Datasäkerhetspolicy för evangelisk-lutherska kyrkan i Finland

14.4.2026

Datasäkerhetspolicy för evangelisk-lutherska kyrkan i Finland

Innehållsförteckning

Datasäkerhetspolicy för evangelisk-lutherska kyrkan i Finland

1 INLEDNING

Datasäkerhetspolicyn definierar datasäkerhets- och dataskyddsarbetets syften, ansvar och organisering inom evangelisk-lutherska kyrkan i Finland och 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 CENTRALA TERMER

Datasäkerheten omfattar alla de arrangemang för att säkerställa informationens användbarhet, integritet och konfidentialitet[1]. I stället för ordet datasäkerhet används ofta också ordet informationssäkerhet. De betyder 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.

Datasäkerheten handlar inte bara om teknik, utan om människors arbetssätt. Alla ska vara medvetna om hur man kan sörja för datasäkerheten. Det handlar inte heller om enstaka åtgärder utan om en fortlöpande och systematisk verksamhet som inriktar sig på följande 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 data och databehandling mot avsiktliga och oavsiktliga hot orsakade av människor och människors åtgärder 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.

[1] Det finns flera olika definitioner av datasäkerhet. I detta sammanhang tillämpas den ordlista och definitionerna i den som ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI) har sammanställt (på finska).

4. **Säker användning av uppgifter och datasystem**: Ett delområde inom datasäkerheten som granskar frågor som gäller skyddet av organisationens automatiska och manuella databehandling.

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

6. **Programvarusäkerhet**: Ett delområde inom datasäkerheten som granskar skyddet av organisationens datorprogram samt licensiering 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 organisationens datanät och frågor som gäller skyddet av organisationens datakommunikation.

9. **Cybersäkerhet:** Ett delområde inom datasäkerheten som fokuserar på att garantera säkerheten av data, datasystem och utrustning i nätmiljön.

10. **Informationspåverkan**: Verksamhet genom vilken man systematiskt strävar efter att påverka den allmänna opinionen, människornas beteende och beslutsfattarna samt därigenom samhällets funktionsförmåga.

Datasäkerhetsarbetet anknyter också till beredskapsplanering och beredskap för störningssituationer och undantagsförhållanden i samhället. Statsrådets säkerhetsstrategi för samhället definierar hotmodeller som samhällets olika aktörer ska beakta i sina beredskapsåtgärder.

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 är det fråga om vem som får behandla personuppgifter, vems uppgifter och vilka specifika uppgifter personen får behandla och i vilket syfte.

EU:s allmänna dataskyddsförordning började tillämpas från och med 25.5.2018. Dataskyddsförordningen är lagstiftning som ska tillämpas direkt, precis som vilken lag eller förordning som helst som godkänts av riksdagen. Dessutom har den en starkare ställning på det sättet att en nationell lag eller förordning inte får stå i strid med EU:s dataskyddsförordning. 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. Varje anställd ansvarar för att en god datasäkerhet förverkligas.

3.2 Kyrkomötet

Kyrkomötet drar upp riktlinjer för rikskyrkans och församlingarnas datasäkerhet 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 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. Sådana bestämmelser är bland annat dataskyddslagen (1050/2018), lagen om offentlighet i myndigheternas verksamhet (621/1999, offentlighetslagen), lagen om tjänster inom elektronisk kommunikation (917/2014), lagen om integritetsskydd i arbetslivet (759/2004), förvaltningslagen (434/2003), lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagen om trossamfundens medlemsregister (614/1998) och lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009).

- Kyrkans centralfonds budget samt verksamhets- och ekonomiplan: Kyrkomötet fastställer budgeten för kyrkans centralfond och behandlar verksamhets- och ekonomiplanen. Dessa innehåller också frågor som gäller datasäkerhetens utveckling.

3.3 Kyrkostyrelsens plenum

Kyrkostyrelsens plenum har följande uppgifter i anslutning till datasäkerhet:

- Tillsätta ledningsgruppen för kyrkans datasäkerhet
- Utfärda kyrkans datasäkerhetsbestämmelser[2]

[2] Kyrkans datasäkerhetsbestämmelse är en med stöd av kyrkolagen eller kyrkoordningen bindande föreskrift för församlingarna.

3.4 Kyrkostyrelsens ämbetskollegium

Kyrkostyrelsens ämbetskollegium har följande uppgifter i anslutning till datasäkerhet:

- 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 Kyrkostyrelsen

Kyrkostyrelsen:

- producerar gemensamma IT-tjänster för hela kyrkan
- ansvarar för att kyrkans gemensamma tjänster är säkra och reglerar deras användning.

Exempel på kyrkans gemensamma datasystem är medlemsdatasystemet Kirjuri, kyrkans gemensamma M365-miljö, AD-användarkatalogen, identitetshanteringssystemet och Kyrknätets kärna.

3.6 Kyrkans säkerhetsoperationstjänster (SOC)

SOC (Secure Operations Center) är ett centrum som övervakar och administrerar organisationens datasäkerhet. Kyrkans SOC-tjänst lyder under Kyrkostyrelsen och har sin egen förvaltningsmodell. Kyrkans säkerhetsoperationstjänster:

- observerar och analyserar datasäkerhetshändelser och -incidenter i realtid
- reagerar på observerade datasäkerhetsavvikelser i syfte att begränsa och stoppa missbruk

3.7 Kyrkans datasäkerhetschef

Kyrkans datasäkerhetschef:

- Ansvarar för underhållet av [3]kärnan, datasäkerheten och säkerheten i Kyrknätet
- Fungerar som ansvarsperson för kärnan i Kyrknätets sammanslutningsabonnent med rätt att behandla nödvändiga identifieringsuppgifter

[3] Efter de ändringsarbeten som inleddes 2022 består Kyrknätet av en kärna som upprätthålls av serviceleverantören och därmed förknippade regionala nätverk som förvaltas av IT-områdena samt av datorsalnät av leverantörer som undertecknat servicecentralavtalet

- 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.

3.8 Ledningsgruppen för kyrkans datasäkerhet

Ledningsgruppen för kyrkans datasäkerhet:

- Följer datasäkerhetsläget och utvecklingsbehoven i hela kyrkan.
- Bereder ett förslag om kyrkans datasäkerhetspolicy och dess uppdatering till Kyrkostyrelsens plenum
- Bereder ett förslag till allmänna datasäkerhetsbestämmelser och deras uppdatering till Kyrkostyrelsens plenum
- 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.

3.9 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, systemen för Kyrkans servicecentrals system, församlingsvalssystemet, e-posten evl.fi och systemen för församlingsarbete på webben.

3.10 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.

3.11 Församlingens kyrkoråd eller den kyrkliga samfällighetens gemensamma kyrkoråd

I anslutning till datasäkerhetsfrågor ska församlingens kyrkoråd eller den kyrkliga samfällighetens gemensamma kyrkoråd:

- Ansvara för att de bestämmelser och anvisningar om datasäkerheten som getts församlingsenheten iakttas.
- Se till att en datasäkerhetsgrupp har tillsatts för församlingsenheten. Gruppen bör helst vara gemensam för alla församlingar inom IT-samarbetsområdet.
- Se till att en datasäkerhetsansvarig har utsetts i församlingsenheten. Den ansvariga bör helst vara gemensam för alla församlingar inom IT-samarbetsområdet.
- Se till att det har utsetts en eller flera kontaktpersoner för datasäkerhetsfrågor i församlingsenheten på så sätt att samtliga anställda inom enheten känner sin kontaktperson.

3.12 IT-områdets dataadministrationschef

IT-områdets dataadministrationschef ansvarar för:

- Datasäkerheten i IT-områdets eget regionala nätverk
- De praktiska åtgärder som genomförandet av datasäkerheten förutsätter inom det egna IT-området utgående från kyrkans datasäkerhetspolicy, de gemensamma datasäkerhetsbestämmelserna och beslut av församlingens kyrkoråd eller den kyrkliga samfällighetens gemensamma kyrkoråd

3.13 IT-områdets / församlingsenhetens datasäkerhetsgrupp

Datasäkerhetsgruppen:

- Upprätthåller bestämmelser, anvisningar och rekommendationer om datasäkerheten i IT-områdets församlingsenheter på så sätt att de är i linje med kyrkans gemensamma datasäkerhetspolicy och kyrkans gemensamma datasäkerhetsbestämmelser.
- Övervakar att datasäkerhetsbestämmelser, anvisningar och rekommendationer följs.
- Behandlar aktuella datasäkerhetsfrågor.

- Planerar och ordnar utbildning om datasäkerhet i samarbete med den datasäkerhetsanvariga och kontaktpersonerna.

3.14 IT-områdets / församlingsenhetens datasäkerhetsansvariga

Datasäkerhetsansvariga:

- Utvecklar datasäkerheten i IT-områdets församlingar kontinuerligt och aktivt.
- Svarar för informationen om anvisningar, rekommendationer och bestämmelser som gäller datasäkerhet till kontaktpersonerna, cheferna och alla anställda.
- Tar emot observationer om händelser och avvikelser med anknytning till datasäkerheten och rapporterar regelbundet om dem till datasäkerhetsgruppen och kyrkans datasäkerhetschef.

En närmare beskrivning och regler för den datasäkerhetsansvarigas uppgifter ges i församlingsenhetens datasäkerhetsbestämmelser och/eller datasäkerhetsanvisningar.

3.15 Kontaktperson för datasäkerhetsfrågor i den ekonomiska församlingsenheten

Kontaktpersonen för datasäkerheten:

- Ser till att de anvisningar, rekommendationer och bestämmelser om datasäkerhet som hen 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. Förfarandena beskrivs närmare i församlingsenhetens datasäkerhetsbestämmelser.

En närmare beskrivning och regler för kontaktpersonens uppgifter ges i församlingsenhetens 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.

3.16 Chefen

Chefen är skyldig att

- vidarebefordra information om bestämmelser, anvisningar och rekommendationer som gäller datasäkerheten till sina egna medarbetare
- ordna introduktion för nya medarbetare i 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 egna 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 observerade missförhållanden i datasäkerheten

En närmare beskrivning och regler för chefens uppgifter ges i församlingsenhetens datasäkerhetsbestämmelser och/eller datasäkerhetsanvisningar.

3.14 Medarbetare

I detta sammanhang avses med medarbetare personer i anställningsförhållande, förtroendevalda, frivilligarbetare eller inhyrd arbetskraft. Trots många olika ansvariga instanser kan medarbetarens eget ansvar för datasäkerheten inte betonas tillräckligt. Medarbetaren är skyldig att

- göra sig förtrogen med de datasäkerhetsbestämmelser och anvisningar som gäller medarbetaren och att iaktta dem i sitt dagliga arbete samt även annars vara särskilt omsorgsfull vid behandlingen av personuppgifter
- rapportera till sin chef och församlingens kontaktperson för datasäkerhetsfrågor om observerade missförhållanden och avvikelser i datasäkerheten.

En närmare beskrivning och regler för medarbetarens uppgifter ges i församlingsenhetens datasäkerhetsbestämmelser och/eller datasäkerhetsanvisningar.

3.18 Revisorer

Vid upphandling av revisionstjänster för förvaltningen och ekonomin ska datasäkerhetsaspekter beaktas. IT-områdets värdförsamlingar ska ta med granskningen av dataadministrationen och datasäkerheten som ett separat uppdrag i anbudsförfrågan om revisionen för nästa fullmäktigeperiod. Det rekommenderas att denna granskning görs regelbundet. Värdförsamlingen skickar uppgifter om granskningen av datasäkerheten till IT-områdets församlingar och Kyrkostyrelsens dataadministration. Vid granskningen av datasäkerheten ska revisorerna ta hänsyn till att alla datasäkerhetsfrågor inte hör till IT-områdets värdförsamlings ansvar.

3.19 Personuppgiftsansvarig

Med den personuppgiftsansvarige[4] 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.

[4] Mer information om den personuppgiftsansvariges roll och ansvar finns på Kyrkans webbplats om dataskydd https://evl.fi/sv/dataskydd/

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 lämpliga tekniska och organisatoriska åtgärderna för att säkerställa att endast personuppgifter som behövs för varje särskilt syfte behandlas som standard.

Inom kyrkan är den personuppgiftsansvarige vanligen församlingen, centralregistret eller båda. En församling som hör till centralregistret kan ha register, vars ansvar för behandlingen av personuppgifter inte har överförts till centralregistret.

3.20 Dataskyddsombud

En församling, en kyrklig samfällighet, domkapitlet och Kyrkostyrelsen är skyldiga att utse ett eget dataskyddsombud[5]. Ett dataskyddsombud kan utses för flera församlingar eller domkapitel.

Dataskyddsombudet:

- Ge den personuppgiftsansvarige och dennes anställda information och råd om skyldigheterna enligt dataskyddsbestämmelserna.
- Följer upp att dataskyddsbestämmelserna iakttas vid behandlingen av personuppgifter.
- Är kontaktperson gentemot tillsynsmyndigheten (dataombudsmannen).
- Är oberoende 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.

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

3.21 Kontaktperson för dataskyddsfrågor i den ekonomiska församlingsenheten

Kontaktpersonen för dataskyddet:

- Ser till att de anvisningar, rekommendationer och bestämmelser om dataskydd som hen har fått meddelas alla anställda.
- Deltar som stöd för cheferna i introduktionen av nya medarbetare i frågor som gäller dataskydd.
- Tar emot anmälningar om händelser och avvikelser i anslutning till dataskyddet i församlingen och rapporterar om dem till IT-områdets / församlingens data-skyddsombud och till församlingens chefer.

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 organiserar datasäkerhetsutbildningen 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 för datasäkerheten deltar i introduktionen för att främja förmedlingen av information om datasäkerheten.

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 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.