Bilag til It-Strategi 2010-2012

Arkitekturprincipper

for

Kirkenettet

version 3, feb. 2011

Itk-dnr.: 7755-11

Indholdsfortegnelse

Arkitekturprincipper for Kirkenettet
Vedtaget af It-Styregruppen d. 3. Februar 2011,
Itk-Dnr.: 7755-11

Kirkeministeriets IT-Kontor

Rådhusstræde 2 1466 København K

it-kontoret@km.dk www.kirkenettet.dk

1 It-strategiens arkitekturgrundlag

Nærværende arkitekturprincipper er udviklet i samarbejde med Rambøll Management og er gældende for Kirkenettet.

IT- og Telestyrelsens publikationer/hjemmeside med krav og anbefalinger vedrørende it-arkitektur og brug af standarder er fundamentet for de 27 principper, der er gældende for nyanskaffelser og systemudskiftninger i Kirkenettet.

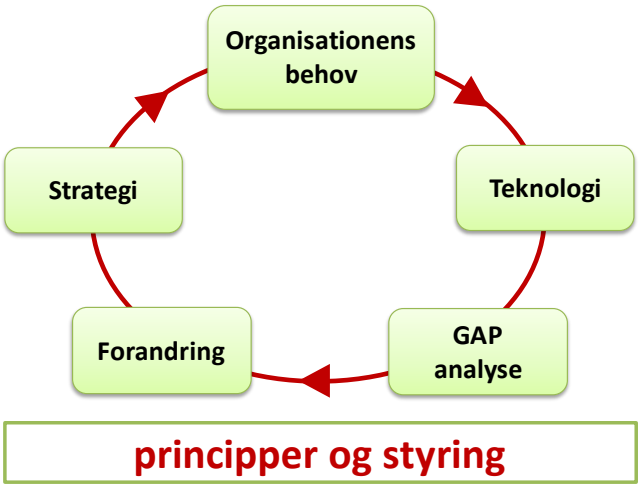
Principperne skal følges i forbindelse med anskaffelser og ændringer af en eksisterende løsning.

I forbindelse med alle projekter skal projektejer sikre, at projektet efterlever principperne, og skal redegøre herfor over for It-Kontorets ledelse.

En projektejer kan indstille til It-Kontorets ledelse, at et eller flere principper fraviges. Baggrunden skal forklares og dokumenteres efter tesen "følg-eller-forklar".

En sammenhængende forretnings- og it-arkitektur er en forudsætning for at kunne realisere det fulde potentiale ved den samlede digitaliseringsindsats.

1.1 Grundlaget for arbejdet med arkitektur



Grundlaget for arkitekturen er Kirkeministeriets og folkekirkens opgaver (strategi og forretning i figuren herover), som beskrives i helt overordnet.

Denne beskrivelse er grundlaget for retning og midler i forhold til Kirkenettet henholdsvis til systemer, der i øvrigt anvendes i Kirkeministeriet og folkekirken, og som skal kommunikere (udveksle data) med Kirkenettet.

1.2 Kirkeministeriets og folkekirkens opgaver

Kirkeministeriets kerneopgaver er betjening af ministeren og ledelse af ministerområdet med udfærdigelse af lovgivning, administration af love og regler og den overordnede styring af de myndigheder, som hører under ministeriet. Kirkeministeriet skal understøtte folkekirken ved at sikre rammer og vilkår, der fremmer kirkens liv og vækst

Folkekirken er på den ene side underlagt de samme regler, som man skal administrere efter i offentlige myndigheder. Som en konsekvens heraf tager it-strategien sigte på, at arbejdet med de administrative opgaver sker på grundlag af fælles centralt styrede løsninger og efter regler og principper, som gælder for den offentlige forvaltning

Når der på den anden side er tale om kirkens egentlige opgaver, så tager strategien sigte på, at den infrastruktur, som understøtter de administrative løsninger, også kan være et fundament for at bruge it i det kirkelige og pastorale arbejde og dermed til evangeliets forkyndelse, sakramenternes forvaltning, oplæring i kristendom m.m.

Den folkekirkelige organisation med sogne (menighedsråd), provstier (provstiudvalg), stifter (stiftsråd) og parallelt hermed ministeriet er udgangspunktet for arbejdets organisering og tilrettelæggelse.

It-understøttelse af de administrative opgaver kræver forretningsgange, informationer og systemer til:

- styring og opfølgning på aktiviteter og økonomi
- understøttelse af folkekirkens organisation, herunder information om de organisatoriske enheder
- administration af folkekirkens ansatte og de folkevalgte
- administration Kirkeministeriets organisation og ansatte
- personregistrering og registrering af kirkelige hændelser.

Personregistreringen, som folkekirken udfører, omfatter den grundlæggende registrering af danske borgere med fødsel, civilstandsændring, død og begravelse. Det er opgaver, der har indgribende juridiske konsekvenser for den enkelte borger, og der er krav om en ensartet registrering af høj kvalitet. Der tilmed tale om følsomme oplysninger, hvilket stiller høje krav til sikkerheden.

De ovennævnte opgaver løses i en struktur med mere end 2.000 sogne, 107 provstier, 10 stifter og Kirkeministeriet. Desuden indgår opgaver med personregistrering i Sønderjylland, hvor det er kommunerne, som varetager opgaven, men ved hjælp af folkekirkens system.

Der er mere end 4.500 ansatte, som har adgang til Kirkenettet, og mere end 17.000 folkevalgte, der anvender systemer med tilknytning til Kirkenettet. Personregistreringen omfatter mere end 5 millioner borgere.

Hovedopgaverne i ministeriet og i folkekirken er på tværs af den organisatoriske struktur illustreret i figuren:

Politik	**Folkekirkelige opgaver**	**Intern administration**	**Person-registrering**
Lovgivning og relationer til Folketinget og offentligheden	*Tro og kirke, personale og økonomi*	*Kirkeministeriets personale og økonomi*	*CPR og Den elektroniske Kirkebog*

Til at løse de nævnte opgaver er der etableret arbejdsgange, et sæt af fælles begreber og it-understøttelse med en række systemer.

Hovedopgaverne understøttes it-mæssigt således:

- Politik understøttes gennem brug af ESDH-, ledelsesinformations- og statistiksystemer.
- Personregistrering understøttes af CPR, Den elektroniske Kirkebog og personregistrering.dk.
- Folkekirkelige opgaver understøttes af It-Skrivebordet, løn-, økonomi- og ESDH-systemer.
- Intern administration understøttes af løn-, økonomi- og ESDH-systemer.

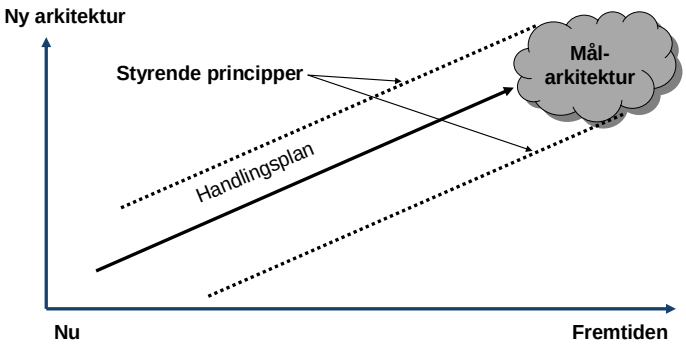
Desuden understøttes alle hovedopgaverne af generelle kontorstøtteværktøjer, e-mail, intranet, ekstranet og internet. Hertil kommer systemer som KIS (Kirkenettets InformationsSystem), der leverer data om struktur, institutioner og personer til systemer i alle hovedopgaver, og endvidere OIM, som bruges af de sikkerhedsansvarlige, og som automatiserer dele af brugeradministrations-processen.

1.3 Byplanskitse

En byplan for Kirkenettet består af en målarkitektur, et sæt principper, der er styrende for anskaffelserne og it-udviklingen, samt - efterhånden som nye projekter eller moderniseringer af eksisterende fagsystemer sættes i værk - en handlingsplan for at nå fra "nu-tilstanden" til den ønskede målarkitektur.

Kirkeministeriets og folkekirkens opgaver, som de er beskrevet i It-Strategi 2010-12, understøttes i it-mæssig henseende af Kirkenettet, der i denne forbindelse skal opfattes som den samlede it-infrastruktur, som Kirkeministeriet og alle folkekirkens godt to tusinde institutioner anvender.

Afhængigt af opgaverne er der fra de enkelte it-arbejdspladser adgang til relevante fagsystemer. For sognenes vedkommende eksempelvis til CPR og Den elektroniske Kirkebog.



1.4 Målarkitektur og styrende principper

Målarkitekturen er et udtryk for, hvor organisationen vil hen med it-arkitekturen. Det er et langsigtet mål, som ikke skal nås på én gang, men ved at alle projekter, der involverer it-teknologi, overholder en række styrende principper.

Den fremtidige arkitektur er nedenfor beskrevet gennem et sæt af egenskaber, der konkretiserer, hvordan de 7 standarder og de retningslinjer, som er gjort gældende fra 1. januar 2008, såvel som de generelle principper i Regeringens Hvidbog om it-arkitektur, udmøntes i Kirkenettet.

Der er fokus på de grundlæggende forhold, som alle systemer skal leve op til, og som skal vurderes i forhold til ethvert system, der anskaffes eller ændres. Der kan være tale om, at nogle systemer skal leve op til skærpede krav på nogle områder.

Arbejdet med arkitektur skal ses i tæt sammenhæng med:

- sikkerhedsarbejdet efter DS484
- brugen af metoder (som eksempelvis ITIL)
- den anvendte projektmodel.

2 Principper for arkitektur i Kirkenettet

Ønsket om og behovet for at effektivisere processerne ved frit at kunne udveksle data og få systemerne til at interagere samt de obligatoriske krav om anvendelse af en række nærmere fastsatte standarder har resulteret i opstillingen af en række principper, som *skal* inddrages ved nyanskaffelser og større ændringer af eksisterende fagsystemer.

Efterlevelse af principperne skal medvirke til, at Kirkenettet kan interagere med omverdenen, at data kan udveksles, samt at Kirkenettet kan leve op til målsætningerne i *Digitaliseringsstrategien*[1].

2.1 Krav om fleksible it-strukturer

De alment gældende krav om fleksibilitet og omstillingsparathed, der præger disse årtier, gælder i fuldt omfang også i Kirkeministeriet og folkekirken.

Samlet set er der tale om, at folkekirken, som alle andre organisationer, har taget teknologien til sig i bestræbelserne på at betjene borgere og medlemmer bedre, men også med det formål at udnytte egne ressourcer mere effektivt.

Kirkenettets fagsystemer og infrastruktur skal derfor struktureres, så de kan understøtte opgaver og fremadrettet udvikling.

Fagsystemerne, der benyttes i de 4 hovedområder[2], skal karakteriseres og bedømmes i forhold til, hvordan arbejdet i hovedområderne forventes at udvikle sig. Derud fra kan det fastlægges, hvilke services, der er fælles for mange arbejdsprocesser, og hvilke der er specifikke for det enkelte område, og man kan fastlægge forandringspotentialet og levetiden for de enkelte fagsystemer og services.

Helt konkret blev det i forbindelse med indførsel af det nye KIS bestemt, at

- KIS' opgave er at levere data om strukturer, institutioner og personer til alle andre fagsystemer
- KIS skal håndtere understøttelse af en fleksibel organisationsstruktur.

Med hensyn til udviklingen i personregistrering er digitalisering af

- borgernes kommunikation med personregisterførerne
- udvekslingen af oplysninger med sygehuse (regioner) og kommuner

en del af den moderniseringsproces, der resulterer, i at et nyt CPR-system og en elektronisk Kirkebog sættes i drift i løbet af 2011.

Endelig har udviklingen i de folkekirkelige opgaver resulteret i et nyt intranet, Kirkeårsportalen (idriftsat oktober 2010), og et projekt til integrationen mellem de fagsystemer, der anvendes til styringen af den lokale økonomi (sogne og provstier) (planlagt til januar 2011).

[1] Strategi for digitalisering af den offentlige sektor 2007-2010, www.modernisering.dk

[2] Kirkeministeriet, stifterne, provstierne og sognene

1. Princip	Systemanskaffelser vurderes i forhold til applikationslandkort
Definition	Systemanskaffelser og forbedringer vurderes i forhold til et samlet service-, applikations- og integrationslandkort.
Begrundelse	Kirkeministeriets og folkekirkens opgaver skal i stigende grad kunne løses sammenhængende og fleksibelt.
Konsekvens	Enhver service og applikation skal leve op til krav om udveksling af data og/eller indgå i en sammenhængende brugergrænseflade. Service-, applikations- og integrationslandkortene skal opdateres af projekter, der tilføjer eller fjerne systemer, services eller applikationer. Ansvaret er projektlederens.

2. Princip	Levetid og forandringsbehov
Definition	Hver service og applikation karakteriseres med levetid og forandringsbehov.
Begrundelse	Kravene til en service og applikation vil afhænge af, hvor lang levetid den har, og hvilke løbende forandringsbehov, den forventes at have.
Konsekvens	Vurdering af levetid og forandringsbehov skal indgå i opstillingen af krav til applikationen. Lang levetid eller højt forandringsbehov medfører højere krav til overholdelse af it-arkitekturprincipperne. Ved enkle løsninger med kort forventet levetid kan arkitekturprincipperne lettere fraviges. Hvis principperne er blevet fraveget, og levetiden viser sig at være længere end forventet, udestår der en tilpasningsopgave.

3. Princip	Genbrug før indkøb - standardløsninger før egenudvikling
Definition	Genbrug løsninger, før der indkøbes løsninger. Indkøb standardløsninger, før der udvikles egne løsninger.
Begrundelse	Eksisterende løsninger har ofte funktionalitet, som ikke udnyttes, og den skal udnyttes, før der anskaffes nye løsninger. Man kan opnå større fleksibilitet ved at anvende standardløsninger, hvor egenudviklede løsninger ofte vil rette sig mod en meget konkret opgave og derfor ikke kan genbruges.
Konsekvens	Ved enhver analyse af behov skal det for hele opgaven og for delopgaver vurderes, om der allerede findes løsninger i Kirkenettet, og/- eller om der findes standardløsninger.

4. Princip	Udnyt standardsystemerne bedre
Definition	Standardsystemerne skal udnyttes bedre og mere effektivt.
Begrundelse	Der anvendes mange standardsystemer som Office, hvor kun en del af mulighederne udnyttes. Der kan opnås gevinster ved at udnytte disse systemer bedre.
Konsekvens	Før der anskaffes nye systemer, skal det undersøges, om eksisterende systemer kan anvendes. Eksisterende systemer skal periodisk underkastes en undersøgelse af, om de kan anvendes bedre. For at en god udnyttelse kan sikres, skal følgende overholdes: - Uddannelse af kernebrugere / superbrugere af systemerne skal sætte disse i stand til at anvende systemerne mere effektivt, mere innovativt og til flere formål. - Periodisk og systematisk opsamling af forbedringsønsker og oplevede problemer skal danne grundlag for f. eks. uddannelse og tilpasninger med henblik på mere effektiv systemudnyttelse.

5. Princip	Strømlign arbejdsgange og/- eller struktur før digitalisering
Definition	Genstanden for et it-projekt, eksempelvis en arbejdsgang eller en struktur, skal simplificeres, før it-understøttelse udvikles.
Begrundelse	Ikke alene er der brug for et billede af målarkitekturen på it-niveau, men også for målarkitekturen på forretningsniveau. Dermed mindskes risikoen for at "asfaltere den slagne vej", hvor en ny vej er ønsket. Enklere arbejdsgange eller strukturer er ofte billigere at it-understøtte end mere komplicerede. Når først it-understøttelsen er på plads, er det typisk dyrere at ændre arbejdsgange eller strukturer.
Konsekvens	Før der anskaffes nye systemer, skal det undersøges, om det er relevant og muligt at omlægge arbejdsgange eller at simplificere strukturer.

6. Princip	Fuld it-understøttelse er ikke nødvendigvis god it-understøttelse
Definition	Fuld it-understøttelse kan have væsentligt større total-omkostninger og medføre flere afledte problemstillinger end en mindre komplet understøttelse.
Begrundelse	At få indarbejdet alle specialtilfælde, eksempelvis undtagelser i den folkekirkelige struktur, er dyrere og modarbejder princippet om at udnytte standardsystemer bedre.
Konsekvens	Estimer totalomkostningen ved at understøtte 95 % - 98 % af opgaven med it i stedet for at gøre det 100 %. En it-løsning, der ikke dækker fuldt ud, kræver løbende en manuel indsats. Omkostningen til denne og risikoen for fejl i behandlingen skal afdækkes for at skaffe et fuldt overblik over økonomien for

	Kirkeministeriet og folkekirken og for samfundet.

7. Princip	**En systemejer er ansvarlig for projektet efter færdiggørelse**
Definition	Systemer skal forvaltes efter leveranceforløbet for at sikre gevinst-realisering og fortsat opgaveunderstøttelse, det er systemejerens ansvar.
Begrundelse	It-projekter skaber sjældent værdi i sig selv, men kræver opfølgning og fokus på den organisatoriske implementering, før formålet med projektet er opfyldt, og gevinsterne er realiseret.
Konsekvens	Systemejeren skal udpeges som en del af projektforløbet.

8. Princip	**Brug fællesoffentlige komponenter**
Definition	Løsninger, der er rettet til borgere, virksomheder og andre myndigheder, anvender fællesoffentlige komponenter.
Begrundelse	Der er etableret en række fællesoffentlige komponenter, som kan bruges i Kirkenettet.
Konsekvens	I Kirkenettet skal anvendes fælles komponenter som NemID, NemLog-in m.fl.

2.2 Krav om samspil mellem it-services

Ministeriets og folkekirkens opgaver medfører, at der vil være krav til it-systemerne om samspil med andre myndigheder og andre parter i det hele taget. Nogle opgaver løses i tæt samspil med andre, nogle andre opgaver kræver information fra atter andre, og hertil kommer, at der også skal leveres information.

Det politiske arbejde betyder samarbejde om folketingsspørgsmål.

Personregistrering indebærer et samarbejde med kommunerne, regionerne (sygehusene), Sundhedsstyrelsen og med CPR-Kontoret.

Også inden for eget område er der stigende krav til samspil mellem systemerne.

For at kunne indgå i samspil med andre skal der dels være krav til snitflader og kommunikation, dvs. transportvejene, dels krav til indholdet i det kommunikerede, dvs. betydningen og semantikken. Kombinationen realiserer Hvidbogens arkitekturprincip om interoperabilitet.

2.3 Snitflader, kommunikation og datakilder

Service- og applikationslandkortet er opdelt i en række områder, der er forskellige med hensyn til snitflader og kommunikationsmuligheder:

- Kirkenettet, der er et lukket netværk med mulighed for såvel synkron som asynkron kommunikation.
- CPR's og Den elektroniske Kirkebogs fælles platform og lukket netværk
- Partnere som sygehuse og kommuner er tilgængelige over åbne netværk.

For hver udveksling af oplysninger mellem systemer skal der tages stilling til, hvilken grad af pålidelighed opgaven kræver for kommunikationens gennemførsel, og hvilken grad af sikkerhed der skal til for at sikre, at data er ens på begge sider af kommunikationen. Dette repræsenteres som et integrationslandkort, som med basis i service- og applikationslandkortet fokuserer på at specificere kommunikationen.

9. Princip	**Kommunikation mellem hovedopgaver baseres på Kirkenettet**
Definition	Kommunikationen mellem services, applikationer og klienter skal baseres på Kirkenettet, som er Kirkeministeriets og folkekirkens sikrede netværk.
Begrundelse	Kommunikationen skal overholde høje krav til sikkerhed, hvilket ligger til grund for opbygningen og den fortsatte udvikling af Kirkenettet.
Konsekvens	Kirkeministeriets og folkekirkens systemer kommunikerer via Kirkenettet. Da størstedelen af kommunikationen samles i dette område, vil der blive - øget behov for udveksling af information (her skal der anvendes en vifte af teknologier) - øget behov for tidstro udveksling af information; webservices frem for eller i samspil med batch (natlige ajourføringer). Der vil blive større krav til pålideligheden og dermed mere overvågning af processerne. Det betyder krav om at skabe et samlet overblik og senere et ansvar for udvekslingsopgaver.

10. Princip	**Sikker opkobling til systemer uden for Kirkenettet**
Definition	Systemer, som drives uden for Kirkenettet og anvendes af brugere i Kirkenettet (f. eks. CPR/Den elektroniske Kirkebog og FLØS (Folkekirkens LØnService), skal forbindes med Kirkenettet med tilstrækkelig sikkerhed og kapacitet.
Begrundelse	Kommunikationen skal overholde høje krav til sikkerhed, og disse krav skal også sikres, hvor systemet drives af tredjepart, og hvor der etableres forbindelse fra Kirkenettet til systemet f. eks. over internettet.
Konsekvens	Afhængigt af teknologiske krav, anvendelse og krav til sikkerhed kan der etableres forskellige typer af forbindelser: - en sikret tunnel mellem Kirkenet og et eksternt driftscenter - en direkte opkobling fra de enkelte klienter til systemet. Der skal i hvert enkelt tilfælde ske en grundig vurdering af behov og muligheder, før der vælges en løsning.

11. Princip	**Personregistrering udføres i samspil med CPR-applikationer.**
Definition	Personregistrering udføres gennem tæt og synkron kommunikation med CPR-applikationer.
Begrundelse	Opgaverne i personregistrering ligger i tæt forlængelse af CPR-kontorets opgaver om at vedligeholde og formidle CPR-oplysninger.
Konsekvens	Platform og kommunikation i forbindelse med personregistrering aftales sammen med CPR-kontoret. Dette krav er vigtigt for at fastholde beslutningen om at optræde som én kunde i forhold til markedet.

12. Princip	Eksternt system til system-kommunikation (B2B) baseres på SOAP og/- eller REST webservices
Definition	System til system-kommunikation med eksterne parter baseres på SOAP- og/ eller REST-webservices efter anbefalinger fra ITST.
Begrundelse	Ved at stille services og data til rådighed på en åben fællesoffentlig platform skal der i Kirkenettet kun vedligeholdes én type snitflader og én kommunikation med andre. Desuden skal krav om anvendelse af åbne standarder efterleves (B103). Ved system til system- kommunikation med særlige behov (f. eks. store datamængder) skal der tages stilling til, om der kan anvendes andre løsninger, hvis SOAP-og/ eller REST-webservices ikke kan klare opgaven tilfredsstillende.
Konsekvens	Dette krav vedrører den kommunikation, der sker på systemniveau mellem systemer. Der stilles krav til eksterne samarbejdsparter om at efterleve disse standarder, herunder anvendelsen af XML, som er en del af SOAP- og REST-webservices-anbefalingerne. Valget mellem SOAP og REST skal foretages via afvejning af projektets nonfunktionelle krav, herunder sikkerhed. Der stiles efter en afvikling af hidtidige løsninger på dette område som kommaseparerede filer, ODBC m.v. For kommunikation med særlige behov, f. eks. overførsel af data til ledelsesinformation, kan der blive brug for at anvende andre standardiserede løsninger. Såfremt kommunikationen indeholder personfølsomme oplysninger, skal den foregå enten via en sikret tunnel, via direkte netværk eller ved kryptering af beskeden gennem anvendelse af et OCES-certifikat.

13. Princip	Data skal læses fra og opdateres i masterdata-kilden.
Definition	I et miljø med mange datakilder, der kommunikerer med hinanden, skal det sikres, at disse data vedligeholdes konsistent via en masterdata-tilgang.
Begrundelse	Der er brug for at sikre konsistente data, og for at disse er aktuelle. Det kræver, at disse data opdateres i og læses fra samme kilde.
Konsekvens	KIS indeholder masterdata for ansatte og folkevalgte, installationssteder og folkekirkelig struktur. OIM indeholder masterdata for brugernes stillinger og de sikkerhedsansvarlige. Data om brugere og installationssteder vedligeholdes autoritativt i KIS. For at være sikker på, at KIS afspejler de seneste data, skal data, der ændres andre steder, opdateres rettidigt i KIS.

	Data om den folkekirkelige struktur vedligeholdes manuelt efter forskrifterne. Kopier af data anvendes kun til læseformål. I det omfang kopidata er nødvendige for f. eks. performance, skal disse opdateres fra masterdata-kilden så hyppigt, at data efterlever de forretningsmæssige krav om korrekthed.

2.4 Betydning - semantik

Udveksling af information mellem systemer kræver, at informationsindholdet er standardiseret og struktureret.

I forhold til personregistrering er der er en høj grad af strukturerede data. Ligeledes er data om strukturer, institutioner og personer i Kirkeministeriets og folkekirkens opgaver i høj grad standardiseret.

Der kan forventes et øget behov for statistik og ledelsesinformation, blandt andet til brug på web, hvilket medfører et behov for standardisering af data på tværs i Kirkeministeriet og folkekirken.

14. Princip	**Veldefinerede oplysninger i dataudvekslinger**
Definition	Betydningen af oplysninger i dataudvekslinger skal være veldefinerede.
Begrundelse	Udveksling af data mellem systemer kræver, at data kan genbruges direkte eller konverteres automatisk, hvilket i begge tilfælde kræver, at data er entydigt defineret på tværs af systemerne.
Konsekvens	En klar og konsekvent organisering af: - ejerskab til information og dens repræsentation i data - definition af informationers betydning og af datasyntaks herunder eventuelt datasammensætning til information - informationers klassifikation (taksonomi og begrebsmodel) - datas struktur og relationer (datamodel) - datas placering i tilgængelige metadataløsninger. Overstående skal dokumenteres for nye systemer og integrationer mellem systemer.

15. Princip	**XML og OIOXML**
Definition	Der skal anvendes XML og OIOXML som datastandardiseringssprog.
Begrundelse	Brug af en åben standard gør, at data og dataudvekslinger kan genbruges fra system til system. Løsninger kan baseres på standardspecifikationer og teknologi frem for at blive opfundet fra gang til gang.
Konsekvens	Der skal anvendes OIOXML i kommunikation med eksterne parter/systemer

	- mellem Kirkenettet og eksterne parter (It-Kontoret skal arbejde for at der skabes sådanne standarder, hvor de ikke findes) - internt i Kirkenettet anvendes OIOXML, hvor der er OIOXML-standarder hvorimod der internt i Kirkenettet - indtil videre - kan anvendes CSV-filer til ajourføring.

2.5 Sikkerhed

Kirkeministeriets og folkekirkens hovedopgaver betyder krav om, at information, særligt vedrørende personer (CPR og Den elektroniske Kirkebog), kun kan ses og anvendes af personer og systemer, der har adkomst dertil. Dermed er kravene til sikkerhed af stor betydning, og Kirkenettets implementering heraf skal være veludviklet.

Services og applikationer er placeret i 2 hovedsikkerhedsdomæner:

- Kirkenettet, hvor de organisatoriske og fysiske sikkerhedsforanstaltninger er beskrevet i *Cirkulære om sikkerhedsforanstaltninger i Kirkenettet*.
- CPR's og Den elektroniske Kirkebogs net, hvor sikkerhedsforanstaltningerne er beskrevet i "*Vilkår for CPR online til offentlige*" o.a. vilkår for enkelte produkter.

Hvert domæne kan have yderlige opdelinger, hvilket skal beskrives (f.eks. demilitariserede zoner).

På Kirkenettet eksisterer i dag en gruppemodel for brugere, der anvender services og applikationer, indeholdt i MS Active Directory, vedligeholdt via ILM og OIM. I den forbindelse skal følgende dokumenteres

- hvordan en persons rettigheder kommunikeres til den service eller applikation, der realiserer funktionaliteten
- i hvilket omfang der er brug for digital medarbejdersignatur i forbindelse med eksempelvis personregistering.

På samme måde karakteriseres hver service eller applikation på landkortet, hvor der sker udveksling af oplysninger.

Ud fra dette skal It-Kontoret evaluere sine sikkerhedszoner og beskrive, hvordan *integritet, fortrolighed, sporbarhed og uafviselighed* realiseres dels for hver zone, dels mellem zonerne, dels i forhold til eksterne parter. Eksempelvis sikres integritet og fortrolighed mellem klienterne på kirkekontorerne, og service og applikationer på Kirkenettet gennem VPN.

Der kan forventes stigende krav til sikkerhed, og det kan betyde krav om

- øget sikkerhed ved log-in (f. eks. ved brug af NemLogin)
- øget sikkerhed i det interne net ved
  - at skærpe kravene til pc'er, PDA, mobiltelefoner (dette skal sikre mod, at uvedkommende får adgang til udstyret, til at se data eller til at lave angreb på systemerne)
  - yderligere at opdele Kirkenettet i zoner, så adgangen til systemerne ikke alene afhænger af log-in, men også af netværkets opdeling.

16. Princip	Beskyttelse gennem veldefinerede sikkerhedszoner.
Definition	Kirkenettets services og applikationer beskyttes mod fjendtlig indtrængning gennem et antal veldefinerede sikkerhedszoner.
Begrundelse	Kirkenettets services og applikationer stiller meget forskellige krav til sikkerheden – og meget høje krav på nogle områder. Desuden er den fysiske afgrænsning til Kirkenettet ikke tilstrækkelig til at håndtere behovene – flere applikationer tilgås over internettet, ligesom der skal være adgang til Kirkenettet "udefra". For at kunne håndtere både den meget høje sikkerhed og på den anden side fleksibiliteten og et overkommeligt ressourceforbrug, deles netværket op i et antal sikkerhedszoner, hvor hver zone kan modsvare et behov.
Konsekvens	Det enkelte system skal overholde reglerne for den sikkerhedszone, det er placeret i.

17. Princip	Høj sikkerhed i kommunikation til CPR og Den elektroniske Kirkebog gennem kryptering
Definition	Der skal være høj sikkerhed i kommunikationen fra arbejdspladserne til Personregistrering, hvilket skal opnås ved kryptering.
Begrundelse	Sikkerhedskravene til Personregistrering er meget høje og kræver stor sikkerhed for personregisterførerens adgang til systemet og sikrer samtidig mod andres uretmæssige adgang dertil.
Konsekvens	Kommunikationen mellem personregisterførernes arbejdspladser og systemet skal være krypteret.

18. Princip	Sporbarhedslogning af brugen af systemer
Definition	For alle systemer skal der udføres en sporbarhedslogning af grupperne personregisterførere, borgere og administratorer.
Begrundelse	Uanset hvor sikkert et system er, vil der være risiko for uretmæssig anvendelse. Det er derfor vigtigt, at alle hændelser logges, og at loggen overvåges og analyseres, så misbrug opdages og efterforskes.
Konsekvens	For ethvert system skal der ske en vurdering af niveauet for logning, analyse og kontrol i forhold til en vurdering af risiko for og konsekvens af sikkerhedsbrud. For kritiske systemer som CPR og Den elektroniske Kirkebog skal der gennemføres systematisk analyse og kontrol af loggen. Ansvaret for logning samt overvågning og analyse af loggen skal placeres, og der skal udarbejdes et regelsæt, så det sikres, at overvågningen gennemføres. Der skal være funktionsadskillelse mellem anvendelsessiden af et system

	og log-arbejdet.
19. Princip	**AD er kernesystem i brugerstyringen**
Definition	Microsoft Active Directory (AD) håndterer data om brugere og adgangskontrol, og andre systemer skal anvende data og eventuelt adgangskontrol.
Begrundelse	Med de mange tusinde brugere af Kirkenettets systemer vil det give et for stort ressourceforbrug at skulle administrere brugerne i hvert enkelt system. Det er desuden et sikkerhedsmæssigt krav, at brugere ændres og slettes, når deres adkomst til Kirkenettets systemer ændres (stillingsskift, fratrædelse). Desuden skal brugernes log-in til systemerne begrænses af hensyn til brugervenligheden.
Konsekvens	Kommende nye applikationer indkøbes med krav om brug af AD som minimumsbrug af brugerdata fra AD og så vidt muligt adgangskontrol via NemLogin.

20. Princip	**Der anvendes medarbejdercertifikater (OCES) til sikring af brugernes identitet**
Definition	Til autenticitetssikring i log-in til Kirkenettet anvendes snarest muligt NemLogin.
Begrundelse	Flere og flere medarbejdere skal tilgå eksterne systemer, hvor log-in med medarbejdercertifikat er krævet. Til udveksling af sikker mail er det også nødvendigt med medarbejdercertifikat. De store krav til sikkerheden i Kirkenettet og det stigende antal sikkerhedstrusler nødvendiggør en skærpet sikkerhedsindsats. Med indførelse af medarbejdercertifikater tilføjes et ekstra element til sikkerheden (ud over brugernavn og password). Ved at bruge medarbejdercertifikater til log-in generelt vil brugerne ikke skulle håndtere flere forskellige log-in-situationer.
Konsekvens	Der skal etableres en effektiv udrulning og administration af medarbejdercertifikater som en del af brugeradministrationen. Brugerne skal uddannes til at håndtere medarbejdercertifikaterne. *Identiteten* af brugeren sikres under udleveringen af medarbejder-certifikater. *Autentificeringen* af brugeren over for systemet sker via medarbejder-certifikater. *Autorisationen* af brugeren sker i forhold til hans/hendes stilling.

21. Princip	Der skal være særlig fokus på sikkerhed ved enhver forandring i it-systemerne
Definition	Ved hver ændring af en eksisterende service eller applikation og hver nyanskaffelse skal der være særligt fokus på sikkerheden.
Begrundelse	Særligt ved ændringer i systemer og ved nyanskaffelser opstår der erfaringsmæssigt sikkerhedsmæssige risici, som det kræver opmærksomhed at undgå.
Konsekvens	Der skal ved enhver ændring og nyanskaffelse ske en sikkerhedsmæssig vurdering og planlægning af sikkerhedstiltag.

2.6 Driftssikkerhed

Kirkeministeriets og folkekirkens hovedopgaver betyder krav om, at opgaverne udføres kontinuerligt og 24/7/365 dvs. på alle ugens dage herunder søn- og helligdage.

Det stiller krav om stabilitet og kapacitet i centrale systemer og i Kirkenettet, dog således at der er forskellige krav og muligheder i de forskellige dele af det samlede system.

Der er brug for at sikre, at løsninger og data er tilgængelige efter nedbrud.

Der er også brug for at sikre adgangen på længere sigt til løsningerne og dermed sikre mod, at opgaver ikke vil kunne blive løst ved en leverandørs ophør. Ud fra en risikovurdering må der sikres f. eks. garantier fra leverandører, udlevering af kildekode eller deponering af kildekode.

22. Princip	Monitorér og estimér belastning
Definition	It-Kontoret monitorerer og estimerer belastningen af Kirkenettets services og applikationer.
Begrundelse	For at undgå overbelastning og dermed manglende adgang til applikationer skal belastningen løbende overvåges, og det skal desuden løbende estimeres, hvordan belastningen kan forventes at udvikle sig, særligt i forbindelse med nyanskaffelser og andre ændrede forudsætninger.
Konsekvens	For hver gruppe, karakteriseret ved rettigheder til at anvende en eller flere services eller applikationer, anslås volumen i gruppens aktiviteter, og hvilken variation over tid It-Kontoret forventer i disse aktiviteter. Herudfra anslås, hvorledes Kirkenettets systemer forventes belastet.

23. Princip	Performancekrav til alle services og applikationer
Definition	It-Kontoret opstiller konkrete performancekrav til alle sine services og applikationer. Performancekravene er Svartid: Fra brugeren aktiverer funktionen til resultatet er tilgængeligt for brugeren. Driftstid: Det tidsrum på døgnet, hvor servicen eller applikationen er tilgængelig. Oppetid: Den procentdel af åbningstiden, hvor servicen skal svare, og den andel af klienterne, som dette skal gælde for. Retableringstid: Den tid, der må gå, inden servicen eller systemet fungerer igen i tilfælde af nedbrud (katastrofe).
Begrundelse	For at sikre, dels at applikationerne fungerer tilfredsstillende i den daglige drift, dels for at sikre, at der er taget højde for retableringstiden i forbindelse med ikke planlagte hændelser.
Konsekvens	Følgende er mindstekravene for enhver service eller applikation i Kirkenettet. De skal genvurderes og kan skærpes i forhold til de enkelte services, hvis der er forretningsmæssig begrundelse for det. Svartid: Driftsstid: Oppetid: Retableringstid: } Vurderingen foretages i henhold til den senest gældende risikoanalyse

2.7 Tilgængelighed og brugbarhed for personer

Det er afgørende for effekten af investeringerne af it-services og applikationer, at tilgængeligheden og brugbarheden er tilpasset hver persongruppe, således at Kirkenettets brugere opnår en høj grad af brugervenlighed over for alle forskellige grupper.

24. Princip	Tilgængelighed for alle
Definition	Kirkens websteder skal indrettes i overensstemmelse med de obligatoriske fællesoffentlige principper om tilgængelighed for alle.
Begrundelse	Kirkens websteder skal betjene alle landets borgere og skal derfor leve op til krav om tilgængelighed for alle. Det samme gælder for websteder på Kirkenettet, hvor der skal tages hensyn til ansatte med handicap.
Konsekvens	For websteder skal der ved design og funktionalitet sikres tilgængelighed for personer med funktionsnedsættelse. Hvor det ikke er muligt at gøre det fælles design og den fælles funktionalitet tilgængelig for alle, skal der indrettes særskilte faciliteter for personer med funktionsnedsættelse. Webstederne indrettes i overensstemmelse med reglerne fra IT- og Telestyrelsen ("tilgængelighed i praksis")

25. Princip	Målrettede brugerflader
Definition	I Kirkenettet er brugerflader målrettet de brugergrupper, som anvender dem.
Begrundelse	Kirkenettet servicerer mange forskellige brugergrupper, og der skal både tages hensyn til brugervenlighed, effektivitet og ressourceforbrug i udviklingen.
Konsekvens	For hver brugergruppe skal It-Kontoret karakterisere - hvilke typer klienter eller terminaler services skal kunne betjene - om der skal tages hensyn til funktionshæmmede - hvilken indlæringskurve der er acceptabel - om der ske overholdes en grafisk designmanual.

26. Princip	Forenkle og harmonisere brugerflader
Definition	It-Kontoret forenkler og harmoniserer brugerflader, så den enkelte bruger i højere grad oplever en ensartet it-arbejdsplads.
Begrundelse	For den enkelte bruger vil enkle og ensartede brugerflader på tværs af systemerne betyde mindre oplæring, en lettere arbejdssituation og større effektivitet. Særligt for brugere med begrænset anvendelse er enkelhed og overskuelighed afgørende.
Konsekvens	Applikationer indarbejdes i f.eks. intranettet og/eller It-Skrivebordet.

27. Princip	Forenkle log-in
Definition	Log-in i Kirkenettet skal balanceres med krav om sikkerhed.
Begrundelse	På den ene side skal der arbejdes på, at man kun én gang skal logge på til mange systemer. På den anden side skal sikkerheden skærpes, i takt med at flere systemer er omfattet f.eks. med certifikat eller biometri.
Konsekvens	Der kan ikke arbejdes på enklere log-in, uden at der samtidig arbejdes på at fastholde eller forøge sikkerheden.