CIR1H nr 9479 af 28/06/2024 (Gældende)

Cirkulære om informationssikkerhed og persondatabeskyttelse for By-, Land- og Kirkeministeriet og den danske folkekirke

Ministerium: By-, Land- og Kirkeministeriet

Journalnummer: By-, Land- og Kirkemin., 2023-10015

Cirkulære om informationssikkerhed og persondatabeskyttelse for By-, Land- og Kirkeministeriet og den danske folkekirke

By-, Land- og Kirkeministeriet understøtter folkekirken ved at sikre tidssvarende administrative rammer for folkekirkens virke. Det sker bl.a. 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. By-, Land- og Kirkeministeriet bistår med at sikre, at fælles it-systemer og procedurer lever op til krav om informationssikkerhed og persondatabeskyttelse.

Cirkulærets bestemmelser fastsætter således en række organisatoriske foranstaltninger og procedurer vedr. bl.a. sikkerhedsorganisation, autorisering af brugere samt om de lokale sikkerhedsansvarliges tilsyn m.v., der skal understøtte en adfærd, som medvirker til sikring af både informationssikkerhed og persondatabeskyttelse i By-, Land- og Kirkeministeriet og i folkekirken (sikker adfærd).

Cirkulærets bestemmelser fastlægger desuden de konkrete retningslinjer for informationssikkerhed og persondatabeskyttelse, som informationssikkerhedspolitikken for By-, Land- og Kirkeministeriet og folkekirken fastlægger.

I medfør af § 25 i lov om folkekirkens økonomi, jf. lovbekendtgørelse nr. 424 af 19. april 2023, fastsættes følgende**:**

Kapitel 1

Anvendelsesområde

§ 1. Dette cirkulære gælder for By-, Land- og 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 cirkulære om fælles dataansvar i forbindelse med Kirkeministeriets fælles systemer vedrørende økonomi-, betalings-, administrations-, HR- og lønområdet.

Stk. 2. Myndigheder og institutioner, som ikke er forpligtet til at benytte de af By-, Land- og Kirkeministeriet leverede systemer, jf. stk. 1, 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. Cirkulæret gælder for alle brugere med adgang til Kirkenettet og for al brug af Kirkenettet.

Kapitel 2

Sikkerhedsorganisationen

§ 2. By-, Land- og Kirkeministeriet og de folkekirkelige myndigheder og institutioner er hver især ansvarlige for overholdelse af kravene til informationssikkerhed og persondatabeskyttelse (sikker adfærd). Den enkelte myndighed og institution er som udgangspunkt ansvarlig for at sikre den registreredes rettigheder i henhold til reglerne om persondatabeskyttelse.

Stk. 2. Lokale sikkerhedsansvarlige, jf. cirkulærets bilag om Kirkenettets sikkerhedsansvarlige, fører tilsyn med persondata- og informationssikkerheden lokalt og skal sikre, at brugerne udviser en sikker adfærd.

§ 3. Provster, biskopper, rektorer og kontorchefer kan skriftligt bemyndige en anden person som deres stedfortræder i rollen som lokal sikkerhedsansvarlig. Den lokale sikkerhedsansvarlige oppebærer stadig ansvaret for varetagelsen af de opgaver som hører til rollen som sikkerhedsansvarlig og er stadig ansvarlig for dennes brugere og sin stedfortræder. Den lokale sikkerhedsansvarlige har pligt til at føre tilsyn med, at stedfortræder overholder dette cirkulære.

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

Stk. 3. I sognet er menighedsrådsformanden som udgangspunkt den lokale sikkerhedsansvarlige for menighedsrådets valgte medlemmer og kirkefunktionærer mfl. jf. cirkulærets bilag 1. Menighedsrådet kan dog beslutte at tillægge rollen til et andet af menighedsrådets medlemmer, herunder til en sognepræst.

Kapitel 3

Brugere og anvendelse af udstyr

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

Stk. 2. En bruger kan tilgå Kirkenettet fra en Kirkenet-pc. Adgang til Kirkenettet via Folkekirkens IntraNet fra en privat pc eller mobil enhed, opnås via en krypteret forbindelse.

Stk. 3. Folkekirkens It er ansvarlige for driften af systemer og services på Kirkenettet, og der gælder fælles dataansvar ved brugen af disse systemer og services, jf. Cirkulære om fælles dataansvar i forbindelse med Kirkeministeriets fælles systemer vedrørende personregistrering, sognebåndsløsning samt valg i folkekirken.

§ 5. 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, der gemmes lokalt 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.

§ 6. Adgang til Kirkenettet via Folkekirkens IntraNet fra en privat pc eller mobil enhed, opnås via en krypteret forbindelse. Hvis adgangen til Kirkenettet via Folkekirkens IntraNet opnås fra en privat pc eller mobil enhed, gælder dette cirkulære for den behandling af informationer, som finder sted i den forbindelse.

Stk. 2. 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.

§ 7. En Kirkenetbruger er en autoriseret 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, autoriseres til adgang til relevante systemer og services i Kirkenettet.

§ 8. En udvalgsbruger er en autoriseret bruger, som har tilknytning til enten et menighedsråd, et provsti- eller et stiftsudvalg, eller andre udvalg som kirkegårdsbestyrelser, regnskabssamarbejder m.v. og som med MitID skal tilgå Kirkenettets systemer og services via Folkekirkens IntraNet fra en privat pc eller mobil enhed.

Stk. 2. Udvalgsbrugere kan autoriseres til 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

§ 9. Den lokale sikkerhedsansvarlige autoriserer Kirkenetbrugeres adgang til systemer og informationer via Kirkenettets elektroniske brugeradministration ud fra den konkrete brugers specifikke arbejdsbetingede behov.

Stk. 2. Den lokale sikkerhedsansvarlige må kun autorisere en brugers adgang til systemer og informationer, som ligger inden for den sikkerhedsansvarliges ansvarsområde.

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

Stk. 4. Inden 24 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 24 timer erklærer sig indforstået, jf. stk. 4, spærres brugerens adgang automatisk. Adgangen kan genåbnes ved at rette henvendelse til Folkekirkens It. Ved genåbning påbegyndes en fornyet frist på 24 timer, jf. stk. 4.

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 lokale sikkerhedsansvarlige eller Folkekirkens It.

Stk. 7. Den lokale 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.

§ 10. Udvalgsbrugere tildeles adgang til systemer og informationer i kraft af deres konstitution i udvalget eller af udvalgets sikkerhedsansvarlige via brugeradministrationen på Folkekirkens IntraNet.

Stk. 2. Ved oprettelse af nye udvalgsbrugere sendes en e-mail til menighedsrådets fortrolig-postkasse om, at menighedsrådets lokale sikkerhedsansvarlige skal udlevere gældende informationssikkerhedspolitik samt gældende cirkulære om informationssikkerhed og persondatabeskyttelse til den eller de nye brugere, og at vedkommende har pligt til at læse dokumenterne.

§ 11. Den lokale sikkerhedsansvarlige skal omgående fratage brugerens adgang, 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 brugerkonto skal den lokale sikkerhedsansvarlige påse, at der opsættes autosvar på den tilhørende postkasse på Kirkenettet, som oplyser om, at henvendelser til postkassen ikke besvares.

Stk. 4. Den lokale sikkerhedsansvarlige skal sørge for, at udvalgsbrugeres adgang og rettigheder øjeblikkeligt ændres eller nedlægges som følge af ændringer i de valgte udvalgsbrugeres konstitution eller ved udtræden af udvalget.

§ 12. Den lokale 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 lokale sikkerhedsansvarlige en mail med anvisning af fremgangsmåde og frist for genautorisering.

Stk. 3. Den lokale 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.

§ 13. En Kirkenetbruger på orlov kan beholde adgang til sin postkasse og OneDrive, hvis den lokale sikkerhedsansvarlige tildeler brugeren en orlovsrolle i brugeradministrationen.

§ 14. Den lokale 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 lokale sikkerhedsansvarlige anmode Folkekirkens It om denne adgang. Adgangen vedrører alene tjenstlige informationer og skal ske under overværelse af en bisidder i et på forhånd fastlagt og afgrænset tidsrum.

§ 15. 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 (to-faktor-godkendelse), f.eks. en SMS eller brug af en app. De tilgængelige muligheder for to-faktor-godkendelse fastsættes af Folkekirkens It.

Kapitel 5

Adgang til og adgangskontrol i Kirkenettet

§ 16. Kirkenetbrugere tildeles ved oprettelse et brugernavn og en midlertidig adgangskode. Ved første indlogning på Kirkenettet, jf. § 9, stk. 4, skal brugeren ændre sin midlertidige adgangskode til en personlig adgangskode, jf. § 18, stk. 1.

§ 17. Brugernavnet for en Kirkenetbruger er personligt, og adgangskoden er fortrolig. Det er ikke tilladt at dele 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 hvert sin fortrolige adgangskode.

§ 18. Kirkenetbrugere skal overholde følgende krav til adgangskoden:

– Adgangskoden skal udskiftes efter højst ét års brug.
– Længden af adgangskoden skal være mindst 15 tegn, heraf mindst ét stort bogstav, mindst ét lille bogstav og mindst ét 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 24 skift.
– Adgangskoden skal straks ændres, hvis den kan være blevet kendt af andre.
– Adgangskoder skal være unikke og må ikke genbruges i andre systemer.

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 MitID.

§ 19. Når MitID anvendes til indlogning, gælder MitID's regler for krav til adgangskoder.

§ 20. Adgang til visse programmer opnås ikke alene gennem indlogningen til Kirkenettet, men kræver yderligere selvstændig indlogning. Personligt brugernavn og fortrolig 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 persondata

§ 21. Når brugeren arbejder på Kirkenettet, herunder på Folkekirkens IntraNet, må brugeren udelukkende fremsøge de 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.

Stk. 3. Arbejdsrelaterede data må ikke gemmes på privat udstyr, og heller ikke på sociale medier (f.eks. Facebook), uden særskilt hjemmel.

Stk. 4. Arbejdsrelaterede data i fysisk form må kun indscannes, hvis det sker til et krypteret, tjenstligt drev eller til en krypteret, tjenstlig USB-nøgle.

§ 22. Adgang til alle fysiske lokaliteter skal sikres med den fornødne adgangskontrol for at beskytte mod uvedkommendes adgang.

§ 23. Fysiske dokumenter, der indeholder personoplysninger eller fortrolige oplysninger, skal opbevares forsvarligt i forhold til disses karakter og 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.

§ 24. Arbejdsrelaterede digitale dokumenter og filer m.v. skal som udgangspunkt journaliseres i myndighedens arkiv, eksempelvis ESDH-system, Kirkeportalen eller Den Digitale Kirkebog.

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

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, hvis det medtages ved rejser.

Stk. 7. Brugeren skal logge af eller låse sin it-arbejdsstation (f.eks. bærbar, pc, tablet, mobiltelefon), hver gang den forlades.

§ 25. Alle mails sendt fra og til Kirkenettets mailsystem sendes som standard med kryptering.

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

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

§ 26. Kirkenettets SMS-service, og SMS generelt, må ikke anvendes til forsendelse af fortrolige eller følsomme personoplysninger.

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.

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

Stk. 2. Det er dog tilladt for brugere at anvende deres personlige postkasse på Kirkenettet samt adgangen til internettet til private, ikke-kommercielle formål, når anvendelsen sker på forsvarlig vis og ikke udsætter Kirkenettet for sikkerhedsmæssige risici. De nærmere retningslinjer for brugen af internettet fremgår af Pc-Supportforum.

§ 28. Brugere med autoriseret adgang til en sognepostkasse, menighedsrådspostkasse eller en personlig postkasse på Kirkenettet har pligt til at anvende denne ved afsendelse og modtagelse af tjenstlig kommu-

nikation eller i forbindelse med hvervet som menighedsrådsmedlem. Kommunikation rettet til eller fra en kirkelig myndighed skal altid foregå via myndighedens postkasse på Kirkenettet.

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

Kapitel 7

Den lokale sikkerhedsansvarliges tilsyn

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

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

Stk. 3. Den lokale sikkerhedsansvarliges tilsyn, jf. stk. 1, skal bl.a. omfatte, at:

- Der kun anvendes systemer og services på Kirkenettet bag login, hvortil der er erhvervet licens,
- Der ikke sker uautoriserede indgreb i det installerede udstyr,
- Der ikke tilkobles ekstraudstyr, der kræver fysisk indgriben i installeret udstyr,
- Der kun tilkobles udstyr, som er godkendt til brug i Kirkenettet,
- Der kun installeres programmer, som er godkendt til brug i Kirkenettet, og hvortil der er erhvervet licens,
- Der behandles personoplysninger i overensstemmelse med reglerne om persondatabeskyttelse.

§ 30. Den lokale 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.

§ 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 lokale sikkerhedsansvarlige konstaterer brud på sikker adfærd, skal vedkommende sørge for, at der straks tages de nødvendige skridt til at sikre informationssikkerhed og persondatabeskyttelse, 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 informations- og/eller persondatasikkerheden

§ 32. Brugere skal med det samme give besked til deres lokale sikkerhedsansvarlige, hvis de bliver bekendt med en sikkerhedshændelse., der indebærer mulighed for en kompromittering af informationssikkerheden. Dette gælder også, hvis der er tale om et muligt brud på persondatasikkerheden. På Folkekirkens IntraNet findes en procedure for håndtering af brud på persondatasikkerheden.

Stk. 2. Brugere skal omgående informere Folkekirkens It, hvis en sikkerhedshændelse, jf. stk. 1, vedrører systemer på Kirkenettet.

Stk. 3. Brugere og disses lokale sikkerhedsansvarlige skal uden ugrundet ophold medvirke til at afhjælpe eller modvirke negative konsekvenser af sikkerhedshændelser, jf. stk. 1, inden for deres respektive arbejds- og ansvarsområder.

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 informations- og persondatasikkerheden 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. Ansatte 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 ansatte, såfremt den ansatte under support bliver opmærksom på, at en bruger begår alvorlige forseelser i forhold til dette cirkulæres bestemmelser, inddrage brugerens lokale sikkerhedsansvarlige eller andre relevante instanser, såfremt den ansatte vurderer, at der er behov herfor.

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

Stk. 2. Folkekirkens It skal kontrollere, at den daglige backup er gennemført, og at data kan genskabes på baggrund heraf.

§ 36. Folkekirkens It gennemfører tilbagevendende kontroller af Kirkenettet. Kontrollerne udføres i henhold til ISO 27001 og databeskyttelseslovgivningen, og disse består bl.a. i at:

- risikovurdere forretningsprocesserne for By-, Land- og 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 backup er korrekte, og at data kan genskabes
- overvåge serverkapaciteten og om fornødent tilføre ekstra kapacitet
- 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 1. juli 2024.

Stk. 2. Cirkulæreskrivelse af 1. oktober 2007 om tjenstlig post til folkekirkens præster og cirkulære nr. 10009 af 8. december 2021 om informationssikkerhed for Kirkeministeriet og Den danske folkekirke ophæves.

By-, Land- og Kirkeministeriet, den 28. juni 2024

Ulla Brynning Kristiansen

/ Tobias Kunø Knudsen

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 By-, Land- og Kirkeministeriet
	Stift	Stiftskontorchef	Kontorchef for HR i By-, Land- og Kirkeministeriet
	Stift	Medarbejdere på stiftsadministrationen	Stiftskontorchef
	Stift (stiftsudvalg)	Udvalgsmedlemmer, valgte	Stiftskontorchef
By-, Land og Kirke-ministeriet	By-, Land- og Kirkeministeriet	Departementschefen	Kontorchef for HR i By-, Land- og Kirkeministeriet
	By-, Land- og Kirkeministeriet	Afdelingschef	Kontorchef for HR i By-, Land- og Kirkeministeriet
	By-, Land- og Kirkeministeriet	Kontorchef	Afdelingschef
	By-, Land- og Kirkeministeriet	Medarbejdere	Nærmeste kontorchef eller chefkonsulent med personaleansvar
Uddannelses-institutioner	Uddannelsesinstitution	Rektor	Kontorchef for HR i By-, Land- og Kirkeministeriet
	Uddannelsesinstitution	Medarbejdere	Rektor
Andre	Skiftende	DSUK-provst	Biskop over Fyens Stift
	Skiftende	DSUK-præster	DSUK provst
	Sønderjyske kommuner	Personregisterførere	Enhedschef, Personregistrering
	It-leverandører	It-konsulent	Souschef It-governance

	By-, Land- og 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. Beslutningen skal dokumenteres skriftligt.