Kirkon yleiset tietoturvamääräykset 2011

Hyväksytty kirkkohallituksen virastokollegiossa 10.2.2011

Tähän dokumenttiin viitataan ”Meidän kirkon tietoturvapolitiikka 2011” -nimisessä dokumentissa puhuttaessa kirkon yleisistä tietoturvamääräyksistä.

Siirtymätaso: Kaikilta seurakunnilta vaadittava taso vuoden 2011 lopussa. Kyse on tietoturvallisuuden minimitasosta 1.12.2011 voimaan tulevan kirkkolain 16 luvun säännösten mukaisesti.

Perustaso: Se taso, joka seurakunnalla tai keskusrekisterillä on oltava, jotta se voi saada Kirjuri-jäsentietojärjestelmässä valtakunnalliset tietojen käsittelyn ja asiakaspalvelun oikeudet.

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.
Siirtymätaso	1. Jokaisella seurakuntataloudella tulee olla nimetty tietoturvan yhdyshenkilö, joka vastaa saamiensa ohjeiden, suositusten ja määräysten tiedottamisesta sekä kokoaa raporttia seurakuntataloudessa havaituista tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista IT-alueen tietoturvavastaavalle. 2. Jokaisella IT-alueella tulee olla tietoturvaryhmä, jonka tehtävänä on laatia ja ylläpitää oman alueensa tietoturvapolitiikkaa ja tietoturvallisuuteen liittyviä ohjeita, suosituksia ja määräyksiä kirkon tietoturvallisuuden johtoryhmän laatimien koko kirkkoa koskevien linjausten puitteissa. Suuremmissa seurakuntatalouksissa, joissa koetaan oman toiminnan laajuuden ja erityistarpeiden sitä edellyttävän, on mahdollisuus perustaa oma tietoturvaryhmä, joka tarkentavaa edelleen IT-alueen tietoturvaryhmän laatimia ohjeita, suosituksia ja määräyksiä paikallisia tarpeita vastaaviksi ja joka käsittelee paikallisia ajankohtaisia tietoturvallisuutta koskevia kysymyksiä. 3. Tietoturvan yhdyshenkilöllä tulee olla riittävästi työaikaa tehtäviensä suorittamiseen.
Perustaso	1. Tietoturvallisuustyötä tekevien työntekijöiden toimenkuvauksiin on päivitettävä tieto työntekijän rooleista ja vastuista. 2. Seurakuntataloudessa on oltava riittävästi ammattitaitoista henkilöstöä, jotta tässä dokumentissa esitettyjen turvallisuusvaatimusten käytännön toteuttaminen on realistisesti mahdollista, ottaen huomioon mm. henkilöstön lomat ja muut poissaolot. 3. Tietoturvallisuuden resursointi huomioidaan seurakuntatalouden budjetissa.

Osa-alueen nimi	1.2 Tietoturvapolitiikka ja -ohjeistukset
Tavoitteet	Tarvittavat politiikat ja ohjeistukset ovat olemassa, ne pidetään ajan tasalla ja käyttäjien saatavilla. Käyttäjiä koulutetaan ja informoidaan säännöllisesti uusista ohjeista ja määräyksistä.
Siirtymätaso	1. IT-alueella/seurakuntatalouksilla on oltava ajantasainen tietoturvapolitiikka ja sitä tarkentavat ohjeistukset, jotka ovat linjassa koko kirkon ylemmän tason politiikkojen ja ohjeistusten kanssa. Ajan tasalla oleva tietoturvapolitiikka ja ohjeistukset tulee olla aina työntekijöiden saatavilla. 2. Tieto olemassa olevista tietoturvapolitiikoista ja ohjeistuksista 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. Seurakuntataloudella on oltava toimivat käytännöt tietojen elinkaaren hallintaa varten, kattaen tietojen luokittelun, säilyttämisen, välittämisen ja tuhoamisen. 5. Työntekijöille järjestetään säännöllisiä tietoturvakoulutuksia tai tietoiskuja, jossa kerrataan olemassa olevia ohjeita ja kerrotaan uusista. 6. Työntekijöiltä tulee vaatia salassapitositoumuksen allekirjoittamista ennen töiden aloittamista.
Perustaso	1. Tietoturvallisuuteen liittyvien ohjeiden ja määräysten noudattamista valvotaan ja poikkeamiin puututaan. 2. Seurakuntatalouden on velvollinen auditoimaan tietoturvallisuutensa tason säännöllisesti ulkopuolisen tahon toimesta. 3. Tietoturvallisuuteen liittyviä riskejä on arvioitava vähintään vuosittain. Arviointimenetelmä on kirjallisesti dokumentoitu. Uusiin ja muuttuneisiin riskeihin on reagoitava asian mukaisesti. 4. Henkilöstön osallistumista tietoturvakoulutuksiin ja tietoturvaohjeistuksiin tutustumista tulee seurata.

Osa-alueen nimi	1.3 Yhteistyökumppanit ja ulkoisten palveluiden hallinta
Tavoitteet	Ulkopuolisilta toimijoilta vaaditaan samaa tietoturvallisuuden tasoa kuin mitä omassa toiminnassa pyritään toteuttamaan. Tietoturvallisuus otetaan huomioon jo uusien hankkeiden ja hankintojen alkumetreillä.
Siirtymätaso	1. Ulkoistusten ja IT-palveluiden mahdollisen hankinnan yhteydessä ulkopuolisilta työntekijöiltä on edellytettävä riittävää koulutusta ja ammattitaitoa. 2. Ulkopuolisilta työntekijöiltä tulee vaatia salassapitositoumuksen allekirjoittamista ennen töiden aloittamista. 3. Ulkopuolisia työntekijöitä sitovat sama säännöt kuin kirkon omaa henkilöstöäkin. Ulkopuolisen työntekijän palkkaava taho on velvollinen saattamaan tiedoksi kaikki asiaan liittyvä ohjeistus. 4. Seurakuntataloudella on nimetty vastuuhenkilö ulkoisille toimijoille.
Perustaso	1. Seurakuntataloudella on kirjallinen ja ajantasainen dokumentaatio, jossa kuvataan sen osallistuminen erilaisissa alihankinta- ja yhteistyöverkostoissa. 2. Kumppaneille asetetaan tarvittavat tietoturvavaatimukset jo tarjouspyyntö- tai sopimusneuvotteluvaiheessa. 3. Kumppaneiden kanssa järjestetään riittävän usein palavereja, joissa tietoturvallisuuteen liittyviä asioita kuten havaittuja ja toteutuneita riskejä sekä tulevaisuuden tarpeita käsitellään.

Osa-alueen nimi	1.4 Toimintaprosessit
Tavoitteet	Seurakuntatalouden toiminta on suunnitelmallista ja toistettavaa. Poikkeamatilanteisiin reagoidaan määrätietoisesti ja tietoa jaetaan IT-alueiden välillä.
Siirtymätaso	1. IT-alueella/seurakuntatalouksilla on toimivat prosessit IT-toimintojensa hoitamiseen. Prosesseja on tarpeen mukaan päivitettävä vastaamaan muuttuneita tilanteita. Prosesseissa on otettu tietoturvallisuusnäkökulma huomioon. 2. Seurakuntataloudella on valmiussuunnitelma, jonka toimivuutta testataan säännöllisesti myös tietoturvallisuuden osalta. 3. Avaintoimintojen ja –prosessien toiminnan kannalta suojeltavat kohteet on tunnistettu ja luokiteltu. 4. Seurakuntatalous on tiedostanut toimintaansa koskevan lainsäädännön.
Perustaso	1. IT-alueella/seurakuntatalouksilla on oltava toimivat prosessit, joiden avulla tietoturvapolitiikkaa ja ohjeistusta arvioidaan vuosittain ja tarpeen mukaan päivitetään vastaamaan uusia haasteita. 2. IT-alueella/seurakuntatalouksilla on oltava prosessit ja ohjeistukset tietoturvapoikkeamien varalta. Näiden tulee ottaa kantaa tietoturvapoikkeamien havaitsemiseen, niihin reagoimiseen, seuraamusten käsittelyyn ja normaalitoimintaan palaamiseen. 3. Tietoturvapoikkeamat tulee raportoida huolellisesti ja tehdä jälkikäteen analyysi, jotta poikkeaman syntymissyyt saadaan tunnistettua ja korjaavia toimenpiteitä toteutettua. 4. Tietoturvapoikkeamista vaihdetaan tietoa muiden IT-alueiden tietoturvaryhmien kanssa ja muiden alueiden kokemuksia hyödynnetään.

2. Tietoverkkojen tietoturvallisuus

Osa-alueen nimi	2.1 Tietoverkkojen käyttäminen ja kehittäminen
Tavoitteet	Tietoturvallisuusvaatimukset otetaan huomioon tietoverkkoja suunniteltaessa ja niitä käytettäessä.
Siirtymätaso	1. Kaiken tietoliikenteen IT-alueen alueverkon ja ulkopuolisten verkkojen välillä tulee kulkea KIRKKO-verkon ja sen keskitetyn palomuurin kautta. Jos suoria yhteyksiä Internetiin muodostetaan nimettyä tarkoitusta varten (esimerkiksi hallintayhteys yhteen palvelimeen ulkoiselle toimijalle) on kyseinen liikenne eristettävä muusta alueverkosta (esimerkiksi virtuaaliverkkoja käyttämällä) ja dokumentoitava huolellisesti. 2. Seurakuntatalouden tietoverkkoon ei saa liittää muita kuin seurakuntatalouden omia, annetut vaatimukset täyttäviä laitteita. Mahdollista vierailijakäyttöä varten on hankittava erillinen Internet-liittymä, joka on eristetty KIRKKO-verkosta. 3. Langattomia verkkoja toteutettaessa on otettava huomioon niihin kohdistuvat tietoturvariskit. Päätelaitteiden tunnistaminen ja liikenteen salaaminen on toteutettava varmenteita ja vahvoja salausalgoritmeja käyttäen 802.1x standardin suositusten mukaisesti.
Perustaso	1. Muut kuin aktiivisessa käytössä olevat kytkinportit tulee sulkea. 2. Pääsy verkon aktiivilaitteiden hallintakäyttöliittymiin on suojattava vahvalla salasanalla. 3. Seurakuntatalouden verkko tulee jakaa virtuaaliverkkoihin hallittavuuden ja turvallisuuden lisäämiseksi. Esimerkiksi työasemille ja palvelimille on syytä luoda omat verkkosegmenttinsä.

3. Työasemien tietoturvallisuus

Osa-alueen nimi	3.1 Työasemien sovellukset ja käyttöjärjestelmät
Tavoitteet	Työasemien käyttöjärjestelmien säännöllisestä päivittämisestä huolehditaan. Valmistajan tuen piiristä poistuneita käyttöjärjestelmiä käyttävät työasemat on poistettava käytöstä.
Siirtymätaso	1. Kaikkien seurakuntatalouden käytössä olevien työasemien käyttöjärjestelmäversioiden tulee olla valmistajan tuen piirissä ja yrityskäyttöön tarkoitettuja. Windows-käyttöjärjestelmien osalta tämän dokumentin kirjoitushetkellä tämä tarkoittaa Windows XP SP3, Windows Vista SP1 tai Windows 7 käyttöjärjestelmiä. 2. Työasemissa on oltava ajanmukaiset ja automaattisesti päivittyvät tuotteet virusten ja haittaohjelmien torjuntaan, sekä ohjelmistotason palomuuri. 3. Työasemien käyttöjärjestelmien ja sovellusten turvallisuuspäivitykset on asennettava kaikkiin työasemiin automaattisesti ja ajallaan.
Perustaso	1. Kaikki vanhentuneita käyttöjärjestelmiä käyttävät työasemat on päivitettävä tai poistettava verkosta. 2. Työasemien sovellusten toiminta päivitysten jälkeen on syytä varmistaa testityöasemilla ennen päivitysten jakamista.

Osa-alueen nimi	3.2 Työasemien käyttäminen
Tavoitteet	Työasemia käytetään vain seurakuntatalouden työntekijöiden toimesta työtehtävien suorittamiseen. Paikallisten järjestelmävalvojaoikeuksien rajoittamisella pidetään luvattomien ja tarpeettomien ohjelmien asentaminen kurissa.
Siirtymätaso	1. Seurakuntatalouden työasemat (paitsi erikseen muuhun käyttöön nimetyt laitteet) on tarkoitettu työnantajan määräämien työtehtävien suorittamiseen. 2. Työasemia ei saa koskaan luovuttaa ulkopuolisten, esimerkiksi perheenjäsenten tai vierailijoiden käyttöön. Käyttäjä on itse vastuussa huolimattomuutensa mahdollisista vaikutuksista. 3. Asianmukaisesti suojatun ja ajantasaisesti päivitetyn työaseman käyttäminen myös julkisissa verkoissa (esimerkiksi hotel-

	lien vierasverkot ja kotiverkot) on sallittua. 4. Muiden kuin työtehtävien suorittamisen kannalta välttämättömien ohjelmien (esimerkiksi pelien) asentaminen työasemiin on kiellettyä. 5. Työasemien työpöydän automaattiset lukkiutumisasetukset on otettava käyttöön.
Perustaso	1. Työasemien levyresursseja ja palveluita ei tule jakaa verkossa muiden laitteiden tai palvelujen käyttöön. 2. Salausominaisuuksilla varustettuja UBS-muistilaitteita tulee suosia luottamuksellista tietoa kuljetettaessa. Muiden kuin työnantajan omistuksessa olevien muistilaitteiden liittämistä työasemiin tulee välttää.

Osa-alueen nimi	3.3 Työasemien hallinta
Tavoitteet	Työasemien hallintaoikeuksia annetaan vain ammattitaitoisille IT-ammattilaisille. Seurakuntataloudet huolehtivat siitä, että sovitut tietoturva-asetukset on käytössä kaikissa työasemissa.
Siirtymätaso	1. Päällekkäisten nimien aiheuttamien ristiriitatilanteiden välttämiseksi tietoverkkoon liitettävät työasemat on nimettävä yhteisten sääntöjen mukaisesti. 2. Tietoturva- ja selainasetukset tulee asettaa työasemiin keskitetysti siten, että käyttäjät eivät pysty niitä muuttamaan. 3. Käytössä olevista ohjelmistoista pidetään yllä ajantasaista dokumentaatiota. 4. Vain määrätyillä IT-henkilöillä saa olla ohjelmistojen asennukset mahdollistavat oikeudet työasemiin.
Perustaso	1. Työasemissa ei tule olla paikallisia käyttäjätunnuksia tai –ryhmiä työntekijöiden käyttöön. Näitä on oikeus käyttää vain ylläpitotarkoituksiin. 2. Työasemien mahdollinen etähallinta on rajoitettava suoritettavaksi vain tietyiltä määrättyjen IT-henkilöiden käytössä olevilta työasemilta tai tukipalvelimilta. Etäyhteyksien muodostaminen työasemiin tulee sallia vain asiaan oikeutetuilta nimetyiltä ylläpitäjiltä. Työntekijää tulee informoida ennen etätukitoimenpiteiden suorittamista ja tarvittaessa pyytää työnteki-

jän suostumus toimenpiteen suorittamiseen.

3. Työasemien perustason ”koventamisesta” tulee huolehtia. Esimerkiksi työasemien tarpeettomat palvelut tulee poistaa käytöstä.
4. Kannettavien työasemien kiintolevyt tulee soveltuvin osin salata. Erityishuomiota tulee kohdistaa työasemiin, joiden käyttäjät tyypillisesti käsittelevät luottamuksellista ja salaista materiaalia työasemillaan.
5. Työasemavarmenteiden käyttöä seurakuntatalouden omistamissa työasemissa suositellaan työasemien tunnistamista mahdollisia palveluita käytettäessä.

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 poistettava käytöstä.
Siirtymätaso	1. IT-alueella/seurakuntatalouksilla käytössä olevien palvelinten käyttöjärjestelmäversioiden tulee olla valmistajan tuen piirissä. Windows-käyttöjärjestelmien osalta tämän dokumentin kirjoitushetkellä tämä tarkoittaa Windows 2003 SP2 ja Windows 2008 palvelinkäyttöjärjestelmiä. Mahdollisia vanhentuneita käyttöjärjestelmäversioita käyttävät palvelimet tulee verkkoteknisesti (esimerkiksi virtuaaliverkkoja käyttämällä) eristää muusta työasema- ja palvelinympäristöstä. 2. Palvelinten käyttöjärjestelmien turvallisuuspäivitykset on asennettava kaikkiin palvelimiin automaattisesti ja ajallaan. 3. Palvelimissa on oltava ajanmukaiset ja automaattisesti päivittyvät tuotteet virusten ja haittaohjelmien torjuntaan tai verkkosegmentti, jossa palvelimet sijaitsevat, on suojattava erikseen palomuurilla, joka kykenee suodattamaan tietoliikenteen haittaohjelmistojen varalta.
Perustaso	1. Kaikki vanhentuneita käyttöjärjestelmiä käyttävät palvelimet on päivitettävä tai poistettava verkosta. 2. Palvelinten sovellusten toiminta päivitysten jälkeen varmistetaan testipalvelimilla ennen päivitysten jakamista tuotantoympäristöön. 3. Palvelinten perustason ”koventamisesta” tulee huolehtia. Esimerkiksi tarpeettomat palvelut tulee poistaa käytöstä.

Osa-alueen nimi	4.2 Palvelinten hallinta
Tavoitteet	Palvelinten sijoittelussa otetaan huomioon palvelun jatkuminen ja tilojen fyysinen turvallisuus. Palvelinten ylläpitotunnuksia ei käytetä päivittäisessä työasemakäytössä.
Siirtymätaso	1. Päällekkäisten nimien aiheuttamien ristiriitatilanteiden välttämiseksi tietoverkkoon liitettävät palvelimet on nimettävä yhteisten sääntöjen mukaisesti. 2. Palvelinten hallintaa varten on määrätyillä IT-henkilöillä oltava omat henkilökohtaiset tunnuksensa, joita ei käytetä normaaliin päivittäiseen työasemakäyttöön. 3. Palvelimet tulee sijoittaa asianmukaisiin lukittuihin laitetiloihin. Tarpeen mukaan laitetiloissa on oltava toimiva kulunvalvonta ja joiden jäähdytys ja palonsammutusjärjestelmät on mitoitettu laitemäärään.
Perustaso	1. Kriittisiä palvelimia varten on turvattava häiriötön virransaanti akkuja tai varavirtalaitteita käyttämällä. 2. Kriittiset palvelimet tulee toteuttaa vikasietoisesti, ottaen huomioon palvelinten kahdentaminen, kuormantasaus, varalaiteratkaisut sekä huoltosopimukset.

Osa-alueen nimi	4.3 Varmistaminen ja dokumentointi
Tavoitteet	Kattavalla ja ajantasaisella dokumentoinnilla ja varmistuksilla edistetään vakavista ongelmatilanteista toipumista ja järjestelmämuutoksiin varautumista.
Siirtymätaso	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.

Perustaso	1. Palvelinten palauttamista varmistuksista on testattava säännöllisesti. 2. Kopiota varmistusmediaa tulee säilyttää eri palotilassa kuin palvelinta josta varmistus on otettu. 3. Toimialueen GPO (Group Policy Object) ryhmäkäytäntöobjektit on dokumentoitava huolellisesti, jotta niiden kohdennusta ja yhteisvaikutuksia voidaan helpommin seurata. 4. Toimialueen ryhmien Description-kenttiin on ylläpidon helpottamiseksi syytä kirjoittaa lyhyt selostus ryhmän käyttötarkoituksesta.

5. Käyttöoikeuksien turvallisuus

Osa-alueen nimi	5.1 Käyttöoikeuksien elinkaaren hallinta
Tavoitteet	Käyttöoikeuksien elinkaaresta huolehditaan, käyttäjille jo myönnettyjen oikeuksien tarpeellisuutta arvioidaan säännöllisesti ja tarpeettomat oikeudet poistetaan.
Siirtymätaso	1. Käyttöoikeuksien elinkaaren hallinnasta (tilaus, muutos, poisto) on huolehdittava kirkon yhteisen TYP-järjestelmän kautta mikäli mahdollista. Muussa tapauksessa käytetään manuaalista TYP-prosessien mukaista työnkulkua tunnusten ja niiden muutosten käsittelyssä. 2. Kirjuri-järjestelmän käyttöoikeudet hallitaan ainoastaan TYP-järjestelmän kautta. 3. Esimies on velvollinen tilaamaan tunnuksia alaisilleen ja huolehtimaan tarpeettomien tunnusten poistamisesta ajallaan. 4. Esimiehet ovat velvollisia tarkistamaan alaistensa käyttöoikeuksien tilanteen säännöllisesti. 5. Lähtökohtaisesti käyttäjille on syytä myöntää vähäisimmät mahdolliset työtehtävien suorittamisen mahdollistavat oikeudet järjestelmiin. 6. Päällekkäisten käyttäjätunnusten aiheuttamien ristiriitatilanteiden välttämiseksi on toimialueiden käyttäjätunnukset luotava yhteisten sääntöjen mukaisesti. Päällekkäisyyksien käsittelyssä noudatetaan JHS 161-suositusta.
Perustaso	1. Seurakuntataloudella on toimivat prosessit jo myönnettyjen käyttöoikeuksien tarpeellisuuden arvioimiseen. Tarpeettomaksi jääneet käyttöoikeudet poistetaan.

Osa-alueen nimi	5.2 Käyttöoikeuksien henkilökohtaisuus
Tavoitteet	Käyttäjä vastaa omalla tunnuksillaan tehdyistä väärinkäytöksistä, joten tunnuksista ja niihin liittyvistä salasanoista pidetään hyvää huolta.
Siirtymätaso	1. Käyttäjätunnukset järjestelmiin ovat henkilökohtaisia ellei toisin ole todettu. 2. Henkilökohtaisia tunnuksia ei saa antaa toisten käyttöön. Tunnukseen liittyvää salasanaa ei saa kertoa kenellekään, eikä niitä saa säilyttää muistiin kirjoitettuna paikoissa, joissa ne ovat ulkopuolisten löydettävissä. Omilla käyttäjätunnuksilla avattuja työasemia ja sovelluksia ei saa jättää toisten käyttöön. Käyttäjä vastaa itse tunnuksillaan tapahtuvasta väärinkäytöstä. 3. Järjestelmien käyttäjätunnuksiin liittyvien salasanojen on oltava riittävän vahvoja, jotta mahdollisen väärinkäyttäjän ei ole niitä liian helppo arvata. Salasana tulee olla vähintään 8 merkkiä pitkä ja sen tulee sisältää vähintään kolmea seuraavista: numeroita, isoja kirjaimia, pieniä kirjaimia ja erikoismerkkejä. Seurakuntatalous vastaa järjestelmien salasanojen kompleksisuusvaatimuksista. 4. Salasanat on myös vaihdettava riittävän usein, toimialueen tunnusten tapauksessa kolmen kuukauden välein ja salasanahistorian on oltava riittävän pitkä samojen salasanojen toistuvan käytön ehkäisemiseksi. Salasanoille on myös määritettävä yhden päivän vähimmäisikä salasanahistorian kiertämisen vaikeuttamiseksi. 5. Kirjuri-järjestelmään voi kirjautua ainoastaan käyttämällä kirkon varmennepalvelun avulla luotuja varmenteita.
Perustaso	1. Oikeuksia levyjakoihin tai järjestelmiin ei tule antaa suoraan käyttäjille vaan ryhmille. Oikeuksien myöntämisessä on syytä noudattaa valmistajan suosituksia. 2. Työasemille kirjautumisessa on suositeltavaa käyttää kirkon varmennepalvelun avulla luotuja varmenteita.