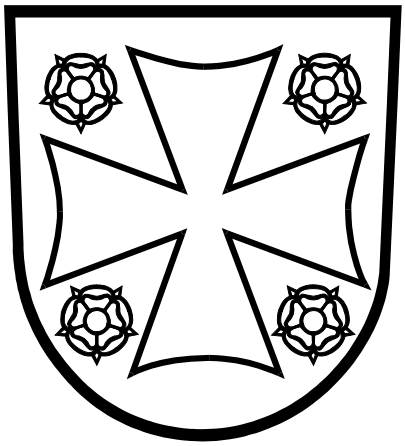
KIRKON YLEISET TIETOTURVAMÄÄRÄYKSET

21.3.2019



Sisältö

1 Tietoturvallisuuden hallinta

Osa-alueen nimi	**1.1 Resursointi**
Tavoitteet	Tietoturvallisuuteen liittyvien käytännön tehtävien hoitoon on varattu riittävä määrä resursseja. Myös varahenkilöratkaisut on otettu huomioon.
Vaatimukset	1. Jokaisella IT-alueella/seurakuntataloudella[1] tulee olla tietoturvaryhmä. Sen tehtävänä on laatia ja ylläpitää oman alueensa tietoturvapolitiikkaa ja tietoturvallisuuteen liittyviä määräyksiä ja -ohjeita koko kirkkoa koskevien linjausten mukaisesti. Lisäksi se valvoo tietoturvamääräysten ja -ohjeiden noudattamista, käsittelee ajankohtaisia tietoturvallisuutta koskevia kysymyksiä sekä suunnittelee ja järjestää tietoturvallisuuteen liittyvää koulutusta yhteistyössä tietoturvavastaavan ja tietoturvan yhdyshenkilöiden kanssa. Suuressa seurakuntataloudessa voidaan tarvittaessa perustaa oma tietoturvaryhmä, jos toiminnan laajuuden ja erityistarpeiden katsotaan sitä edellyttävän. Tällöin tietoturvaryhmä tarkentaa IT-alueen tietoturvaryhmän laatimia määräyksiä ja ohjeita paikallisia tarpeita vastaaviksi ja käsittelee paikallisia ja ajankohtaisia tietoturvallisuutta koskevia kysymyksiä. 2. Jokaisella IT-alueella/seurakuntataloudella tulee olla nimetty tietoturvavastaava. Hänen tehtävänään on kehittää jatkuvasti ja aktiivisesti alueen seurakuntien tietoturvallisuutta. Hän vastaa tietoturvallisuuteen liittyvien määräysten ja ohjeiden tiedottamisesta tietoturvan yhdyshenkilöille, esimiehille ja kaikille työntekijöille. Lisäksi hän ottaa vastaan havaintoja tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista ja raportoi ne säännöllisesti tietoturvaryhmälle. Valtakunnallisia järjestelmiä ja palveluita koskevissa tapahtumista ja poikkeamista raportoidaan myös kirkon tietoturvapäällikölle. 3. Jokaisella seurakuntataloudella tulee olla nimetty tietoturvan yhdyshenkilö. Hän huolehtii tietoturvallisuuteen liittyvien määräysten ja -ohjeiden tiedottamisesta kaikille työntekijöille ja osallistuu esimiesten tukena uusien työntekijöiden perehdyttämiseen tietoturvallisuutta koskevissa kysymyksissä. Lisäksi hän ottaa vastaan ilmoituksia seurakuntataloudessaan havaituista tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista ja raportoi niistä tietoturvavastaavalle ja oman seurakuntataloutensa esimiehille.

[1] IT-alue on kahden tai useamman itsenäisen seurakuntatalouden sopimuspohjainen IT-yhteistyöalue. Seurakuntatalous on itsenäinen seurakunta tai seurakuntayhtymä. Mitä tässä asiakirjassa sanotaan seurakuntataloudesta, koskee vastaavasti myös tuomiokapitulia ja kirkkohallitusta. Merkinnällä IT-alue/seurakuntatalous tarkoitetaan tässä asiakirjassa sitä, että asia koskee kaikkia seurakuntatalouksia, mutta asia on järkevä järjestää yhteisenä koko IT-alueella. Esimerkiksi tietoturvaryhmän on järkevää olla yhteinen IT-alueen kaikkien seurakuntien kanssa.

4. Jokaisella seurakuntataloudella tulee olla nimetty tietosuojavastaava. Hänen tehtävänään on huolehtia EU:n tietosuoja-asetuksen tietosuoja-vastaaville asettamista tehtävistä.

5. Työnantaja vastaa, että tietoturvavastaavalla ja tietoturvan yhdyshenkilöllä on riittävästi työaikaa tehtäviensä suorittamiseen.

6. Tietoturvallisuustyötä tekevien työntekijöiden tehtävänkuvauksiin on päivitettävä tieto työntekijän rooleista ja vastuista.

7. IT-alueella/seurakuntataloudessa on oltava riittävästi ammattitaitoista henkilöstöä, jotta turvallisuusvaatimusten käytännön toteuttaminen on realistisesti mahdollista ottaen huomioon mm. henkilöstön lomat ja muut poissaolot.

8. Tietoturvallisuuden resursointi otetaan huomioon IT-alueen ja seurakuntatalouden talousarviossa ja toiminta- ja taloussuunnitelmassa.

Osa-alueen nimi	**1.2 Tietoturvapolitiikka, tietoturvamääräykset ja tietoturvaohjeet**
Tavoitteet	Tarvittavat politiikat, määräykset ja ohjeet ovat olemassa ja ne pidetään ajan tasalla ja käyttäjien saatavilla. Käyttäjiä koulutetaan ja informoidaan säännöllisesti uusista määräyksistä ja ohjeista.
Vaatimukset	1. IT-alueella/seurakuntataloudella on oltava ajantasainen tietoturvapolitiikka ja sitä tarkentavat määräykset ja ohjeet, jotka ovat linjassa koko kirkon tietoturvamääräysten kanssa. Asiakirjojen tulee olla työntekijöiden saatavilla. 2. Tieto olemassa olevista tietoturvapolitiikoista, -määräyksistä ja -ohjeista on välitettävä koko henkilökunnalle. Esimiehet ovat velvollisia välittämään tietoa alaisilleen. 3. Tietoturvallisuuteen liittyviä riskejä on arvioitava säännöllisesti ja säännönmukaisesti. Uusiin ja muuttuneisiin riskeihin on reagoitava asian mukaisesti. 4. IT-alueella/Seurakuntataloudella on oltava toimivat käytännöt tietojen elinkaaren hallintaan. Tietojen elinkaari kattaa niiden luokittelun, säilyttämisen, välittämisen ja tuhoamisen. 5. Työntekijöille järjestetään säännöllistä tietoturvakoulutusta. 6. Työntekijöiden on allekirjoitettava salassapitositoumus ennen työn aloittamista. 7. Vapaaehtoistyöntekijöiden ja luottamushenkilöiden, jotka käyttävät seurakunnan tietojärjestelmiä tai voivat tehtävässään päästä käsiksi arkaluontoiseen tietoon, tulee allekirjoittaa salassapitositoumus. 8. Tietoturvallisuuteen liittyvien määräysten ja ohjeiden noudattamista valvotaan ja poikkeamiin puututaan. 9. IT-alue/Seurakuntatalous on velvollinen auditoimaan[2] tietoturvallisuutensa tason säännöllisesti tai merkittävien muutosten yhteydessä ulkopuolisen tahon tekemänä. 10. IT-alueella/Seurakuntataloudella on ajantasainen ohjeistus sosiaalisen median käytöstä.

[2] Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) on laatinut laajan tietoturvasanaston. Sen mukaisia ja tietoturva-alan vakiintuneita käsitteitä on käytetty myös tässä asiakirjassa. Auditointi on arviointi/testaus, jonka tarkoituksena on tarkastella esimerkiksi tietoturvamekanismien toimivuutta.

Osa-alueen nimi	**1.3 Yhteistyökumppanit ja ulkoisten palveluiden hallinta**
Tavoitteet	Ulkopuolisilta toimijoilta vaaditaan samaa tietoturvallisuuden tasoa kuin omassa toiminnassa toteutetaan. Tietoturvallisuus otetaan huomioon heti uusia hankkeita ja hankintoja aloitettaessa.
Vaatimukset	1. Ulkoistusten ja IT-palveluiden hankinnan yhteydessä ulkopuolisilta työntekijöiltä on edellytettävä riittävää koulutusta ja ammattitaitoa. 2. Ulkopuolisten työntekijöiden tulee allekirjoittaa salassapitositoumus ennen työn aloittamista. 3. Ulkopuolisia työntekijöitä sitovat samat tietoturvamääräykset ja -ohjeet kuin kirkon omaa henkilöstöä. Ulkopuolisen työntekijän palkkaava taho on velvollinen saattamaan tiedoksi kaikki asiaan liittyvä ohjeistus. 4. Seurakuntataloudella on nimetty vastuuhenkilö ulkopuolisille toimijoille. 5. Yhteistyökumppaneille asetetaan tarvittavat tietoturvavaatimukset jo tarjouspyyntö- tai sopimusneuvotteluvaiheessa. 6. Yhteistyökumppaneiden kanssa järjestetään riittävän usein kokouksia, joissa käsitellään tietoturvallisuuteen liittyviä asioita kuten havaittuja ja toteutuneita riskejä sekä tulevaisuuden tarpeita. 7. Henkilötietojen käsittelyn vastuukysymykset tulee ottaa huomioon sopimuksessa tai sopimuksen liitteessä yhteystyökumppanien ja ulkoisten toimittajien tapauksessa, joissa toiminta täyttää tietosuoja-asetuksen määrittelemän henkilötietojen käsittelijän tunnusmerkit.

Osa-alueen nimi	**1.4 Toimintaprosessit**
Tavoitteet	Seurakuntatalouden toiminta on suunnitelmallista ja toistettavaa. Poikkeamatilanteisiin reagoidaan määrätietoisesti ja tietoa jaetaan IT-alueiden välillä.
Vaatimukset	1. IT-alueella/seurakuntataloudella on toimivat prosessit IT-toimintojensa hoitamiseen. Prosesseja on tilanteen muuttuessa päivitettävä. Prosesseissa on otettu huomioon tietoturvallisuusnäkökulma. 2. Seurakuntataloudella on valmiussuunnitelma, jonka liitteenä on IT-alueen valmiussuunnitelma. Valmiussuunnitelmien toimivuutta testataan säännöllisesti. 3. Avaintoimintojen ja –prosessien toiminnan kannalta suojeltavat kohteet on tunnistettu ja luokiteltu. 4. Seurakuntatalous tuntee toimintaansa sääntelevät lait ja muut säädökset ja määräykset. 5. IT-alueella/seurakuntataloudella on oltava toimivat prosessit, joiden avulla tietoturvapolitiikkaa ja ohjeistusta arvioidaan vuosittain ja päivitetään tarpeen mukaan. 6. IT-alueella/seurakuntataloudella on oltava prosessit ja ohjeistukset tietoturvapoikkeamien varalta. Niissä tulee ottaa kantaa tietoturvapoikkeamien havaitsemiseen, niihin reagoimiseen, seuraamusten käsittelyyn ja normaalitoimintaan palaamiseen. 7. Tietoturvapoikkeamat on raportoitava ja analysoitava jälkikäteen poikkeamien syntymissyiden tunnistamiseksi ja korvaavien toimenpiteiden toteuttamiseksi 8. Tietoturvapoikkeamista vaihdetaan tietoa IT-alueiden tietoturvaryhmien välillä ja muiden alueiden kokemuksia hyödynnetään. Kirkon tietoturvapäällikkö vastaa toiminnan koordinoinnista.

2 Tietoverkkojen tietoturvallisuus

Osa-alueen nimi	**2.1 Tietoverkkojen käyttäminen ja kehittäminen**
Tavoitteet	Tietoturvallisuusvaatimukset otetaan huomioon tietoverkkoja suunniteltaessa ja niitä käytettäessä.
Vaatimukset	1. Kaiken tietoliikenteen KIRKKO-verkon[3] ja ulkopuolisten verkkojen välillä on kuljettava KIRKKO-verkon keskitetyn palomuurin kautta. Suoria yhteyksiä Internettiin tai muihin verkkoihin saa muodostaa vain erityisen painavista syistä. Jos suoria yhteyksiä muodostetaan (esimerkiksi hallintayhteys palvelimeen ulkoiselle toimijalle) on kyseinen liikenne eristettävä KIRKKO-verkosta (esimerkiksi erillisiä Internet-liittymiä käyttämällä) ja dokumentoitava huolellisesti. 2. IT alueen tietoverkon on oltava tietoturvallinen ja hyvin dokumentoitu. IT alue ja Kirkkohallitus käyvät yhdessä läpi alueen tietoverkon turvallisuuden. 3. Seurakuntatalouden KIRKKO-verkkoliittymään ei saa liittää muita kuin seurakuntatalouden/IT-alueen omia, tämän dokumentin vaatimukset täyttäviä laitteita. Mahdollista vierailijakäyttöä varten on hankittava erillinen Internet-liittymä, jonka liikenne on eristetty KIRKKO-verkosta. 4. Langattomia verkkoja toteutettaessa on otettava huomioon niiden tietoturvariskit. Päätelaitteiden tunnistaminen ja liikenteen salaaminen on toteutettava varmenteita ja vahvoja salausalgoritmeja käyttäen 802.1x standardin suositusten mukaisesti. 5. Pääsy verkon aktiivilaitteiden hallintakäyttöliittymiin on suojattava vahvalla[4] salasanalla. 6. KIRKKO-verkossa toimivia palveluita voidaan käyttää KIRKKO-verkkoon liitettyjen toimipisteiden ulkopuolelta käsin seuraavin edellytyksin: a) niiden käyttämistä varten on luotu KIRKKO-verkon palomuuriin tietoturvasääntö ja palvelu sijaitsee käyttötarkoitukseen kuuluvalla tietoturvavyöhykkeellä. b) palvelu on julkaistu KIRKKO-verkon keskitettyjen etätyöpalveluiden kautta.

[3] KIRKKO-verkko on Suomen evankelis-luterilaisen kirkon suojattu sisäverkko, johon kaikkien seurakuntatalouksien paikalliset verkot kuuluvat.

[4] Vahva salasana on vähintään 10 merkkiä pitkä, se sisältää vähintään kolmea merkkityyppiä (numeroita, isoja kirjaimia, pieniä kirjaimia ja erikoismerkkejä), eikä se ole vuosiluku, päivämäärä, minkään kielen sana tai nimi tai sanan tai nimen muunnelma.

7. Kirkon jäsentietojärjestelmän käyttäminen KIRKKO-verkon ulkopuolelta on kiellettyä. Toiminnallisten sovellusten, joista on rajapinta jäsentietojärjestelmään tai joihin on talletettu tietoja jäsentietojärjestelmästä, käyttö KIRKKO-verkon ulkopuolelta on kiellettyä. Sovellusten etäkäyttö voidaan sallia vain, jos jäsentietojärjestelmästä rajapintayhteyksien kautta noudettavien tietojen käyttö estetään. Esimerkiksi tarjoamalla erillinen rajoitettu käyttöliittymä, josta kyseisiä tietoja hyödyntävät toiminnot on poistettu käytöstä.

8. Palvelinten jotka sisältävät jäsentietoja tai joilla jäsentietoja käsitellään tulee sijaita Suomen rajojen sisäpuolella ja palvelintilojen jossa palvelinlaitteet sijaitsevat tulee täyttää vähintään Valtionvarainministeriön tason 3 (VAHTI 2/2013) mukaiset vaatimukset.

9. IT-alueen tulee toimittaa Kirkkohallitukselle kattava dokumentaatio palvelinympäristöstä ja palvelimista, jossa jäsentietoja säilytetään tai joilla jäsentietoja käsitellään ja ulkopuolisen tahon suorittama auditointiraportti jolla todennetaan tilojen ja ympäristöjen vaatimuksenmukaisuus.

3 Työasemien ja mobiililaitteiden tietoturvallisuus

Osa-alueen nimi	**3.1 Työasemien sovellukset ja käyttöjärjestelmät**
Tavoitteet	Työasemien käyttöjärjestelmät päivitetään säännöllisesti. Valmistajan tuen piiristä poistuneita käyttöjärjestelmiä käyttävät työasemat on poistettu käytöstä.
Vaatimukset	1. Kaikkien seurakuntatalouden käytössä olevien KIRKKO-verkkoon liitettyjen työasemien käyttöjärjestelmäversioiden on oltava valmistajan tuen piirissä sekä yrityskäyttöön tarkoitettuja. 2. Työasemissa on oltava ajanmukaiset ja automaattisesti päivittyvät ohjelmat virusten ja haittaohjelmien torjuntaan sekä ohjelmistotason palomuuri. 3. Työasemien käyttöjärjestelmien ja sovellusten turvallisuuspäivitykset on asennettava kaikkiin työasemiin ajallaan. 4. Työasemien sovellusten toiminta päivitysten jälkeen varmistetaan testityöasemilla. 5. Sovellusten tietoliikennettä tulee valvoa ja poikkeaviin trendeihin puuttua. [5] 6. Kannettavien Windows-työasemien kovalevyt tulee salata.

[5] IT-alueiden virtuaalipalomuurit tarjoavat mahdollisuuden seurata IT-alueen verkon tietoliikennettä KIRKKO-verkon ytimeen sovellustasolla.

Osa-alueen nimi	**3.2 Työasemien käyttäminen**
Tavoitteet	Työasemia käyttävät vain seurakuntatalouden työntekijät työtehtävien suorittamiseen. Luvattomien ja tarpeettomien ohjelmien asentaminen estetään paikallisten järjestelmävalvojan[6] oikeuksien rajoittamisella.
Vaatimukset	1. Seurakuntatalouden työasemia saa käyttää vain työnantajan määräämien työtehtävien suorittamiseen (poikkeuksena erikseen muuhun käyttöön nimetyt laitteet). 2. Henkilökohtaista työasemaa ei saa koskaan luovuttaa ulkopuolisten, esimerkiksi perheenjäsenten tai vierailijan käyttöön. Työaseman haltija on itse vastuussa huolimattomuudestaan aiheutuvista seurauksista. 3. Asianmukaisesti suojatun ja ajantasaisesti päivitetyn työaseman käyttäminen julkisissa verkoissa on sallittua (esimerkiksi hotellien vierasverkot ja kotiverkot). 4. Muiden kuin työtehtävien kannalta välttämättömien ohjelmien (kuten pelien) asentaminen työasemiin on kiellettyä. 5. Työasemien työpöydän automaattiset lukkiutumisasetukset on otettava käyttöön. Erityiskäyttöön (esityskäyttö) tarkoitetuissa työasemissa voidaan käyttää poikkeavia lukkiutumisaika-asetuksia. 6. Työasemien levyresursseja ja palveluita ei saa jakaa verkossa muiden laitteiden tai palveluiden käyttöön. 7. Luottamuksellista tietoa kuljetettaessa on käytettävä salausominaisuuksilla varustettuja USB-muistilaitteita. Muiden kuin työnantajan omistuksessa olevia muistilaitteita työasemiin liitettäessä on niiden tietoturvallisuudesta varmistuttava.

[6] Järjestelmän ylläpitorooli, johon kuuluvilla käyttäjillä on laajoja käyttöoikeuksia kohdejärjestelmään, palvelimeen tai työasemaan.

Osa-alueen nimi	**3.3 Työasemien hallinta**
Tavoitteet	Työasemien hallintaoikeuksia annetaan vain ammattitaitoisille IT-ammattilaisille. Seurakuntatalouden kaikissa työasemissa käytetään sovittuja tietoturva-asetuksia.
Vaatimukset	1. Tietoverkkoon liitettävät työasemat on nimettävä yhteisten sääntöjen mukaisesti, jotta päällekkäisistä nimistä aiheutuvat ristiriitatilanteet vältetään. 2. Tietoturva- ja selainasetukset on asetettava työasemiin keskitetysti siten, että käyttäjät eivät pysty niitä muuttamaan. 3. Käytössä olevista ohjelmistoista pidetään yllä ajantasaista dokumentaatiota. 4. Vain nimetyillä IT-henkilöillä saa olla työasemiin sellaiset oikeudet, jotka mahdollistavat ohjelmistojen asennuksen. 5. Työasemissa ei saa olla paikallisia käyttäjätunnuksia tai ryhmiä työntekijöiden käytettävissä. Näitä on oikeus käyttää vain ylläpitotarkoituksissa. Poikkeuksena tästä ovat vierailijatunnukset yhteiskäyttökoneissa. 6. Työasemien mahdollinen etähallinta on rajoitettava tehtäväksi vain tietyiltä nimettyjen IT-henkilöiden käytössä olevilta työasemilta tai tukipalvelimilta. Etäyhteyksiä työasemiin voivat muodostaa vain asiaan oikeutetut nimetyt ylläpitäjät. Työaseman haltijaa on informoitava ennen etätukitoimenpiteiden tekemistä ja tarvittaessa on pyydettävä hänen suostumusta toimenpiteeseen.

Osa-alueen nimi	**3.4 Mobiililaitteiden käyttö**
Tavoitteet	Mobiililaitteiden tietoturvallisuuden perusteista huolehditaan. Kadonneiden tai varastettujen älypuhelinten, tablet-laitteiden tai vastaavien kautta tiedot (sähköpostit, pilvilevytilat, sijaintitiedot) voivat päätyä vääriin käsiin.
Vaatimukset	1. Työnantajan omistamaa mobiililaitetta ei saa koskaan luovuttaa ulkopuolisten, esimerkiksi perheenjäsenten tai vierailijan käyttöön. Laitteen haltija on itse vastuussa huolimattomuudestaan aiheutuvista seurauksista. 2. Käyttöjärjestelmäpäivitykset on ajettava ajallaan työnantajan omistamiin laitteisiin. Omien henkilökohtaisten laitteiden käyttäjien tulee itse huolehtia laitteiden riittävästä päivittämisestä, ja laitteen omistaja on itse vastuussa laitteen käytön mahdollisesti aiheuttamien ongelmien korjaamisen kustannuksista. 3. Mobiililaitteissa joilla käsitellään työhön liittyvää tietoa (esimerkiksi luetaan työsähköposteja) tulee olla käytössä näytön PIN-koodilukitus. 4. Sovellusten asentaminen valmistajan oman verkkokaupan (Google Play, Apple App Store yms.) ulkopuolelta on kiellettyä työnantajan omistamiin laitteisiin, poislukien IT-alueiden asennettavaksi hyväksymät sovellukset. Omien henkilökohtaisten laitteiden omistaja on itse vastuussa siitä, että laitteeseen asennetut sovellukset ovat luotettavista lähteistä. Huomioi myös sovellusten edellyttämät oikeudet puhelimeesi. Tarkista aika-ajoin asentamiesi sovellusten oikeudet mobiililaitteestasi. Myös asennettujen sovellusten soveltuvuus kaupalliseen käyttöön tulee huomioida sovelluksia työkäyttöön tarkoitettuun mobiililaitteeseen asennettaessa. 5. Bluetooth yhteyttä käytettäessä huolehditaan siitä, että laite ei ole jatkuvasti näkyvissä kaikille muille laitteille.

4 Palvelinten tietoturvallisuus

Osa-alueen nimi	**4.1 Palvelinten sovellukset ja käyttöjärjestelmät**
Tavoitteet	Palvelinten käyttöjärjestelmien säännöllisestä päivittämisestä huolehditaan. Valmistajan tuen piiristä poistuneita käyttöjärjestelmiä käyttävät palvelimet on poistettu käytöstä.
Vaatimukset	1. IT-alueella/seurakuntataloudella käytössä olevien palvelinten käyttöjärjestelmäversioiden on oltava valmistajan tuen piirissä. Mahdollisia vanhentuneita käyttöjärjestelmäversioita käyttävät palvelimet tulee eristää muusta työasema- ja palvelinympäristöstä verkkoteknisesti (esimerkiksi virtuaaliverkkoja käyttämällä). 2. Palvelinten käyttöjärjestelmien turvallisuuspäivitykset on asennettava kaikkiin palvelimiin seuraavasti: kriittiseksi luokitellut päivitykset viimeistään kuukauden sisällä niiden julkaisusta ja muut tietoturvapäivitykset kahden kuukauden sisällä. 3. Palvelimissa on oltava ajanmukaiset ja automaattisesti päivittyvät ohjelmat virusten ja haittaohjelmien torjuntaan. Vaihtoehtoisesti se verkkosegmentti, jossa palvelimet sijaitsevat, on suojattava erikseen sellaisella palomuurilla, joka kykenee suodattamaan tietoliikenteen haittaohjelmistojen varalta. 4. Kaikki vanhentuneita käyttöjärjestelmiä käyttävät palvelimet on päivitettävä tai poistettava verkosta.

Osa-alueen nimi	**4.2 Palvelinten hallinta**
Tavoitteet	Palvelimet on sijoitettu siten, että palvelun keskeytymätön jatkuminen ja palvelinten fyysinen turvallisuus ovat taatut. Palvelinten ylläpitotunnuksia ei käytetä päivittäisessä työasemakäytössä.
Vaatimukset	1. Tietoverkkoon liitettävät palvelimet on nimettävä yhteisten sääntöjen mukaisesti, jotta päällekkäisten nimien aiheuttamat ristiriitatilanteet vältetään. 2. Palvelinten hallintaa varten on nimetyillä it-henkilöillä oltava henkilökohtaiset tunnukset, joita ei käytetä normaalissa päivittäisessä työasemakäytössä. 3. Palvelimet on sijoitettava asianmukaisiin lukittuihin laitetiloihin. Tarpeen mukaan laitetiloissa on oltava toimiva kulunvalvonta-, sekä jäähdytys- ja palonsammutusjärjestelmät. 4. Kriittisille palvelimille on turvattava häiriötön virransaanti akkuja tai varavirtalaitteita käyttämällä. 5. Kriittiset palvelimet on toteutettava vikasietoisesti ottaen huomioon muun muassa palvelinten kahdentaminen, kuormantasaus, varalaiteratkaisut sekä huoltosopimukset.

Osa-alueen nimi	**4.3 Varmistaminen ja dokumentointi**
Tavoitteet	Palvelinten toiminta dokumentoidaan kattavasti ja varmistetaan säännöllisesti. Dokumentoinnilla ja varmistuksilla edistetään vakavista ongelmatilanteista toipumista ja järjestelmämuutoksiin varautumista.
Vaatimukset	1. Palvelimista on otettava säännöllisesti riittävät varmuuskopiot. Varmistusten palauttamista varten tulee olla olemassa prosessit ja selkeät ohjeistukset. 2. Jokaisesta palvelimesta on laadittava yksityiskohtainen palvelindokumentti, josta käy ilmi muun muassa palvelimen sijainti ja käyttötarkoitus, oleellisimmat tekniset laite- ja ohjelmistotiedot, tietoliikenneasetukset, turvallisuusmääritykset, riippuvuussuhteet toisten palvelinten palveluista ja resursseista sekä nimetyt vastuuhenkilöt yhteystietoineen. Dokumentin ajan tasalla pysymisestä on huolehdittava koko palvelimen elinkaaren ajan. 3. Varmuuskopioiden toimintaa ja kattavuutta on testattava säännöllisesti. 4. Varmistusmediaa on säilytettävä eri palotilassa kuin palvelinta, josta varmistus on otettu.

5 Käyttöoikeuksien tietoturvallisuus

Osa-alueen nimi	**5.1 Käyttöoikeuksien elinkaaren hallinta**
Tavoitteet	Käyttöoikeuksien elinkaaresta huolehditaan, käyttäjille jo myönnettyjen oikeuksien tarpeellisuutta arvioidaan säännöllisesti ja tarpeettomat oikeudet poistetaan.
Vaatimukset	1. Käyttöoikeuksien elinkaaren hallinnasta (tilaus, muutos, poisto) on huolehdittava pääsääntöisesti kirkon yhteisen IHA[7]-järjestelmän kautta. 2. Kirjuri-jäsentietojärjestelmän käyttöoikeudet hallitaan ainoastaan IHA-järjestelmän kautta. 3. Esimies on velvollinen tilaamaan alaisilleen tarpeelliset tunnukset sekä käyttöoikeudet seurakunnan käyttämiin tietojärjestelmiin ja huolehtimaan tarpeettomien tunnusten poistamisesta ajallaan. 4. Vapaaehtoistyöntekijöiden tunnuksista ja käyttöoikeuksista vastaa kyseisen projektin/toiminnon vastuuhenkilö. 5. Käyttäjille myönnetään järjestelmiin ainoastaan tehtävien suorittamisen tarvittavat oikeudet. 6. Päällekkäisten käyttäjätunnusten aiheuttamien ristiriitatilanteiden välttämiseksi on toimialueiden käyttäjätunnukset luotava yhteisten sääntöjen mukaisesti. Päällekkäisyyksien käsittelyssä noudatetaan JHS 161-suositusta[8]. 7. Seurakuntataloudella on toimivat prosessit jo myönnettyjen käyttöoikeuksien tarpeellisuuden arvioimiseen. Tarpeettomaksi tulleet käyttöoikeudet poistetaan.

[7] IHA-järjestelmä on Kirkkohallituksen TYP (Työasemien Yhteiset Palvelut) hankkeessa toteutettu identiteettienhallintajärjestelmä.

[8] JHS-suositukset hyväksyy julkisen hallinnon tietohallinnon neuvottelukunta JUHTA.

Osa-alueen nimi	**5.2 Käyttöoikeuksien henkilökohtaisuus**
Tavoitteet	Tunnuksista ja niihin liittyvistä salasanoista pidetään hyvää huolta.
Vaatimukset	1. Järjestelmien käyttäjätunnukset ovat henkilökohtaisia. 2. Henkilökohtaisia tunnuksia ei saa antaa toisen henkilön käyttöön. Tunnuksiin liittyviä salasanoja ei saa kertoa kenellekään, eikä niitä saa säilyttää muistiin kirjoitettuna paikoissa, joissa ne ovat ulkopuolisen löydettävissä. Omilla käyttäjätunnuksilla avattua työasemaa ja sovelluksia ei saa jättää toisten käyttöön. Käyttäjä on vastuussa siitä, ettei hänen tunnuksillaan tapahdu väärinkäyttöä. 3. Järjestelmien käyttäjätunnuksiin liittyvien salasanojen on oltava riittävän vahvoja. Salasana tulee olla vähintään 12 merkkiä pitkä, se sisältää vähintään kolmea merkkityyppiä (numeroita, isoja kirjaimia, pieniä kirjaimia ja erikoismerkkejä), eikä se ole vuosiluku, päivämäärä, minkään kielen sana tai nimi tai sanan tai nimen muunnelma. Seurakuntatalous vastaa siitä, että järjestelmien salasanat täyttävät kompleksisuusvaatimukset. 4. Salasanat on vaihdettava riittävän usein, toimialueen tunnukset kuuden kuukauden välein. Salasanahistorian on oltava riittävän pitkä samojen salasanojen toistuvan käytön ehkäisemiseksi. 5. Oikeuksia levyjakoihin tai -järjestelmiin ei tule antaa suoraan käyttäjätunnuksille, vaan ne annetaan ryhmille.