Cirkulære om informationssikkerhed, herunder sikkerhedsforanstaltninger i Kirkenettet

Cirkulæret omhandler informationssikkerhed inden for Kirkeministeriets ressort, herunder sikkerhedsforanstaltninger i Kirkenettet.

Desuden omhandler cirkulæret Kirkeministeriets godkendelse af øvrige it-systemer.

Cirkulærets anvendelsesområde
§ 1. Cirkulæret omfatter alle institutioner, ansatte, folkevalgte og frivillige inden for Kirkeministeriets ressort i forbindelse med handlinger og adfærd, der ligger inden for cirkulærets anvendelsesområde.

Stk. 2. Cirkulæret omfatter endvidere alle brugere med adgang til Kirkenettet og al brug af Kirkenettet. Det gælder for alle Kirkenet-pc'er, uanset om de er placeret i administrationskontorer, embedsboliger eller private hjem m.v.

Stk. 3. Samtlige personer, jf. stk. 1 og stk. 2, skal udvise en adfærd, der er egnet til at understøtte informationssikkerheden inden for Kirkeministeriets ressort.

Stk. 4. I cirkulærets Bilag 5 er der fastsat bestemmelser vedrørende de it-systemer, som Kirkeministeriet godkender.

Definitioner
§ 2. Kirkenettet er et lukket netværk med tilhørende programmer og it-udstyr, som er etableret i og mellem hovedsageligt folkekirkelige myndigheder, institutioner og ansatte. Ved Kirkenettet forstås desuden løsninger og services, der kan anvendes via internettet eller øvrige medier, og som udbydes af Folkekirkens It. For menighedsråds- og andre udvalgsmedlemmer, som har adgang til services via Kirkenettet, gælder *Cirkulære om Menighedsråds- og andre udvalgsmedlemmers brug af Kirkenettet.*

Stk. 2. En Kirkenet-pc er en pc med en række præinstallerede programmer leveret af Folkekirkens It.

Stk. 3. En bruger er en person, som er tildelt et brugernavn og en adgangskode til Kirkenettet. Brugernavnet og adgangskoden er strengt personlige og må ikke benyttes af andre end brugeren selv. Hver bruger er tildelt en personlig postadresse og tilhørende postkasse på Kirkenettet.

Stk. 4. Autorisation er kombinationen af et brugernavn og en adgangskode, som tilsammen giver adgang til Kirkenettet eller et program tilknyttet Kirkenettet.

Stk. 5. Et installationssted er en fysisk adresse, som har adgang til Kirkenettet.

Stk. 6. En sikkerhedsansvarlig er en person, som har et sikkerhedsmæssigt ansvar for en eller flere brugere og for et eller flere installationssteder med adgang til Kirkenettet. Den sikkerhedsansvarlige har ansvaret for at føre tilsyn med, at der inden for vedkommendes tilsynsområde udvises en adfærd, der er egnet til at understøtte informationssikkerheden inden for Kirkeministeriets ressort.

Stk. 7. Informationssikkerhed er en betegnelse for, at informationers fortrolighed, integritet og tilgængelighed til hver en tid er sikret i overensstemmelse med det regelgrundlag som den enkelte information og den enkelte institution og person, jf. § 1, stk. 1-2, er underlagt.

Organisatoriske forhold
§ 3. Afdelingschefen for Personale- og It-afdelingen i Kirkeministeriet er den øverste

sikkerhedsansvarlige for Kirkenettet og de tilhørende systemer. Afdelingschefen er dermed ansvarlig for, at de fastsatte retningslinjer for informationssikkerheden overholdes.

§ 4. Folkekirkens It står for den daglige drift af Kirkenettet og træffer herunder de fornødne foranstaltninger, som skal opretholde og kontrollere informationssikkerheden på Kirkenettet.

§ 5. Lokale sikkerhedsansvarlige tildeler, ændrer og fratager brugerne autorisation. De skal desuden føre løbende tilsyn med, at oplysninger ikke misbruges eller kommer til uvedkommendes kendskab, og at der inden for deres tilsynsområde udvises en adfærd, der er egnet til at understøtte informationssikkerheden inden for Kirkeministeriets ressort.

Stk. 2. Det er de sikkerhedsansvarliges ansvar, at it-udstyr i de lokaler, hvor fortrolige eller personhenførbare informationer behandles, er opstillet således, at uvedkommende forhindres i at se disse data, og herunder tilse, at udskrifter opbevares sikkert og/eller makuleres.

Stk. 3. De sikkerhedsansvarlige skal desuden føre tilsyn med, at der inden for deres tilsynsområde udvises en adfærd, der er egnet til at understøtte informationssikkerheden inden for Kirkeministeriets ressort.

Stk. 4. Ved tildeling af rettigheder til Kirkenettet skal de sikkerhedsansvarlige sikre, at de pågældende brugere får udleveret det gældende sikkerhedscirkulære, og at brugerne overholder cirkulærets regler og sikkerhedsforskrifter. De sikkerhedsansvarlige skal påtale, hvis regler og forskrifter ikke overholdes, herunder hvis der udvises en adfærd, der er egnet til at kompromittere informationssikkerheden inden for Kirkeministeriets ressort.

Stk. 5. Hvis en bruger efter en påtale fortsat tilsidesætter sikkerhedsforskrifterne, eller i øvrigt udviser en adfærd, der er egnet til at kompromittere informationssikkerheden inden for Kirkeministeriets ressort, skal den sikkerhedsansvarlige sørge for, at der straks træffes de fornødne skridt til at sikre informationssikkerheden, herunder om fornødent at Folkekirkens It straks spærrer den pågældende brugers autorisation.

Stk. 6. En fortegnelse over de sikkerhedsansvarlige fremgår af cirkulærets Bilag 1.

Autorisation af brugere

§ 6. Autorisation af nye brugere, ændring af og fratagelse af autorisation for eksisterende brugere foretages af de sikkerhedsansvarlige. Dette sker via Kirkenettets elektroniske brugeradministration.

Stk. 2. Når en autorisation er ekspederet, jf. stk. 1, fremsendes stamkortet, som findes i Bilag 2, samt brugerens adgangskode til Kirkenettet, til den sikkerhedsansvarliges e-mail. Desuden sendes sikkerhedscirkulæret til brugerens e-mail.

Stk. 3. Den sikkerhedsansvarlige skal sørge for, at brugerens adgangskode snarest udleveres til brugeren.

Ved første log-in på Kirkenettet skal brugeren læse e-mailen med sikkerhedscirkulæret og inden for 24 timer erklære sig indforstået med, at anvendelsen af Kirkenettet skal ske i henhold til sikkerhedscirkulæret. I modsat fald spærres brugerens autorisation efter 24 timer.

Endvidere skal brugeren ved første log-in ændre adgangskoden, jf. de i § 8 anførte bestemmelser.

Stk. 4. Retningslinjer for autorisation af brugere i uddannelsesinstitutioner og hos leverandører, frivillige samt sønderjyske personregisterførere fremgår af Bilag 3.

§ 7. Ved tildeling af autorisation er det den sikkerhedsansvarliges ansvar, at brugeren kun autoriseres til programmer eller tildeles rettigheder, som denne har brug for.

Stk. 2. For personregisterførere skal den sikkerhedsansvarlige tillige afgrænse de myndigheder, som brugeren må registrere på vegne af.

Stk. 3. Den lokale sikkerhedsansvarlige skal, som angivet i § 6, fratage en autorisation ved ændret arbejdsfordeling, fravær længere end 6 måneder og ved fratræden.

Adgang til og adgangskontrol i Kirkenettet

§ 8. De fastsatte regler om adgangskoder skal forhindre, at uautoriserede brugere får adgang til Kirkenettet. Den enkelte bruger skal derfor overholde følgende om adgangskoden:

- Adgangskoden skal udskiftes efter højst 90 dages brug.
- Længden af adgangskoden skal være mindst 8 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 tre skift.
- Adgangskoden skal straks ændres, hvis den kan være blevet kendt af andre.

Stk. 2. Når NemID anvendes til indlogning, gælder NemID's regler for krav til adgangskoder.

Stk. 3. Når adgang til programmer ikke opnås gennem indlogningen til Kirkenettet, afkræves brugeren fornyet indlogning. Brugernavn og adgangskode kan afvige fra brugerens autorisation til Kirkenettet og skal følge reglerne for det pågældende program.

Stk. 4. Autorisationen vil automatisk blive spærret, hvis indtastningen af den tilhørende adgangskode er mislykkedes for mange gange. Autorisationer, som er blevet spærret, vil først kunne benyttes efter henvendelse til Folkekirkens It.

§ 9. Fra en bærbar Kirkenet-pc kan der via en åben internetforbindelse og et særligt program etableres en sikker adgang til Kirkenettet. En tilsvarende adgang kan også opnås med et mobilt modem, som er anskaffet gennem Folkekirkens It. Regler for anvendelse af mobil adgang fremgår af cirkulærets Bilag 4. Manglende overholdelse af reglerne vil medføre lukning af mobil adgang.

§ 10. Ved arbejdet med Kirkenettets systemer må brugeren ved søgninger og opslag udelukkende skaffe sig adgang til oplysninger, som er nødvendige for at kunne udføre pålagte funktioner og opgaver. Adgang til og anvendelse af det åbne internet er dog ikke underlagt denne begrænsning.

Stk. 2. Det er tilladt at anvende mail og internet til private formål. Det er derimod ikke tilladt at anvende mail og internet til at drive privat virksomhed.

Stk. 3. Hvis en bruger bliver opmærksom på, at brugeren selv eller andre brugere har adgang til systemer og/eller oplysninger, som er mere vidtgående, end vedkommende er autoriseret til eller har tjenstligt behov for, skal brugeren straks underrette den lokale sikkerhedsansvarlige eller Folkekirkens It.

§ 11. Enhver privat anvendelse af CPR/Den Elektroniske Kirkebog er strengt forbudt.

Stk. 2. Alle forespørgsler og databehandlinger i CPR/Den Elektroniske Kirkebog registreres på den enkelte brugers autorisation. Denne registrering danner grundlag for kontrol af brugen af CPR/Den Elektroniske Kirkebog.

De sikkerhedsansvarliges tilsyn med informationssikkerheden
§ 11 a. De sikkerhedsansvarlige skal løbende føre tilsyn med, at institutioner og personer, jf. § 1, stk. 1 og 2, udviser en adfærd, der er egnet til at understøtte informationssikkerheden inden for Kirkeministeriets ressort.

Stk. 2. I forbindelse med tilsynet skal den sikkerhedsansvarlige ved observationer og gennem samtaler skabe sig et indtryk af, om den stedlige adfærd og de stedlige forhold er egnet til at understøtte informationssikkerheden inden for Kirkeministeriets ressort. Den sikkerhedsansvarlige skal i den forbindelse i fornødent omfang give råd og vejledning, og efter omstændighederne egentlige påbud med henblik på at understøtte informationssikkerheden.

De sikkerhedsansvarliges kontrol af brugen af udstyr og programmer
§ 12. For den daglige brug af udstyr og programmer, herunder for, hvilket udstyr der må tilsluttes Kirkenettet, gælder Bilag 4: "Retningslinjer for brug af programmer og udstyr i Kirkenettet".

Stk. 2. De sikkerhedsansvarlige skal løbende føre tilsyn med, at der

- ikke sker uautoriseret 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.

Stk. 3. Der foretages automatisk logning af transaktioner i økonomi- og lønsystemer samt i systemer, som behandler personhenførbare data. Ved mistanke om misbrug af et af disse systemer kan de sikkerhedsansvarlige ved Folkekirkens It rekvirere en benyttelsesstatistik.

Stk. 4. Retningslinjer for sikring af it-installationerne i ministeriet, stiftsadministrationerne og Folkekirkens It samt for sikkerhedskopiering m.m. fremgår af Bilag 4.

Stk. 5. Det udstyr, som er godkendt på Kirkenettet, må ikke samtidigt tilkobles andre netværk end Kirkenettet. Retningslinjer for tilslutning af udstyr fremgår af Bilag 4.

Opgaver og regler for Folkekirkens It og dets medarbejdere
§ 13. Folkekirkens It, som er driftsansvarlig for Kirkenettet, skal have etableret faste arbejdsrutiner, der sikrer, at de fornødne sikkerhedsforanstaltninger er implementeret og er virksomme.

Stk. 2. For Kirkenettet som helhed skal det sikres, at anvendelsen af internet og mail m.m. kan ske sikkert. Såfremt kommunikationen med specifikke netsteder og lign. udgør en sikkerhedsmæssig risiko, skal adgangen dertil spærres.

Stk. 3. Det skal sikres, at ingen pc kan tilkobles Kirkenettet uden aktivering af programmer, som overvåger og eventuelt installerer nødvendige opdateringer til virusbeskyttelse m.m.

Stk. 4. Efter nærmere fastsatte intervaller opsamles tekniske informationer, som bruges til

- kontrol af uautoriserede log-in-forsøg
- deaktivering af autorisationskoder, som ikke har været brugt i 100 dage
- overvågning af, at der kun installeres godkendt udstyr på Kirkenettet
- kontrol af, at pc'er og servere er installeret med de rigtige programversioner.

§ 14. 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 deres opfyldelse af nærværende kontrol- og sikkerhedsforanstaltninger og i deres hjælp til brugerne igennem Folkekirkens It.

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.

Stk. 3. Det er forbudt at registrere brugernes adfærd på internettet, herunder forsøge at skaffe sig oplysning om, hvilke adresser en bruger benytter. Dette gælder også for en brugers mail-trafik.

Stk. 4. Ved afhjælpning af et teknisk problem kan Folkekirkens It eller en leverandør få information om, hvilke internet- og/eller mailadresser en bruger korresponderer med. De informationer, der derved opnås adgang til, skal behandles fortroligt. Det er brugerens ansvar at lukke de systemer, som ikke er relateret til løsningen af det pågældende tekniske problem.

Stk. 5. 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.

§ 15. Folkekirkens It skal sikre, at der regelmæssigt gennemføres kontrol af, at de implementerede sikkerhedsforanstaltninger virker.

Stk. 2. Mindst én gang om året skal det uvarslet efterprøves, om Kirkenettet har den fornødne sikkerhed mod uautoriseret indtrængen, samt konstateres, om data og systemer kan genskabes på grundlag af foretagne sikkerhedskopieringer.

§ 16. Folkekirkens It skal årligt foretage en gennemgang af sikkerhedsbestemmelserne for at sikre, at de er fyldestgørende og afspejler de faktiske forhold i og omkring Kirkenettet.

§ 17. Cirkulæret træder i kraft den 30. marts 2017.

Stk. 2. Samtidig ophæves Kirkeministeriets cirkulære af 6. juni 2016 om sikkerhedsforanstaltninger i Kirkenettet.

Kirkeministeriet den 30. marts 2017

Steffen Brunés
Afdelingschef

/ Torben Stærgaard
It-chef