Forsvarsministeriets it-strategi 2005 - 2009

Indholdsfortegnelse

INDLEDNING

Forsvarsministeriets overordnede it-strategi dækker hele ministerområdet og tager udgangspunkt i ministerområdets formål og opgaver.

Strategien dækker forligsperioden 2005-2009 og fastlægger de centrale principper og målsætninger, der er grundlag for planlægning, implementering og anvendelse af informationsteknologi (it) ved koncernens myndigheder.

It-strategien ajourføres som minimum hvert andet år.

Udarbejdelse af strategien

Strategien er udarbejdet af en koncernfælles Projektgruppe It-strategi, der er sammensat af repræsentanter fra Forsvarsministeriet og ministerområdets niveau I-myndigheder. Strategien tager udgangspunkt i Statens it-råds "Skabelon for en it-strategi for et ministerområde - en vejledning" (juni 2004).

It-strategien er godkendt af Forsvarsministeriet i december 2004.

MISSION OG IT-VISION

Forsvarsministeriets overordnede mission er at

”Arbejde for fred og sikkerhed” og *”at skabe resultater, der bidrager til fred og sikkerhed og som anerkendes i ind- og udland.”*

It er et af redskaberne, der skal understøtte ovennævnte. Derfor er it-visionen, at

”It skal understøtte Forsvarsministeriets overordnede mission gennem tilvejebringelse af effektive og sikre redskaber til håndtering og udnyttelse af informationer.”

Specifikt for det operative område er it-visionen at

”Opnå nødvendig integration og interoperabilitet mellem Forsvarets, totalforsvarets samt vore allierede og andre samarbejdspartneres kommunikations- og informationssystemer for at sikre optimal løsning af sikkerheds- og beredskabsrelaterede opgaver.”

Ud over den operative opgave og de tilhørende nødvendige støtteopgaver, er effektiv og sikker (konfidentialitet, integritet og tilgængelighed) betjening af borgere og virksomheder et prioriteret område. Forsvarsministeriets myndigheder skal kunne yde den nødvendige informationsformidling 24 timer i døgnet samt gennemføre en serviceorienteret og kvalificeret elektronisk betjening af borgere og virksomheder.

Forsvarsministeriet ønsker med denne strategi at fortsætte den igangværende effektivisering og optimering af it-anvendelsen med henblik på frigørelse af ressourcer til løsning af ministerområdets kerneopgaver.

Ud over at fastlægge de centrale principper og målsætninger for it-udviklingen rettes der særlig fokus på følgende:

- Strategisk anvendelse af internet inden for ministerområdet.
- Strategisk anvendelse og udvikling af Forsvarets Integrerede Informatiknetværk (FIIN).
- Strategisk anvendelse og udvikling af operative systemer.

Hertil kommer strategiske digitale projekter, der har indflydelse på koncernens forretningsudvikling samt strategiplaner for ministerområdets integrerede virksomhedsstyringssystem DeMars (Dansk Forsvars Management- og Ressourcestyringssystem).

It-strategien omsættes i en række handlingsplaner, der kontinuerligt er under udvikling og opdatering. De enkelte myndigheder kan inden for disse rammer udarbejde supplerende handlingsplaner, der skal støtte målet og de forretningsprocesser, der er gældende for myndigheden.

FORRETNINGSMÆSSIGE KRAV, HERUNDER KOMPETENCER

Indledning

Generelt skal tiltag på it-området, fx projekter, standardisering m.m., være begrundet i kravet om effektiv anvendelse af ministerområdets ressourcer i lyset af kerneopgaverne eller i specifikke politiske krav til Forsvarsministeriets virksomhed.

Den øverste ledelses virke er i stigende grad blevet ændret, idet behovet for tæt samspil mellem Forsvarsministeriet og underliggende myndigheder er vokset. It skal derfor understøtte en bred vifte af ledelses-, kerne- og støtteprocesser i forbindelse med myndighedernes opgaveløsning.

Det er vigtigt at planlægge de nødvendige forandringer i forbindelse med fastlæggelsen af nye it-systemers funktionalitet, således at it-systemerne ikke blot fastholder eksisterende arbejdsgange, men optimerer disse set i lyset af de it-mæssige muligheder og de aktuelle mål for det myndighedsområde, it-systemet skal virke i.

Business case

Anvendelsen af business cases er en nødvendig forudsætning for at identificere og realisere eventuelle effektiviseringsgevinster. Det er vigtigt, at der på et tidligt tidspunkt skabes begrundede forventninger om de gevinster, som kan høstes, når et projekt er gennemført.
Der skal udarbejdes en business case inden iværksættelse af it-projekter. Metoder og værktøjer til estimering af potentialet og rentabiliteten i nye it-investeringer er under stadig udvikling. Det afgørende for anvendelsen af metode/værktøj er, at det på grundig vis afdækker de elementer, der indgår ved implementeringen af det aktuelle it-system. Ved mindre projekter, hvor det ikke er lønsomt at udarbejde en business case, eller hvor det er givet, at et bestemt projekt skal implementeres, kan hovedreglen fraviges.

Effektmåling af it-anvendelsen

Efter implementering af it-projekter skal der foretages en evaluering set i relation til den opstillede business case eller i relation til opstillede politiske krav. Der foretages målinger før og efter implementering af digitale projekter med henblik på opgørelse af eventuelle gevinster.

Understøttelse af forretningsprocesser

Det overordnede forretningsmæssige krav er, at it skal understøtte den operative virksomhed og de tilhørende processer, herunder forvaltningsmæssige, der gennemføres for at løse myndighedens opgaver. Endvidere skal it understøtte den igangsatte rationalisering og effektivisering af stabs- og støttestrukturen til fordel for de operative kapaciteter.

Understøttelsen af denne proces i blandt andet det integrerede virksomhedsstyringssystem DeMars kan opgøres i følgende:

- Et ajourført datagrundlag.
- En hensigtsmæssig præsentation af informationer.
- En tilstrækkelig vidensdeling for løsning af opgaven.
- Online adgang til systemer, data og informationer, hvor det er nødvendigt.

- Gennemførelse af nødvendig og tilstrækkelig uddannelse af brugerne.

Datagrundlag
Data skal i videst mulig omfang dannes ved kilden og herefter, via infrastrukturen, kunne anvendes i alle øvrige meningsfulde sammenhænge. I den forbindelse skal datakvaliteten prioriteres, så der er sikkerhed for, at de informationer, der præsenteres, er opdaterede og valide. Dette gælder for hele spektret fra opstillingen af retvisende regnskaber til operative sammenhænge.

Præsentation af informationer
Data skal kunne behandles og sammensættes, så de udgør relevante informationer. De ønskede informationer skal være tilgængelige som nødvendig støtte i beslutningsprocessen.

Vidensdeling
Data, informationer og viden skal være bredt tilgængelige, og således styrke fleksibilitet, viden og kompetencer inden for ministerområdet. It-systemerne - der i denne sammenhæng blandt andet omfatter sags- og dokumenthåndteringssystemer, elektroniske arkiver, økonomi- og ressourcestyringssystemer, informationssystemer, herunder geografiske informationssystemer, operative systemer, intranet og internet - skal understøtte dette.

De operative systemer omfatter i denne sammenhæng kommunikations- og informationssystemer,[1] men ikke it-systemer integreret i specifikke våbensystemer mv.

Anvendelsen af data skal til stadighed baseres på de gældende militære sikkerhedsbestemmelser og øvrige relevante sikkerhedskrav, fx persondataloven.

Adgang til systemer
Kommunikations- og informationssystemerne skal kunne producere og formidle den nødvendige information til gennemførelsen af den operative virksomhed døgnet rundt.

Kompetencer
Koncernens it-kompetencer centraliseres med henblik på en styrkelse af it-miljøet. For den koncernfælles it-drift centraliseres kompetencerne ved Projektorganisation Koncernfælles IT-driftsmyndighed, på sigt Forsvarets Koncernfælles Informatiktjeneste. Denne tjeneste baseres på egne kompetencer og på støtte fra civile leverandører og de funktionelle tjenester. Der vil i et vist omfang fortsat være behov for, at den operative struktur og støttestrukturen råder over decentrale it-kompetencer. Drift af deployerbare it-systemer varetages af den operative og logistiske struktur i overensstemmelse med de operative behov.

[1] På engelsk benævnt Communications and Information Systems (CIS-systemer)

IT-STYRING OG -ORGANISERING

Indledning
For at de vedvarende krav til effektivisering kan realiseres, er det afgørende, at strategien forankres i koncernens øverste ledelse.

It-styring og -organisering (It-governance)
Styring af it-området er forankret i Forsvarsministeriets departement, som fastlægger de strategiske mål samt godkender og iværksætter væsentlige it-initiativer og it-projekter inden for koncernen. Ligeledes foretager departementet overordnet opfølgning og kontrol af it-virksomheden.

Forsvarskommandoen varetager på vegne af Forsvarsministeriet udmøntningen af it-strategien inden for den koncernfælles it-virksomhed gennem udarbejdelse af handlingsplaner, varetagelse af projektledelse og implementering af projekter og initiativer på it-området samt rådgiver departementet. Forsvarets Efterretningstjeneste rådgiver i it-sikkerhedsanliggender.

Det udførende niveau for koncernfælles it systemers drift og vedligeholdelse placeres ved Projektorganisation Koncernfælles IT-driftsmyndighed, på sigt Forsvarets Koncernfælles Informatiktjeneste.

Overordnede retningslinjer for kvalitetsstyring og –sikring af it-processerne
Kvalitetsstyring og -sikring af it-processerne opnås grundlæggende ved at gennemføre disse efter internationalt anerkendte modeller og metoder.

It-driftsprocessers styring
ITIL[2]-processerne sikrer, at it-services bliver leveret på et defineret kvalitetsniveau med større professionalisme og med totalt fokus på forretningens mål. ITIL processerne, herunder Service Level Management, giver grundlag for effektiv løbende vurdering og afstemning af forventninger, krav og behov for it-ydelser mellem it-organisationen og forretningen.

It-projekters styring
It-projekter skal som udgangspunkt styres ved anvendelsen af PRINCE2[3] modellen. Dette gælder både for projekter med egen projektledelse og projekter med ekstern projektledelse. Anvendelsen af denne model betyder, at projektet opererer med kontrolleret opstart, udførelse, afslutning samt evaluering gennem anvendelse af en struktureret projektstyringsmetode. PRINCE2 er en struktureret metode til projektledelse, som omfatter alle aspekter i et projekt fra idé til opstart og initiering over udførelse til afslutning, herunder:

- Ændrings- og konfigurationsstyring, hvor ændringer dokumenteres og godkendes for optimal kvalitet af projektets resultat.
- Projektorganisation med en klar placering af ansvar og kompetencer.

[2] IT Infrastructure Library (ITIL) er en samling af erfaringer "best practices" for driftsledelse.
[3] PRINCE er en forkortelse af Projects IN Controlled Environments.

- Kvalitetsstyring integreret med organisationens kvalitetsstyringssystem.
- Ledelse og kontrol af projektets aktiviteter for opnåelse af defineret kvalitet af projektets resultat inden for budgetteret tid og økonomi.
- Risikostyring, hvor risici løbende identificeres, analyseres, estimeres og styres gennem hele projektet.

Herudover skal it-sikkerhed indgå som et aspekt i samtlige af projektets faser.

Udliciteringsstrategi
Placeringen af it-opgaverne, så de løses mest hensigtsmæssigt og mest effektivt, skal løbende vurderes. Det overordnede princip for levering af it-ydelser er, at de ikke i sig selv er en kerneopgave for ministerområdets opgaveløsning, hvorfor det til stadighed skal undersøges, om ydelserne kan leveres bedre eller billigere af andre.

De overordnede styringsorganer i koncernfælles regi
Strategien er retningsgivende for en række koncernfælles fora, der sikrer en optimal og koordineret it-udvikling af koncernen, dels på det forretningsmæssige område og dels på det it-faglige område.

IT-ARKITEKTUR

Indledning

Det er en målsætning at arbejde mod en teknologisk sammensmeltning af FIIN- og internet-miljøerne. Den integration af miljøerne må dog ikke resultere i en uacceptabel forringelse af den funktionalitet og den sikkerhed (konfidentialitet, integritet og tilgængelighed), der tilbydes på FIIN-miljøet. Det fremtidige netværk skal ikke nødvendigvis baseres på lejede faste linjer. Mulighederne for at frigøre sig fra de lejede linjer skal løbende undersøges.

Det skal i strategiperioden undersøges nærmere, om der med fordel kan indføres IP-telefoni (telefoni over datanetværk) i koncernen.

Uklassificeret segment

Med henblik på at samordne myndighedernes individuelle anvendelse af internettet skal der etableres ét koncernfælles netværk. Netværket etableres under anvendelse af den offentlige sektors standarder samt i overensstemmelse med principperne for arkitektur for digital forvaltning, hvorved it-løsningen sammentænkes med forretningens mål og strategier. Efterfølgende sigtes mod en tilslutning til Statens it-net, når dette er etableret.

I totalforsvarssammenhæng skal behovet for informationsudveksling mellem relevante aktører identificeres.

Til Tjenestebrug segment

Infrastrukturen på FIIN skal til stadighed vedligeholdes i takt med den teknologiske udvikling og de forretningsmæssige og operative krav. Den tekniske udvikling af FIIN skal ske, så FIIN fortsat overholder gældende it-sikkerhedsbestemmelser. De udviklingsprincipper, der gælder for FIIN, skal som udgangspunkt følge de principper, der gælder for den offentlige sektor på it-området.

Højere klassificeret segment

Forsvarsministeriet vil fortsat arbejde med opkobling af relevante operative netværk til NATO's tilsvarende netværk for at sikre interoperabilitet og på sigt klargøre til netværks baserede operationer (NBO)[4].

[4] På engelsk benævnt NATO Network Enabling Capabilities (NNEC).

IT-SIKKERHED

Indledning

Sikkerheden i de it-systemer, som hører under Forsvarsministeriets ansvarsområde, skal være tilstrækkelig til at sikre konfidentialitet, integritet og tilgængelighed i henhold til de krav, der er opstillet til systemerne. Netværk/it-systemer må ikke tilsluttes andre netværk/it-systemer uden forudgående godkendelse fra Forsvarets Efterretningstjeneste.

Styringen af it-sikkerheden tager udgangspunkt i gældende principper for Risk Management.

Den øgede digitalisering inden for koncernen stiller fortsat krav om efterlevelse af de fastsatte sikkerhedsbestemmelser, samtidig med, at de øgede udad rettede aktiviteter stiller krav om fleksible sikkerhedsløsninger. Ledelsen og den etablerede sikkerhedsorganisation på alle niveauer skal derfor sikre, at medarbejderne uddannes og motiveres bedst muligt til at opretholde et højt sikkerhedsniveau.

It-sikkerhed Uklassificeret segment

Med den øgede digitale betjening af borgere og virksomheder samt kravene til den offentlige sektors digitalisering generelt som en prioriteret del af Forsvarsministeriets virksomhed, er det afgørende, at it-sikkerheden er etableret på et forsvarligt niveau. Forsvarsministeriet skal som minimum leve op til de statslige sikkerhedskrav, der tager udgangspunkt i Dansk Standard 484-1 samt til krav i forbindelse med tilkobling til Statens it-net.

It-sikkerhed Til Tjenestebrug segment

It-sikkerheden implementeres som defineret i nationale, NATO- og kommende EU-sikkerhedsbestemmelser.

It-sikkerhed højere klassificeret segment

It-sikkerhed implementeres som defineret i nationale og internationale (NATO, EU mv. bestemmelser). Det betyder, at såvel netværk, installationer mv., der behandler informationer klassificeret Fortroligt eller højere samt udstyr og applikationer skal godkendes af Forsvarets Efterretningstjeneste.

Særlige fokusområder

Identifikation

Ved udvikling og opdatering af forsvarets it-systemer skal der anvendes metoder, der øger sikkerheden for, at dataudveksling sker mellem servere og brugere på autoriseret og godkendt måde. Det betyder, at servere og brugere får tildelt godkendte digitale identiteter, for eksempel i form af digitale certifikater (digital signaturer). Forudsætningen for administration af digitale certifikater, herunder at disse er valide, er, at der etableres infrastrukturer hertil, såkaldt Public Key Infrastructure (PKI)).

I NATO er der påbegyndt etablering af en NATO PKI. NATO har henstillet til medlemsnationerne, at nationale PKI løsninger kan samarbejde med NATO PKI, hvor der sker udveksling af informationer mellem nationale systemer og NATO systemer. Danmark har fastlagt

en PKI infrastruktur i hvilken digitale certifikater - i form af Offentlige Certifikater til Elektronisk Signatur (OCES-certifikater) - kan anvendes. Forsvaret bør klarlægge om OCES-certifikater er interoperable med NATO PKI, hvis der skal ske udveksling af informationer mellem it-systemer, hvor disse certifikater anvendes.

Nationale kryptograferingsprodukter

Af hensyn til nationale behov for beskyttelse af klassificeret information skal muligheden for udvikling af nationale kryptograferingsprodukter fremmes. Dette arbejde koordineres af sikkerhedsmyndigheden (Forsvarets Efterretningstjeneste).

Multilateral sikkerhed

Det er et grundlæggende krav til sikkerhed i et netværk, at der foreligger en sikkerhedsmodel, der beskriver, hvilke sikkerhedsmekanismer netværket indeholder, hvilke sikkerhedskrav der er vedrørende de data, netværket transporterer, og hvilke sikkerhedskrav der er til de personer og servere, der håndterer data i netværket.

Multilateral sikkerhed i forbindelse med sammenkobling af netværk bør benytte ovennævnte sikkerhedsmodeller som grundlag for opstilling af krav til de funktionelle sammenkoblinger mellem netværkene, der skal etableres. Denne model benyttes allerede af Forsvarets Efterretningstjeneste som grundlag for sikkerhedsvurdering ved sammenkobling af net.

ØKONOMI, OPTIMERING AF IT-DRIFTEN OG INDKØB

Grundlæggende princip

Styring og forvaltning af informatikvirksomheden i Forsvaret udvikles i overensstemmelse med Forsvarets styringsprincipper. I takt med at Forsvarets styrings- og virksomhedsmodel skaber grundlag for en mere forretningsorienteret ledelse af driftsvirksomheden, udvikles et større fællesskab inden for ministerområdet og skaber derved basis for en stadig optimering af it-driftsstrukturen.

Den centrale informatikvirksomhed

Forsvarets Informatikplan (FIP) omfatter planlægningsgrundlaget for den centrale informatikvirksomhed i koncernen og indeholder midler til opstilling af informatikkapacitet[5] og til drift af informatikkapacitet[6]. Størstedelen af rammerne er bundet til driften af eksisterende infrastruktur og applikationer, og kun kendte og godkendte planer for opstilling af ny kapacitet er medtaget.

Koncernfælles centraliseret it-drift

Der er etableret en centraliseret it-drift med henblik på effektivt at understøtte ministerområdets forretningsprocesser. Den koncernfælles driftsmyndighed overtager ansvaret for anskaffelse, drift og vedligeholdelse af den koncernfælles infrastruktur og de fælles applikationer, der afvikles på infrastrukturen. Som konsekvens af centraliseringen af it-driften centraliseres indkøbsfunktionen ved den koncernfælles driftsmyndighed.

I overensstemmelse med statens regnskabsreform værdifastsættes statens kontoradministrative it udstyr og aktiveres i anlægsregnskabet.

Informatikomkostningerne fordeles til den operative virksomhed, henholdsvis støttevirksomheden ved intern afregning eller ved faktura fra Forsvarskommandoen til Forsvarsministeriet og andre niveau I-myndigheder. Afskrivninger fra den registrerede værdi af informatikkapaciteten og omkostninger til drift og forvaltning opsamles på kapacitetscentre, hvorfra omkostningerne fordeles.

Indkøb

Indkøb foretages så vidt muligt centralt under anvendelse af koncernens rammeaftaler for standard produkter (COTS), der overholder åbne og anerkendte standarder, samt lever op til koncernens krav til sikkerhed.

For it-systemer til primær operativ anvendelse er anskaffelse i vid udstrækning delegeret til den brugende myndighed.

[5] Fx nye applikationer, nye elementer i infrastrukturen eller tilføjelse af ny funktionalitet til eksisterende systemer.

[6] Fx driftsafvikling, overvågning, fejlrettelse, mindre vedligeholdelse, system- og sikkerhedsadministration samt brugerservice.

DIGITAL FORVALTNING

Indledning

Digital forvaltning omhandler den bedst mulige udnyttelse af it gennem effektivisering og digitalisering af interne arbejdsgange og administrative processer. Den digitale forvaltning udvikles inden for koncernen ved gennemførelse af en række projekter.

It-baseret virksomhedsstyring

Forsvarsministeriet har et moderne, it-baseret integreret virksomhedsstyringssystem benævnt DeMars, som for hele ministerområdet samler styring og forvaltning af økonomi, materiel, personel og struktur samt tilvejebringelse af ledelsesinformation. DeMars skal som udgangspunkt løse koncernens styrings- og forvaltningsopgaver. Ministeriet har hermed stort set erstattet alle ældre administrative systemer og vil i videst muligt omfang lade DeMars løse fremtidige styrings- og forvaltningsopgaver, samt omlægge de få tilbageblevne ældre systemer. Den fortsatte anvendelse og udvikling af DeMars skal således bidrage til en effektiv digital forvaltning inden for Forsvarsministeriets område.

Elektronisk sags- og dokumenthåndtering (ESDH)

Digital sagsbehandling er et centralt område i den digitale forvaltning. Et vigtigt element i digital sagsbehandling er ESDH. Med henblik på at overholde fællesstatslige standarder og sikre den nødvendige informationsudveksling og dokumentation inden for koncernen, og på sigt med resten af den offentlige sektor, skal implementeringen af ESDH ske i rammen af det Fællesoffentlige Elektroniske Sags- og Dokumenthåndteringsprojekt (FESD).

Forsvarsministeriet har igangsat processen med henblik på at implementere en FESD-løsning i koncernen.

Hindringer for digital forvaltning

Forvaltningsmæssige hindringer for digital forvaltning skal fortsat søges imødegået. Ved udarbejdelse af nyt forvaltningsgrundlag samt ved rettelser af eksisterende må der ikke stilles formkrav, der vil kunne udgøre en hindring for digital kommunikation, eller for at berørt sagsbehandling m.v. kan ske digitalt. Dette kan dog fraviges såfremt særlige forhold gør sig gældende, fx i relation til retssikkerhed, militær sikkerhed, lovgivningsmæssige forhold eller lignende.

Centralisering af it-driften

Forsvarsministeriet vil fortsætte med at identificere områder, der er egnet til standardisering og centralisering. I forbindelse med identificering bør det undersøges om disse områder med fordel kan udliciteres.

Forvaltning af frivilligt og reservepersonel

Frivilligt personel, herunder Hjemmeværnets frivillige, samt personel af reserven skal selv kunne gennemføre en større grad af selvforvaltning for dels at højne servicekvaliteten og dels for at øge effektiviteten i denne forvaltning.

Betjening af borgere og virksomheder m.fl.
Forsvarsministeriet ønsker at bidrage til at realisere regeringens vision om digital forvaltning:

"Digitalisering skal bidrage til at skabe en effektiv og sammenhængende offentlig sektor med høj servicekvalitet, hvor borgere og virksomheder er i centrum."

Forsvarsministeriet vil sætte særlig fokus på følgende områder udpeget af regeringen:

- Den offentlige sektor skal levere sammenhængende ydelser med borgere og virksomheder i centrum.
- Digital forvaltning skal skabe øget servicekvalitet og frigøre ressourcer.
- Den offentlige sektor skal arbejde og kommunikere digitalt.
- Digital forvaltning skal baseres på en sammenhængende og fleksibel it-infrastruktur.
- Offentlige ledere skal gå forrest og sikre, at deres organisation kan realisere visionen.

Den borger- og virksomhedsrettede forvaltning
Forsvarsministeriets myndigheder skal tilbyde borgere og virksomheder mulighed for selvbetjening m.v. i den udstrækning, det er hensigtsmæssigt. Myndighedernes hjemmeside skal fortsat udvikles, så de imødekommer brugernes behov. Tilgængeligheden skal overholde gængse standarder ved anvendelse af blandt andet Referenceprofilen samt krav, der stilles af offentlige myndigheder om informationsudveksling, fx krav om sikker kommunikation ved anvendelse af digital signatur.

Forsvarsministeriets portal på internettet
I anvendelsen af koncernens hjemmesider på internettet skal der etableres en overordnet portal, der skal virke som en samlet indgang til ministerområdets hjemmesider. Portalen skal indledningsvis henvise til koncernens øvrige hjemmesider, men på sigt - og på baggrund af en interessentanalyse - yde en mere målrettet information, herunder stille services/tjenester til rådighed til de forskellige brugere.

I forbindelse med etablering af en portal for Forsvarsministeriet skal der gennemføres en designmæssig koordinering af de eksisterende hjemmesider med henblik på at lette informationssøgningen for brugerne. Koordineringen skal munde ud i retningslinjer for design, herunder "branding" og en mere ensartet navigering på Forsvarsministeriets hjemmesider.

DEN OPERATIVE VIRKSOMHED

Indledning

Forsvarsministeriets hovedopgave (den operative virksomhed) retter sig primært mod det militærspecifikke område, hvor ministerområdets samlede aktiviteter dækker et bredt spektrum af opgaver. Nogle opgaver er støtteprocesser til hovedopgaver, mens andre, fx redningsberedskabet, kystredning og miljøovervågning er hovedopgaver i sig selv.

Den operative virksomhed

Virksomheden inden for det operative område omfatter blandt andet anskaffelse og drift af kommunikations- og informationssystemer.

Forsvarsministeriet vil i perioden fokusere på, at der udarbejdes den nødvendige overordnede arkitektur for kommunikations og informationssystemer med henblik på at sikre en nødvendig interoperabilitet mellem disse, til DeMars samt relevante systemer i NATO og ved øvrige samarbejdspartnere (militære og civile).

I forbindelse med udsendelse af NATO Response Force vil det blive et krav til de allokerede styrker, at de er interoperable inden for CIS på et vist fastsat niveau med de andre nationers deltagende styrker. En metode, der kan fastsætte og måle det krævede niveau, er under udarbejdelse i NATO regi, hvorefter Forsvarsministeriet forventer at adoptere metoden nationalt.

Definition og senere implementering af NATO netværks baserede operationer (NBO), vil på sigt markant ændre ledelse og udførelse af alle typer operationer. Forsvarsministeriet vil fokusere på dette emne i de kommende år.

Den operative virksomhed rettet mod det civile samfund anvender i stor udstrækning internettet, der derfor har stor betydning for opfyldelsen af opgaverne. Koncernen skal i udviklingen af de kommende services på internettet anvende både nationalt og internationalt almindeligt gældende udvekslingsstandarder. Koncernen skal arbejde på at følge anbefalingerne i den åbne digitale forvaltning, der er møntet på at fremme dataudveksling og samarbejde.

OVERSIGT OVER HANDLINGSPLANER

Indledning
Handlingsplanerne konkretiserer de første års udvikling/implementering af it-strategien. Dette område er under konstant forandring, hvilket medfører en kontinuerlig opdatering af denne del af it-strategien.

Studievirksomhed
Forsvarskommandoen følger løbende den teknologiske udvikling inden for CIS. På baggrund af de stillede operative behov bliver der udfærdiget et koncept for CIS med tilhørende underliggende delstudier omhandlende specifikke emner inden for CIS. Disse delstudier bliver opdateret hvert andet år.

Udvikling af netværksbaserede operationer
Forsvarskommandoen har nedsat en styringsgruppe med underliggende grupper med henblik på at styre forsvarets overgang til netværksbaseret forsvar og netværksbaserede operationer (NBO). I det fortsatte arbejde vil Beredskabsstyrelsen, politiet m.fl. blive inddraget. Arbejdet skal på it-området munde ud i etableringen af et NBO-netværk, hvor man er i stand til at udveksle operative og administrative informationer fra såvel internationale som nationale operationer og præsentere disse på en platform, hvor information er tilgængelig i den rette form og på rette tid.

DeMars udviklingsplan
Videreudviklingen af DeMars styres af eksterne krav, fx lovgivning, overenskomster m.v. samt interne behov og ønsker for at forbedre styring og forvaltning af Forsvarsministeriets ressourcer. På den baggrund udarbejdes løbende plan for den videre udvikling af DeMars. DeMars skal som udgangspunkt løse ministerområdets styrings- og forvaltningsopgaver. Den fortsatte anvendelse og udvikling af DeMars skal således bidrage til en effektiv digital forvaltning inden for Forsvarsministeriets område.

Elektronisk sags- og dokumenthåndteringssystem
Elektronisk sags- og dokumenthåndteringssystem skal implementeres i koncernen. Med henblik på at overholde fællesstatslige standarder og sikre den nødvendige informationsudveksling på sigt inden for centraladministrationen, skal implementeringen af Elektronisk sags- og dokumenthåndteringssystem ske i rammen af det ”Fællesoffentlige Elektroniske Sags- og Dokumenthåndteringsprojekt (FESD)”.

Softwarepolitik
Der udarbejdes en politik, der på strategisk niveau fastsætter ministerområdets anvendelse af leverandør-ejet software kontra open source mv.

Udliciteringspolitik
Der udarbejdes en politik, der fastsætter omfanget for den fremtidige udlicitering af it-området, herunder udpegning af områder/funktioner, som koncernen ikke ønsker udliciteret.

Business case værktøj
Mulige Business case værktøjer til brug ved digitaliseringsprojekter skal fortløbende undersøges med henblik på anvendelse af "Best Practise". Indledningsvis anvendes "Værktøj til værdiestimering", der er udsendt af Den Digitale Taskforce.

Analyse af mulighederne for etablering af ét fælles netværk
Mulighederne for en reel anvendelse af kun ét netværk til transmission af uklassificerede og klassificerede (Til Tjenestebrug) informationer skal undersøges nærmere under skyldig hensyntagen til de sikkerhedsmæssige aspekter. Denne løsning er på længere sigt. På kort sigt undersøges muligheden for at benytte internettet som det primære produktionsmiljø for uklassificeret informationsudveksling og sagsbehandling for at starte processen, og anvende FIIN som sekundært netværk til klassificeret informationsudveksling (Til Tjenestebrug segment).

Geografisk informationssystem (GIS)
Koncernens GIS-anvendelse koordineres og optimeres med henblik på fælles produktvalg og integrerede løsninger, der muliggør maksimal udnyttelse af registrerede data.

Tværministeriel forsøgsvirksomhed
Som statslig bygherre deltager Forsvarsministeriet (Forsvarets Bygningstjeneste) i udviklingen af projekt Det Digitale Byggeri, initieret af Erhvervs- og Byggestyrelsen, med det formål at fastlægge bygherrekrav for gennemførelse af statslige byggeprojekter. Digital styring og administration af forsøgsprojekter gennemføres på internettet.

Forvaltning af frivilligt og reservepersonel
Der skal implementeres, og løbende videreudvikles systemer, som muliggør en større grad af selvforvaltning af frivilligt personel, herunder Hjemmeværnets frivillige, samt personel af reserven. Disse systemer skal sikre en høj servicekvalitet samt en effektivisering af denne forvaltning.