STRATEGI FOR STYRING AF KIRKENETTET 2023-2025

Den 1. januar 2023
Akt nr. 259408

Baggrund

Digitalisering i folkekirken sker i et samspil mellem overordnede målsætninger, teknologiske muligheder og konkrete beslutninger. Digitaliseringsstrategien 2020-2025 for folkekirken og Kirkeministeriet udstikker generelle pejlemærker og principper for digitalisering i folkekirken i et 5-årigt perspektiv. Digitaliseringsstrategien understøttes af en *Strategi for styring af Kirkenettet*, som med en 3-årig tidshorisont beskriver, hvilke teknologier, it-politikker og styringsmodeller Folkekirkens It vil anvende som grundlag for at levere og udvikle it-ydelser til folkekirken og Kirkeministeriet.

Strategi for styring af Kirkenettet lægger sig endvidere op ad de rammer, der er fastlagt i gældende It-arkitekturprincipper for Folkekirkens It og Informationssikkerhedspolitik for Kirkeministeriet og Den danske folkekirke.

Strategien medvirker til at understøtte personregistrering som samfundsvigtig funktion samt de forretningskritiske processer i Kirkeministeriet og folkekirken.

Folkekirkens It er den enhed i Kirkeministeriet, som varetager drift og udvikling af folkekirkens og Kirkeministeriets fælles digitale løsninger. Som en del af Kirkeministeriet er Folkekirkens It underlagt de almindelige forvaltningsmæssige og statslige regler samt revision.

Kirkeministeren har nedsat en It-Følgegruppe, som rådgiver Kirkeministeriet om it-strategiske overvejelser, forretningsudvikling, økonomisk styring og prioritering. Folkekirkens It er sekretariat for It-Følgegruppen.

It-Følgegruppen rådgiver om fælles og centrale digitaliseringsinitiativer, inden der træffes beslutning om iværksættelse. Den enkelte myndighed og institution tager aktivt stilling til og beslutter, hvordan man ønsker at bruge digitaliseringen lokalt inden for de gældende regler og rammer.

Strategi for styring af Kirkenettet indeholder bl.a. rammer for valg af teknologi og anskaffelse af nye it-løsninger, hvilken infrastruktur og arkitektur der arbejdes ud fra m.v. Strategien skal således sikre, at konkrete digitaliseringsinitiativer kan gennemføres med de mest hensigtsmæssige tekniske midler tillige med det rette niveau af sikkerhed og beskyttelse af personoplysninger.

Strategi for styring af Kirkenettet bidrager til optimal udnyttelse af de midler, der anvendes på it via en sammenhængende og veltilrettelagt styring, herunder effektiv anvendelse af eksterne leverandører samt rettidig vedligeholdelse og fornyelse af it-infrastrukturen.

Denne strategi er dermed Folkekirkens It's værktøj til at sikre fælles forståelse og konsistens i arbejdet vedrørende følgende temaer:

- Den anvendte it-arkitektur (afsnit 1)
- Den anvendte it-infrastruktur (afsnit 1)
- Den valgte teknologi (afsnit 2)
- Den fastlagte informationssikkerhed og databeskyttelse (afsnit 3)
- Den valgte placering af opgaveløsningen, hhv. internt eller ved eksterne leverandører (afsnit 4)
- Den vedtagne styringsmodel for it og leverandører (afsnit 5).

Indholdsfortegnelse

Hvordan efterleves strategien?

Strategi for styring af Kirkenettet[1] (herefter Strategien) er Folkekirkens It's værktøj til fastlægge rammerne for anskaffelse af it-systemer, udvikling, styring og it-vedligehold samt udfasning af it-systemerne således, at Kirkenettets it-systemportefølje til enhver tid bedst muligt understøtter Kirkeministeriet og folkekirkens forretningsbehov og dermed skaber mest mulig værdi.

På baggrund af Strategien udarbejder og vedligeholder Folkekirkens It et teknologisk roadmap, der for en treårig periode tydeliggør de nødvendige driftsmæssige initiativer, eksempelvis ved udløb af teknologier og standarder.

Desuden et roadmap, som omfatter standardapplikationer og andet forretningsprogrammel. Dette roadmap giver et overblik over applikationsporteføljen (systemer i drift), herunder indgåede kontrakter vedr. applikationer og den anvendte teknologiunderstøttelse.

Formålet med de to roadmaps er at sikre en kontinuerlig styring af teknologierne i Kirkenettet og give et overblik over arkitektur og aftaler vedrørende applikationer og forretningsprogrammel.

Roadmaps er til tjenstlig brug og indgår ikke i den offentliggjorte strategi.

Herudover vedligeholdes i forhold til digitaliseringsstrategien et overblik over igangværende projekter i forretningsudvikling og projekt – projektporteføljen.

Applikationsporteføljen og projektporteføljen er sammenhængende, da færdige projektløsninger indgår i applikationsporteføljen ved projektafslutning. Omvendt kan idriftsatte applikationer afføde et behov for fornyelse eller større justeringer, der foranlediger igangsættelse af nyt projekt.

Strategien godkendes af Folkekirkens It's ledelse og revideres som hovedregel årligt.

[1] Kirkenettet dækker over programmer, services og it-udstyr, som er etableret for Kirkeministeriet og de folkekirkelige myndigheder, institutioner og ansatte.
En bruger kan tilgå Kirkenettet fra en Kirkenet-pc, og et udvalg af services kan anvendes fra en privat pc eller mobil enhed.

1 It-målsætninger

1.1 Hvilken it-arkitektur er der brug for?

1.1.1 Behov afledt af digitaliseringsstrategien

1.1.1.1 Grundlæggende it-arkitektur

Der arbejdes mod en platformsuafhængighed på Kirkenettet, og at der leveres it, som understøtter en 'brug dit ejet udstyr'-tilgang ('BYOD'[2]). Der vil ofte blive stillet det krav til it-løsninger, at de fungerer responsivt og kan afvikles på både pc og mobile platforme, jf. afsnit 2 om teknologivalg.

For at kunne opfylde dette skal Folkekirkens It kunne tilpasse arkitekturen og derfor konstant være opmærksom på alt, hvad der rører sig, og i hvilken retning udviklingen går. I forbindelse med anskaffelse af enhver ny løsning skal der være en åben dialog således, at systemerne ikke risikerer uforvarende at blive afhængige af en bestemt teknologi eller udelukkende kan interagere med én type udstyr.

Den til Digitaliseringsstrategien hørende handlingsplan fastlægger, hvilke services og systemer der skal være til rådighed på Kirkenettet.

Der anvendes adskilte udviklings-, test- og produktionsmiljøer, og udvikling må ikke ske i test- og produktionsmiljøer. Test af nye systemer på testmiljøet skal sikre, at de nye systemer er kompatible med allerede eksisterende systemer inden idriftsættelse. Samtidig sikrer Folkekirkens It, at de nødvendige standarder er korrekt anvendte, at dokumentation er til stede, samt at løsningen kan afvikles i et stabilt driftsmiljø.

1.1.1.2 Fleksibel it-infrastruktur

Folkekirkens It skal levere en it-infrastruktur, der hurtigt og sikkert kan tilføjes ressourcer, når der opstår behov herfor. Ligeledes skal der sikkert og hensigtsmæssigt kunne lukkes for systemer, der ikke længere er i brug.

For at sikre, at Kirkenettet har en fleksibel it-infrastruktur, anvendes der ydelser fra flere leverandører.

Det er vigtigt løbende at overveje, hvilke fleksibilitetsbehov ved nye systemer der kan og skal tilgodeses med den bagvedliggende it-infrastruktur.

1.1.1.3 Økonomi og effektivitet

Ved valg af it-arkitektur anvendes en totaløkonomisk betragtning. Det analyseres, hvilken arkitektur og med hvilken fleksibilitet der skal udbydes services og til hvilke produkter. Analysen beror på parametre for tilgængelighed, sikkerhed, brugervenlighed samt hastighed, hvilket er grundelementerne i valget af teknologi og leverandør.

På denne baggrund vælges den arkitektur, som samlet set vurderes økonomiske mest fordelagtig, når der tages højde for ovennævnte parametre samt de

[2] Bring your own device.

medarbejderressourcer, der skal anvendes til udvikling, implementering, drift og vedligehold af arkitekturen.

1.2 Teknologier, der understøtter arkitekturen

På baggrund af ovenstående mål for it-arkitekturen anvender Folkekirkens It den it-infrastruktur, som beskrives i det følgende.

1.2.1 Miljøer/platforme, herunder versioner

For at sikre en stabil drift af it på Kirkenettet leverer Folkekirkens It it på både fysiske servere og virtuelle servere (VMware).

1.2.1.1 Netværk/datalinjer

Kirkenet-pc'er[3], der kobler op på Kirkenettet, bliver godkendt via de på pc'en aktiverede sikkerhedspolitikker. Denne godkendelse skal leveres fra servere, der skal være placeret på to fysisk adskilte lokationer. Endvidere placeres strømnettet også på to fysisk adskilte lokationer med henblik på at sikre høj oppetid for Kirkenettets systemer og services.

Det skal være muligt for de enkelte folkekirkelige institutioner frit at kunne vælge, hvilken leverandør institutionen ønsker til dataforbindelse. Ved hjælp af en VPN-forbindelse skabes automatisk en krypteret adgang til Kirkenettet fra Kirkenet-pc'en.

Folkekirkens It skal til enhver tid kunne levere ydelser og systemer til en aktiv dataforbindelse.

På Kirkenettet skal der være etableret foranstaltninger (firewall), som beskytter den data, der går ind til og ud fra Kirkenettet.

1.2.1.2 Azure

På Kirkenettet anvendes Azure, der er Microsofts cloudcomputing platform. Folkekirkens It vælger mellem Platform as a service (PaaS), Infrastruktur as a service (IaaS) og Software as a service (SaaS)[4] ud fra en samlet vurdering af den mest hensigtsmæssige løsning, når Azure økonomisk og infrastrukturmæssigt vil være det bedste valg.

Azure anvendes til løsninger, hvor der er behov for løbende at op- og nedskalere kapaciteten, eks. Valgsystemet til understøttelse af menighedsrådsvalg, samt til testmiljøer, da Azure giver denne mulighed samt at kunne lukke, når miljøerne ikke anvendes. Endvidere benyttes Azure til produktion i forhold til anvendelse og administration af Office365.

Microsoft Azure Active Directory (Azure AD)-tjenesten anvendes til styring af trust mellem Kirkenettets on premises AD-løsning og AD i Azure. Dette omfatter almindeligt logon og/eller multifaktorgodkendelse, som beskytter Kirkenettets brugere.

---

[3] En Kirkenet-pc er en pc med præinstallerede programmer, som leveres af Folkekirkens It. Kirkenet-pc'er er sikret med kryptering af harddisken.

[4] De forskellige services er nærmere beskrevet i Digitaliseringsstyrelsens Vejledning i anvendelse af cloudservices (juli 2020). Vejledningen ses her.

1.2.1.3 Operativsystemer på servere

Operativsystemer (OS) på servere anvendes i to versioner bagud. En ny version af et OS anvendes først, når den første samlede opdatering foreligger (update 1). Der vil derfor være en kontinuerlig proces med opgradering af servere, der sikrer, at gamle versioner løftes til den seneste godkendte version. Dette vil i perioder medføre, at der kan eksistere op til tre samtidige OS-versioner.

Der anvendes Windows som OS på alle servere i Kirkenettet på nær til hjemmesideservere (se AWS nedenfor), hvor der anvendes en LAMP-konfiguration.

1.2.1.4 Amazon Web Services

I Amazon Web Services (AWS) findes den Linux-baserede cloud-løsning, hvor de offentligt tilgængelige hjemmesider er placeret. Der benyttes hovedsageligt IAAS-løsninger (EC2 og S3) i AWS.

Hjemmesiderne er med placeringen i AWS adskilt fra den øvrige del af Kirkenettet. Dermed minimeres skaden, såfremt hjemmesiderne rammes af vellykkede angreb.

Den daglige drift af AWS-løsningen varetages af en ekstern part, der sørger for patching af de dele, som AWS ikke varetager. Herudover er den eksterne part ansvarlig for backup og overvågning samt den tekniske dialog med AWS.

1.2.2 Påvirkning af it-infrastrukturen

For at sikre et stabilt og sikkert miljø på Kirkenettet vedligeholder Folkekirkens It et overblik over tidspunkter (servicevinduer) for, hvornår hardware og software (OS, Office-pakke m.v.) skal udskiftes.

Dette overblik fremgår af det teknologiske roadmap, som løbende vedligeholdes.

1.3 Udfasning af it-systemer

Det skal sikres, at it-systemer udfases forsvarligt og korrekt, herunder at data håndteres i overensstemmelse med gældende lovgivning, at aflevering sker til Rigsarkivet i henhold til evt. foretagen anmeldelse, og at udgifter til it-systemet ophører.

Folkekirkens It skal sammen med berørte leverandører bistå den forretningsmæssige systemejer med at udarbejde en plan for nødvendige aktiviteter ved udfasning af et it-system.

Ved udfasning og dermed ophør af behandlingsaktiviteter i forbindelse med personoplysninger skal det besluttes i forbindelse med kontraktens ophør, om data behandlet af en leverandør enten skal slettes helt, eller om data skal tilbageleveres, hvorefter eksisterende kopier af data skal slettes.

1.4 Arbejdspladsudstyr

Strategien fastlægger en politik i forhold til arbejdspladsudstyr, der betyder, at det udstyr, som anvendes, skal ses i sammenhæng med, hvad det skal bruges til.

Pc'er og særligt udstyr som attestprintere, der skal tilkobles Kirkenettet, skal anskaffes gennem Folkekirkens It. Øvrigt udstyr kan i nogle tilfælde anskaffes

gennem Folkekirkens It, men også købes hos andre leverandører, eks. multifunktionsprintere.

I udgangspunktet tilbyder Folkekirkens It følgende typer af udstyr:

- Stationære og bærbare pc'er
- Printere
- Andet tilbehør til en it-arbejdsplads, eks. skærme, mus/tastatur, udstyr til videomøder m.v.

Udstyr købes via Kirkenettets bestillingsside. Inden køb kan foretages, skal institutionen have indgået en drifts- og indkøbsaftale med Folkekirkens It samt have tilmeldt sig til PBS-betalingsaftale.

Smartphones og tablets skal institutionerne selv anskaffe uden om Folkekirkens It.

2 Teknologivalg

2.1 Krav til udvikling

Ved udviklingen af applikationer til Kirkenettet skal gældende standarder for tilgængelighed, sikkerhed, brugervenlighed samt hastighed og grafisk konsistens i forhold til brugerfladen overholdes.

Som udgangspunkt skal applikationer kunne anvendes på den type udstyr, som brugeren foretrækker i den givne situation. Dvs. at løsningerne i videst muligt omfang skal være responsive og derved kunne tilpasse sig brugerinteraktionen, så de kan benyttes både på en mobil, en tablet eller en pc. Således sikres den maksimale brugervenlighed i brugen af applikationen.

Udvikling skal ske efter principper, som sikrer god databeskyttelse, hvilket vil sige databeskyttelse gennem design (privacy by design) og databeskyttelse gennem standardindstillinger (privacy by default). Dette skal sikre bl.a. minimering af data med personoplysninger, pseudonymisering, kryptering af data, korte opbevaringsperioder og begrænset adgang til data, jf. Vejledning om Behandlingssikkerhed og Databeskyttelse gennem design og standardindstillinger (Juni 2018).[5]

2.2 Brugerstyring

2.2.1 Brugere på Kirkenettet

Brugeradministrationen i Kirkenettet (AD og MIM) er baseret på informationer fra Kirkenettets Informationssystem (KIS), som indeholder masterdata (stamoplysninger) på sogne, menighedsråd, folkekirkens og Kirkeministeriets personale m.v. Den aktive styring af rettigheder (adgang) til informationer, portaler, filer m.m. sker gennem Microsofts Active Directory (AD).

Oven på AD ligger der en brugeradministrationsløsning baseret på Microsoft Identity Manager (MIM) således, at Kirkenettets sikkerhedsansvarlige selv kan håndtere administrationen af deres egne Kirkenetbrugere.

På Kirkeministeriets og folkekirkens intranet – Den Digitale Arbejdsplads (DAP) – findes en løsning til administration af udvalgsbrugeres[6] rettigheder og adgange.

Brugerstyringen skal - hvor det er muligt - ske via ovennævnte systemer, som nedsætter ekspeditionstiden og minimerer risikoen for menneskelige fejl.

Som udgangspunkt skal systemer i Kirkenettet kunne implementeres med AD. På den måde sikres det, at administrationen af adgangen til systemerne sker via de dertil oprettede brugergrupper. Dette skal ske inden for de krav til single-sign-on, der fastlægges i it-arkitekturprincipperne.

[5] Vejledningen ses på Datatilsynets hjemmeside under Vejledninger.
[6] Udvalgsbrugere er menighedsråds- og provstiudvalgsmedlemmer samt øvrige eksterne brugere med tilknytning til menighedsrådet.

2.2.2 It-medarbejdere og it-administratorer

Styring af leverandørers og Folkekirkens It's adgang til servere og services på Kirkenettet sker med Microsoft-værktøjet Privileged Access Management (PAM) og Privileged Identity Management (PIM). Der tillades kun adgang med unikke brugere, og al adgang logges. Brugerne skal være oprettet i MIM, før de kan få adgang via PAM og/eller PIM.

En bruger fra en leverandør skal forespørge om adgang på forhånd, og i forespørgslen anføres begrundelse for adgangen, tidspunkt for adgangen, samt hvor lang tid adgangen skal være åben med et maksimum på 8 timer. Adgangen opnås først, når den er godkendt af Folkekirkens It.

Enkelte brugere hos Kirkenettets driftsleverandør har direkte adgang via PAM og PIM for at kunne opretholde den løbende drift, men også her skal adgangen begrundes.

2.3 Integrationsteknologier

Som udgangspunkt benyttes der altid en standard til udveksling af data mellem de forskellige systemer, interne som eksterne. Det betyder bl.a., at de systemer, som Folkekirkens It stiller til rådighed, i muligt omfang skal udstille relevante brugergrænseflader (api'er) efter alment anerkendte it-standarder. Læs yderligere om integration i it-arkitekturprincipperne.

2.4 Applikationer og forretningsprogrammel

Applikationer og forretningsprogrammel til Kirkenettet skal af hensyn til videreudvikling, vedligeholdelse og kvalitet, så vidt det er muligt, være standard- og/eller rammesystemer. Det vil som hovedregel også sikre det bedste forhold mellem pris og kvalitet. Det betyder, at særligt systemudvikling, som omfatter mere end konfiguration, begrænses.

I visse tilfælde vil folkekirkens særlige struktur og opgaver tilsige løsninger, som designes og udvikles specifikt til folkekirken. Udvikling af den slags helt nye systemer for folkekirken forudsætter i givet fald en nærmere afgrænsning af projektet, samt at systemet afprøves under kontrollerede forhold og i øvrigt ikke kompromitterer hverken sikkerhed eller databeskyttelse.

Applikationer og forretningsprogrammel anskaffes som hovedregel med tilhørende vedligeholdelses- og opgraderingsaftaler. Overblik over applikationer og forretningsprogrammel fremgår af et applikationsroadmap, som løbende vedligeholdes.

Når der sker systemudvikling, skal nedenstående krav overholdes.

2.4.1 Applikationer med integration i Folkekirkens It's brugerstyring

Applikationer, der har behov for at integrere med Folkekirkens It's brugerstyring, skal udvikles på Microsoft-teknologier. Til dette benyttes primært MS SQL som database, og IIS benyttes som webserver.

Folkekirkens digitale løsninger skal være robuste, stabile i drift, brugervenlige og velfungerende. Derfor baseres digitalisering i folkekirken som hovedregel på

teknologier, der har en vis udbredelse, og på metoder, som er velafprøvede. Det gælder især for administrative systemer på områder, hvor folkekirkens behov er sammenlignelige med andre offentlige institutioners.

Folkekirken skal med andre ord ikke være 'first-mover' med hensyn til ny teknologi – men gerne være dem, der følger lige efter, hvor det giver teknologisk mening i forhold til den øvrige infrastruktur og Strategien. Og hvor det bærende element er, at der direkte eller indirekte er en brugermæssig værdi at hente.

2.4.2 Applikationer, der primært retter sig mod offentligt tilgængelige hjemmesider

De offentligt tilgængelige hjemmesider udvikles i et open source Content Management System, enten i TYPO3 eller NEOS. Disse programmer implementeres på en server konfigureret med Linux/MySQL/PHP.

Disse hjemmesider skal være placeret i et cloud-miljø leveret af en anden leverandør end leverandøren til Kirkenettets øvrige cloud-løsninger og er derfor placeret i AWS. Denne opsplitning er begrundet i et ønske om at minimere risici, såfremt et cloud-miljø bliver utilgængeligt eller udsat for angreb, jf. også afsnit 1.2.1.4.

3 Informationssikkerhed og databeskyttelse

De specifikke retningslinjer, der skal sikre fortrolighed, integritet, tilgængelighed og autenticitet gældende for applikationer og data, er fastlagt i og reguleret af Informationssikkerhedspolitik for Kirkeministeriet og Den danske folkekirke samt Cirkulære om informationssikkerhed for Kirkeministeriet og Den Danske folkekirke.

Politikken og cirkulæret er udarbejdet i henhold til den gældende statslige sikkerhedsstandard, ISO 27001, samt databeskyttelseslovgivningen[7] og gældende vejledninger om informationssikkerhed og databeskyttelse.

3.1 Organisering

Ledelsen i Folkekirkens It har med reference til departementschefen det generelle ansvar for informationssikkerheden på Kirkenettet og træffer beslutning om gennemførelse af overordnede strategiske projekter af informationssikkerhedsmæssig karakter.

For Kirkeministeriet og folkekirken er der udpeget en databeskyttelsesrådgiver og en it-sikkerhedskoordinator, som har fokus på databeskyttelse og informationssikkerhed.

Der er desuden nedsat et informationssikkerhedsudvalg for Kirkeministeriet og folkekirken, som består af repræsentanter fra ledelse og medarbejdere i departement og stiftsadministrationer samt repræsentanter fra en række folkekirkelige organisationer. Kontorchefen for Folkekirkens It er formand for informationssikkerhedsudvalget, mens it-sikkerhedskoordinatoren varetager sekretariatsbetjening af udvalget.

Det forretningsmæssige ansvar er forankret ved system- og dataejere, som ved behandling af personoplysninger endvidere vil være dataansvarlige. Systemejerne bistås af de tekniske systemansvarlige i Folkekirkens It.

I det daglige træffes dispositioner og afgørelser af Folkekirkens It's ledelse, og disse afgørelser effektueres umiddelbart.

3.2 Sikkerhedsniveau – målsætninger

Folkekirkens brug af digitale løsninger skal ske på en tryg og sikker måde, som fastholder den høje tillid, som samfundet har til folkekirken. Folkekirkens mange myndigheder og institutioner skal overholde databeskyttelseslovgivningen og gældende it-sikkerhedsstandarder og -krav.

Et højt digitalt sikkerhedsniveau opnås med en kombination af sikre systemer og sikker adfærd. Folkekirkens It sikrer løbende, at Kirkenettets systemer overholder de gældende sikkerheds- og databeskyttelsesstandarder. Det er

[7] Databeskyttelsesforordningen (Europa-Parlamentet og rådets forordning (EU) 2016/679 af 27. april 2016) samt Databeskyttelsesloven (LOV nr. 502 af 23/05/2018).

samtidig et væsentligt hensyn ved udvikling af nye digitale løsninger, at sikkerhed tænkes ind fra starten, således at brugervenlighed og sikker adfærd indgår i løsningsdesignet.

Sikkerhedsniveauet på Kirkenettet er fastlagt ud fra en risikobaseret tilgang og er beskrevet nærmere i informationssikkerhedspolitikken. Den risikobaserede tilgang betyder, at der er fokus på driften af de mest forretningskritiske processer og it-aktiver samtidig med, at der også er den nødvendige sikkerhed for øvrige processer og aktiver. Der skal implementeres de sikkerhedsforanstaltninger på Kirkenettet, der er nødvendige for at opretholde sikkerhedsniveauet i forhold til det aktuelle trusselsbillede.

Viser en risikovurdering, at sandsynligheden for en sikkerhedshændelse er højere end middel, skal Folkekirkens It – under hensyntagen til de økonomiske forhold og efter aftale med systemejeren – implementere 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 bragt ned på lav.

3.3 Styring – realisering af målsætning

Til styring af arbejdet med informationssikkerhed og databeskyttelse, herunder gennemførelse af risikoanalyser, anvendes værktøjer anbefalet af Statens netværk for informationssikkerhed, Digitaliseringsstyrelsen samt Center for Cybersikkerhed.

Folkekirkens It, særligt it-sikkerhedskoordinatoren, deltager i relevante fora, uddannelser, konferencer m.v. for at sikre, at den fornødne sikkerhedsmæssige viden er til stede for at kunne opretholde et højt sikkerhedsniveau på Kirkenettet.

Ved anskaffelse af nye it-systemer samt ved væsentlige ændringer foretages der en risikovurdering og evt. en konsekvensanalyse.

En systematisk risikovurdering af forretningskritiske processer og de tilhørende it-aktiver foretages årligt, og på baggrund heraf fastlægges behovet for evt. yderligere sikringsforanstaltninger.

Folkekirkens It gennemfører jævnligt informationskampagner og lignende aktiviteter for at øge bevidstheden om informationssikkerhed og databeskyttelse på Kirkenettet og gældende retningslinjer samt for at skærpe bevidstheden omkring eget ansvar for opretholdelse heraf.

3.4 Beredskab og kontrol

Beredskabs- og retableringsplaner skal altid foreligge i et sådant omfang, at forretningskritiske processer kan udføres i videst mulig udstrækning uden sikkerhedsmæssig påvirkning. Planerne skal afprøves løbende for at sikre disses aktualitet.

Gennemførelse af tilbagevendende it-sikkerhedsreviews og kontroller skal sikre den fortsatte overholdelse af gældende standarder og regler.

4 Hvilke opgaver løses internt – hvilke eksternt?

It-ydelser til Kirkenettets brugere leveres af såvel interne medarbejdere i Folkekirkens It som eksterne it-leverandører.

I det følgende beskrives de principper, der fastlægger hvilke it-kompetencer og hvilken opgaveløsning, der er nødvendige at have internt i Folkekirkens It, samt hvilke kompetencer og hvilke typer opgaver der vil blive indkøbt efter behov.

4.1 Principper for anvendelse af interne og eksterne it-kompetencer i Folkekirkens It

Valget af, hvorvidt en given opgave ved Folkekirkens It skal varetages internt eller eksternt, baseres på følgende overordnede princip:

- Opgaver skal løses fagligt forsvarligt og med den lavest mulige omkostning, samtidig med at Folkekirkens It sikres leverancesikkerhed samt reel mulighed for styre og kontrollere de it-ydelser, der leveres til slutbrugerne.

De følgende principper er formuleret for i praksis at støtte realiseringen af det overordnede princip:

- Folkekirkens It vil internt opretholde kompetencer til opgaver hvor:
  - Der kræves stort kendskab til Kirkenettets brugere og dyb viden om arbejdsprocesser.
  - Der forudsættes intern varetagelse for at sikre nødvendig styring og kontrol med de leverede it-ydelser, f.eks. projekt- og leverandørstyring samt sikring af persondata.

- Opgaver, der primært løses internt, er arbejdet med strategi og governance vedrørende Kirkenettet, sikkerhed og databeskyttelse, herunder opfølgning på compliancestatus, supporthåndtering med tilhørende vejledning og uddannelse m.fl.

- Folkekirkens It vil indkøbe ekstern bistand til opgaver kendetegnet ved:
  - Specialistopgaver, hvor Folkekirkens It's størrelse ikke giver kritisk masse til at opretholde den nødvendige kompetence.
  - Standardopgaver, som kan indkøbes billigere end ved intern produktion.
  - Adgang til skalerbare ressourcer med periodisk behov for bistand.

- Opgaver, der typisk søges ekstern bistand til, er vurdering af sikkerheds- og driftsmæssige problemstillinger, juridisk og ledelsesmæssig rådgivning samt udvikling af applikationer. Dertil kommer de forretningskritiske ydelser, der leveres af eksterne it-leverandører inden for flerårige aftaler, herunder drift af store it-systemer som ESDH og løn samt drift af servere.

Efter behov kan den interne opgavevaretagelse suppleres med ekstern bistand.

5 It-Governance

It-governance handler om tilrettelæggelsen af arbejdet med it og digitalisering, særligt når det gælder ansvar, ledelse og organisering. De grundlæggende retningslinjer for it-governance i folkekirken er fastlagt af kirkeministeren i 2017, og omfatter fem hovedprincipper[8]:

1. Kirkeministeriet har ansvaret for Folkekirkens It
2. It-Følgegruppen rådgiver om strategiske it-spørgsmål
3. Brugere inddrages fra først til sidst
4. Folkekirken tager ejerskab for de digitale løsninger
5. Digitale løsninger skal kunne betale sig.

Dette udmønter sig i forhold til Folkekirkens It's daglige arbejde i den tilbagevendende gennemførelse af konkrete styringsaktiviteter, eks. vedrørende sikkerhed og databeskyttelse, hvilket er nærmere beskrevet i afsnit 3, men også vedrørende gennemførelse af projekter og leverandørstyring.

5.1 Gennemførelse af it-projekter

Når projekter helt eller delvist finansieres af fællesfonden er det et krav, at dette sker i henhold til *Retningslinjer for organisering og styring af it-projekter*.

Retningslinjerne bygger på statens it-projekt[9]- og programmodeller[10] samt Økonomistyrelsens vejledninger om it-udviklingsprojekter[11].

Formålet med retningslinjerne er dels at fastlægge de overordnede rammer og principper for organisering og styring og dels at beskrive, hvordan de udmøntes i praksis, herunder opliste de obligatoriske styringsdokumenter, som skal fastholde målsætningen om, at it-projekter forankres i forretningen og herudover sikre, at:

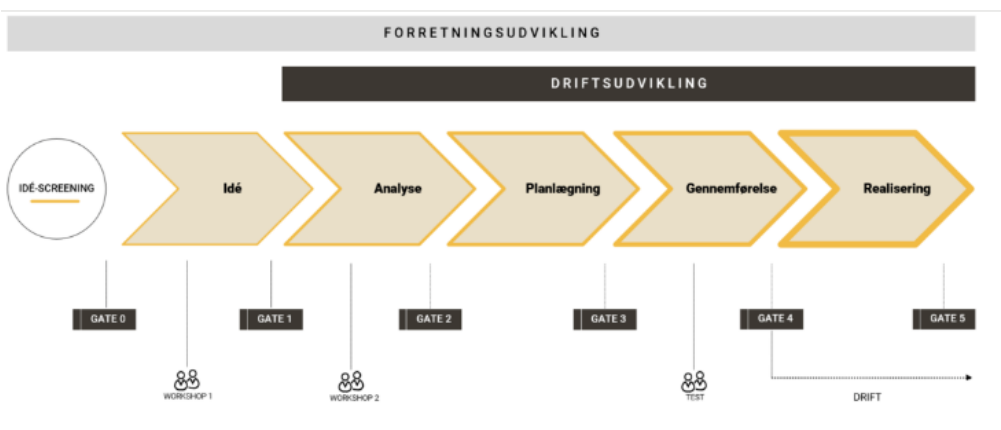
1. Det er tydeligt, hvordan og af hvem beslutninger træffes
2. Der i hele projektperioden sker en løbende opfølgning til projektets styregruppe, samt at
3. Alle omkostninger til et projekt opgøres.

Endelig at det som en del af det samlede projektgrundlag fremgår, hvilke og hvor mange ressourcer organisationen skal bidrage med i udviklingsfasen, hvilke behov der er for at ændre i eksisterende arbejdsgange, samt hvordan organisationens brugere uddannes og trænes.

I forbindelse med større projekter sikres brugerne indflydelse på det færdige resultat ved nedsættelse af en bruger- og/eller referencegruppe.

Projektmodellens faser er; Idé, Analyse, Planlægning, Gennemførelse og Realisering.

[8] De fem hovedprincipper er nærmere beskrevet på Folkekirkens It's hjemmeside.
[9] Vejledning til statens it-projektmodel, Digitaliseringsstyrelsen 2019
[10] Vejledning til den fællesstatslige programmodel, Digitaliseringsstyrelsen 2016
[11] Økonomistyrelsens vejledning om it-udviklingsprojekter



I projektforløbets idéfase skal it-sikkerhedskoordinator og databeskyttelsesrådgiver inddrages med henblik på at sikre forankring og overholdelse af de informationssikkerheds- og databeskyttelsesmæssige retningslinjer og principper i projektet.

Forretningsudviklingsprojekter og driftsudviklingsprojekter følger samme projektforløb. Forretningsudviklingsprojekter forelægges It-Følgegruppen, mens driftsudviklingsprojekter som hovedregel ikke forelægges for It-Følgegruppen, men derimod for Folkekirkens It's ledelse.

For hvert projekt vurderes det, hvilken udviklingsmetode der skal anvendes. Vandfaldsmetoden med forholdsvis få og faste projektfaser kan med fordel anvendes, når det fra start er meget veldefineret, hvad den ønskede løsning er. Agil udvikling med mange og korte udviklingsforløb (sprints) anvendes typisk, hvor det i højere grad er ønskeligt at have fleksibilitet ift., hvordan den endelige løsning skal være. Uanset valg af vandfald eller agil udvikling anvendes traditionel projektledelse som styringsredskab for tid, kvalitet, økonomi samt varetagelse af interessenter og styring af risici. I praksis vil Folkekirkens It typisk anvende en blanding af vandfald og agil udviklingsmetode, jf. også scenarier i Statens It-projektmodel.

Det tilstræbes, at initiativet og ansvaret for nye digitale løsninger og videreudvikling af eksisterende systemer i videst muligt omfang skal forankres hos systemejeren - det sted i folkekirken, som skal drage nytte af et system.

Derfor sidder den relevante enhed i folkekirken med som projektejer, når der skal formuleres krav og specifikationer for en digitale løsning, når den konkrete løsning skal vælges, og når fordele, ulemper og gevinster skal vurderes.

Folkekirkens It understøtter både udvikling og drift med it-faglig bistand på grundlag af tydelige projekt- og leveranceaftaler med den ansvarlige enhed i folkekirken. Folkekirkens It vil således almindeligvis stille en projektleder til rådighed for projekterne.

5.2 Leverandørstyring

Folkekirkens It har et koncept for leverandørstyring, der omfatter følgende:

- Governancemodel for leverandørstyring

- Overblik over relevant dokumentation og information
- Systemunderstøttelse af drift, support, vedligeholdelse og videreudvikling
- Standardisering af leverandørkrav (bidrage til sammenlignelighed og forenkling af leverandørstyringen).
- Gennemførelse af årligt tilsyn med leverandører til den samfundsvigtige funktion, personregistrering, og de forretningskritiske systemer.

Leverandørstyringen understøttes af processer for håndtering af kald, fejl og fejlrettelse, som er baseret på ITIL[12].

[12] ITIL (**I**nformation **T**echnology **I**nfrastructure **L**ibrary) er et koncept for levering af it-serviceydelser.