Kirkeministeriet

Informationssikkerhedspolitik

for Kirkeministeriet og Den danske folkekirke

December 2021
Akt nr. 199686

Kirkeministeriet

1. Indledning

I Kirkeministeriet og Den danske folkekirke (herefter folkekirken) sker behandlingen af informationer, herunder personoplysninger, dels manuelt og dels i fælles it-systemer, som understøtter udførelsen af opgaverne - herunder i varetagelse af opgaven med personregistrering.

Kirkeministeriet stiller en række fælles systemer til rådighed, som samlet betegnes Kirkenettet. Driften af de fælles it-systemer varetages af Folkekirkens It, der er ansvarlig for at foretage passende tekniske og organisatoriske foranstaltninger for at sikre et tilstrækkeligt sikkerhedsniveau. Af bilag 1 fremgår en beskrivelse af de opgaver, som Folkekirkens It varetager.

Det er som udgangspunkt de enkelte myndigheders og institutioners ansvar at overholde kravene, der bliver stillet til informationssikkerhed og databeskyttelse, herunder den behandling af personoplysninger, som finder sted i forbindelse med anvendelse af de fælles systemer. Ansvarsfordelingen står nærmere beskrevet i cirkulærer om fælles dataansvar[1].

På baggrund af denne informationssikkerhedspolitik for Kirkeministeriet og folkekirken (herefter Sikkerhedspolitikken) fastlægger "Cirkulære om informationssikkerhed for Kirkeministeriet og Den danske folkekirke" (herefter Sikkerhedscirkulæret) de konkrete retningslinjer for, hvordan alle i Kirkeministeriet og folkekirken skal agere for at understøtte sikker adfærd i forbindelse med behandling af data og informationer, herunder personoplysninger. Overholdelse af disse regler omtales i det følgende samlet som "sikker adfærd".

Alle, der er omfattet af Sikkerhedspolitikken, skal handle på en ansvarlig, etisk og lovlig måde. Desuden er alle forpligtet til at administrere oplysninger og viden med den fornødne omhu og diskretion, uanset om den er fysisk, elektronisk eller verbal.

1.1. Formål med informationssikkerhedspolitikken

Informationssikkerhed handler grundlæggende om beskyttelse af oplysninger, så fortrolighed, integritet og tilgængelighed bevares. Informationssikkerhed omfatter den nødvendige beskyttelse af samtlige ressourcer, der indgår i eller bidrager til Kirkeministeriets og folkekirkens behandling og kommunikation af data og informationer digitalt eller i papirform m.m.

Formålet med Sikkerhedspolitikken er at definere og fastlægge de overordnede rammer og principper for beskyttelse af Kirkeministeriets og folkekirkens data og informationer, der behandles via Kirkenettet.

[1] Se cirkulære nr. 9351 af 23. maj 2018 om fælles dataansvar i forbindelse med Kirkeministeriets fælles systemer vedrørende økonomi-, betalings-, administrations-, HR og lønområdet og cirkulære nr. 9447 af 15. juni 2021 om fælles dataansvar i forbindelse med Kirkeministeriets fælles systemer vedrørende personregistrering, valg til menighedsråd samt sognebåndsløsning.

Et højt sikkerhedsniveau er ikke kun et krav for at kunne overholde lov- og myndighedskrav, men også en kvalitetsparameter i forhold til at kunne tilbyde et sikkert Kirkenet og tilhørende services til Kirkeministeriet og de folkekirkelige myndigheder, borgere samt øvrige samarbejdspartnere. Den statslige standard for informationssikkerhed[2] skal overholdes på Kirkenettet. Ved behandling af personoplysninger finder databeskyttelsesreglerne, dvs. Databeskyttelsesforordningen (GDPR) og de supplerende bestemmelser i Databeskyttelsesloven m.fl., desuden anvendelse.

Sikkerhedspolitikken skal udmøntes gennem implementering af relevante sikkerhedsforanstaltninger, som skal beskytte data og informationssystemer med udgangspunkt i tre centrale begreber:

- ✓ **Fortrolighed**, at information ikke kommer til uvedkommendes kendskab
- ✓ **Integritet**, at information forbliver pålidelig, korrekt og intakt
- ✓ **Tilgængelighed**, at relevant information kan tilgås og anvendes, når der er behov for det

Informationssikkerhed kræver at it-sikkerheden er på plads, men it-sikkerhed er blot ét element i at sikre egne og andres informationer. Uanset fysiske og tekniske foranstaltninger spiller den menneskelige faktor, dvs. den måde ledelse, ansatte, folkevalgte og frivillige (i Sikkerhedspolitikken benævnt brugerne) handler og agerer på, en afgørende rolle i forhold informationssikkerheden.

Derfor beskriver Sikkerhedspolitikken forhold gældende for både tekniske og organisatoriske foranstaltninger.

1.2. Hovedmålsætninger med informationssikkerhedspolitikken

Sikkerhedspolitikken skal understøtte Kirkeministeriets og folkekirkens virke i forhold til at sikre stabilitet i behandlingen af data, fortrolighed i forhold til følsomme data samt pålidelighed i datas indhold. Det sikres ved, at alle i Kirkeministeriet og folkekirken i deres daglige virke lever op til almindeligt anerkendte principper for informationssikkerhed. Herved understøtter informationssikkerheden borgernes forventning om troværdighed.

Sikkerhedspolitikken skal være med til at sikre, at de data og informationer, som Kirkeministeriet og folkekirken kommunikerer til borgere, myndigheder og samarbejdspartnere, er tilgængelige, forbliver fortrolige, når de er af fortrolig karakter, og fremstår med et korrekt indhold.

Målet med informationssikkerhedspolitikken er at:

[2] Den statslige standard - ISO/IEC 27001 er en referenceramme, der anvendes som rettesnor og redskab for tilrettelæggelse og styring af informationssikkerheden i Kirkeministeriet og folkekirken.

- Øge opmærksomheden om informationssikkerhed i det daglige arbejde
- Understøtte fortrolig behandling, transmission og opbevaring af data
- Sikre mod forsøg på tilsidesættelse af sikkerhedsforanstaltninger.
- Opnå høj driftssikkerhed og minimeret risiko for nedbrud og tab af data.
- Opnå korrekt funktion af it-systemerne med minimeret risiko for manipulation af data og systemer og fejl i disse.
- Sikre data og systemer ud fra risikobaseret vurdering af, hvad der er nødvendigt at gøre og under hensyntagen til de økonomiske rammer.

1.3. Sikkerhedspolitikkens omfang

Sikkerhedspolitikken oplister de beslutninger, som ledelsen i Kirkeministeriet har truffet med henblik på nærmere at fastlægge det tilstrækkelige sikkerhedsniveau samt definere de krav, der skal stilles, for at sikkerhedsniveauet opretholdes.

Derfor fastlægges omfanget af Sikkerhedspolitikken således, at den gælder:

- For alle ansatte i Kirkeministeriet og de folkekirkelige institutioner uanset ansættelsesform, herunder også eksterne konsulenter.
- For alle folkekirkens folkevalgte og frivillige.
- For alle eksterne samarbejdspartnere, herunder leverandører
- Når ansatte, folkevalgte og frivillige har adgang til og behandler personoplysninger samt øvrige informationer, som led i opgaver der udføres i Kirkeministeriet og folkekirken
- For alle behandlinger af informationer uanset, om det sker ved hjælp af pc'er og it-systemer eller i form af fysiske dokumenter
- For alle de fælles systemer i Kirkenettet og alle data i Kirkeministeriet og folkekirkens besiddelse.
- Alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af organisationens it-systemer og papirarkiver.

Behandling af personoplysninger må kun ske efter ledelsesmæssig instruktion, medmindre behandling sker i henhold til anden lovgivning. Dette skal sikres af den dataansvarlige myndighed.

2. Sikkerhedsniveau og risikovurdering

Sikkerhedsniveauet er en betegnelse for den generelle sikkerhed, der gennem implementerede foranstaltninger er i systemer og i hele organisationen til at imødegå de kendte risici.

Opretholdelse af det vedtagne sikkerhedsniveau er en fortløbende proces. Det vurderes løbende, hvad der er af relevante trusler, og hvor stor sandsynligheden er for at disse trusler indtræffer, den sårbarhed der er tillige med konsekvensen heraf.

Det sikkerhedsniveau, som denne Sikkerhedspolitik fastsætter, er efter høring i Informationssikkerhedsudvalget besluttet af Kirkeministeriets ledelse ud fra en

vurdering af de forretningsmæssige risici, som ledelsen ønsker at imødegå og styre.

Risikostyringen sker ved en tilbagevendende risikovurdering af Kirkenettet, og er baseret på årlige risikoanalyser af de forretningskritiske processer samt de understøttende it-aktiver i Kirkenettet.

Viser risikovurderingen, at sandsynligheden for en sikkerhedshændelse er højere end middel, skal der under hensyntagen til de økonomiske forhold implementeres sikkerhedsforanstaltninger til at nedbringe sandsynligheden og dermed den samlede risiko.

Såfremt konsekvensen ved en forretningskritisk proces er høj eller meget høj, skal sandsynligheden for og/eller konsekvensen ved en hændelse på tilsvarende måde søges nedbragt til lav.

Risikovurderingen skal opdateres ved eventuelle væsentlige ændringer i it-systemerne, ændringer i anvendelse af systemerne eller ved større organisatoriske ændringer. På baggrund heraf foretages eventuelt efterfølgende tilretning af Sikkerhedspolitikken, retningslinjer m.m.

I bilag 2 er risikovurdering af Kirkenettet nærmere beskrevet.

3. Organisering og ansvar

Kirkeministeriets ledelse har det overordnede ansvar for informationssikkerheden på Kirkenettet og træffer beslutning om gennemførelse af overordnede strategiske projekter af informationssikkerhedsmæssig karakter, samt ansvar for nærværende Sikkerhedspolitik.

Der er nedsat et Informationssikkerhedsudvalg for Kirkeministeriet og folkekirken med henblik på at rådgive Kirkeministeriet om hensigtsmæssig implementering af krav til informationssikkerhed i Kirkeministeriet og folkekirken. Udvalget består af repræsentanter fra ledelse og medarbejdere i Kirkeministeriet og stiftsadministrationer samt fra en række organisationer, som repræsenterer folkekirkens øvrige ledelser og medarbejdere. It- og digitaliseringschefen er formand for udvalget.

I Kirkeministeriet er der udpeget en databeskyttelsesrådgiver (DPO) for Kirkeministeriet og folkekirken, der vejleder Kirkeministeriet og folkekirken i spørgsmål om persondatabeskyttelse. Databeskyttelsesrådgiveren medvirker i samarbejde med Folkekirkens It's it-sikkerhedskoordinator til, at der opretholdes det nødvendige niveau af databeskyttelse og informationssikkerhed, eksempelvis ved tilbagevendende ledelsesrapportering.

Hertil kommer – i forhold til brugen af Kirkenettet – en organisation med lokale sikkerhedsansvarlige, som har et sikkerhedsmæssigt ansvar for en eller flere brugere og for et eller flere installationssteder med adgang til Kirkenettet. De lokale sikkerhedsansvarlige er placeret i en struktur, der følger den folkekirkelige struktur. For præsternes vedkommende følges den sædvanlige tilsynsstruktur:

biskop – provst – præst. En oversigt over de sikkerhedsansvarlige ses i Sikkerhedscirkulærets bilag 1.

De sikkerhedsansvarlige skal føre tilsyn med, at brugerne i det lokale tilsynsområde udviser en adfærd, der understøtter informationssikkerheden. Sikker adfærd omfatter blandt andet, at oplysninger ikke misbruges eller kommer til uvedkommendes kendskab.

Menighedsrådene er ansættelsesmyndighed for kirkefunktionærer og dermed sikkerhedsansvarlig for kirkefunktionærer med adgang til Kirkenettet. I udgangspunktet er rollen som sikkerhedsansvarlig tillagt menighedsrådets formand. Efter menighedsrådets beslutning kan rollen tillægges et andet af de valgte medlemmer eller til en sognepræst.

Når en kordegn fungerer som personregisterfører, er dennes sikkerhedsansvarlige dog altid den kirkebogsførende sognepræst.

3.1. Styringsprincipper

Informationssikkerhed og persondatabeskyttelse er et fælles anliggende i Kirkeministeriet og folkekirken. Nærmere regler herom fremgår af lovgivningen samt af regler fastsat af Kirkeministeriet, herunder denne Sikkerhedspolitik og Sikkerhedscirkulæret.

Som bruger af systemerne er den enkelte institution eller myndighed (eksempelvis en stiftsadministration eller et menighedsråd), dataansvarlig, dvs. ansvarlig for den behandling af personoplysninger, som finder sted.

It-sikkerhedskoordinatoren sikrer med reference til Kirkeministeriets ledelse, at informationssikkerhed integreres i alle forretningsgange og behandling af data samt i driftsopgaver og it-projekter. Tilsvarende sikrer koordinatoren, at Informationssikkerhedsudvalget, som koordinatoren er sekretariat for, høres og orienteres.

3.2. Eksterne samarbejdspartnere

Kirkeministeriet har et samarbejde med Center for Cybersikkerhed (CFCS) og Kirkenettet er tilsluttet CFCS' sensornetværk med det formål at understøtte et højt informationssikkerhedsniveau ved at forebygge, opdage og bidrage til at imødegå cyberangreb.

Alle samarbejdspartnere, der har adgang til data og til Kirkenettet, skal efterleve de samme retningslinjer som gælder for brugerne i Kirkeministeriet og folkekirken.

De sikkerhedskrav, der stilles til de eksterne samarbejdspartnere og herunder leverandører, er fastsat i ISO 27001 samt databeskyttelsesreglerne, og kravene er udmøntet i skriftlige aftaler[3] med de eksterne samarbejdspartnere.

[3] *Governance for Kirkenettet*, som fastsætter de krav, som leverandørerne med deres underskrift forpligter sig til at overholde.

I de tilfælde, hvor en samarbejdspartner behandler personoplysninger efter instruks fra den dataansvarlige, skal den dataansvarlige indgå en skriftlig databehandleraftale med databehandleren, der så vidt muligt skal være baseret på Datatilsynets standard-kontraktbestemmelser om databehandleraftaler.

4. Brugeradfærd

Informationssikkerhed og persondatabeskyttelse vedrører enhver anvendelse af Kirkenettet, og alle brugere har et medansvar for at opretholde det ønskede sikkerhedsniveau i Kirkeministeriet og folkekirken ved at være bekendt med Sikkerhedspolitikken og de gældende retningslinjer for sikker adfærd.

For at sikre, at der til stadighed er et tilstrækkeligt opmærksomhedsniveau i Kirkeministeriet og folkekirken, skal der løbende ske uddannelse i emner inden for informationssikkerhed og databeskyttelse. Dette kan være gennem aktiviteter såsom informationskampagner, uddannelse og løbende orienteringer på Den Digitale Arbejdsplads (DAP).

I det daglige arbejde er det den lokale sikkerhedsansvarliges ansvar inden for sit område at sørge for instruktion i forhold til korrekt anvendelse af systemer samt i forhold til den ønskede adfærd.

Den lokale sikkerhedsansvarlige skal løbende føre tilsyn med, at brugerne overholder gældende retningslinjer.

Retningslinjer for brugeradfærd på udvalgte områder, som f.eks. e-mail og internet, adgangskoder, rapportering af sikkerhedshændelser samt den sikkerhedsansvarliges tilsyn, er nærmere beskrevet i Sikkerhedscirkulæret.

Overtrædelse af Sikkerhedspolitikken eller Sikkerhedscirkulæret vil efter omstændighederne kunne medføre disciplinære sanktioner for ansatte i Kirkeministeriet og folkekirken.

4.1. Funktionsadskillelse

Retningslinjer suppleret med interne kontroller skal sikre, at der er tilstrækkelig funktionsadskillelse, hvor dette er påkrævet, f.eks. i regnskabs- og lønfunktioner. Såfremt der ikke kan tilvejebringes en fuldstændig funktionsadskillelse, skal der tages højde herfor ved udarbejdelse af instrukser for arbejdet samt udførelse af intern kontrol. Medarbejdere, der skal udføre kontrol, skal have et så stort kendskab til området, at de kan foretage en relevant kontrol.

I videst muligt omfang skal it-systemer understøtte funktionsadskillelse.

Der skal desuden tilstræbes uafhængighed af nøglepersoner gennem videndeling og etablering af person-backup, hvor dette er muligt.

5. Beskyttelse af Kirkenettet

For at sikre et stabilt og driftssikkert Kirkenet skal der være implementeret de nødvendige sikkerhedsforanstaltninger. Krav til beskyttelsen er nærmere beskrevet i bilag 1.

For at kunne opklare sikkerhedshændelser og sikre driftsstabiliteten på Kirkenettet foretages der en generel logning og sikkerhedsovervågning af Kirkenettet.

5.1. Adgang til Kirkenettet

Fra en Kirkenet-pc opnås fuld adgang til Kirkenettet via en sikker-forbindelse.

Fra en almindelig pc, mobiltelefon og tablet er der adgang til udvalgte services på Kirkenettet, f.eks. Den Digitale Arbejdsplads (DAP). Fra DAP er der videre adgang til en række andre services, som tilbydes via Kirkenettet, f.eks. lønsystemet FLØS.

Der må kun tilsluttes pc'er til Kirkenettet, der er anskaffet gennem Folkekirkens It. Alle Kirkenet-pc'er har installeret et aktivt og opdateret antivirusprogram, der kan opdage, rense og beskytte mod forskellige former for skadevoldende programmer og er desuden indrettet så data og informationer krypteres når brugeren ikke anvender pc'en.

5.2. Mobilt udstyr og fjernarbejdspladser

Sikkerhedspolitikken gælder også for alt it-udstyr ud over Kirkenet-pc'er, der tilgår services på Kirkenettet.

I Sikkerhedscirkulæret er der fastlagt de konkrete regler, som skal overholdes ved brug af mobilt udstyr og fjernarbejdspladser.

5.3. Sikker kommunikation

Al kommunikation af fortrolige og/eller følsomme personoplysninger via mail til modtagere uden for folkekirken, f.eks. privatpersoner, andre offentlige myndigheder og virksomheder, skal ske via en krypteret dataforbindelse.

Kirkenettet stiller forskellige løsninger til rådighed, som alle understøtter sikker kommunikation.

6. Fysisk beskyttelse af informationer

Såvel it-udstyr som fysiske lokaliteter skal beskyttes mod uvedkommendes adgang.

It-udstyr skal desuden beskyttes mod den ødelæggelse og skade, der kan følge af brand, vandskade, strømsvigt og andre skader som følge af hændelser i det omkringliggende miljø.

Den lokale sikkerhedsansvarlige skal påse, at brugerne varetager det ansvar, som de alle har for at beskytte it-udstyr og bærbare datamedier. De nærmere retningslinjer for brugen af it-udstyr på Kirkenettet fremgår af Pc-Supportforum på adressen: support.kirkenettet.dk/sikkerhed.

Fysisk sikkerhed er nærmere beskrevet i Sikkerhedscirkulærets kapitel 6.

7. Adgangsstyring

7.1. De forretningsmæssige krav til adgangsstyring

Alle informationsaktiver (programmel, udstyr, data, informationer og databærende medier) skal i nærmere specificeret omfang være beskyttet mod uautoriseret adgang.

På Kirkenettet anvendes elektronisk brugeradministration, der giver adgang til systemer ud fra de rettigheder, som den lokale sikkerhedsansvarlige har tildelt brugeren. Brugeradministrationssystemet kan via logning danne grundlag for efterfølgende kontrol.

I særlige tilfælde, hvor tjenstlige behov tilsiger det, kan den lokale sikkerhedsansvarlige få adgang til en anden brugers konto, hvis brugeren er fraværende eller ophørt. Dette er beskrevet nærmere i Sikkerhedscirkulæret.

7.2. Administration af brugeradgange

Tildeling, ændring og sletning af brugeradgange til systemer og data foretages af den sikkerhedsansvarlige ud fra brugerens arbejdsbetingede behov og i overensstemmelse med datas klassifikation. Adgang og brugerrettigheder til systemer og data inddrages, når brugeren ikke længere har et sådant arbejdsbetinget behov.

Den lokale sikkerhedsansvarlige har ansvaret for at de tildelte adgange er korrekte.

7.3. Brugerens ansvar

Alle brugere er ansvarlige for deres personlige adgang til Kirkenettet samt tilhørende fortrolige adgangskode, og skal følge de retningslinjer, der er angivet i Sikkerhedscirkulæret.

En bruger er forpligtet til at underrette sin lokale sikkerhedsansvarlige eller Folkekirkens It, hvis vedkommende bliver opmærksom på, at brugeren selv eller andre brugere har adgang til systemer eller informationer, som er mere vidtgående, end brugerens arbejdsbetingede behov begrunder. Dette er beskrevet nærmere i Sikkerhedscirkulæret.

8. Styring af sikkerhedshændelser

8.1. Sikkerhedshændelse eller sikkerhedsbrud

En sikkerhedshændelse er en samlebetegnelse for forskellige typer af tekniske og menneskeskabte fejl eller handlinger, der kan udgøre en risiko for de informationer og data, herunder personoplysninger, som behandles på Kirkenettet.

Ved en **sikkerhedshændelse** kan oplysninger på Kirkenettet blive kompromitteret, herunder ved at der hændeligt eller ulovligt sker:

- uautoriseret videregivelse eller adgang til oplysninger (brud på fortrolighed),
- ændring af oplysninger (brud på integritet),
- manglende adgang til, tab eller tilintetgørelse af oplysninger (brud på tilgængelighed).

Et **sikkerhedsbrud** er et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Der er tale om et sikkerhedsbrud, når personoplysninger er blevet kompromitteret ved en sikkerhedshændelse.

8.2. Håndtering af sikkerhedshændelser

En væsentlig faktor i informationssikkerhedsarbejdet består i at reagere på hændelser af sikkerhedsmæssig karakter. Derfor skal sikkerhedsmæssige hændelser rapporteres, og der skal ske opfølgning herpå.

Alle brugere har pligt til at rapportere sikkerhedshændelser til deres lokale sikkerhedsansvarlige således, at en sikkerhedshændelse snarest kan imødegås, så vidt muligt inden den udvikler sig til et sikkerhedsbrud.

Den lokale sikkerhedsansvarlige skal derfor omgående give besked til Folkekirkens It om hændelsen, hvis hændelsen vedrører systemer på Kirkenettet. Folkekirkens It skal følge op på hændelsen, herunder sikre udbedring af fejl samt dokumentere hændelsesforløbet.

8.3. Håndtering af sikkerhedsbrud

I tilfælde af et sikkerhedsbrud som omfatter personoplysninger skal den dataansvarlige myndighed eller institution indberette dette til Datatilsynet hurtigst muligt og inden for 72 timer efter, at den dataansvarlige er blevet opmærksom på bruddet. Datatilsynet skal dog ikke informeres, hvis den dataansvarlige vurderer, at det er usandsynligt, at bruddet kan medføre risiko for registrerede personers rettigheder eller frihedsrettigheder.

Såfremt det er sandsynligt, at bruddet vil indebære en høj risiko for de registrerede personers rettigheder, skal den dataansvarlige ligeledes underrette de registrerede uden unødig forsinkelse.

Kirkeministeriets databeskyttelsesrådgiver (DPO) skal altid orienteres i tilfælde af brud på persondata-sikkerheden.

Kontaktoplysninger vedrørende Kirkeministeriets og folkekirkens DPO kan ses på km.dk.

Kirkeministeriet

9. Revision

Kirkeministeriet foretager årligt en revision af Sikkerhedspolitikken og Sikkerhedscirkulæret. Revisionen foretages på grundlag af dels risikovurderingen for Kirkenettet og dels den løbende overvågning og rapportering om sikkerhedshændelser.

10. Godkendelse

Sikkerhedspolitikken er den 16. november 2021 forelagt for Informationssikkerhedsudvalget i Kirkeministeriet og folkekirken og den 18. november 2021 for Kirkeministeriets Samarbejdsudvalg og efterfølgende godkendt af Kirkeministeriets ledelse.

København den 7. december 2021

Christian Dons Christensen
Departementschef

11. Ikrafttrædelse

Sikkerhedspolitikken træder i kraft den 10. december 2021 og erstatter både den tidligere godkendte informationssikkerhedspolitik og den tidligere godkendte persondatapolitik for Kirkeministeriet og Den danske folkekirke.

Kirkeministeriet

Bilag 1. Styring og drift af Kirkenettet

Driften af de fælles it-systemer på Kirkenettet varetages af Folkekirkens It, som er ansvarlig for at implementere de tekniske og organisatoriske foranstaltninger, der sikrer det sikkerhedsniveau, som Kirkeministeriets ledelse har besluttet på baggrund af de foretagne risikovurderinger.

Der etableres sikkerhedsforanstaltninger med henblik på at beskytte data og informationssystemer mod at blive kompromitteret.

Sikkerhedsforanstaltningerne rettes mod alle former for trusler, interne og eksterne, hændelige fejl og uheld, samt bevidst skadevoldende handlinger og misbrug for at sikre, at it-driftssikkerheden og effektiviteten af Kirkenettet kan opretholdes, samt at konsekvenser af sikkerhedsbrud reduceres til et acceptabelt niveau.

Folkekirkens It vejleder desuden de folkekirkelige myndigheder, institutioner og brugerne i sikkerhedsmæssige spørgsmål samt koordinerer og følger op på informationssikkerhedsrelaterede aktiviteter.

For at sikre en stabil og sikker drift af Kirkenettet skal alle leverandører til Kirkenettet samt Folkekirkens It – foruden denne Politik samt Sikkerhedscirkulæret – overholde de regler og procedurer, der fremgår af proceduren "Governance i Kirkenettet". Procedurerne gælder for alt arbejde på Kirkenettets miljøer, herunder ved installation af nye udgaver af it-systemer samt ændringer af eksisterende.

I det følgende beskrives de it-driftsmæssige opgaver, som Folkekirkens It varetager. Der vil være udarbejdet retningslinjer og procedurer som supplement til beskrivelsen.

1. Netværk og drift

1.1. Styring af driftsmiljø

Folkekirkens It beskytter Kirkenettet mod uautoriseret adgang, hvilket f.eks. sker via adgangskontrol og adskillelse af netværkstjenester, hvor dette er hensigtsmæssigt.

Der er etableret firewall-løsninger, der beskytter mod forbindelse til upålidelige netværk. Netværket overvåges løbende med henblik på at opdage og udbedre brud på sikkerheden.

En forudsætning for hurtig imødegåelse af driftsforstyrrelser er, at der er etableret redundans af forretningskritiske systemer, og at der er etableret procedurer for daglig sikkerhedskopiering (backup).

Serverkapacitet overvåges løbende på alle produktionsservere for at sikre pålidelig drift og tilgængelighed.

Kirkenettets driftsleverandører er ansvarlige for den løbende opdatering til anvendte operativsystemer samt installation af nødvendige sikkerhedsrettelser (benævnt patches og hotfixes). Sidstnævnte vil typisk ske i dialog med Folkekirkens It.

Af *Governance i Kirkenettet* fremgår retningslinjer for anvendelse af data på udviklings- og testmiljøer, hvor der er særligt fokus på beskyttelse af persondata. Installation af systemer og ændringer (softwarepakker og konfiguration) styres ligeledes af *Governance i Kirkenettet*, og der anvendes som udgangspunkt standardopsætninger for konfiguration af systemkomponenter, som kontrollerer kendte sårbarheder.

For at sikre stabil drift af Kirkenettet er der etableret funktionsadskillelse således, at udvikling, test og produktion holdes adskilt i forskellige miljøer og på forskellige segmenter. Nye systemer og ændringer til eksisterende systemer testes inden installation i driftsmiljøet således, at tilgængelighed og integritet sikres.

Udarbejdede procedurer, fordeling af ansvarsområder og anvendt teknologi skal understøtte denne funktionsadskillelse.

1.2. Logning og overvågning

Folkekirkens It sikrer, at der foretages logning i forretningskritiske systemer, og at der foretages den fornødne logning til sikring af Kirkenettets drift samt opfølgning på sikkerhedshændelser.

Logs kontrolleres løbende med henblik på at opdage og spore uautoriserede handlinger, og i så fald at kunne føre disse tilbage til enkeltpersoner eller identificerbart netværksudstyr.

Som en del af logningen skal sikkerhedsrelaterede hændelser registreres, hvilket sker i henhold til *Procedure for håndtering af sikkerhedshændelser*[4].

Logfiler må ikke anvendes til at spore enkeltpersoners handlinger, medmindre der er tale om ulovlige handlinger, alarmer fra antivirus/antispam, eller ved mistanke om ikke tilladt adfærd.

1.3. Styring af administrative rettigheder

Folkekirkens It er ansvarlig for styring af rettigheder og adgange, herunder adgange til netværk for systemadministratorer.

Alle brugere og alt netværksudstyr skal være identificeret, og der skal være opdaterede fortegnelser herfor.

Der er implementeret sikkerhedsforanstaltninger således, at adgangskontroller til systemer og data ikke kan omgås, og der er implementeret timeout i forbindelse med adgang til forretningskritiske systemer og netværk.

[4] Aktnr. 165716 af april 2021

1.4. Sårbarhedsstyring

Folkekirkens It indhenter løbende informationer om sårbarheder i de anvendte systemer på Kirkenettet ved at gennemføre tilbagevendende sårbarhedstests. Dette sker i form af interne tests såvel som tests foretaget af eksterne parter. De fundne sårbarheder skal evalueres, og passende foranstaltninger implementeres.

1.5. Sikkerhedskopiering

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. Det kontrolleres, at den daglige sikkerhedskopiering er gennemført, og at data kan genskabes på baggrund heraf. Backup opbevares eksternt på en anden geografisk og sikker lokalitet, hvor sikkerheden jævnligt kontrolleres.

Den enkelte bruger skal selv sikre egne data, som er gemt lokalt på Kirkenet-pc'en.

2. Anskaffelse, udvikling og vedligeholdelse af systemer

Folkekirkens It udvikler som udgangspunkt ikke selv systemer, og der anvendes i videst muligt omfang standard og/eller rammesystemer.

Ved udvikling af systemer til Kirkenettet skal gældende standarder for tilgængelighed, sikkerhed m.v. overholdes. Udvikling skal ske efter principper, som sikrer god databeskyttelse, herunder databeskyttelse gennem design (privacy by design) og databeskyttelse gennem standardindstillinger (privacy by default).

Alle nyanskaffelser og væsentlige ændringer af systemer og services på Kirkenettet skal ske i henhold til *Folkekirkens It's arkitekturprincipper*[5]. Disse principper sikrer, at nyanskaffelser og ændringer sker i henhold til den fælles it-arkitektur således, at der sikres en fælles ramme for alle it-tiltag.

Folkekirkens It etablerer godkendelsesprocedurer for nye systemer, nye versioner og opdateringer af eksisterende systemer. Godkendelsesprocedurerne beskriver krav til dokumentation, specifikationer, test, kvalitetskontrol og en styret implementeringsproces.

Systemvedligeholdelse sker ved servicevinduer, der om muligt placeres uden for almindelig arbejdstid.

Når driftsmiljøet ændres, skal kritiske forretningssystemer gennemgås og testes for at sikre, at der ikke er utilsigtede, afledte virkninger på den daglige drift og sikkerhed.

Databeskyttelsesrådgiveren inddrages i nødvendigt omfang ved anskaffelse af it-systemer og gennemførelse af de dertil hørende risiko- og konsekvensanalyser.

[5] På Folkekirkens It's hjemmeside ses Folkekirkens It's arkitekturprincipper

2.1. Sikkerhedskrav til it-systemer

De sikkerhedskrav, der skal stilles til systemers behandling af data, skal fastlægges, inden der foretages anskaffelse og udvikling af systemer.

Det enkelte system skal have implementeret sikkerhedsforanstaltninger, som er tilstrækkelige i forhold til de data, som systemet behandler, de forretningsmæssige funktioner, som systemet varetager, og de databeskyttelseshensyn, der skal varetages i forhold til de registrerede.

Sikkerhedskravene fastlægges bl. a. gennem en obligatorisk risikoanalyse og eventuelt en konsekvensanalyse af de behandlingsaktiviteter systemet skal understøtte. Eksempler på foranstaltninger er antivirusbeskyttelse, kryptering og pseudonymisering-/anonymisering. Der skal desuden tages stilling til behovet for ind- og uddatavalidering.

Databeskyttelsesrådgiveren inddrages i nødvendigt omfang, herunder ved anskaffelse af it-systemer, udarbejdelse af vejledninger samt ved risiko- og konsekvensanalyser.

3. Klassifikation af systemer med tilhørende data

For at sikre at Kirkenettets systemer og data har det rigtige sikkerhedsniveau, skal disse identificeres og klassificeres. Folkekirkens It vedligeholder en fortegnelse over alle væsentlige it-aktiver, både hardware og software, hvor klassifikationen er angivet på baggrund af følgende kategorier[6]:

Offentlige eller almindelige data/systemer:

- Data danner aldrig eller kun sjældent grundlag for beslutninger.
- Systemer er offentligt tilgængelige eller indeholder kun almindelige personoplysninger.

Forretningskritiske data/systemer:

- Systemer, hvor driftsforstyrrelser kan medføre, at størstedelen af myndighedens brugere ikke kan udføre deres arbejde, eller at myndigheden vanskeligt kan overholde sine forvaltningsmæssige forpligtigelser.
- Forretningskritiske beslutninger bliver taget på grundlag af disse data.
- Data skal behandles med en høj grad af fortrolighed (herunder personoplysninger).

Samfundskritiske data/systemer:

- Systemer, som er vigtige for national sikkerhed eller for kritisk infrastruktur, hvor misbrug af data vil have store konsekvenser, eller hvor driftsforstyrrelser kan have stor betydning for økonomien i staten og folkekirken eller for mange borgere og virksomheder.

[6] Digitaliseringsstyrelsens definition: https://digst.dk/styring/kasseeftersyn-af-det-statslige-it-omraade/

Eksempler på klassificeringer:

	Offentlige/Almindelige	Forretningskritiske	Samfundskritiske
Data	Almindelige personoplysninger Offentlige forretningsoplysninger	Fortrolige og følsomme personoplysninger Forretningskritiske oplysninger	Politiske oplysninger eller oplysninger, som er kritiske for driften i staten
Systemer	Hjemmesider	F2, FLØS, KAS, GIAS og SAS	Den digitale Kirkebog
Processer	Kommunikation	Personaleadministration og Kapital- og gravstedsadministration	Personregistrering

4. Leverandørstyring

Forinden indgåelse af en kontrakt med en it-leverandør til Kirkenettet, skal Folkekirkens It foretage en risikovurdering af leverandøren, som skal medvirke til, at der bliver stillet de rette krav til it-leverandøren.

Risikovurderingen skal gennemføres tilbagevendende under kontraktforholdet for at sikre, at forholdene omkring it-leverandøren fortsat er tilfredsstillende.

I forbindelse med indgåelse af en kontrakt, skal der – hvor det kræves – indgås en databehandleraftale. Datatilsynets standardskabelon for databehandleraftale skal så vidt muligt anvendes.

Folkekirkens It fører tilsyn med it-leverandører således, at disse også udviser en sikker adfærd, og at Sikkerhedspolitikken, Sikkerhedscirkulæret og Governance for Kirkenettet samt gældende regler overholdes.

5. It-beredskabsplan for Kirkenettet

Folkekirkens It vedligeholder en it-beredskabsplan for Kirkenettet med en praktisk anvisning af, hvorledes Folkekirkens It opretholder et beredskab, der er egnet til at håndtere en større sikkerhedshændelse.

Beredskabets formål er at sikre Kirkenettets robusthed over for følgerne af nedbrud, ulykker og katastrofer, og at it-understøttelsen af de forretningskritiske processer i videst mulig udstrækning kan ske uden negativ sikkerhedsmæssig påvirkning.

Ved den årlige risikovurdering af Kirkenettet, som beskrevet ovenfor, identificeres de forretningskritiske processer og dermed også de systemer og data, som er kritiske, samt den maksimalt acceptable nedetid for de forretningskritiske processer. Det er disse systemer og data, som it-beredskabsplanen har et særligt fokus på.

Den udarbejdede it-beredskabsplan for Kirkenettet suppleres af beredskabsplaner fra de leverandører til Kirkenettet, der leverer hosting- og/eller driftsydelser.

It-beredskabsplanen ajourføres minimum en gang årligt samt ved væsentlige ændringer og hændelser, og planen skal testes løbende, eksempelvis ved gennemførelse af beredskabsøvelser med Kirkeministeriets ledelse samt Informationssikkerhedsudvalget.

Kirkeministeriet

Akt nr. 187504

Bilag 2. It-risikostyring og -vurdering

Formålet med risikostyring på Kirkenettet er at identificere, styre og håndtere de risici, som måtte opstå, samt at implementere og vedligeholde de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger.

I vurderingen af, om foranstaltninger er passende, skal der lægges vægt på:

- Behandlingens karakter, omfang, sammenhæng og formål
- De sandsynlige risici for den registreredes rettigheder
- Det aktuelle tekniske niveau
- Implementeringsomkostningerne

Risikostyringen sker igennem tilbagevendende risikovurdering af Kirkenettet, som Folkekirkens It er ansvarlig for gennemførelsen af. Risikovurderingen foretages på baggrund af en årlig risikoanalyse af de forretningskritiske processer samt de understøttende it-aktiver på Kirkenettet. Herved konstateres, hvorvidt det aktuelle risikobillede ligger inden for rammerne af det sikkerhedsniveau, der er fastsat i Sikkerhedspolitikken.

Risikoanalysen består af to analyser:

- konsekvensanalyse
- sårbarhedsanalyse.

Konsekvensanalyser foretages af de forretningsmæssige system- og dataejere i Kirkeministeriet og folkekirken, og sårbarhedsanalyser foretages af de systemansvarlige i Folkekirkens It.

Resultatet af den samlede risikovurdering med anbefaling om eventuelle yderligere sikringsforanstaltninger, forelægges for Kirkeministeriets ledelse til godkendelse. Desuden forelægges rapporten for systemejere for de forretningskritiske processer samt for Informationssikkerhedsudvalget. Ved forelæggelsen erklærer disse sig bekendt med de opgjorte risici og risikovurderingen af Kirkenettet. Systemejerne er som risikoejere ansvarlige for den nærmere håndtering af de opgjorte risici.

Information om nye trusler og sårbarheder

Folkekirkens It skal holde sig løbende orienteret om mulige nye trusler mod sikkerheden på Kirkenettet og eventuelle sårbarheder i systemer og services på Kirkenettet. Dette gøres ved hjælp af udmeldinger, advarsler m.v. fra Datatilsynet, Center for Cybersikkerhed (CFCS) og øvrige relevante sikkerhedsvirksomheder, organisationer og myndigheder.

Kirkeministeriets ledelse samt berørte systemejere skal informeres om nye trusler og sårbarheder, såfremt disse potentielt kan berøre en eller flere forretningsprocesser og systemer. Disse trusler og sårbarheder skal i fornødent omfang modvirkes ved implementering af tilstrækkelige organisatoriske og tekniske sikkerhedsforanstaltninger.