KYRKANS DATASÄKERHETSPOLICY

Säkerhetspolicy för datasystem inom Evangelisk-lutherska kyrkan i Finland

21.3.2019

KYRKANS DATASÄKERHETSPOLICY

Säkerhetspolicy för datasystem inom Evangelisk-lutherska kyrkan i Finland

Innehåll

KYRKANS DATASÄKERHETSPOLICY

Säkerhetspolicy för datasystem inom Evangelisk-lutherska kyrkan i Finland

1 INLEDNING

I säkerhetspolicyn fastställs datasäkerhets- och dataskyddsarbetets mål, ansvar och organisering inom Evangelisk-lutherska kyrkan i Finland och i dess verksamhetsenheter. Datasäkerhetspolicyn har meddelats till hela kyrkans personal och samarbetspartner, och alla kyrkligt anställda i arbets- och tjänsteförhållande samt frivilliga medarbetare och personer i förtroendeställning ska handla i enlighet med policyn. Policyn preciseras i kyrkans datasäkerhetskrav och i andra anvisningar som gäller hela kyrkan eller IT-området.

2 VIKTIGA TERMER

Dataskyddet omfattar alla åtgärder som vidtas för att säkerställa informationens användbarhet, integritet och konfidentialitet[1]. I stället för dataskydd används ofta begreppet datasäkerhet. De avser samma sak.

Användbarhet i datasäkerhetssammanhang betyder att informationen är tillgänglig för dem som har rätt till den vid önskad tidpunkt. Tillgängligheten hotas bland annat av oförutsedda skador på datorer, telenät och dataprogram. Sådana kan inträffa till exempel till följd av ett överraskande fel i en teknisk komponent, ett mänskligt fel i ett datorprogram eller ett skadligt program med kriminellt ursprung eller en så kallad nätattack.

Integritet i datasäkerhetssammanhang betyder att informationen överensstämmer med den ursprungliga. Hot mot integriteten är bland annat mänskliga fel eller missförstånd när datorprogram skapas eller när information sparas. Integriteten hotas även av avsiktliga kriminellt utförda ändringar av information, till exempel vid penningtransaktioner eller i innehållet på internetsidor.

Konfidentialitet betyder att ingen obehörig får tillgång till informationen eller kan behandla den. Hoten mot konfidentialiteten är desamma som mot integriteten. Dessutom äventyras konfidentialiteten om processerna för administrationen av användarrättigheterna eller tillämpningen av dem är dåligt skötta.

Datasäkerhet handlar inte enbart om teknik, utan även om människors arbetssätt. Alla ska vara medvetna om hur man kan säkerställa datasäkerheten. Det handlar inte om enstaka åtgärder utan om en fortlöpande och systematisk verksamhet som inriktar sig på följande åtta delområden inom datasäkerhetsarbetet:

1. **Administrativ datasäkerhet:** Ett delområde inom datasäkerheten som granskar organisationens olika handlingspolicyer, verksamhetslinjer, ledning, organisering, placeringen av funktionerna inom organisationen, resursfördelningen och ansvarsfördelningen.

2. **Personalsäkerhet:** Ett delområde inom datasäkerheten som granskar skyddet av organisationens information och informationsbehandling mot medvetna och omedvetna hot från människor och de åtgärder människor vidtar för att säkerställa datasäkerheten.

3. **Fysisk datasäkerhet:** Ett delområde inom datasäkerheten som granskar alla sådana åtgärder som hör ihop med det fysiska skyddet av organisationens produktions- och verksamhetslokaler och genom vilka man försöker förhindra att all den information som organisationen behöver varken förstörs till sina fysiska eller icke-fysiska egenskaper, skadas eller hamnar i fel händer. Fysisk säkerhet avser även upprätthållandet av informationens användbarhet till den del som lokallösningarna kan vara till nytta eller eventuellt hinder för detta.

4. **Säkerhet vid användning av data och datasystem:** Ett delområde inom datasäkerheten som granskar frågor som rör automatisk och manuell informationsbehandling i organisationen.

[1] Det finns många olika definitioner av datasäkerhet. I detta sammanhang tillämpas den ordlista och definitionerna i den som ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) har sammanställt (på finska).

5. **Utrustningssäkerhet**: Ett delområde inom datasäkerheten som granskar skyddet av organisationens databehandlings- och datakommunikationsutrustning.

6. **Programvarusäkerhet**: Ett delområde inom datasäkerheten som granskar skyddet av de datorprogram organisationen använder samt licenser för och registrering av program.

7. **Datamaterialsäkerhet:** Ett delområde inom datasäkerheten som granskar all information i alla olika lagringsformat som organisationen behöver i sin dagliga verksamhet samt skyddet av den.

8. **Datakommunikationssäkerhet:** Ett delområde inom datasäkerheten som granskar skyddet av de datanät som organisationen använder sig av och datakommunikationen i dem.

Datasäkerhetsarbetet anknyter även till beredskapsplaneringen och beredskapen inför störningar och exceptionella situationer i samhället. Statsrådet fattade 23.11.2006 ett principbeslut om tryggandet av samhällets livsviktiga funktioner. I det redogörs för hotmodeller som samhällets olika aktörer ska vara beredda på i sina beredskapsåtgärder. Den första av dessa hotmodeller är störningar i den elektroniska infrastrukturen.

I samband med datasäkerhet talar man även ofta om dataskydd. Dataskydd hänför sig till rättigheter och skyldigheter samt särskilt till en grundläggande rättighet som är förknippad med integritetsskydd. I dataskyddet handlar det om vem som får behandla personuppgifter, vems uppgifter och vilka specifika uppgifter personen får behandla och i vilket syfte.

EU:s allmänna dataskyddsförordning ska tillämpas från och med den 25 maj 2018. Dataskyddsförordningen är lagstiftning som ska tillämpas direkt, precis som vilken lag eller förordning som helst som godkänts av riksdagen. Den har dessutom en starkare ställning på så sätt att en nationell lag eller förordning inte får stå i strid med EU:s dataskyddsförordning. I detta fall ska bestämmelserna i dataskyddsförordningen tillämpas. Bestämmelserna i dataskyddsförordningen kompletteras och preciseras med nationell lagstiftning till den del dataskyddsförordningen tillåter att den nationella prövningsmarginalen får justeras på detta sätt.

3 ORGANISERINGEN AV KYRKANS DATASÄKERHETSARBETE

3.1 Allmänt

I de följande avsnitten behandlas organiseringen av datasäkerhetsarbetet samt aktörerna och deras roller. Beskrivningen har gjorts ur församlingsenheternas perspektiv. Samma principer tillämpas anpassat även på kyrkans centralförvaltning och stiftens domkapitel.

3.2 Kyrkomötet

Kyrkomötet drar upp linjerna för hela kyrkans och församlingarnas datasäkerhetsfrågor i följande sammanhang:

- Kyrkolagen och kyrkoordningen: Kyrkomötet ger förslag till riksdagen om stiftande av kyrkolag och godkänner kyrkoordningen. I kyrkolagen och kyrkoordningen ingår också bestämmelser om datasäkerhet. Bland annat finns det i 16 kap. i både kyrkolagen och kyrkoordningen bestämmelser om datasäkerheten för kyrkobokföringen och medlemsdatasystemet Kirjuri.

- Allmän lagstiftning: I samband med datasäkerhetsfrågor ska hänsyn tas även till allmän lagstiftning, som har bestämmelser om datasäkerhet och som med stöd av kyrkolagen eller annars direkt gäller även den kyrkliga förvaltningen. Det handlar bland annat om personuppgiftslagen, lagen om offentlighet i myndigheternas verksamhet, lagen om dataskydd vid elektronisk kommunikation, lagen om integritetsskydd i arbetslivet, förvaltningslagen, lag om elektronisk kommunikation i myndigheters verksamhet, lagen om trossamfundens medlemsregister och lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster.

- Kyrkans centralfonds budget och verksamhets- och ekonomiplan: Kyrkomötet fastställer kyrkans centralfonds budget och behandlar verksamhets- och ekonomiplanen. Dessa innehåller även frågor som gäller utvecklingen av datasäkerheten.

3.3 Kyrkostyrelsens plenum

Kyrkostyrelsens plenum har följande uppgifter i anslutning till datasäkerhet:

- Tillsätta en ledningsgrupp för kyrkans datasäkerhet
- Utfärda kyrkans datasäkerhetsbestämmelser[2]

3.4 Kyrkostyrelsens ämbetskollegium

Kyrkostyrelsens ämbetskollegium har följande uppgifter i anslutning till datasäkerhet:

[2] Kyrkans datasäkerhetsbestämmelser är en föreskrift som är bindande för församlingarna och som ges med stöd av kyrkolagen eller kyrkoordningen.

- Utse en datasäkerhetschef för kyrkan.
- Vid hotad datasäkerhet eller i exceptionella situationer utfärda en datasäkerhetsbestämmelse för kyrkan som gäller högst fyra månader.
- Utfärda allmänna datasäkerhetsanvisningar och rekommendationer som kompletterar kyrkans datasäkerhetsbestämmelser samt särskilda datasäkerhetsanvisningar i anslutning till arbetsområdesvisa datasystem och grundläggande datateknik.

3.5 Kyrkans datasäkerhetschef

Kyrkans datasäkerhetschef:

- Ansvarar för underhållet av Kyrknätet och trafiken mellan nätets kommunikationstjänster samt datasäkerheten och säkerheten.
- Fungerar som ansvarsperson för Kyrknätets sammanslutningsabonnent med rätt att behandla nödvändiga identifikationsuppgifter.
- Rätt att vidta omedelbara skyddsåtgärder inom ramen för den finländska lagstiftningen.
- Utser i enskilda fall skriftligt i förväg de personer som deltar i behandlingen av identifieringsuppgifter och rapporterar utan oskäligt dröjsmål om behandlingen av identifieringsuppgifter till dataadministrationschefen.
- Utarbetar vid överraskande hot mot datasäkerheten eller i undantagssituationer en datasäkerhetsbestämmelse som fastställs av Kyrkostyrelsens ämbetskollegium.
- Ansvarar för att ge information eller ordna informationsgivningen i datasäkerhetsfrågor till församlingarna, medierna och andra externa aktörer.
- Ordnar mottagandet och behandlingen av de utvärderings- och händelserapporter som församlingarna utarbetar om datasäkerheten.

Kyrkans datasäkerhetschef ansvar dock inte för datasäkerheten eller dataskyddet i anslutning till innehållet i datasystemen. Datasäkerhetschefen utses av Kyrkostyrelsens ämbetskollegium.

3.6 Ledningsgruppen för kyrkans datasäkerhet

Ledningsgruppen för kyrkans datasäkerhet:

- Följer datasäkerhetsläget och utvecklingsbehoven i hela kyrkan.
- Bereder ett förslag till datasäkerhetspolicy för kyrkan och uppdatering av den.
- Bereder ett förslag till allmänna datasäkerhetsbestämmelser för kyrkan och uppdatering av dem.
- Bereder anvisningar och rekommendationer som kompletterar kyrkans datasäkerhetspolicy och allmänna datasäkerhetsbestämmelser.
- Styr och stöder anordnandet av utbildning i kyrkans datasäkerhetspolicy, datasäkerhetsbestämmelser och datasäkerhetsanvisningar och annan förankring av dessa.
- Lägger fram initiativ om utarbetande av mer ingående dataskyddsbestämmelser och dataskyddsanvisningar för olika verksamhetsområdens datasystem och deras funktioner eller grundläggande datateknik inom olika delområden.

3.7 Datasäkerhetsbestämmelser och anvisningar för kyrkans gemensamma datasystem

Den som äger innehållet och den som äger tekniken för kyrkans gemensamma datasystem för enskilda verksamhetsområden ansvarar tillsammans för upprättandet och iakttagandet av datasäkerhetskraven för den informationsegendom som ingår i systemet eller som behandlas med det. Lösningarna får inte strida mot kyrkans datasäkerhetspolicy och de allmänna datasäkerhetsbestämmelserna.

Exempel på datasystem som är gemensamma för kyrkan är medlemsdatasystemet Kirjuri, Kyrkans servicecentrals system, församlingsvalssystemet, e-posten evl.fi och systemen för församlingsarbete på webben.

3.8 Datasäkerhetsbestämmelser och anvisningar för kyrkans grundläggande datateknik

Ägarna till den grundläggande datateknikens (IT-infrastrukturens) olika delområden ansvarar för planeringen och skötseln av datasäkerheten för områdena i fråga. Lösningarna får inte strida mot kyrkans datasäkerhetspolicy och de allmänna datasäkerhetsbestämmelserna.

Exempel på dessa delområden är Kyrknätets centraliserade internetbrandvägg och dess gemensamma routrar och växlar.

3.9 Församlingens kyrkoråd eller den kyrkliga samfällighetens gemensamma kyrkoråd

Församlingens kyrkoråd eller den kyrkliga samfällighetens gemensamma kyrkoråd har följande uppgifter i anslutning till datasäkerhet:

- Ansvara för att de bestämmelser och anvisningar om datasäkerheten som getts församlingsenheten iakttas.
- Ser till att en datasäkerhetsgrupp har tillsatts för församlingsenheten. Gruppen bör helst vara gemensam för alla församlingar inom IT-samarbetsområdet.
- Ser till att en datasäkerhetsansvarig har utsetts i församlingsenheten. Den ansvariga bör helst vara gemensam för alla församlingar inom IT-samarbetsområdet.
- Ser till att det har utsetts en eller flera kontaktpersoner för datasäkerhetsfrågor i församlingsenheten på så sätt att samtliga anställda inom enheten känner till sin kontaktperson.
- Godkänner församlingsenhetens egen datasäkerhetspolicy. Den ansvariga bör helst vara gemensam för alla församlingar inom IT-samarbetsområdet. I policyn ges närmare riktlinjer för hur datasäkerheten i församlingsenheten sköts och vilka roller, ansvar och rättigheter de olika aktörerna har. Den anger även hur den interna kontrollen av datasäkerheten ska ordnas.

3.10 IT-områdets/församlingsenhetens datasäkerhetsgrupp

Datasäkerhetsgruppen:

- Upprätthåller bestämmelser, anvisningar och rekommendationer om datasäkerhetspolicyn och datasäkerheten i IT-områdets församlingsenheter så att

de svarar mot kyrkans gemensamma datasäkerhetspolicy och kyrkans gemensamma datasäkerhetsbestämmelser.
- Övervakar att datasäkerhetsbestämmelser, anvisningar och rekommendationer följs.
- Behandlar aktuella frågor om datasäkerhet.
- Planerar och ordnar utbildning om datasäkerhet i samarbete med den datasäkerhetsanvariga och kontaktpersonerna.

3.11 IT-områdets datasäkerhetsansvariga

Den datasäkerhetsansvariga:

- Utvecklar fortlöpande och aktivt datasäkerheten inom IT-områdets församlingar.
- Svarar för informationen om anvisningar, rekommendationer och bestämmelser som gäller datasäkerhet till kontaktpersonerna, cheferna och alla anställda.
- Tar emot observationer om händelser och avvikelser i anknytning till datasäkerheten och rapporterar regelbundet om dem till datasäkerhetsgruppen och kyrkans datasäkerhetschef.
- Godkänner vid överraskande hot mot datasäkerheten eller i exceptionella situationer en datasäkerhetsbestämmelse som gäller högst två månader.

En närmare beskrivning och regler för den datasäkerhetsansvarigas uppgifter ges i IT-områdets/församlingsenhetens datasäkerhetspolicy, datasäkerhetsbestämmelser och/eller datasäkerhetsanvisningar.

3.12 Kontaktperson för datasäkerhetsfrågor i den ekonomiska församlingsenheten

Kontaktpersonen för datasäkerhetsfrågor:

- Ser till att de anvisningar, rekommendationer och bestämmelser om datasäkerhet som han/hon har fått meddelas alla anställda.
- Deltar som stöd för cheferna i introduktionen av nya medarbetare i datasäkerhetsfrågor.
- Tar emot anmälningar om händelser och avvikelser som observerats i datasäkerheten i församlingen och rapporterar om dessa till den datasäkerhetsansvariga i IT-området/församlingen och till cheferna i sin egen församling. Praxisen beskrivs närmare i IT-områdets/församlingsenhetens datasäkerhetspolicy och/eller datasäkerhetsbestämmelser.

En beskrivning och regler för datasäkerhetskontaktpersonens uppgifter ges närmare i IT-områdets/församlingsenhetens datasäkerhetspolicy, datasäkerhetsbestämmelser och/eller datasäkerhetsanvisningar. Inom en del IT-områden har man kommit överens om att alla församlingsenheter har sin egen IT-kontaktperson. Då kan IT-kontaktpersonen även vara kontaktperson för datasäkerhetsfrågor.

3.13 Chefen

Chefen är skyldig att

- vidarebefordra information om bestämmelser, anvisningar och rekommendationer som gäller datasäkerheten till sina medarbetare
- ordna introduktion för nya medarbetare kring bestämmelser, anvisningar och rekommendationer om datasäkerhet och se till att medarbetarna har förstått och lärt sig dessa saker
- se till att medarbetarna följer de bestämmelser och anvisningar som har getts
- i fråga om sina medarbetare svara för att användarrättigheterna till datasystemen motsvarar behoven i arbetsuppgifterna
- se till att datasäkerhetsbestämmelser och anvisningar för chefens eget verksamhetsområde tas fram om sådana ännu inte finns
- ingripa i alla missförhållanden som han/hon observerar i datasäkerheten

En närmare beskrivning och regler för chefens uppgifter ges i IT-områdets/församlingsenhetens datasäkerhetspolicy, datasäkerhetsbestämmelser och/eller datasäkerhetsanvisningar.

3.14 Medarbetare

I detta sammanhang avses med medarbetare personer i anställningsförhållande, förtroendevalda, volontärer eller inhyrd arbetskraft. Medarbetaren är skyldig att

- sätta sig in i de datasäkerhetsbestämmelser och anvisningar som gäller honom/henne och att iaktta dem i sitt dagliga arbete
- ta hänsyn till aktsamhetsplikten enligt personuppgiftslagen och god informationshantering enligt offentlighetslagen
- rapportera till sin chef och församlingens kontaktperson för datasäkerhetsfrågor om missförhållanden och avvikelser som han/hon observerar i datasäkerheten.

En närmare beskrivning och regler för medarbetarens uppgifter ges i IT-områdets/församlingsenhetens datasäkerhetspolicy, datasäkerhetsbestämmelser och/eller datasäkerhetsanvisningar.

3.15 Revisorerna

I Kyrkostyrelsens cirkulär 35/2010 behandlades 19.10.2010 ändringar i revisionen och valet av revisorer för fullmäktigeperioden 2011–2014. Där konstateras bl.a. följande:

”Med revisionstjänster avses den granskning av förvaltningen och ekonomin som föreskrivs i 15 kap. 11–13 § i kyrkoordningen. Den som utför den lagstadgade revisionen ska även granska separat angivna uppdrag som t.ex. redovisningar av EU-projekt och byggnadsbidrag. Värdförsamlingarna för de avtalsbaserade IT-samarbetsområdena ska inkludera granskningen av dataadministrationen och datasäkerheten i sin anbudsförfrågan om revisionen för inkommande fullmäktigeperiod. IT-samarbetsområdenas värdförsamlingar ska upphandla granskningen av dataadministrationen och datasäkerheten 2011 i god tid innan Kirjuri tas i bruk och därefter årligen kring årsskiftet så att granskningsresultaten finns tillgängliga för medlemsförsamlingarnas revisorer på vårvintern och våren. Värdförsamlingarna skickar uppgifterna från granskningen av datasäkerheten till samarbetsförsamlingarna och Kyrkostyrelsens dataadministration. Vid granskningen ska god revisionssed iakttas och revisionslagen följas i tillämpliga delar.”

3.16 Den personuppgiftsansvarige

Med den personuppgiftsansvarige[3] avses en fysisk eller en juridisk person, en myndighet, ett ämbetsverk eller ett annat organ som självständigt eller tillsammans med andra definierar syftena och metoderna för behandling av personuppgifter.

Den personuppgiftsansvarige:

- Ansvarar för behandlingen av personuppgifter.
- Är skyldig att vidta de behövliga tekniska och organisatoriska åtgärder med vilka det kan säkerställas och påvisas att behandlingen följer gällande lagstiftning, med beaktande av den senaste tekniken och genomförandekostnaderna samt behandlingens karaktär, omfattning, sakförhållande och syften samt av de risker av varierande sannolikhet och storlek som behandlingen orsakar fysiska personers rättigheter och friheter.
- Är skyldig att vidta de behövliga tekniska och organisatoriska åtgärder med vilka det säkerställs att utgångspunkten är att endast sådana personuppgifter som behövs för ett visst särskilt syfte behandlas.

Inom kyrkan är den personuppgiftsansvarige vanligen församlingen, centralregistret eller båda. En församling som hör till centralregistret kan ha register där behandlingen av personuppgifter inte har lagts ut till centralregistret.

3.17 Dataskyddsombud

En församling, en kyrklig samfällighet, domkapitlet och Kyrkostyrelsen är skyldiga att utse ett eget dataskyddsombud[4]. Ett dataskyddsombud kan utses för flera församlingar eller domkapitel.

Dataskyddsombudet:

- Ger den personuppgiftsansvarige och dess anställda information och råd om skyldigheterna enligt dataskyddsbestämmelserna.
- Kontrollerar att dataskyddsbestämmelserna iakttas vid behandlingen av personuppgifter.
- Är kontaktperson mot tillsynsmyndigheten (dataombudsmannen).
- Är obunden och får inte ta emot anvisningar i samband med skötseln av sina uppgifter. Dataskyddsombudet ska känna till dataskyddslagstiftningen och förfaringssätten i branschen.

Det bör beaktas att dataskyddsombudet inte ansvarar för lagligheten hos behandlingen av personuppgifter som görs av den personuppgiftsansvarige och är inte heller skyldig att korrigera observerade tekniska eller organisatoriska brister i behandlingen av personuppgifter.

---

[3] Mer information om den personuppgiftsansvariges roll och skyldigheter finns på Kyrkans webbplats om dataskydd https://nuotta.evl.fi/Tietosuoja/SitePages/Kotisivu.aspx

[4] Mer information om dataskyddsombudets roll och uppgifter finns på Kyrkans webbplats om dataskydd https://nuotta.evl.fi/Tietosuoja/SitePages/Kotisivu.aspx

4 CENTRALA RIKTLINJER FÖR KYRKANS DATASÄKERHETSARBETE

4.1 Mål och principer

Kyrkans mål är att i en tillräcklig och ändamålsenlig omfattning trygga att information, datasystem, tjänster och datanät som är viktiga för kyrkans verksamhet fungerar och att förhindra obehörig användning av dem samt oavsiktligt och avsiktligt förstörande och förvanskning av information. Avsikten är dessutom att upprätthålla ett systematiskt och kontinuerligt utvecklingsarbete för identifiering, bedömning och hantering av hot och risker. Utöver tryggandet av informationsbehandlingen under normala förhållanden bereder sig kyrkan även för störningar och exceptionella förhållanden så att verksamheten kan fortsätta så störningsfritt som möjligt och att man kan återgå till det normala så fort som möjligt.

Vid såväl manuell som datateknisk behandling av information måste man sörja för informationens konfidentialitet, integritet och användbarhet i alla de former som informationen förekommer i och under hela dess livscykel.

4.2 Förankring av policyn

Förmedlingen av information om anvisningar, rekommendationer och bestämmelser som gäller datasäkerhet sker på det sätt som anges i avsnitt 3. Kyrkans datasäkerhetschef vidarebefordrar informationen till IT-områdenas datasäkerhetsansvariga och de i sin tur till kontaktpersonerna för datasäkerhetsfrågor i församlingarna inom sitt IT-område. IT-områdets datasäkerhetsansvariga och datasäkerhetsgrupp ordnar datasäkerhetsutbildning inom sitt område. Som informationskanal används även Kyrkostyrelsens cirkulär, kyrkans gemensamma webbtjänster och IT-områdenas egna webbtjänster.

Befintligt datasäkerhetsmaterial delas ut till nya medarbetare och är en del av introduktionen av nya medarbetare. Kontaktpersonerna i datasäkerhetsfrågor deltar i introduktionen för fördjupad information om datasäkerhetsfrågor.

Ledningsgruppen för kyrkans datasäkerhet granskar och tar ställning till anvisningar och föreskrifter som gäller datasäkerhet. Anvisningarna och föreskrifterna sparas elektroniskt så att de är tillgängliga för alla medarbetare.

4.3 Översyn och utvärdering

Ledningsgruppen för kyrkans datasäkerhet svarar för att regelbunden översyn och utvärdering av datasäkerhetspolicyn samt övriga datasäkerhetsbestämmelser och datasäkerhetsanvisningar ordnas på övergripande nivå i kyrkan och IT-områdenas datasäkerhetsgrupper ser till att detta ordnas på lokal nivå. En utvärdering ska alltid göras när det har skett förändringar som inverkar på datasäkerheten. Sådana är till exempel betydande exceptionella situationer, sårbarhet av nytt slag (virus osv.), organisationsförändringar eller förändringar i den tekniska grundstrukturen.

Församlingarnas revisorer och i synnerhet revisorerna i IT-områdenas värdförsamlingar anlitas vid utvärderingen av hur datasäkerheten har utfallit. Revisorerna kan som oberoende tredje part bedöma hur väl anvisningarna och

bestämmelserna har omsatts i praktiken och inom vilka områden det finns behov av att effektivisera verksamheten.

4.4 Påföljder av missbruk

Om man misstänker eller om det finns bevis för händelser som äventyrar datasäkerheten, eller om det finns motiverad grund att misstänka att en medarbetare har gjort sig skyldig till brottslig verksamhet eller missbruk, ska arbetsgivaren utreda saken och förhindra att det felaktiga agerandet fortsätter. Arbetsgivaren kan tillgripa de sanktioner som arbets- och tjänstelagstiftningen möjliggör. Arbetsgivaren ska vid behov underrätta polisen om lagstridigt förfarande för eventuell brottsutredning.