi kirkkoneuvostoissa
- esimiehille järjestetään perehdyttämistilaisuuksia rovastikunnittain 30.6.2012 mennessä
- käsiohje jaetaan kaikille alueen työntekijöille sähköpostin välityksellä
- syksyllä järjestetään mahdollisuus osallistua ’nettitenttiin’. Tentillä selvitetään tietoturvamääräysten omaksuminen.

3.3 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.

3.4 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