**CIR1H nr 10009 af 08/12/2021 (Historisk)**

# Cirkulære om informationssikkerhed for Kirkeministeriet og Den danske folkekirke

Ministerium: By-, Land- og Kirkeministeriet

Journalnummer: Kirkemin., j.nr. 2021-6536

## Senere ændringer til forskriften

CIR1H nr 9479 af 28/06/2024

# Cirkulære om informationssikkerhed for Kirkeministeriet og Den danske folkekirke

Kirkeministeriet understøtter folkekirken blandt andet ved at sikre tidssvarende administrative rammer for folkekirkens virke. Det sker blandt andet i medfør af §§ 9, 10 og 17 f i lov om folkekirkens økonomi samt i form af bistand til udvikling af fælles systemer og rammer i dialog med folkekirkens interessenter. Kirkeministeriet sikrer herved, at fælles systemer og rammer lever op til kravene om informationssikkerhed og databeskyttelse.

## Kapitel 1

*Anvendelsesområdet*

**§ 1.** Nærværende cirkulære udmønter de konkrete retningslinjer for informationssikkerhed, som informationssikkerhedspolitikken for Kirkeministeriet og folkekirken fastlægger.

*Stk. 2.* Cirkulæret gælder for Kirkeministeriet og de folkekirkelige myndigheder og institutioner, som anvender de fælles systemer på Kirkenettet. De myndigheder og institutioner, som skal anvende de fælles systemer på Kirkenettet, har pligt til at gøre sig bekendt med indholdet af dette cirkulære samt cirkulærer om fælles dataansvar ved behandling af personoplysninger i de fælles systemer.

Myndigheder og institutioner, som ikke er forpligtet til at benytte de af Kirkeministeriet leverede systemer, men som vælger at benytte disse, anvender systemerne på samme vilkår, som gælder for myndigheder og institutioner, der er forpligtet til at anvende dem.

*Stk. 3.* Endvidere gælder dette cirkulære for alle brugere med adgang til Kirkenettet og for al brug af Kirkenettet.

## Kapitel 2

*Sikkerhedsorganisationen*

**§ 2.** Kirkeministeriet og folkekirkens myndigheder og institutioner er hver især ansvarlige for overholdelse af kravene til informationssikkerhed og databeskyttelse. Den enkelte myndighed og institution er som udgangspunkt ansvarlig for at sikre den registreredes rettigheder i henhold til reglerne om databeskyttelse.

*Stk. 2.* Lokale sikkerhedsansvarlige i forhold til Kirkenetbrugere og udvalgsbrugere har ansvaret for informationssikkerheden lokalt og skal sikre, at brugerne udviser en sikker adfærd.

*Stk. 3.* Organisationens sikkerhedsansvarlige fremgår af bilag 1.

**§ 3.** Provster, biskopper, rektorer og kontorchefer kan skriftligt bemyndige en anden person som deres stedfortræder i rollen som lokal sikkerhedsansvarlig. Den lokale sikkerhedsansvarlige er ansvarlig for sin stedfortræder.

*Stk. 2.* De kirkebogsførende sognepræster er sikkerhedsansvarlige for personregistreringen. Såfremt der er flere kirkebogsførende sognepræster i samme pastorat, varetages rollen som sikkerhedsansvarlige for personregistreringen af de kirkebogsførende sognepræster i henhold til den aftalte fordeling af pastoratets sogne.

*Stk. 3.* I menighedsråd er formanden som udgangspunkt den sikkerhedsansvarlige. Menighedsrådet kan dog beslutte at tillægge rollen til et andet af menighedsrådets medlemmer eller til en sognepræst.

Kapitel 3

*Brugere og anvendelse af udstyr*

**§ 4.** Kirkenettet er et lukket netværk, hvortil der hører systemer og services samt it-udstyr, som er etableret for Kirkeministeriet og de folkekirkelige myndigheder, institutioner samt ansatte og folkevalgte (brugerne).

*Stk. 2.* En bruger kan tilgå Kirkenettet fra en Kirkenet-pc eller fra en privat pc eller mobil enhed via den Digitale Arbejdsplads (DAP) til udvalgte systemer og services.

*Stk. 3.* Folkekirkens It stiller de fælles systemer i Kirkenettet til rådighed for brugerne.

**§ 5.** Den Digitale Arbejdsplads giver adgang til dele af Kirkenettet og er samtidigt en lukket og sikker platform, hvor der kan deles informationer i Kirkeministeriet og folkekirken.

**§ 6.** En Kirkenet-pc er en pc med præinstallerede programmer, som leveres af Folkekirkens It.

*Stk. 2.* Alle Kirkenet-pc'er er sikret med kryptering af harddisken, og dermed er informationer gemt på pc'en beskyttet mod uvedkommende. Krypteringen fungerer, når pc'en er låst eller slukket.

*Stk. 3.* Alle Kirkenet-pc'er kan tilsluttes en åben internetforbindelse. Ved hjælp af en VPN-forbindelse opretter Kirkenet-pc'en automatisk en krypteret adgang til Kirkenettet. VPN-forbindelsen skal altid aktiveres ved opstart af pc'en og må ikke afbrydes under anvendelsen.

**§ 7.** Hvis adgangen til Kirkenettet via den Digitale Arbejdsplads opnås fra en privat pc eller mobil enhed, gælder dette cirkulære for den behandling af informationer, som finder sted i den forbindelse.

*Stk. 2.* Arbejdsrelaterede data, som indeholder personoplysninger eller fortrolige oplysninger, må brugeren ikke gemme på privat udstyr.

*Stk. 3.* Folkekirkens It yder support til brug af de af Kirkenettets systemer og services, der kan anvendes på privat udstyr. Folkekirkens It yder ikke i øvrigt support til privat udstyr.

**§ 8.** En Kirkenetbruger er en bruger, som tilgår Kirkenettets systemer og services fra en Kirkenet-pc. Systemer på Kirkenettet, som findes i en web-udgave/app, kan Kirkenetbrugeren også anvende fra en privat pc eller mobil enhed.

*Stk. 2.* En Kirkenetbruger kan, alt efter brugerens specifikke arbejdsbetingede behov, gives adgang til relevante systemer og services i Kirkenettet.

**§ 9.** En udvalgsbruger er en bruger, som har tilknytning til enten et menighedsråd, et provsti- eller et stiftsudvalg, og som med NemID/MitID skal tilgå Kirkenettets systemer og services fra en privat pc eller mobil enhed.

*Stk. 2.* Udvalgsbrugere kan have adgang til en udvalgspostkasse og -kalender, dokumentarkiver samt andre relevante systemer, der er knyttet til den eller de roller som udvalgsbrugeren varetager.

Kapitel 4

*Brugeres autorisering*

**§ 10.** Kirkenetbrugere tildeles af den sikkerhedsansvarlige adgang til systemer og informationer via Kirkenettets elektroniske brugeradministration ud fra brugerens specifikke arbejdsbetingede behov.

*Stk. 2.* Den sikkerhedsansvarlige må kun tildele en bruger adgang til systemer og informationer, som er en del af den sikkerhedsansvarliges ansvarsområde.

*Stk. 3.* Ved oprettelse modtager Kirkenetbrugeren et stamkort i sin postkasse samt links til den gældende informationssikkerhedspolitik samt –cirkulære.

*Stk. 4.* Inden 72 timer efter at brugeren logger på første gang, skal brugeren læse de modtagne dokumenter samt erklære sig indforstået med, at anvendelsen af Kirkenettet skal ske i henhold til reglerne.

*Stk. 5.* Hvis brugeren ikke inden 72 timer erklærer sig indforstået, jf. stk. 4, spærres brugerens adgang. Adgangen kan genåbnes ved at rette henvendelse til Folkekirkens It. Ved genåbning påbegyndes en fornyet frist på 72 timer.

*Stk. 6.* Hvis en bruger bliver opmærksom på, at vedkommende selv eller andre har adgang til systemer eller informationer, som er mere vidtgående, end brugerens arbejdsbetingede behov begrunder, skal brugeren straks underrette sin sikkerhedsansvarlige eller Folkekirkens It.

*Stk. 7.* Den sikkerhedsansvarlige skal snarest og i fornødent omfang inddrage brugerens adgang til ét eller flere systemer, hvis brugeren ikke længere har et arbejdsbetinget behov for adgangen.

**§ 11.** Udvalgsbrugere tildeles automatisk adgang til systemer og informationer i kraft af deres konstitution i udvalget eller af udvalgets sikkerhedsansvarlige via brugeradministrationen på den Digitale Arbejdsplads.

*Stk. 2.* Ved oprettelse af nye udvalgsbrugere sendes til menighedsrådets fortrolig-postkasse en e-mail om, at menighedsrådets sikkerhedsansvarlige skal udlevere den gældende informationssikkerheds-politik samt -cirkulære til den eller de nye brugere, som har pligt til at læse dokumenterne.

**§ 12.** Den sikkerhedsansvarlige skal fratage brugerens adgang omgående, når brugeren ikke længere har behov for denne, eksempelvis når brugeren fratræder.

*Stk. 2.* En Kirkenetbrugerkonto gemmes i 100 dage efter nedlæggelse af brugerens sidste rolle. I denne periode vil det være muligt at genskabe Kirkenetbrugerens postkasse og OneDrive.

*Stk. 3.* Inden nedlæggelse af brugeradgang skal den sikkerhedsansvarlige påse, at der opsættes autosvar på den tilhørende Kirkenet-postkasse, som oplyser om, at henvendelser til postkassen ikke besvares.

*Stk. 4.* Udvalgsbrugeres adgang og rettigheder ændres eller nedlægges øjeblikkeligt som følge af de valgte udvalgsbrugeres konstitution eller udtræden af udvalget.

**§ 13.** Den sikkerhedsansvarlige skal hvert halve år kontrollere, at hver af de brugere, som vedkommende har autoriseret, kun er tildelt de rettigheder, som brugeren har et arbejdsmæssigt behov for.

*Stk. 2.* Forud for genautoriseringen modtager den sikkerhedsansvarlige en mail med anvisning af fremgangsmåde og frist for genautorisering.

*Stk. 3.* Den sikkerhedsansvarlige modtager påmindelser om genautoriseringen inden fristens udløb. Hvis den sikkerhedsansvarlige ikke foretager genautoriseringen inden fristens udløb, lukkes den brugerrolle, som den sikkerhedsansvarlige har tildelt brugeren.

**§ 14.** En Kirkenetbruger på orlov kan beholde adgang til sin postkasse og OneDrive, hvis den sikkerhedsansvarlige tildeler brugeren en orlovsrolle.

**§ 15.** Den sikkerhedsansvarlige kan i særlige tilfælde, hvor tjenstlige behov tilsiger det, inden for sit sikkerhedsområde få adgang til en anden brugers konto, hvis brugeren er fraværende eller ophørt. I så fald skal den sikkerhedsansvarlige anmode Folkekirkens It om denne adgang. Adgangen vedrører alene tjenstlige informationer og skal ske under overværelse af en bisidder for brugeren i et på forhånd fastlagt og afgrænset tidsrum.

**§ 16.** Når en bruger åbner sin postkasse via webmail fra en ikke-Kirkenet-pc, skal brugeren logge ind med både brugernavn og adgangskode samt en anden faktor, f.eks. en SMS eller brug af en app.

## Kapitel 5

*Adgang til og adgangskontrol i Kirkenettet*

**§ 17.** Kirkenetbrugere tildeles brugernavn og et midlertidigt kodeord. Ved første indlogning på Kirkenettet skal brugeren ændre sit midlertidige kodeord til et personligt kodeord, jf. § 19, stk. 1.

**§ 18.** Brugernavnet for en Kirkenetbruger er personligt, og adgangskoden er fortrolig. Det er ikke tilladt at dele sit brugernavn eller sin adgangskode med andre, herunder kolleger eller familiemedlemmer.

*Stk. 2.* Flere personer kan benytte samme Kirkenet-pc, men altid ved at anvende hvert sit personlige brugernavn og kodeord.

**§ 19.** Kirkenetbrugere skal overholde følgende krav til adgangskoden:
– Adgangskoden skal udskiftes efter højst 90 dages brug.
– Længden af adgangskoden skal være mindst 12 tegn, heraf mindst 1 stort bogstav, mindst 1 lille bogstav og mindst 1 ciffer (tal).
– Brugerens egne navne og brugernavn må ikke indgå i adgangskoden.
– Æ, ø og å må ikke indgå i adgangskoden.
– Adgangskoden må ikke genbruges ved de næste 10 skift.
– Adgangskoden skal straks ændres, hvis den kan være blevet kendt af andre.

*Stk. 2.* Autorisationen vil automatisk blive spærret, hvis indtastningen af den tilhørende adgangskode er mislykkedes for mange gange. En Kirkenetbruger kan selv genåbne en spærret adgang med sit NemID/MitID.

**§ 20.** Når NemID/MitID anvendes til indlogning, gælder NemID/MitID's regler for krav til adgangskoder.

**§ 21.** Adgang til visse programmer opnås ikke alene gennem indlogningen til Kirkenettet (ved SSO – SingleSignOn), men kræver yderligere selvstændig indlogning. Brugernavn og adgangskode til sådanne programmer kan afvige fra brugerens autorisation til Kirkenettet og skal følge reglerne for det pågældende program.

## Kapitel 6

*Beskyttelse af informationer og data*

**§ 22.** Når brugeren arbejder på Kirkenettet, herunder på den Digitale Arbejdsplads, må brugeren udelukkende fremsøge oplysninger, som er nødvendige for at kunne udføre sine funktioner og opgaver.

*Stk. 2.* Enhver privat anvendelse af informationer og data i Kirkenettets tjenstlige systemer er forbudt.

**§ 23.** Adgang til alle fysiske lokaliteter skal sikres med den fornødne adgangskontrol mod uvedkommendes adgang.

*Stk. 2.* Lokaler, hvor der opbevares personoplysninger, skal være aflåst, når ingen medarbejdere er til stede.

**§ 24.** Fysiske dokumenter, der indeholder personoplysninger eller fortrolige oplysninger, skal opbevares på en måde, så de ikke er tilgængelige for uvedkommende, men kun er tilgængelige for personer med et arbejdsbetinget behov for at anvende dem.

*Stk. 2.* Efter endt anvendelse skal dokumenter, som indeholder personoplysninger eller fortrolige oplysninger, journaliseres i overensstemmelse med offentlighedslovens § 15. Hvis journalisering ikke er nødvendig, skal dokumenterne makuleres.

*Stk. 3.* Ved arbejdsdagens ophør må dokumenter med personoplysninger eller fortrolige oplysninger ikke ligge frit fremme på brugerens arbejdsplads, herunder en eventuel hjemmearbejdsplads.

**§ 25.** Arbejdsrelaterede digitale dokumenter skal som udgangspunkt journaliseres i myndighedens arkiv, eksempelvis ESDH-system, Menighedsrådsarkivet eller Den Digitale Kirkebog.

*Stk. 2.* Arbejdsrelaterede digitale dokumenter, som skal deles med andre brugere i enheden, og som ikke skal journaliseres, gemmes på myndighedens fælles drev eller i menighedsrådsarkivet.

*Stk. 3.* Bærbare medier, som anvendes til at gemme dokumenter med personoplysninger eller fortrolige oplysninger, skal være krypterede.

*Stk. 4.* En Kirkenet-pc og evt. tilhørende skærm skal placeres således, at skærmen ikke umiddelbart kan aflæses af uvedkommende. Hvis skærmen er synlig for andre, skal skærmen dækkes med et filter, som

forhindrer, at uvedkommende kan se dens indhold. Kirkenet-pc'en skal desuden så vidt muligt opbevares uden for fysisk rækkevidde for uvedkommende.

*Stk. 5.* Mobilt udstyr skal være sikret med en PIN- eller adgangskode, der sikrer en tilfredsstillende sikkerhed mod adgang fra uautoriserede personer.

*Stk. 6.* Mobilt udstyr og dokumenter med personoplysninger eller fortrolige oplysninger m.v. skal altid medbringes som håndbagage ved rejser.

*Stk. 7.* Brugeren skal logge af eller låse sin it-arbejdsstation (fx bærbar, PC, tablet, mobiltelefon), hver gang den forlades.

**§ 26.** Kirkenettets mailsystemer sender som standard med kryptering.

*Stk. 2.* Når en bruger sender personoplysninger fra en postkasse på Kirkenettet, der er fortrolige eller følsomme, kan disse sendes til modtagerens almindelige mailadresse i de tilfælde, hvor Kirkenet- eller udvalgsbrugeren er helt sikker på modtagerens identitet.

*Stk. 3.* Såfremt brugeren ikke med sikkerhed kan afgøre, om en mailadresse tilhører den person, der skal sendes fortrolige eller følsomme personoplysninger til, skal oplysningerne sendes med Digital Post til vedkommendes CPR- eller CVR-nummer.

**§ 27.** Kirkenettets SMS-service og SMS generelt må ikke anvendes til forsendelse af personoplysninger, der er fortrolige eller følsomme.

*Stk. 2.* App'en "Signal", som er installeret på Kirkenet-pc'er og anvender kryptering, må anvendes til forsendelse af personoplysninger, der er fortrolige eller følsomme.

**§ 28.** Det er ikke tilladt at anvende Kirkenettets systemer og programmer til kommerciel privat virksomhed.

*Stk. 2.* Det er ikke tilladt at opsætte en generel regel om videresendelse af mails til en postkasse uden for Kirkenettet.

*Stk. 3.* Det er dog tilladt for brugere at anvende deres personlige postkasse samt adgangen til internettet til private formål, når anvendelsen sker på forsvarlig vis og ikke udsætter Kirkenettet for sikkerhedsmæssige risici.

## Kapitel 7

*Den sikkerhedsansvarliges tilsyn*

**§ 29.** Den sikkerhedsansvarlige skal – inden for sit myndighedsområde – føre tilsyn med, at brugerne udviser en sikker adfærd, jf. § 2, stk. 2.

*Stk. 2.* I forbindelse med tilsynet skal den sikkerhedsansvarlige - ved observationer og gennem samtaler - skabe sig et indtryk af, om forholdene er egnet til at understøtte en sikker adfærd. Den sikkerhedsansvarlige skal i nødvendigt omfang give råd og vejledning, samt efter omstændighederne egentlige påbud, med henblik på at understøtte sikker adfærd.

*Stk. 3.* Den sikkerhedsansvarlige skal løbende føre tilsyn med, at der:

- ikke sker uautoriserede indgreb i det installerede udstyr,
- ikke tilkobles ekstraudstyr, der kræver fysisk indgriben i installeret udstyr,
- kun tilkobles udstyr, som er godkendt til brug i Kirkenettet,
- kun installeres programmer, som er godkendt til brug i Kirkenettet, og hvortil der er erhvervet licens.

**§ 30.** Den sikkerhedsansvarlige skal påse, at de brugere, som vedkommende har autoriseret, varetager det ansvar, som de har for at beskytte it-udstyret. De nærmere retningslinjer for brugen af it-udstyr på Kirkenettet fremgår af Pc-Supportforum under afsnittet Kirkenet-pc.

**§ 31.** Den lokale sikkerhedsansvarlige skal påtale, hvis der er brugere, der ikke overholder reglerne, herunder, hvis der udvises en adfærd, der ikke er sikker.

*Stk. 2.* Hvis den sikkerhedsansvarlige konstaterer brud på sikker adfærd, skal vedkommende sørge for, at der straks tages de nødvendige skridt til at sikre informationssikkerhed og databeskyttelse, herunder om fornødent at Folkekirkens It eventuelt spærrer den pågældende brugers adgang.

*Stk. 3.* Overtrædelser af dette cirkulære kan efter omstændighederne medføre personaleretlige sanktioner efter de almindelige ansættelsesretlige regler.

## Kapitel 8

*Brud på informationssikkerheden*

**§ 32.** Brugere skal med det samme give besked til deres sikkerhedsansvarlige, hvis de bliver bekendt med en sikkerhedshændelse. Dette gælder også, hvis der samtidigt er tale om et brud på persondatasikkerheden.

*Stk. 2.* Folkekirkens It skal omgående informeres, hvis hændelsen vedrører systemer på Kirkenettet.

## Kapitel 9

*Opgaver og regler for Folkekirkens It*

**§ 33.** Folkekirkens It varetager den daglige drift af Kirkenettet, herunder sikring af, at der er indført de nødvendige sikkerhedsforanstaltninger, som opretholder og kontrollerer informationssikkerheden på Kirkenettet.

*Stk. 2.* Folkekirkens It skal sikre, at ingen pc kan tilkobles Kirkenettet uden aktivering af programmer, som overvåger og eventuelt installerer nødvendige opdateringer til programmer, virusbeskyttelse m.m.

*Stk. 3.* Folkekirkens It sikrer, at anvendelsen af internet og mail m.m. kan ske sikkert. Såfremt kommunikation fra Kirkenettet med specifikke websteder udgør en sikkerhedsmæssig risiko, skal adgangen dertil spærres.

*Stk. 4.* Folkekirkens It sikrer, at der foretages den fornødne logning til sikring af Kirkenettets drift samt opfølgning på sikkerhedshændelser.

**§ 34.** Medarbejderne i Folkekirkens It og hos leverandørerne til Kirkenettet har tavshedspligt med hensyn til oplysninger, som de måtte komme i besiddelse af. Det gælder både i opfyldelse af kontrol- og sikkerhedsforanstaltninger og ved hjælp til brugerne i supportsituationer.

*Stk. 2.* Det er forbudt at skaffe sig adgang til brugernes arkivområder, dokumenter, postkasser og lignende. Undtaget er dog de tilfælde, hvor dette sker efter udtrykkelig aftale med den pågældende bruger, og da alene med det formål at bistå brugeren i tekniske spørgsmål, eller hvor sådan adgang i øvrigt sker i henhold til dette cirkulære.

*Stk. 3.* Uanset tavshedspligten skal Folkekirkens It's medarbejder, såfremt denne under support bliver opmærksom på, at en bruger begår alvorlige forseelser i forhold til dette cirkulæres bestemmelser, inddrage brugerens sikkerhedsansvarlige eller andre instanser, såfremt medarbejderen vurderer, at der er behov herfor.

**§ 35.** Folkekirkens It sikrer, at der dagligt tages sikkerhedskopi af alle data gemt i de systemer, der er tilgængelige på Kirkenettet, herunder post- og kalenderoplysninger, fælles og personlige drev m.m.

*Stk. 2.* Det kontrolleres, at den daglige sikkerhedskopiering er gennemført, og at data kan genskabes på baggrund heraf.

**§ 36.** Folkekirkens It gennemfører kontroller for specifikke områder af it-driften. Kontrollerne udføres i henhold til ISO 27001 og databeskyttelseslovgivningen, og disse består bl.a. i at:

- risikovurdere forretningsprocesserne for Kirkeministeriet og folkekirken
- føre tilsyn med it-leverandører til Kirkenettet
- foretage og kontrollere logninger med henblik på at opdage og spore uautoriserede handlinger
- teste, at sikkerhedskopier kan genindlæses

- overvåge serverkapaciteten
holde data adskilt mellem test og produktion
- foretage tilbagevendende scanning for sårbarheder.

*Stk. 2.* Herudover gennemføres et antal besøg/stikprøver i folkekirkens institutioner for at sikre overholdelse af gældende regler og give sparring om informationssikkerhed, hvorved en sikker adfærd understøttes.

Kapitel 10

*Ikrafttræden*

**§ 37.** Cirkulæret træder i kraft den 10. december 2021.

*Kirkeministeriet, den 8. december 2021*

Torben Stærgaard
Kontorchef

**Bilag 1.**

**Kirkenettets sikkerhedsansvarlige**

| **Myndighed** | **Arbejdssted** | **Bruger** | **Sikkerhedsansvarlig**[1)] |
|---|---|---|---|
| Sogne | Pastorat | Sognepræst, kbf | Provst |
| | Pastorat | Sognepræst(er) | Provst |
| | Sogn, kordegn | Kordegn (i forbindelse med udførelse af personregistrering) | Sognepræst, kbf |
| | Sogn (kirke og kirkegård) | Kirkefunktionærer m.fl. | Menighedsrådsformand[2)] |
| | Sogn | Personalekonsulenter | Provst |
| | Sogn (menighedsråd) | Menighedsrådsmedlemmer, valgte | Menighedsrådsformand[2)] |
| | | Eksterne brugere tilknyttet menighedsrådet | |
| Provstier | Provsti | Provst | Biskop |
| | Provsti | Provstisekretær | Provst |
| | Provsti (provstiudvalg) | Udvalgsmedlemmer, valgte | Provst |
| | Provsti | Konsulent | Provst |
| | Kirkegårde m/ egen bestyrelse | Kirkegårdsleder | Provst |
| Stifter | Stift | Biskop | Kontorchef for HR i Kirkeministeriet |
| | Stift | Stiftskontorchef | Kontorchef for HR i Kirkeministeriet |
| | Stift | Medarbejdere på stiftsadministrationen | Stiftskontorchef |
| | Stift (stiftsudvalg) | Udvalgsmedlemmer, valgte | Stiftskontorchef |
| Kirke-ministeriet | Kirkeministeriet | Departementschefen | Kontorchef for HR i Kirkeministeriet |
| | Kirkeministeriet | Kontorchef | Kontorchef for HR i Kirkeministeriet |
| | Kirkeministeriet | Medarbejdere | Nærmeste kontorchef |
| Uddannelses-institutioner | Uddannelsesinstitution | Rektor | Kontorchef for HR i Kirkeministeriet |
| | Uddannelsesinstitution | Medarbejdere | Rektor |
| Andre | Skiftende | DSUK-præster | DSUK provst |

| | | | |
|---|---|---|---|
| | Sønderjyske kommuner | Personregisterførere | It- og digitaliseringschefen |
| | It-leverandører | It-konsulent | It- og digitaliseringschefen |
| | Kirkeministeriet, stift eller uddannelsesinstitution | Konsulent, emeritus eller anden tilknyttet, men ikke ansat | Kontorchef/rektor |

1) Provster, biskopper, rektorer og kontorchefer kan iht. § 3 udpege en stedfortræder.

2) Menighedsråd kan beslutte, at rollen som sikkerhedsansvarlig tillægges et andet valgt medlem eller en sognepræst.