Kirkeministeriet

It-sikkerhedspolitik for Kirkenettet, 2017

Folkekirkens IT

Dato: 30. maj 2017

Dokument nr. 146935/17

Sagsbehandler:
Ulla Brynning Kristiansen

Kirkeministeriets opgave er med lovgivning og administrative systemer at skabe rammer for folkekirken og dens virke. Det sker i et nært samspil med folkekirkens institutioner og præster, hvis vigtigste opgave har at gøre med kirkens kerneopgave, nemlig evangeliets forkyndelse, sakramenternes forvaltning, oplæring i kristendom og sjælesorg.

Herudover har Kirkeministeriet og folkekirken ansvaret for civilregistreringen i Danmark.

Kirkenettet, der er folkekirkens fælles it-systemer, understøtter udførelsen af ovennævnte opgaver.

Rammerne for og formålet med it-anvendelsen er fastlagt i Digital Strategi 2016-2020 for Kirkeministeriet og folkekirken samt i nærværende it-sikkerhedspolitik.

It-sikkerhedspolitikken er den overordnede ramme for it-sikkerheden i Kirkeministeriet og folkekirken og dermed for Kirkenettet. Politikken er udarbejdet af It-Sikkerhedsudvalget[1] i Kirkeministeriet og folkekirken og er godkendt af Kirkeministeriets ledelse.

Som et led i den overordnede risikostyring foretager It-Sikkerhedsudvalget en revision af it-sikkerhedspolitikken. Revisionen foretages på grundlag af dels den samlede risikovurdering for Kirkenettet, der foretages hvert 2. år, og dels den løbende overvågning og rapportering om sikkerhedshændelser.

It-sikkerhedspolitikken er udarbejdet i overensstemmelse med ISO 27001.

Formål

Anvendelse af it er en så integreret del af arbejdsrutinerne i Kirkeministeriet og folkekirkens administration, herunder opgaverne med civilregistreringen, at en høj it-sikkerhed har afgørende betydning for den samlede virksomhed.

It-sikkerhedspolitikken definerer rammen for beskyttelse af informationer, der behandles via Kirkenettet, og skal særligt sikre, at kritiske og følsomme informationer, og it-systemer bevarer deres fortrolighed, integritet og tilgængelighed.

Med en it-sikkerhedspolitik, der er udarbejdet af It-Sikkerhedsudvalget og godkendt af ministeriets ledelse, tilkendegives over for alle med relation til Kirkeministeriet og folkekirken, at der er fastlagte regler for behandling af informationer og informationssystemer.

I forhold til Kirkenettets brugere udmøntes it-sikkerhedspolitikken i det daglige gennem cirkulære om informationssikkerhed, herunder sikkerhedsforanstaltninger i Kirkenettet samt procedurer og retningslinjer for specifikke områder som eksempelvis tildeling af rettigheder til it-systemer, tilbagevendende kontroller, opfølgning på sikkerhedshændelser m.v.

[1] It-Sikkerhedsudvalget i Kirkeministeriet og folkekirken består af repræsentanter fra ledelse og medarbejdere i departement og stifter, de folkekirkelige organisationer samt Folkekirkens It.

Samlet set er formålet med it-sikkerhedspolitikken at forebygge sikkerhedsproblemer, begrænse eventuelle skader samt sikre, at informationer ikke mistes og – hvis et uheld opstår – kan genskabes.

Omfang

It-sikkerhedspolitikken er uden undtagelse gældende for alle brugere, der benytter Kirkenettet, og politikken gælder for enhver behandling af data og informationer på Kirkenettet.

Ved indgåelse af aftaler om køb af varer og tjenesteydelser til brug i Kirkenettet skal det sikres, at det vedtagne sikkerhedsniveau fastholdes. Det betyder, at en leverandør, dennes faciliteter og de medarbejdere, som gennem autorisation har adgang til Kirkenettet, skal leve op til kravene i politikken.

I de tilfælde hvor der behandles persondata skal der tillige indgås en skriftlig databehandleraftale.

Sikkerhedsniveau

It-sikkerhedspolitikken sikrer beskyttelse af Kirkeministeriets, folkekirkens og borgernes data og informationer. Der tillades udelukkende adgang til samt brug og offentliggørelse af data og informationer i overensstemmelse med retningslinjerne og under hensyntagen til den til enhver tid gældende lovgivning.

Med henblik på implementering og vedligeholdelse af sikringsforanstaltninger skal resultatet af en udført risikoanalyse altid resultere i, at sandsynligheden for it-sikkerhedshændelser højst er middel. Det skal være målsætningen, at den som hovedregel er lav eller meget lav.

Opretholdelse af det vedtagne sikkerhedsniveau er en fortløbende proces, hvor relevante trusler, sandsynligheden for, at de indtræder samt konsekvensen heraf vurderes. I den løbende vurdering af konkrete trusler skal der om fornødent indhentes ekspertudtalelser til belysning af risikoen.

Risikoanalyse(r)

I alle it-projekter samt ved større forandringer i Kirkenettet foretages en risikoanalyse. Desuden gennemføres hvert andet år en samlet risikoanalyse for Kirkenettets forretningskritiske processer samt de understøttende it-aktiver.

Formålet med risikoanalyserne er at konstatere, hvorvidt det aktuelle risikobillede ligger inden for rammerne af det, der er fastsat i denne it-sikkerhedspolitik.

Viser risikoanalysen, at sandsynligheden for en it-sikkerhedshændelse er højere end middel, skal Folkekirkens It – under hensyntagen til de økonomiske forhold – implementere sikringsforanstaltninger til at nedbringe sandsynligheden og dermed den samlede risiko.

Såfremt konsekvensen ved en kritisk forretningsproces er høj eller meget høj, skal sandsynligheden tilsvarende søges bragt ned under middel.

Det operationelle ansvar for den daglige styring af it-sikkerhedsindsatsen og opretholdelse af det fastlagte sikkerhedsniveau påhviler it-sikkerhedskoordinatoren for Kirkeministeriet og folkekirken.

It-sikkerhedskoordinatoren skal med reference til It-Sikkerhedsudvalget og Kirkeministeriets ledelse sikre, at it-sikkerhed integreres i alle forretningsgange og behandling af data samt driftsopgaver og it-projekter.

Resultatet af den samlede risikoanalyse og eventuelle foranstaltninger, som Folkekirkens It yderligere skal implementere for at nedbringe sandsynligheden for, at en given it-sikkerhedshændelse indtræder, forelægges it-sikkerhedsudvalget, Kirkeministeriets ledelse, stiftskontorcheferne, som tillige er chefer for fællesfondens driftscentre samt rektor for Folkekirkens Uddannelses- og Videnscenter til godkendelse.

Beredskab

Beredskabets formål er at sikre Kirkenettets robusthed over for følgerne af nedbrud, ulykker og katastrofer, og at de forretningskritiske processer i videst mulig udstrækning kan udføres uden sikkerhedsmæssig påvirkning

Folkekirkens It har ansvaret for opretholdelse af en beredskabsorganisation til håndtering af beredskabet i forhold til Kirkenettets forretningskritiske processer og de understøttende it-aktiver.

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

Beredskabsplanen skal ajourføres minimum en gang årligt og skal testes løbende, eksempelvis ved gennemførelse af Beredskabsstyrelsens øvelser med It-Sikkerhedsudvalget.

Beredskabsplanen for Kirkenettet indgår som et bilag til Kirkeministeriets beredskabsplan.

It-sikkerhedsbevidsthed

It-sikkerhed vedrører enhver anvendelse af Kirkenettet. Alle Kirkenettets brugere skal bidrage til at beskytte alle informationer mod uautoriseret adgang, ændring og ødelæggelse samt tyveri.

Bevidsthed om dette ansvar og it-sikkerhedspolitikkens bestemmelser skal brugerne opnå gennem aktiviteter såsom informationskampagner og løbende orienteringer.

Aktiviteterne skal ligeledes medvirke til, at brugerne i det relevante omfang uddannes i it-sikkerhed.

Brud på it-sikkerheden

Såfremt en bruger opdager trusler mod it-sikkerheden eller brud på denne, skal dette straks meddeles til brugerens sikkerhedsansvarlige. Denne skal sikre, at trusler og hændelser eskaleres til Folkekirkens It til videre foranstaltning.

Overtrædelse af bestemmelserne vedrørende it-sikkerhed er en tjenesteforseelse.

Referencer og grundlag

It-sikkerhedspolitikken understøtter følgende dokumenter:

- Justitsministeriets lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (Persondataloven)
- Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen)
- Justitsministeriets cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt
- International Organization for Standardization, ISO 27001
- Digital Strategi 2016-2020 for Kirkeministeriet og folkekirken (dok.nr. 39885-16)
- Risikovurdering 2016 for Kirkenettets forretningskritiske systemer (dok.nr. 142990-16)
- Kirkeministeriets cirkulære om informationssikkerhed, herunder sikkerhedsforanstaltninger i Kirkenettet af 30. marts 2017 (dnr. 8444-17)
- Kirkeministeriets cirkulære af 1. marts 2015 om sikkerhedsforanstaltninger for Den Digitale Arbejdsplads (dok.nr. 118736-14)
- Kirkeministeriets cirkulære nr. 57 af 30. juni 2006[2] om førelse af folkekirkens ministerialbøger i den elektroniske kirkebog og om udfærdigelse af attester og udskrifter m.v.

[2] Under revision.