



FORSVARET

Digital reguleringsplan for Forsvaret

Metadata

KORTTITTEL:	DRP
GRADERING:	UGRADERT
UTGIVER:	Sjef Forsvarsstaben
SAKSBEHANDLENDE AVD.:	FST Teknologi Cyber & IKT
GJELDER FOR:	Forsvaret
HJEMMEL:	Instruks til forsvarssjefens undergitte sjefer 2026-01-01 punkt 4.1.c
IKRAFTTREDELSE:	05-10-2026
FORRIGE VERSJON:	15-02-2023

Innhold

1	Innledning	4
1.1	Formål	4
1.2	Avhengighet til styrende dokumenter og IKT-styringsmodell	4
1.3	Anvendelse	5
1.4	Forvaltning av DRP	5
1.5	Leserveiledning	6
2	Sammendrag av innsatsområder og prinsipper i DRP	7
2.1	Innsatsområder	8
2.2	Prinsipper	9
3	Detaljert beskrivelse av innsatsområder med tilhørende prinsipper	10
3.1	Innsatsområde: Kapabilitetsbasert utvikling av IKT (ARK)	10
3.2	Innsatsområde: Sikker IKT i Forsvaret (SIK)	12
3.3	Innsatsområde: Datadrevet forsvar og KI (DAT)	15
3.4	Innsatsområde: Applikasjoner og applikasjonsutvikling (APP)	16
3.5	Innsatsområde: Forsvarets skyløsning (FSL)	18
3.6	Innsatsområde: IKT-arkitektur og -sikkerhet i digitalisert materiell (DIM)	21
3.7	Innsatsområde: Samvirke med allierte, totalforsvaret og andre relevante aktører (SAM)	22
3.8	Innsatsområde: Gjennomgående forskning, utvikling og innovasjon (FoU&I)	23
3.9	Innsatsområde: Menneske og organisasjon (MEO)	24
3.10	Innsatsområde: Personvern og IKT (PV)	26
4	Begreper	28
5	Forkortelser	35
6	Referanser	37

1 Innledning

Forsvarets digitale reguleringsplan (DRP) gir styrende rammer for Forsvarets *digitale transformasjon*. Endringer i måten krigføring foregår på krever rask styrking av evnen til *multidomeneoperasjoner* (MDO). Avansert datafusjon og kunstig intelligens (KI) er avgjørende for å sikre operativ evne på tvers av domener. Forsvaret skal bevege seg fra en nettverks- og applikasjonssentrisk arkitektur med datasiloer til en moderne *datasentrisk* arkitektur.

Forsvarets digitale transformasjon er en helhetlig endring der teknologi, mennesker, organisasjon og ledelse samvirker for å styrke den operative evnen. Transformasjonen omfatter bedre utnyttelse av Forsvarets eksisterende IKT. Dette er en forutsetning for informasjonsflyt, samvirke og interoperabilitet og operativ evne i MDO.

Forsvarets digitale transformasjon skal styrke kapabilitetene innen situasjonsforståelse, kommando og kontroll, virksomhetsstyring og *interoperabilitet* – og dermed øke den operative evnen. Transformasjonens sentrale byggesteiner er prosjektene *Forsvarets sikre plattformer* (FSP) også omtalt som MilSky, Enterprise Resource Planning (ERP) og datasenter – samt initiativ som Forsvarets KI-senter.¹ For å lykkes med den digitale transformasjonen bør eksisterende og kommende *digitalisert materiell* være interoperabelt med en modernisert *digital grunnmur*.

Realisering av Forsvarets fire hovedmål – operasjoner, beredskap, utholdenhet og utvikling (Forsvarsdepartementet, 2025) – forutsetter rammer for beslutninger som etableres gjennom DRP.

1.1 Formål

Formålet med DRP er å:

- etablere tydelige rammer for beslutningene som styrer Forsvarets digitale transformasjon.
- beskrive handlingsrommet (valg og avveining) for anskaffelser, utvikling, drift og vedlikehold (UDV) av både ny og eksisterende IKT
- sette en felles strategisk retning for den digitale transformasjonen
- definere sentrale begreper for IKT i Forsvaret – beskrevet i kapittel 4.

DRP består av følgende deler:

- *Innsatsområder*, er en tematisk gruppering av *prinsipper* innenfor områder som er kritiske for å lykkes med transformasjonen.
- *Prinsipper*, er retningsgivende og intensjonsbaserte føringer for *IKT-virksomheten*.
- *Begreper*, starten på et systematisk og forvaltet begrepsapparat for IKT i Forsvaret.

1.2 Avhengighet til styrende dokumenter og IKT-styringsmodell

Dette dokumentet (DRP 2026) erstatter DRP fra 2022. Den reviderte versjonen viderefører enkelte innsatsområder og prinsipper. DRP 2026 inneholder ikke tidslinjer eller prioriteringer. Målbilder, tidslinjer og prioritering for IKT-området forvaltes gjennom IKT-styringsmodell – og dokumenteres innenfor Forsvarets fastlagte porteføljestyling, virksomhetsstyring og langtidsplanlegging.

¹ Dette er eksempler på byggesteiner i Forsvarets digitale transformasjon, og ikke ment som en uttømmende liste.

IKT-styringsmodell er Forsvarets rammeverk for enhetlig strategisk styring av Forsvarets IKT. Modellen skal styrke gjennomføringsevnen på IKT-området, og dermed øke operativ evne og bidra til ambisjonene i Forsvarets langtidsplan (LTP) og gjennomføringsplan (FGP).

IKT-styringsmodell er en integrert del av Forsvarets virksomhetsstyring. Forsvarssjefens porteføljestyre (PSM) prioriterer og styrer porteføljen organisert i seks behovsområder. IKT-styringsmodell operasjonaliserer porteføljestyringen av Behovsområde IKT (*fellesfinansiert IKT*), og setter samtidig rammer for *egenfinansiert IKT* i de øvrige fem behovsområdene: Luft, Land, Maritim, Cyber/Space og Understøttelse.

Strategiske føringer og krav kommer til uttrykk gjennom styrende dokumenter. FGP, Forsvarets virksomhetsplan, Veileder for investeringer i forsvarssektoren og Veileder for gevinstrealisering setter overordnede rammer for IKT-styringsmodellen. Videre operasjonaliseres styrende dokumenter for IKT-virksomheten, herunder Digital reguleringsplan (DRP) som overordnet rammeverk, supplert av Forsvarets Datasentrisk Arkitektur (FDSA), Forsvarets skystrategi og KI-policy som en integrert del av modellen.

1.3 Anvendelse

DRP skal inngå i beslutningsgrunnlaget for IKT-beslutninger. Som hovedregel skal prinsippene i DERP legges til grunn og brukes som vurderingskriterier ved:

- utvikling og anskaffelse av nye IKT-løsninger
- videreutvikling eller modernisering av IKT-løsninger
- analyse av eksisterende IKT-portefølje
- beslutninger om utfasing eller konsolidering av IKT-løsninger

Målgruppen for DERP er primært for Forsvarets IKT-virksomhet. IKT-virksomheten omfatter aktører som anskaffer, utvikler, drifter eller vedlikeholder og forvalter *Forsvarets IKT*. Dette inkluderer interne og eksterne aktører, offentlige og private samt industri og akademia. DERP gir rammer for forsvarssektoren, når etatenes prosesser og *data* inngår i Forsvarets *digitale verdikjeder*.

Prinsippene i DERP representerer en ønsket retning for utviklingen av Forsvarets IKT, og skal som hovedregel legges til grunn i relevante beslutninger. Prinsippene varierer i modenhet og tidshorisont, og gjelder både eksisterende føringer og langsiktige ambisjoner som krever gradvis innføring, organisatorisk tilpasning og teknologisk modning.

Prinsippene i DERP kan i enkelte tilfeller stå i motsetning til hverandre. I motsetningstilfeller skal det gjennomføres en dokumentert risikovurdering. Etterlevelse og eventuelle avvik skal vurderes basert på:

- risiko
- Forsvarets *kapabiliteter*
- relevante regelverk og
- teknologisk og organisatorisk modenhet

Ved eventuelle avvik fra prinsippene i DERP skal begrunnelse (inkl. risikovurdering) og eventuelle kompenserende tiltak dokumenteres i beslutningsunderlaget.

1.4 Forvaltning av DERP

Forsvarsstaben (FST) har ansvar for utgivelse, revidering, vedlikehold og godkjenning av DERP.

1.5 Leserveiledning

Kapittel 2 gir et sammendrag av DRP og en oversikt over innsatsområdene med tilhørende prinsipper.

Kapittel 3 utdyper prinsippene for hvert innsatsområde og forklarer deres formål og praktiske betydning, uten å etablere detaljerte krav, prosedyrer eller rollebeskrivelser. Prinsippene i DRP varierer i karakter; noen er teknologiske og applikasjonsnære, mens andre gjelder praksis og metode. Prinsippene varierer i normativ styrke; noen er bindende føringer, andre strategiske ambisjoner. Dette innebærer at formål og praktisk betydning ikke er formulert likt for alle prinsippene.

Forsvaret skal utvikle og forvalte et helhetlig begrepsapparat for IKT, og kapittel 4 er første versjon av dette. Noen begreper i kapittel 4 er også benyttet i andre styrende dokumenter enn DRP, som Forsvarets skystrategi (2026) og Forsvarets datasentriske arkitektur (2026).

Kapittel 5 inneholder forkortelser og kapittel 6 referanser.

Sentrale begreper i teksten er forklart i kapittel 4. Forklarte begreper er *kursivert og fargeuthevet* i teksten første gang de nevnes.

2 Sammenndrag av innsatsområder og prinsipper i DRP

DRP gjelder primært for IKT-virksomheten i Forsvaret.

Forsvaret gjennomgår en digital transformasjon der utnyttelse av data, KI og moderne IKT er avgjørende for utvikling av relevante kapabiliteter som gir operativ evne, beredskap og utholdenhet.

DRP definerer handlingsrommet (valg og avveininger) for anskaffelser, utvikling, drift og forvaltning av Forsvarets IKT. Prinsipper fra DRP skal inngå i beslutningsgrunnlag for Forsvarets digitale transformasjon. DRP skal gi en felles retning, helhetlig prioritering og faktabaserte beslutninger.

Prinsippene i DRP har ulik modenhet. Noen gjelder som føringer i dag, mens andre representerer strategiske mål som realiseres gradvis over tid.

DRP består av ti innsatsområder, hvert med konkrete, retningsgivende prinsipper som Forsvarets IKT-virksomhet skal legge til grunn for praksis, krav og utvikling av IKT.

DRP legger til rette for at IKT-utviklingen er kapabilitetsbasert, datasentrisk og i samsvar med Forsvarets operative behov. Den legger vekt på sikkerhet, interoperabilitet, *portabilitet*, ansvarlig bruk av KI og robusthet i hele konfliktspekteret.

DRP legger til rette for at Forsvaret går fra «systemer og siloer» til kapabiliteter, data og robusthet. Dette skiftet er en forutsetning for at Forsvaret skal lykkes med modernisering, MDO og nasjonal beredskap.

Dette kapitlet gir en oversikt over innsatsområder i kapittel 2.1 og tilhørende prinsipper i kapittel 2.2. For utdyping, se kapittel 3.

2.1 Innsatsområder

Tabellen nedenfor viser en oversikt, med forkortelser og beskrivelse for hvert innsatsområde.

INNSATSOMRÅDE			BESKRIVELSE
	Kapabilitetsbasert utvikling av IKT	ARK	Utvikling og prioritering av IKT med utgangspunkt i Forsvarets kapabiliteter og strategiske mål, basert på dokumentert virksomhetsarkitektur, <i>sporbarhet</i> og <i>virksomhetsdrevet utvikling</i> .
	Sikker IKT i Forsvaret	SIK	Forvaltning av <i>applikasjoner</i> og <i>informasjonssystemer</i> med tydelig eierskap, kontinuerlig risikostyring og et sikkerhetsnivå som er tilpasset operativt behov og trusselbilde.
	Datadrevet forsvar og KI	DAT	Utvikling og bruk av et sikkert, sammenkoblet og datadrevet økosystem, basert på datasuverenitet, dataprodukter, felles styringsmekanismer og ansvarlig bruk av KI.
	Applikasjoner og applikasjonsutvikling	APP	Utvikling og forvaltning av applikasjoner basert på <i>modulær arkitektur</i> , <i>åpne standarder</i> og moderne utviklerpraksis, med vekt på konsolidering, interoperabilitet og helhetlig livssyklusstyring.
	Forsvarets skyløsning	FSL	Skyløsningen som understøtter tilstrekkelig <i>nasjonal kontroll</i> , robusthet, operativ handlefrihet, portabilitet, autonomi og drift på tvers av <i>cloud</i> , <i>core</i> , <i>fog</i> og <i>edge</i> i hele konfliktspekteret.
	Arkitektur og sikkerhet i digitalisert materiell	DIM	Sikker og standardisert informasjonsutveksling og innebygget sikkerhet i design, anskaffelse og forvaltning av digitalisert materiell gjennom hele livsløpet, i samsvar med Forsvarets arkitektur- og sikkerhetskrav.
	Samvirke med allierte, totalforsvaret og andre relevante aktører	SAM	Samvirke og interoperabilitet med allierte, totalforsvaret og andre relevante aktører, som styrker operativ evne og sikrer effektiv utvikling og utnyttelse av IKT.
	Gjennomgående forskning, utvikling og innovasjon (FoU&I)	FoU&I	Strategisk forankret og kapabilitetsorientert FoU, som styrker operativ evne og muliggjør innovasjon i utvikling, anskaffelser og bruk i operasjoner.
	Menneske og organisasjon	MEO	Styring og forankring av digital transformasjon som helhetlig endring i teknologi, organisasjon, ledelse og kompetanse.
	Personvern og IKT	PV	Sikre innebygd personvern og kravstilling i alle IKT løsninger, samt risikobasert behandling av personopplysninger etter etablerte prinsipper.

2.2 Prinsipper

Nedenfor vises en oversikt over prinsipper for hvert av innsatsområdene:

INNSATSOMRÅDE	PRINSIPP
	ARK1 Kapabilitetsbasert arkitektur
	ARK2 Dokumentert virksomhetsarkitektur
	ARK3 Sektororientert arkitekturutvikling
	ARK4 Datadrevet økonomistyring (<i>FinOps</i>)
	SIK1 Eierskap til applikasjoner og informasjonssystemer
	SIK2 Risikobasert sikkerhetsstyring med fortløpende sikkerhetsgodkjenning
	SIK3 <i>Security by Design</i> og <i>zero trust</i>
	SIK4 Digital beredskap og cyberoperativ evne
	DAT1 Datasuverenitet og strategisk handlefrihet
	DAT2 Desentralisert eierskap og ansvar for data og dataenes betydning
	DAT3 Ansvarlig bruk av kunstig intelligens
	APP1 Modulære applikasjoner og løse koblinger
	APP2 Standardisering
	APP3 Moderne applikasjonsutvikling
	APP4 Variantbegrensning
	APP5 <i>Interoperability by Design</i> (innebygd interoperabilitet)
	APP6 Livssyklusstyring av applikasjoner og informasjonssystemer
	FSL1 Portabilitet og teknologiavhengighet
	FSL2 Differensierte plattformtjenester
	FSL3 <i>Autonomi</i> og handlefrihet
	FSL4 Verifisert og <i>føderert identitet</i>
	FSL5 Kritiske applikasjoner i Forsvarets egne datasentre
	DIM1 Kravstille arkitektur og sikkerhet i digitalisert materiell
	SAM1 Integrert samvirke med allierte, totalforsvaret og andre relevante aktører
	SAM2 Strategisk industripartnerskap
	FoU&I1 Strategisk forankret og kapabilitetsorientert FoU&I
	FoU&I2 Kontinuerlig utfordring av eksisterende kapabiliteter og strukturer
	FoU&I3 Innovasjon i utvikling og anskaffelser
	MEO1 Helhetlig styring av digital transformasjon som organisasjonsendring
	MEO2 Kultur for endring og endringsledelse
	MEO3 Brukerinvolvering
	MEO4 Kontinuerlig utvikling og vedlikehold av digital kompetanse

	PV1	Personvern og personopplysningsikkerhet
	PV2	Dataminimering og formålsbegrensning
	PV3	Risikobasert personvernstyring
	PV4	Lagringsbegrensning
	PV5	Tydelig personopplysningsansvar

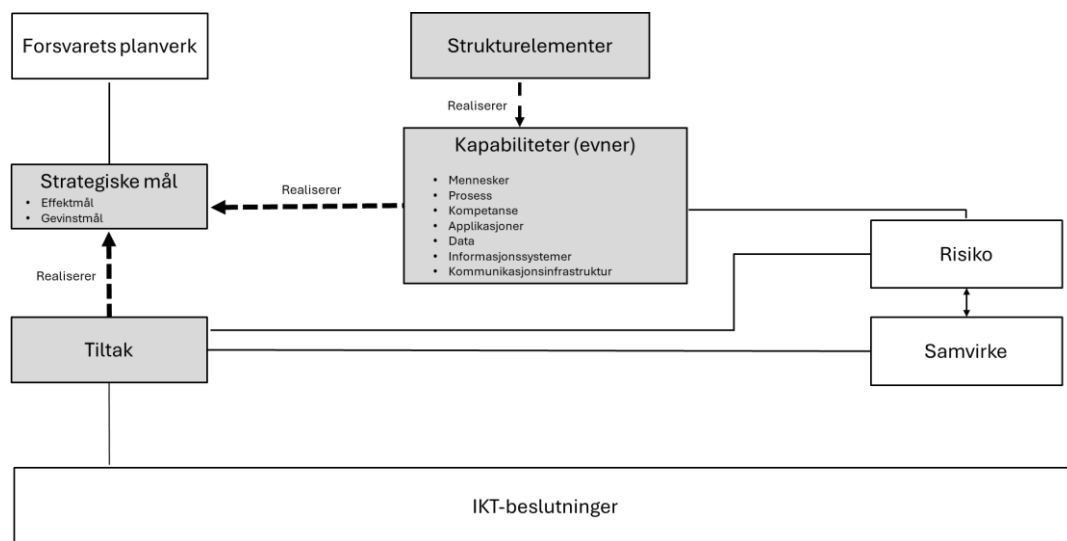
3 Detaljert beskrivelse av innsatsområder med tilhørende prinsipper

I dette kapitlet beskrives prinsippene for hvert innsatsområde. Hvert prinsipp presenteres med kortform, definisjon, formål og praktisk betydning.

3.1 Innsatsområde: Kapabilitetsbasert utvikling av IKT (ARK)

For å lykkes med den digitale transformasjonen skal Forsvaret følge en *kapabilitetsbasert utvikling*. Denne tilnærmingen er forankret i Forsvarets gjennomføringsplan (FGP) og beskrevet i delplan IKT (Forsvarsstaben, 2025).

Figur 2 gir en overordnet beskrivelse av hvordan Forsvarets IKT-arkitektur ses gjennom en kapabilitetsbasert tilnærming:



Figur 1 Overordnet kapabilitetsmodell for Forsvarets IKT-arkitektur. Kjernen i modellen vises i de grå boksene – og viser hvordan strategiske mål realiseres av tiltak og kapabiliteter. *Strukturelement* er det sentrale planelementet i Forsvarets styring i FGP og representerer Forsvarets avdelingsstruktur på et overordnet nivå (ned til bataljonsnivå). De resterende hvite boksene må inngå i en helhet, for å kunne oppnå en kapabilitetsbasert tilnærming.



ARK1: Kapabilitetsbasert arkitektur

Forsvarets IKT skal utvikles og forvaltes basert på en kapabilitetsmodell som beskriver Forsvarets evner (kapabiliteter), og arkitekturen skal organiseres rundt kapabiliteter snarere enn informasjonssystemer eller avdelinger.

Formål

Sikre at tiltak som igangsettes er direkte knyttet til Forsvarets mål, med sporbarhet og faktabaserte beslutningsgrunnlag. Beslutninger skal være dokumenterte, balanserte, sporbare og gjennomsiktede. Kapabilitetsbasert arkitektur skal skape en helhetlig forståelse av hva som må utvikles og forbedres av kapabiliteter for å nå fastsatte mål. Applikasjoner og teknologi skal ikke utvikles eller anskaffes uten tydelig bidrag til kapabilitetsforbedringer, tydelig problemforståelse, plan for realisering og finansiering i et livssyklusperspektiv.

Praktisk betydning

Forsvaret skal bruke kapabilitetsbasert arkitektur som grunnlag for helhetlig prioritering av tiltak og ressursbruk. Distribuert beslutningsmyndighet sikrer leveransehastighet, verdirealisering, samt reduserer beslutningsflaskehalser og styrker handlingsrommet til tverrfaglige team. Ressurser, investeringer og utviklingskapasitet skal brukes på tiltak som gir reell effekt i operasjoner og daglig drift. Kapabilitetene skal prioriteres etter kriterier, for eksempel kritikalitet for Forsvarets operasjoner. Se ARK2 for krav til dokumentert virksomhetsarkitektur og bruk av *kapabilitetskart* og ARK3 for felles sektororientert metodikk for arkitekturarbeid.



ARK2: Dokumentert virksomhetsarkitektur

Forsvarets virksomhetsarkitektur skal dokumenteres i verktøy for arkitektur- og sikkerhetsstyring.

Formål

Ha oversikt over Forsvarets virksomhet, mål, kapabiliteter, leveranser og understøttende IKT. Ha kontroll og oversikt over styrker og svakheter ved Forsvarets IKT. Legge grunnlag for riktige prioritering i utvikling av Forsvarets IKT. Visualisering, rapportering og analyser skal gi underlag for felles problemforståelse. Bidra til at beslutninger om utvikling av Forsvarets IKT er basert på fakta. Holde oversikt og kontroll over Forsvarets applikasjoner og informasjonssystemer. Ha kontroll med teknisk gjeld og sikkerhetstilstand i Forsvarets IKT.

Praktisk betydning

Forsvarets virksomhetsarkitektur skal baseres på en ny kapabilitetsbasert *metamodell*, som inneholder kjerneelementene vist i figur 2. Metamodellen skal være grunnlaget for strukturering og håndtering av data og *ontologier* i DAT2 og for kravstilling av digitalisert materiell i DIM1. Kapabilitetskart skal inngå i beslutningsgrunnlaget, og skal beskrive sammenhenger mellom strategiske mål, applikasjoner, teknologi, materiell, prosesser og *informasjon*. Virksomhetsarkitekturen skal dokumenteres iht. vedtatte standarder i Forsvaret basert på beste praksis og NATOs retningslinjer for arkitektur. Sporbarhet og gjennomsliktighet sikres ved å følge maler. Forsvarets virksomhetsarkitektur skal være dokumentert i Forsvarets løsning for arkitektur- og sikkerhetsstyring.



ARK3: Sektororientert arkitekturutvikling

Felles strukturert arkitekturutvikling og samhandling mellom Forsvaret og etatene i forsvarssektoren.

Formål

Sikre helhetlig utvikling av IKT, gjennom felles forståelse av sammenhenger og samvirke i utviklingen av applikasjoner og digitale verdikjeder som krysser etatsgrensene. Sektororientert arkitekturutvikling skal understøtte effektiv samhandling, informasjonsutveksling og interoperabilitet på tvers av sektoren. Sektoren skal ha en bedre utnyttelse av arkitekturressurser og informasjon, og øke felles evne til å understøtte Forsvarets mål.

Praktisk betydning

Sektororientert arkitekturutvikling innebærer etablering av felles metodikk, bruk av felles prinsipper, referansearkitekturer, standarder og *begrepsapparat*. Ledet av Forsvaret skal sektoren etablere felles samhandlingsarenaer for sektororientert arkitekturutvikling.



ARK4: Datadrevet økonomistyring (FinOps)

Forvalte Forsvarets IKT gjennom datadrevet økonomistyring (FinOps) som sikrer kostnadskontroll, transparens, bærekraft og operativ verdi.

Formål

Å sikre at investeringer, bruk og utvikling av IKT gir målbar effekt, og at Forsvaret unngår kostnadsvekst og teknisk gjeld. Datadrevet økonomistyring skal støtte bærekraftig og sporbar ressursbruk, som er begrunnet i operative behov. Datadrevet økonomistyring skal også legge til rette for ansvarlig utvikling, drift og vedlikehold av IKT.

Praktisk betydning

Forsvaret skal kontinuerlig gjennomføre kostnadsanalyse og forbruksstyring av sin IKT. En felles praksis for data-drevet økonomistyring skal gjelde for alle som utvikler og drifter sky- og containerbaserte *tjenester*. Utviklings- og driftsbeslutninger skal dokumentere verdi, effekt og kostnadseffektivitet. Kostnads- og miljøhensyn skal inngå i arkitektur, livsløpsstyring og teknologivalg. Kapasitetsstyring og teknologivalg skal legge til rette for bærekraftig og energieffektiv drift av Forsvarets IKT.

3.2 Innsatsområde: Sikker IKT i Forsvaret (SIK)

Digital suverenitet, handlefrihet og ivaretagelse av grunnleggende nasjonale funksjoner (GNF) forutsetter at Forsvarets IKT har forsvarlig sikkerhetsnivå. For Forsvaret krever dette tydelig eierskap og kontroll på IKT-porteføljen med tilhørende verdier samt en strategisk forankret sikkerhetsarkitektur. Forsvaret skal ha en kontinuerlig og gjennomgående risikobasert tilnærming iht. de til enhver tid gjeldende forretningsbehov og sikkerhetskrav. Dette krever dynamisk evne til å overvåke, oppdage og håndtere digitale trusler og ivareta digital beredskap. Security by Design, zero trust og datasentrisitet er elementer som legges til grunn for å oppnå dette. Prinsippene i SIK fastsetter sikkerhetskrav og risikobasert styring, mens realisering av disse skjer gjennom arkitektur og plattformvalg i øvrige innsatsområder, særlig FSL og APP.



SIK1: Eierskap til applikasjoner og informasjonssystemer

Alle applikasjoner og informasjonssystemer i Forsvaret skal ha et tydelig eierskap. Eierne har ansvar for etterlevelse av relevante regelverk, jevnlig sikkerhets- og risikovurdering, og iverksetting av nødvendige tiltak ved endringer eller avvik. For eierskap til data se DAT2.

Formål

Sikre at applikasjoner og informasjonssystemer har en ansvarlig eier, og at eier sikrer forsvarlig forvaltning iht. gjeldende regelverk. Sikre at risiko for applikasjonene og informasjonssystemene håndteres systematisk og på en forsvarlig måte gjennom hele livsløpet, inkludert beskytte, oppdatering og forvaltning. Hindre tap av konfidensialitet, integritet og tilgjengelighet.

Praktisk betydning

Roller og ansvar skal være tydelig plassert, slik at ingen applikasjoner og informasjonssystemer blir stående uten oppfølging eller eierskap. Eier skal følge opp applikasjonene og informasjonssystemene i hele levetiden, ivareta tilhørende risiko og avvik (iht. SIK2 og SIK4) og sikre etterfølgelse av DRP sine prinsipper for data og KI (DAT1–DAT3).



SIK2: Risikobasert sikkerhetsstyring med fortløpende sikkerhetsgodkjenning

Forsvaret skal utøve fortløpende sikkerhetsstyring av verdier gjennom hele livsløpet, fra utvikling til innføring og drift.

Formål

Sikre at sikkerhetstiltak bygger på verdi- og risikovurderinger, og at risikobildet er tilgjengelig, forankret og underlagt eierskap og styring. Etablere en dokumentert risikostyringspraksis som understøtter operative behov i fred, krise og krig. Sikre sporbarhet mellom verdi, trussel, tilstand, sikkerhetskrav og tiltak. Dette skal danne grunnlag for et forsvarlig sikkerhetsnivå og fortløpende sikkerhetsgodkjenning.

Praktisk betydning

Alle applikasjoner, informasjonssystemer, informasjon og data skal verdivurderes etter forhåndsdefinerte kriterier i design- og planleggingsfasen. Verdivurderinger skal danne grunnlag for risikobaserte sikkerhetskrav, tiltak og prioriteringer. De skal angi krav til konfidensialitet, integritet og tilgjengelighet, inkludert beskyttelse, tilgangskontroll, overvåking og hendelseshåndtering. Verdi- og risikovurderinger skal holdes oppdatert ved endringer og være tilgjengelige i arkitektur- og sikkerhetsstyringsverktøyet. Identifisert risiko skal være tydelig plassert hos ansvarlig eier, og tiltak skal dokumenteres, prioriteres og tidfestes.



SIK3: Security by Design og zero trust

Sikkerhet er en integrert og designet del av IKT fra plan/idé til utvikling og drift. Sikkerhet skal bygges inn fra start på alle nivå og integreres i UDV gjennom hele livssyklusen basert på Security by Design og zero trust.

Formål

Unngå sårbarheter og sikre nødvendig konfidensialitet, integritet og tilgjengelighet gjennom hele livssyklusen til applikasjoner, informasjonssystem og data. I dette inngår også konfidensialitet, integritet og tilgjengelighet under lagring («at rest») og informasjonsutveksling («transport»). Security by design, som en strukturert prosess, sikrer at sikkerhet blir ivaretatt tidlig og gjennom hele utviklingsløpet. Sikkerhet skal være en integrert del av arkitektur, design, utvikling, bygging, testing, realisering og drift – ikke et separat etterarbeid.

Praktisk betydning

Sikkerhet skal være en del av utviklingsprosessen, og bygge på moderne utviklingspraksis (APP3) og portabilitet (FSL1). Sikkerheten skal følge informasjon og data gjennom hele livssyklusen, og sårbarhetene skal forebygges for å styrke robusthet og motstandskraft. Tilgangsstyringen skal være dynamisk og *attributtbasert* (ABAC), der ingen aktør – internt eller eksternt – gis implisitt tillit. Applikasjoner og informasjonssystemer skal konstrueres slik at de feiler på en trygg måte, og sikkerhetsparametre, policyer og kontroller skal uttrykkes som kode. Forsvaret skal bruke *adaptive policyer* som kan tilpasses trusselbilde og situasjon. Standardisert og maskinlesbar sikkerhetsmerking, og kontinuerlig kontroll av identitet, rettigheter og tilstand beskytter selv om infrastruktur kompromitteres. For særskilte krav til sikkerhetsarkitektur i digitalisert materiell, se DIM1.



SIK4: Digital beredskap og cyberoperativ evne

Forsvarets digitale kapabiliteter skal være robuste, motstandsdyktige og i stand til å oppdage og håndtere digitale trusler samt ved behov gjenopprette nødvendig konfidensialitet, integritet og tilgjengelighet i hele konfliktspekteret – inkludert i Disconnected/disrupted, Degraded, Intermittent and Limited/Low-Bandwidth (DDIL)-situasjoner.

Formål

Sikre at Forsvaret opprettholder nødvendige digitale kapabiliteter i fred, krise og krig. Deler av Forsvarets IKT skal kunne operere autonomt og levere kritiske *funksjoner* ved bortfall av kommunikasjon. *IKT-tjenester* skal raskt kunne gjenopprettes etter hendelser. Styrke evnen til å håndtere cyberangrep, teknisk svikt og bortfall av infrastruktur. Sikre rask gjenoppretting og beskyttelse av data og funksjoner. Understøtte taktisk autonomi når kommunikasjonen er begrenset.

Praktisk betydning

Informasjonssystemer skal designes for autonom drift, feiltoleranse og kontrollert degradert modus. Fog- og edge - miljøer skal støtte lokal prosessering, midlertidig datalagring og synkronisering ved gjenopprettet forbindelse. Overvåkning, deteksjon, respons og gjenoppretting skal kunne gjøres i relevante deler av cloud, core, fog og edge. Det skal være etablerte prosesser for *respons, isolasjon, triage og gjenoppretting*. Alle informasjonssystemer skal ha dokumenterte og testede gjenopprettingsplaner som inkluderer roller, ansvar, tilhørende backupregimer og øvingskrav. Robustheten valideres gjennom jevnlig øvelser, stresstesting og simuleringer. Digital beredskap og cyberoperativ evne skal legges til grunn for arkitektur- og sikkerhetskrav i anskaffelser av digitalisert materiell (se DIM1),

3.3 Innsatsområde: Datadrevet forsvar og KI (DAT)

Evnen til å samle, bearbeide og utnytte data er en avgjørende faktor for fremtidig stridsevne. For å lykkes med MDO og oppnå beslutningsdominans, skal data forvaltes som en varig strategisk ressurs, frikoblet fra enkeltstående applikasjoner og infrastruktur.



DAT1: Datasuverenitet og strategisk handlefrihet

Data er en varig strategisk ressurs som skal forvaltes uavhengig av applikasjoner for å sikre operativ evne.

Formål

Bidra til å ivareta Forsvarets teknologiske og operative handlefrihet. Data bør så langt som mulig frigjøres fra applikasjoner for å motvirke innlåsing og garantere at Forsvaret beholder definisjonsmakten over egne data og deres mening. Data skal forvaltes slik at de er tilgjengelige for deling iht. Finnbare, Anvendelige, Klare, Troverdige, Interoperable, Sikre og Koblede (**FAKTISK**)-prinsippene.

Praktisk betydning

Data skal forvaltes som en selvstendig ressurs, lagres i **åpne formater** og der det er hensiktsmessig og mulig frikobles fra applikasjonene som genererer dem, iht. APP5 og FSL1. Applikasjoner kan lagre data selv, men skal dele felles data gjennom standardiserte grensesnitt. For å maksimere operativ verdi og gjenbruk, skal tilrettelegging av data følge FAKTISK-prinsippene. Videre er det en ambisjon at informasjonen skal bevare sin mening uavhengig av kjøremiljø.



DAT2: Desentralisert eierskap og ansvar for data og dataenes betydning

*Data skal eies og forvaltes av operative domener og fagmiljøer, og tilgjengeliggjøres som kvalitetssikrede **dataprodukter** egnet for gjenbruk, styrt av et felles sett med regler.*

Formål

Sikre at data har høy relevans og kvalitet ved at eierskapet utøves der kompetansen og bruken er størst. Dette gjelder både for de operative domeneene og funksjoner for virksomhetsstyring. Samtidig skal isolerte "datasiloer" motvirkes gjennom en **føderert styringsmodell** som balanserer eierskap i domene med sentrale standarder basert på relevante NATO-standarder og referansemodeller.

Praktisk betydning

Dataprodukter eies av det operative domenet eller fagmiljøet som skaper dem. Eierskapet forplikter til å tilgjengeliggjøre data innenfor fremtidig definerte leveransekrav som garanterer kvalitet og tilgjengelighet for resten av Forsvaret. Forsvaret skal legge til rette for eierskap og styring av eget begrepsapparat og ontologier, slik at definisjonsmakten over dataenes betydning kan ivaretas uavhengig av teknologi eller leverandør. For å oppnå lik tolkning av data og sikre interoperabilitet på tvers av Forsvaret, med totalforsvaret og med allierte, skal domenespesifikke ontologier kobles til og ses i sammenheng med Forsvarets felles ontologi. Data tilgjengeliggjøres som dataprodukter, som skal beskrives med standardiserte **metadata**. Domenene forvalter egne dataprodukter og er ansvarlige for kobling til øvre ontologi. Dataprodukter og begrepsapparat skal forankres i virksomhetsarkitekturen (ARK2). Arkitekturmodeller (ARK2) og interoperabilitet (APP5) er grunnlag for struktur, semantikk og deling. Utpekte domener eier og forvalter autoritative kilder (**grunndata**) og definisjonsmakten for tverrgående entiteter som personell, materiell og geografi. Disse utgjør en omforent sannhet som øvrige domener og informasjonssystemer skal benytte, for å sikre entydighet og eliminere dataduplikater.



DAT3: Ansvarlig bruk av kunstig intelligens

Bruk av kunstig intelligens og andre former for automatisering skal skje på en ansvarlig og etisk måte for å sikre etterprøvbarehet, tillit og kontroll på beslutningsgrunnlaget.

Formål

Sikre at beslutningsstøtte basert på KI og andre former for automatisering er sporbare, transparente og i samsvar med krigens folkerett, annet nasjonalt og internasjonalt lovverk og sektorens KI-strategi. Dette krever, basert på en risikobasert tilnærming, full innsynsrett og eierskap til algoritmer, samt evne til å se hvordan de vil fungere i bruk. Ansvar for beslutningsgrunnlag skal ikke overlates til informasjonssystemer der Forsvaret ikke selv kontrollerer hvordan virkeligheten blir beskrevet og tolket.

Praktisk betydning

Forsvaret skal etablere sporbarhet fra kilde til effektivering, uten "sorte bokser" som hindrer innsyn. Dette innebærer at Forsvaret til enhver tid skal kunne dokumentere hvilket *datasett*, hvilken versjon av koden og hvilke parametere som lå til grunn for en gitt beslutning. Dette er en forutsetning for rettslig etterprøvbarehet etter operasjoner og forvaltning. Algoritmer og modeller som Forsvaret bruker, skal kunne oppdateres fortløpende basert på nye data for å møte et dynamisk trusselbilde. Datasuverenitet behandles i DAT1. Behov for tilgjengelighet og prosessering i fog/edge behandles i FSL2.

3.4 Innsatsområde: Applikasjoner og applikasjonsutvikling (APP)

Dette innsatsområdet omfatter prinsipper for utvikling, forvaltning og modernisering av applikasjoner. Omfanget inkluderer hele livssyklusen for applikasjoner – fra design, utvikling og integrasjon til drift, videreutvikling og utfasing. Målet er å etablere en helhetlig, robust og fleksibel applikasjonsportefølje som muliggjør trygg og effektiv utnyttelse av data (i tråd med DAT) som en strategisk ressurs, både nasjonalt og i alliert samhandling.



APP1: Modulære applikasjoner og løse koblinger

Applikasjoner skal bygges som modulære komponenter med tydelig avgrenset ansvar og veldefinerte grensesnitt.

Formål

Sikre at applikasjoner kan endres, utvikles og driftes uavhengig av hverandre, slik at Forsvaret oppnår høy endringsevne, enklere forvaltning og redusert kompleksitet.

Praktisk betydning

Applikasjoner skal bygges etter prinsipper som *separation of concern* og *strong cohesion*. Hver modul har et avgrenset funksjonsområde og definerte grensesnitt. Integrasjon mellom moduler skal være så begrenset som mulig, men så tydelig som nødvendig. Eldre informasjonssystemer (legacy) skal *innkapsles*, slik at de kan levere data på moderne formater og inngå i en moderne og robust informasjonsutveksling. Modularitet bygger på standardiserte rammeverk i APP2, moderne utviklingspraksis i APP3, og interoperabilitet som beskrevet i APP5.



APP2: Standardisering

Teknologier, utviklingsrammeverk og integrasjonsmekanismer skal være basert på åpne standarder og anerkjente teknologier.

Formål

Redusere diversifisering og kompleksitet, sikre gjenbruk, kostnadseffektiv forvaltning og unngå leverandørinnlåsing.

Praktisk betydning

Forsvaret skal benytte et felles, godkjent sett av utviklingsrammeverk, utviklingsverktøy og integrasjonsmekanismer. Avvik fra fastsatte standarder skal begrunnes og håndteres gjennom etablerte arkitekturstyringsprosesser. Proprietære teknologier kan benyttes der åpne standarder ikke er tilstrekkelige, og avvik skal være særskilt begrunnet. Standardisering muliggjør modulære løsninger (APP1) og portabilitet i FSL1. Avvik fra standarder skal følges opp gjennom arkitekturprosessene (ARK2).



APP3: Moderne applikasjonsutvikling

Applikasjoner skal utvikles og forvaltes gjennom moderne utviklingspraksiser basert på DevSecOps og automatiserte CI/CD-prosesser, med integrert sikkerhet og kvalitet i hele livssyklusen.

Formål

Sikre raske, stabile og sikre leveranser, høy endringsevne og effektiv forvaltning av applikasjoner gjennom hele livssyklusen.

Praktisk betydning

Utvikling, testing, sikkerhetsharding og utrulling automatiseres gjennom standardiserte CI/CD-pipelines. Sikkerhet skal etableres tidlig og kontinuerlig iht. DevSecOps-prinsipper. Kode, konfigurasjon og infrastruktur skal være versjonert og sporbar. Leveranser skal være hyppige, kontrollerte og automatiserte med kontinuerlig forbedring basert på faktisk bruk og tilbakemeldinger fra bruker. DevSecOps og automatisering støtter Security by Design fra SIK3, modularitet fra APP1 og krav til portabilitet i FSL1.



APP4: Variantbegrensning

Forsvaret skal begrense antall applikasjoner som dekker overlappende funksjonelle behov og konsolidere applikasjonsporteføljen mot et styrt og godkjent minimum.

Formål

Redusere antall applikasjoner med overlappende funksjoner. Redusere omfang og kompleksitet i forvaltning av applikasjonsporteføljen og dermed reduserte kostnader. Applikasjonsporteføljen skal til enhver tid balanseres for å sikre best mulig samlet kost/hytte med utgangspunkt i Forsvarets kapabiliteter.

Praktisk betydning

Overlappende applikasjoner skal som hovedregel konsolideres eller fases ut. Nye applikasjoner skal som hovedregel kun etableres dersom dokumenterte behov ikke kan dekkes av gjenbruk eller videreutvikling av eksisterende applikasjoner. Konsolidering av applikasjonsporteføljen skal baseres på kapabilitetsprioriteringer (ARK1). Applikasjonsporteføljen skal styres helhetlig med utgangspunkt i arkitektur og kapabiliteter fra ARK1 og ARK2 og standardisering fra APP2. Mikrotjenester kan inngå i applikasjonsarkitekturen.



APP5: Interoperability by Design (innebygd interoperabilitet)

Interoperabilitet skal bygges inn fra starten av utviklingsløpet, slik at applikasjoner kan utveksle data og fungere sammen med andre informasjonssystemer – nasjonalt og alliert.

Formål

Sikre sømløs datadeling og samvirke internt i Forsvaret og med allierte, totalforsvaret og andre samarbeidspartnere – samt forebygge digitale siloer og teknologiske barrierer.

Praktisk betydning

Grensesnitt, dataformater og utvekslingsmekanismer skal være åpne og harmoniserte. Data skal struktureres og eksponeres slik at de kan forstås, gjenbrukes og valideres på tvers av informasjonssystemer. Relevante NATO-standarder, nasjonale interoperabilitetskrav og FMN-prinsipper skal etterleves i utvikling og anskaffelser. Interoperabilitet skal testes, dokumenteres og inngå i arkitektur- og godkjenningsprosesser. Se DIM1 for arkitektur og sikkerhet i digitalisert materiell.



APP6: Livssyklusstyring av applikasjoner og informasjonssystemer

Applikasjoner og informasjonssystemer skal forvaltes gjennom hele livssyklusen i samsvar med prinsipper for planlagt modernisering, risikohåndtering, teknisk gjeld, kontrollert utfasing og bærekraftig drift og vedlikehold.

Formål

Sikre at Forsvaret har kontroll på teknologisk modenhet, kostnadsutvikling og operativ risiko gjennom hele livssyklusen. Legge til rette for at applikasjoner og informasjonssystemer er moderne, sikre og funksjonelle – fra etablering til utfasing.

Praktisk betydning

Alle applikasjoner og informasjonssystemer skal ha dokumentert livssyklusplan, inkludert oppgraderinger, modernisering og nedleggelse. Teknisk gjeld skal kartlegges og reduseres systematisk. Det skal etableres klare kriterier for utfasing, inkludert når applikasjoner ikke lenger oppfyller behov, sikkerhetskrav eller kostnads-effektivitet. Både egenfinansiert og fellesfinansiert IKT skal inngå i samme styringsmodell. Drift og vedlikehold skal inngå i DevSecOps-modellen, med krav til sikkerhet, monitorering og håndtering.

3.5 Innsatsområde: Forsvarets skyløsning (FSL)

Forsvarets skyløsning (FSL) er en samlebetegnelse for skyplattformer og de nødvendige IKT-tjenestene, applikasjonene og data som benytter disse skyplattformene. FSL er uavhengig av tjeneste- og leveransemønstre som benyttes. FSL skal sikre nasjonal kontroll, høy motstandsdyktighet og operativ handlefrihet i krise og krig, og sikre nødvendig redundans på tvers av *cloud*, core, fog og edge, som beskrevet i Forsvarets skystrategi (2026).



FSL1: Portabilitet og teknologiavhengighet

*FSL skal designes og utvikles med egenskaper som legger til rette for at både applikasjoner og data kan flyttes sømløst mellom **skyplattformer**. Portabilitet og teknologiavhengighet skal være grunnleggende prinsipper ved all utvikling.*

Formål

Sikre at applikasjoner og data kan flyttes på tvers av skyplattformer uten vesentlige tekniske eller økonomiske hindringer. FSL skal også kunne motta applikasjoner og data fra allierte eller totalforsvaret ved behov. Dette forutsetter bruk av åpne standarder og allment anerkjente teknologier som støtter uavhengighet til proprietære løsninger.

Praktisk betydning

FSL skal utvikles med åpne, etablerte standarder samt anerkjente teknologier for å sikre interoperabilitet (APP5). Applikasjonene skal frikobles fra underliggende infrastruktur ved hjelp av containerteknologi, slik at de kan flyttes mellom skyplattformer uten behov for tilpasning. FSL skal inneholde mekanismer som muliggjør automatisert flytting av applikasjoner og data mellom ulike skyplattformer. Arkitekturen skal vurderes eksplisitt opp mot risiko og leverandørbinding. Flytting av applikasjoner og data skal kunne gjennomføres uten uforholdsmessige kostnader eller begrensninger som reduserer Forsvarets handlefrihet. Automatisering, infrastruktur som kode og standardiserte DevSecOps-verktøy skal benyttes for å muliggjøre rask reetablering i alternative miljøer. Portabilitet bygger på bruk av standarder fra APP2 og sikkerhetsprinsipper fra SIK3 og SIK4. Applikasjoner skal kunne flyttes i samsvar med modularitet i APP1.



FSL2: Differensierte plattformtjenester

FSL skal utvikles med differensierte egenskaper som spenner fra sentrale datasentre til den taktiske ytterkanten (Cloud-to-Edge). Tilgjengelige plattformtjenester og kapasitet for prosessering og lagring skal differensieres slik at det er tilpasset reelle behov på tvers av cloud, core, fog og edge.

Formål

Sikre at Forsvaret utvikler plattformegenskaper og kapasitet i de ulike delene av FSL som er nødvendig basert på brukernes reelle behov, herunder krav til responstid, tilgjengelighet og bruk i degraderte situasjoner. Sikre at FSL ikke overdimensjoneres unødvendig. Grad av distribusjon og kapasitet i cloud, core, fog og edge skal fastsettes basert på konkrete operative behov, og ikke som et generelt krav om lik funksjonalitet i alle lag.

Praktisk betydning

Det skal gjennomføres grundige vurderinger av hvilke egenskaper og hvilken kapasitet FSL skal ha, i hele spennet fra cloud til edge. Prosessering av dataprodukter skal så langt som mulig foregå distribuert, fremfor sentralisert. Distribuert drift og autonomi i fog/edge-miljøer skal understøtte datasuverenitet i DAT1, dataprodukter i DAT2 og KI-bruk i DAT3. Fog- og edge-miljøer skal utformes slik at de kan operere selvstendig i DDIL-situasjoner, det vil si ved begrenset, ustabil eller manglende tilkobling til sentrale informasjonssystemer. Data og applikasjoner i fog- og edge-miljøer skal kunne operere autonomt under slike forhold. Når forbindelsen gjenopprettes, skal systemene synkroniseres for å sikre felles situasjonsforståelse.



FSL3: Autonomi og handlefrihet

FSL skal bygges med en distribuert arkitektur som muliggjør autonomi og handlefrihet i Forsvarets operasjoner, uavhengig av geografisk plassering.

Formål

Sikre at Forsvaret skal kunne gjennomføre sine operasjoner på alle nivå, i alle geografiske deler av landet. Dette innebærer at man eliminerer sårbarheter som kan gi manglende tilgang til sentrale tjenester, slik at det også ved ustabil eller manglende kommunikasjon, varierende båndbredde opprettholder intakte sensor-til-effektor-kjeder. Muliggjøre effektiv utnyttelse av data også under degraderte forhold, og understøtte MDO i nasjonal og alliert kontekst. Sikre at utvikling og forvaltning av plattformer og applikasjoner skal kunne gjennomføres uavhengig av tilgang til sentrale tjenester. Prinsippet uttrykker en ambisjon om økt autonomi i kritiske kapabiliteter, ikke et krav om full replikering av alle data og tjenester i alle lag.

Praktisk betydning

FSL utvikles med *skytenester* og egenskaper som man finner i de *hyperskalerbare skyplattformene*, men tilpasset Forsvarets behov og særegenheter. Applikasjoner og data plasseres der de sikrer og understøtter Forsvarets operasjoner på alle nivå, sentralt og regionalt og i taktisk ytterkant. Skyplattformene utvikles med egenskaper som understøtter asynkron samhandling, midlertidig datalagring og kontrollert synkronisering når kommunikasjon gjenopprettes. Informasjonssystemene testes og øves regelmessig for drift under frakoblede og degraderte forhold. Autonomi i alle ledd støttes av differensiering i FSL2 og interoperabilitet i APP5.



FSL4: Verifisert og føderert identitet

*Tilgang til data og applikasjoner skal baseres på *verifisert identitet*. Identiteter skal kunne fødereres mellom Forsvaret, allierte i NATO og totalforsvaret.*

Formål

Sikre at data beskyttes, deles, og utnyttes sikkert, på tvers av organisatoriske og nasjonale grenser, basert på en kjent og verifisert identitet. Sikre at kjente identiteter er knyttet til både personer og maskiner og eventuelt enheter. Sikre at identiteter kan fødereres med allierte i NATO og aktører i totalforsvaret, basert på anerkjente standarder og tillitsrammeverk.

Praktisk betydning

Forsvaret må implementere en løsning for identitetshåndtering inntil en felles identitetsløsning for forsvarssektoren eventuelt er på plass. Tilgang til data styres basert på identitet, attributter og kontekst (f.eks. rolle, sikkerhetsnivå, lokasjon og tid). Føderert identitet benyttes for samhandling med allierte og NATO, med klare tillitsavtaler, sertifikater og standardiserte protokoller. Identitet, autentisering og aksesskontroll er konsistente på tvers av cloud, core, fog og edge. Fødererte identiteter muliggjør interoperabilitet i APP5, datadeling i DAT2, og støtte til alliert samvirke som beskrevet i SAM1.



FSL5: Kritiske applikasjoner i Forsvarets egne datasentre

Kritiske og strategisk viktige applikasjoner og data skal som hovedregel plasseres i Forsvarets egne datasentre, der Forsvaret har full kontroll over plattform, drift og sikkerhet.

Formål

Sikre tilstrekkelig nasjonal kontroll, digital suverenitet og operativ handlefrihet i fred, krise og krig. Redusere risiko knyttet til geopolitisk usikkerhet, leverandørvhengighet og tap av styring over kritiske digitale verdikjeder. Legge til rette for at Forsvaret kan opprettholde og reetablere kritiske digitale kapabiliteter ved bortfall av eksterne tjenester eller internasjonal infrastruktur.

Praktisk betydning

Verdi- og risikovurdering av applikasjoner og data skal danne grunnlag for vurderingen av hvilke som anses som kritisk eller strategisk viktig. Slike applikasjoner og tilhørende data skal som hovedregel driftes på Forsvarets private skyplattform i egne datasentre. Avvik krever begrunnelse basert på risikovurdering.

3.6 Innsatsområde: IKT-arkitektur og -sikkerhet i digitalisert materiell (DIM)

Forsvaret står foran omfattende materiellanskaffelser de neste årene. Moderne operasjoner forutsetter at data fra sensorer, våpensystemer og andre interne informasjonssystemer kan deles sømløst. En slik deling av informasjon er nødvendig for å sikre situasjonsforståelse og effektiv beslutningsstøtte.



DIM1: Kravstille arkitektur og sikkerhet i digitalisert materiell

For å sikre interoperabilitet, datadeling og effektiv utnyttelse av informasjon på tvers av domener, skal krav til IKT-arkitektur og sikkerhet integreres tidlig i fremskaffelse av digitalisert materiell.

Formål

Sikre at digitalisert materiell legger til rette for informasjonsutveksling og interoperabilitet i Forsvarets digitale verdikjeder, både internt og med allierte. Relevante data skal fortrinnsvis flyte automatisk til og fra sensorer, effektorer og styringssystemer i digitalisert materiell. Sikre at arkitektur og sikkerhet blir tilstrekkelig ivaretatt i kravstillingen til digitalisert materiell som skal fremskaffes. Videre skal prinsippet sikre samspill mellom anskaffelsesprosjekter, designansvarlige på materiellsiden, sikkerhetsarkitekter, informasjonsarkitekter og øvrige IKT-arkitekter.

Praktisk betydning

IKT-arkitektur og sikkerhet skal være sentrale hensyn allerede i konsept- og designfasen av nye digitalisert materiellanskaffelser, basert på virksomhetsarkitekturen i ARK2, sikkerhetsprinsipper i SIK4, og interoperabilitetskrav i APP5. Dette innebærer at arkitekturprinsipper, standarder, sikkerhetskrav, datautvekslingskrav og øvrige IKT-arkitekturkrav skal vurderes på lik linje med andre spesifikasjoner for det digitaliserte materialet som skal anskaffes. I tilfeller der Forsvaret ikke kan påvirke IKT-arkitekturen i materialet som skal anskaffes, skal det gjøres arkitekturvurderinger for å sikre at eventuelle avvik gir minimale negative konsekvenser for eksisterende arkitektur.

3.7 **Innsatsområde: Samvirke med allierte, totalforsvaret og andre relevante aktører (SAM)**

Samvirke med allierte, totalforsvaret, industrien og andre relevante aktører er en nøkkelfaktor for Forsvarets digitale transformasjon. Samarbeid om utvikling, drift og vedlikehold av IKT gir tilgang til kompetanse, ny teknologi og innovasjon, samt legger til rette for smidig informasjonssystem- og applikasjonsutvikling, kostnadseffektivisering og økt nasjonal samfunnsnytte.



SAM1: Integrert samvirke med allierte, totalforsvaret og andre relevante aktører

Samvirke med allierte, totalforsvaret og relevante aktører skal være en integrert del av den digitale transformasjonen.

Formål

Sikre at Forsvarets IKT utvikles i samarbeid med relevante partnere, for å øke operativ evne og nasjonal beredskap. Tilnærmingen vil gi helhetlige informasjonssystemer på tvers av forsvarssektoren, totalforsvaret og andre relevante aktører.

Praktisk betydning

Planlegging og utvikling av Forsvarets IKT skal skje i tett dialog med partnere for å unngå siloer og sikre interoperabilitet (APP5). Utviklingsprosjekter skal inkludere representanter fra totalforsvaret tidlig i planleggingen. Allierte og andre relevante aktører deltar ved behov.



SAM2: Strategisk industripartnerskap

Forsvaret skal etablere avtaler og samarbeidsmodeller med industrien som sikrer fleksibilitet, sikkerhet og samfunnsnytte.

Formål

Sikre tilgang til innovasjon, teknologi og nasjonal verdiskaping. Forsvaret er avhengig av industrien for å lykkes med den digitale transformasjonen og understøttelse av MDO.

Praktisk betydning

Forsvaret skal inngå avtaler og samarbeidsmodeller med industrien, som gir økt operativ evne raskere og mer kosteffektivt. Forsvaret skal tilrettelegge for fleksible samarbeidsmodeller. Det skal være en sammenheng mellom spesifikke IKT-kapabiliteter og IKT-sourcingstrategien som utvikles i 2026.

3.8 Innsatsområde: Gjennomgående forskning, utvikling og innovasjon (FoU&I)

Gjennomgående og målrettet forskning, utvikling og innovasjon (FoU&I) for Forsvaret, innebærer å satse på moderne og nyskapende IKT. Dette styrker Forsvarets evne til å møte fremtidige utfordringer og sikrer at Forsvaret har tilgang til kompetanse om moderne teknologi og for økt operativ evne og beredskap.



FoU&I1: Strategisk forankret og kapabilitetsorientert FoU&I

FoU&I i Forsvaret skal forankres i overordnede strategier og mål, slik at tiltak legger til rette for kapabilitetsforbedring som gir økt operativ evne gjennom målrettet ressursbruk.

Formål

Sikre at FoU&I er strategisk forankret, kapabilitetsorientert og -effektdrevet.

Praktisk betydning

Langsiktig FoU&I skal være strategisk forankret og kapabilitetsorientert. Langsiktig FoU&I skal der relevant og mulig omhandle banebrytende konsepter for å øke Forsvarets operative evne. FoU&I skal derfor ikke være siloorientert til domener, grener og doktriner. Forsvaret skal ha mål og hypoteser for alle innovasjonstiltak, samt plan for validering, eventuell skalering, anskaffelse og implementering. Tiltak som ikke oppnår ønsket effekt eller ikke lar seg skalere, skal avsluttes tidligst mulig.



FoU&I2: Kontinuerlig utfordring av eksisterende kapabiliteter og strukturer

Kontinuerlig utfordre og forbedre eksisterende kapabiliteter og strukturer for å bryte kostnadsbaner tidlig i verdikjeden.

Formål

Sikre at Forsvarets digitale transformasjon kan utfordre eksisterende kapabiliteter og strukturer, for å bryte kostnadsbanene gjennom innovasjon så tidlig som mulig i verdikjeden. Forsvaret skal etablere hensiktsmessige kulturer og prosesser for dette.

Praktisk betydning

FoU&I skal utfordre eksisterende kapabiliteter og strukturer for at Forsvaret skal oppnå mest mulig operativ evne ut fra tilgjengelige midler. Innovasjon skal knyttes tett til Forsvarets behov, og utvikles i tett samarbeid med behovseierne.



FoU&I3: Innovasjon i utvikling og anskaffelser

Anskaffelser skal legge til rette for hurtig prototyping, testing og kontinuerlig innovasjon og forbedring.

Formål

Forsvaret skal ivareta og styrke muligheten for innovasjon i utvikling og anskaffelser, samtidig som hensyn til tid, kostnad, ytelse og bærekraft balanseres. Dette skal gjøres ved å stille krav i kontrakter til blant annet åpne grensesnitt, dataprodukter og modulær integrasjon. Forsvaret skal søke å fremme reell konkurranse ved at leverandører skal konkurrere på like vilkår uten vertikal dominans eller innlåsing.

Praktisk betydning

Krav om åpne grensesnitt gir Forsvaret økt fleksibilitet til å velge, bytte, videreutvikle og/eller oppgradere IKT-løsninger over tid. Dette kan styrke konkurransen, redusere avhengighet til enkeltleverandører og legge til rette for bedre kostnadseffektivitet og langsiktig verdiskaping.

3.9 Innsatsområde: Menneske og organisasjon (MEO)

Forsvarets digitale transformasjon forutsetter god styring, en kultur for læring og samarbeid, aktiv brukerinvolvering og målrettet utvikling av digital kompetanse. Samlet legger dette til rette for at nye IKT-løsninger tas i bruk på en effektiv måte, gir ønsket effekt og styrker Forsvarets operative evne – samtidig som risikoen for feilinvesteringer og manglende gevinstrealisering reduseres.



MEO1: Helhetlig styring av digital transformasjon som organisasjonsendring

Digital transformasjon skal styres som en helhetlig organisasjonsendring, der teknologi, mennesker, organisasjon og ledelse inngår som integrerte og gjensidig avhengige elementer.

Formål

Sikre at beslutninger om den digitale transformasjonen er helhetlige, balanserte og bygger på både tekniske og organisatoriske vurderinger. Skape en felles forståelse for formål, konsekvenser og fremdrift, samt muliggjøre systematisk oppfølging, kontinuerlig forbedring og gevinstrealisering. Styrke sammenhengen mellom teknologi, kompetanse, kapabiliteter og operativ evne. Prinsippet skal legge til rette for at tiltak understøtter kapabiliteter (ARK1), gi operativ verdi og ivareta krav til sikkerhet og risiko SIK2.

Praktisk betydning

Beslutningsunderlag skal inkludere vurderinger av konsekvenser for menneske og organisasjon. Forsvaret skal etablere strukturert og kontinuerlig kommunikasjon, med toveis dialog og budskap tilpasset ulike målgrupper. Forsvaret skal tydelig plassere ansvar for oppfølging av tilbakemeldinger og gevinstrealisering etter innføring. Beslutningsgrunnlag for den digitale transformasjonen skal omfatte vurdering av endringskapasitet, kompetansebehov og belastning fra parallelle initiativer. Forsvaret skal utarbeide kompetanseplaner som identifiserer gap og tiltak for å lukke dem. Tiltak skal tilpasses Forsvarets faktiske kapasitet eller vurdere behovet for tilførsel av nødvendig kapasitet.



MEO2: Kultur for endring og endringsledelse

Forsvaret skal fremme en kultur for kontinuerlig utvikling, læring og kunnskapsdeling som støtter digital transformasjon.

Formål

Sikre at ledere setter retning, inspirerer og kobler teknologi til operativ evne. Forsvaret skal styrke evnen til å tilpasse seg endringer, utnytte teknologi og videreutvikle kapabiliteter gjennom systematisk deling av kompetanse og erfaring. Ledere skal bygge relasjoner på tvers av fagmiljøer og omsette teknologiens muligheter til prioriteringer og handlinger med målbar effekt.

Praktisk betydning

Forsvaret skal legge til rette for en kultur preget av nysgjerrighet, læring, eksperimentering og tverrfaglig samarbeid. Ledere skal aktivt lede endring gjennom tydelig retning, prioriteringer, kommunikasjon og oppfølging, samt sikre forankring på tvers av fagmiljøer. Det skal legges til rette for å prøve og feile, og erfaringer og kompetanse skal deles systematisk, blant annet gjennom felles digitale læringsarenaer. Læring og erfaringsdeling skal understøtte kontinuerlig forbedring i utvikling og drift av IKT (APP3) og integreres i arbeidsprosesser og kapabilitetsutvikling (ARK1). Læring skal øke kvaliteten i beslutninger og leveranser, og omfatte erfaringer fra sikkerhetshendelser, risikovurderinger og etterlevelse av sikkerhetskrav (SIK2, SIK3). Oppfølging av prinsippet skjer gjennom etablerte styrings- og utviklingsprosesser i IKT-styringsmodellen.



MEO3: Brukerinvolvering

Forsvarets IKT skal utvikles og forvaltes brukerorientert, basert på dokumenterte behov, slik at løsningene gir nytte, styrker operativ evne og er enkle å ta i bruk.

Formål

Sikre at IKT gir målbar verdi og understøtter Forsvarets operative evne, beredskap og virksomhetsstyring gjennom IKT-løsninger tilpasset brukernes oppgaver og behov. Redusere risiko for feilinvesteringer, lav adopsjon, omgørelser og uønsket praksis. Styrke kvalitet, effektivitet og sikker etterlevelse.

Praktisk betydning

Brukerbehov og forventet nytteverdi skal dokumenteres som en del av beslutningsgrunnlaget (se ARK1 og ARK2). Brukerorientering innebærer tidlig og jevnlig involvering av representative brukere, evaluering av brukeropplevelse og oppgaveløsning, samt iterativ forbedring i samsvar med moderne utviklingspraksis (se APP3). Krav til sikkerhet og kontroll skal integreres uten å skape unødvendig friksjon i oppgaveløsningen (SIK3).



MEO4: Kontinuerlig utvikling og vedlikehold av digital kompetanse

Forsvaret skal kontinuerlig utvikle og vedlikeholde digital kompetanse på tvers av relevante fagmiljøer, som en forutsetning for effektiv og sikker bruk av IKT.

Formål

Sikre at medarbeidere har tilstrekkelig digital kompetanse, herunder forståelse for hvordan data struktureres, beskyttes og utnyttes i en moderne, modulær IKT-arkitektur. Dette legger til rette for trygg og effektiv informasjonsutveksling, økt interoperabilitet og robust cybersikkerhet, med mål om økt motstandsdyktighet og fleksibilitet i møte med nye trusler og teknologiske endringer. Kompetansen skal legge til rette for innovasjon og økt evne til å ta i bruk IKT på nye og mer effektive måter. Digital kompetansen skal understøtte de andre prinsippene i DRP.

Praktisk betydning

Forsvaret skal systematisk bygge digital kompetanse i form av kunnskap, ferdigheter, evne og holdninger, som gjør organisasjonen i stand til å utnytte data sikkert, effektivt og fleksibelt over tid. Økt kompetanse legger til rette for mer effektive arbeidsprosesser, bedre beslutningsgrunnlag, redusert risiko for sikkerhetsbrudd – samt økt evne til innovasjon og ny anvendelse av teknologi. Medarbeiderne skal ha økt forståelse for hvordan data er strukturert, delt og beskyttet. Økt kompetanse legger til rette for at medarbeidere håndterer informasjon riktig som en naturlig del av arbeidshverdagen – og ikke som et tillegg eller hinder – med mål om færre feil i deling og bruk av data, og en mer robust organisasjon.

3.10 Innsatsområde: Personvern og IKT (PV)

Forsvaret skal sikre personvernet ved å bygge det inn som standard i IKT-systemene.

Personopplysninger skal behandles etter etablerte prinsipper og med nødvendig risikostyring. Personvern skal kravstilles når Forsvaret utvikler, kjøper eller bruker digitale løsninger.



PV1: Personvern og personopplysningssikkerhet

Personvern skal ivaretas gjennom hele livssyklusen for informasjon, data, identiteter, prosesser og digitale løsninger. Behandling av personopplysninger skal, ivareta grunnleggende personvernprinsipper, være underlagt risikobasert personvernstyring og basert på innebygd personvern og personvern som standardinnstilling.

Formål

Sikre tillit, ivareta den enkeltes rettigheter og redusere risiko for uforholdsmessige inngrep i personvernet ved utvikling og bruk av digitale løsninger.

Praktisk betydning

Personvern skal vurderes i alle digitaliserings- og moderniseringstiltak. Personvernkrav skal være en innebygd del av arkitektur-, sikkerhets- og anskaffelsesprosesser. Løsninger skal utformes slik at personopplysninger ikke behandles i større omfang enn nødvendig. Prinsippet om *Privacy by design* skal ivaretas i utvikling drift og vedlikehold av Forsvarets IKT. Plassering av systemeierskapet påvirker ikke personvernregelverkets krav til regler for plassering av *Behandlingsansvar*. Dette ansvaret må ivaretas.



PV2: Dataminimering og formålsbegrensning

Personopplysninger skal kun samles inn, deles, lagres og behandles når det er nødvendig for et definert og legitimt formål.

Formål

Sikre at data som er lagret i Forsvarets systemer har et omfang som er tilstrekkelig for formålet

Praktisk betydning

Nødvendighetskravet knyttet til datainnsamling er ikke alltid like klart og vil kunne endres mellom fasene fred, krise og krig. Forsvaret har en svært stor adgang til å innhente og behandle opplysninger ved en eskalering. Det skal ikke samles inn flere personopplysninger enn nødvendig for oppgaven. Personopplysninger skal ikke gjenbrukes til nye formål uten særskilt vurdering. Deling av personopplysninger skal begrenses til aktører med tjenstlig behov. *Anonymisering* eller *pseudonymisering* skal benyttes når formålet kan oppnås uten direkte identifisering



PV3: Risikobasert personvernstyring

Behandlinger som kan medføre høy risiko for enkeltpersoners rettigheter og friheter skal underlegges personvern vurderinger

Formål

Sikre prosesser for vurderinger av personvernkonsekvenser og risikoreduserende tiltak

Praktisk betydning

Ved etablering eller vesentlige endringer av IKT skal det vurderes om behandlingene krever:

- personvernkonsekvensvurdering (DPIA)
- risikoreduserende tiltak



PV4: Lagringsbegrensning

Personopplysninger skal ikke lagres lenger enn nødvendig for formålet, med mindre lov, forskrift eller operative krav tilsier noe annet

Formål

Sikre at personopplysninger lagres i tråd med forskrifter

Praktisk betydning

Alle informasjonssystemer skal ha definerte regler for lagring og sletting av personopplysninger. Opplysninger som ikke lenger er nødvendige skal slettes eller anonymiseres. Behov for langtidslagring skal dokumenteres og baseres på en nødvendighetsvurdering



PV5: Tydelig personopplysningsansvar

Ansvar for behandling av personopplysninger skal være tydelig definert og dokumentert

Formål

Sikre tydelig ansvar for behandling av personopplysninger i Forsvarets IKT

Praktisk betydning

Systemeier skal sikre at personvernkrav er ivarettatt. Dataeier skal ha oversikt over hvilke personopplysninger som behandles. Behandlingsansvar og databehandlerforhold skal være dokumentert. Personvernombud eller personvernrådgiver skal involveres ved behandlinger med vesentlig personvernrisiko

4 Begreper

Dette kapittelet er første versjon av et systematisk og forvaltet begrepsapparat for IKT i Forsvaret. Enkelte begreper er ikke nevnt i DRP, men finnes i andre styrende dokumenter som Forsvarets skystrategi (2026) og Forsvarets datasentriske arkitektur (2026)).

BEGREP	FORKLARING
Adaptive policyer	Policyer som automatisk tilpasses kontekst og risiko, basert på faktorer som bruker, enhet, lokasjon og atferd, for å sikre riktig tilgang og sikkerhetsnivå til enhver tid.
Allmenn sky	En type leveransemodell. Standardiserte skytjenester som leveres på det åpne markedet og er tilgjengelig for alle virksomheter (Direktoratet for forvaltning og økonomistyring, 2025).
Anonymisering	Å gjøre personopplysninger anonyme, slik at det ikke lenger er mulig å avdekke hvem opplysningene gjelder. Anonymiserte opplysninger regnes ikke som personopplysninger.
Applikasjon	Programvare som utfører en eller flere spesifikke funksjoner. Applikasjoner kan utføre eller tilby tjenester for sluttbrukere og for andre applikasjoner eller virksomhetsprosesser (Shirey, aug. 2007). I sammenheng med sky er en applikasjon en samling av skytjenester som understøtter en eller flere virksomhetsprosesser, f.eks. ildledning, situasjonsbilde eller logistikk.
Arkitektur	«The fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution» (NATO, 2026).
Attributtbasert tilgangsstyring (ABAC)	En modell for tilgangsstyring der tilgangsrettigheter tildeles dynamisk basert på en kombinasjon av egenskaper (attributter) ved brukeren, ressursen og den aktuelle konteksten (f.eks. tid og sted).
Autonomi	Evnen til å opprettholde funksjonalitet lokalt uten avhengighet til sentrale tjenester eller kontinuerlig nettverksforbindelse.
Begrepsapparat	Hvordan en virksomhet definerer og bruker begreper. Det består gjerne av definisjoner, avgrensninger, forklaringer og eksempler. Et begrepsapparat er primært laget for mennesker for å sikre en felles forståelse, bedre kommunikasjon og forhindre begrepsforvirring.
Behandlingsansvar	Behandlingsansvarlig» betyr den fysiske eller juridiske personen, offentlige myndigheten, institusjonen eller et annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. (Personvernforordningen artikkel 4 nr. 7)
CI/CD	En metode innen programvareutvikling som automatiserer trinnene mellom å skrive kode og å sette den i produksjon. CI/CD gjør det mulig for utviklingsteam å levere kodeendringer oftere og mer pålitelig gjennom automatisert testing, bygging og distribusjon (IBM, 2025a).
Cloud	Samlebegrep for allmenn sky, nasjonal sky og alliert sky. Slike skyplattformer gir høy elastisitet, der kapasitet kan skaleres raskt opp og ned etter behov. Cloud er ett av fire lag i Forsvarets skyløsning, sammen med core, fog og edge.
Cloud native	Applikasjoner designet for å utnytte egenskapene i skyteknologi fullt ut. Innebærer gjerne bruk av mikrotjenester, konteinere og orkestrering (Cloud native Foundation, 2026).
Containerbaserte applikasjoner	En programvare som pakkes sammen med alle nødvendige komponenter – inkludert kode, biblioteker, konfigurasjonsfiler og kjøretidsmiljø – i en isolert og selvstendig enhet (container). Dette gir portabilitet, skalerbarhet og isolasjon mellom applikasjoner.
Core	Sentralt lag i en distribuert IT-struktur – typisk tilsvarende sentralisert cloud computing. Dette kjennetegnes av store databehandlingsressurser, f.eks. datasentre eller store skyregioner, høy kapasitet og skalerbarhet, optimalt for tung databehandling, langtidslagring og avansert analyse. Ikke lokasjonsnært, noe som innebærer større avhengighet av nettverksforbindelser og potensielt høyere latenstid.
Data	Symboler eller signaler, uten tillagt meningsinnhold før det er satt i en sammenheng (basert på bl.a. Christensen et al., 1999; Floridi, 2002; Kristiansen & Elstad, 2022)
Datadomene	En logisk gruppering av relaterte data tilpasset et spesifikt forretningsområde eller funksjon. Administrert av eksperter med spesialisert funksjonell ekspertise, gir den et rammeverk for organisering, styring og produksjon av dataprodukter. Dette sikrer

	konsistens, klarhet og overholdelse av regulatoriske krav og standarder, samtidig som det legger til rette for effektiv informasjonsdeling.
Datakontrakt	En formell beskrivelse av betingelsene for tilgang til og bruk av et dataprodukt, utarbeidet og forvaltet av dataproduktets eier. Kontrakten beskriver tekniske krav, skjermings- og delingsbetingelser, kvalitetskrav og livssyklusinformasjon
Dataplattform	Et integrert miljø som gjør det mulig å dele og bruke data på tvers av organisasjonen ved å gjøre dem søkbare, tilgjengelige og klare for bruk, og som sikrer at data kan forvaltes gjennom hele livssyklusen.
Dataprodukt	En samling dataobjekter, pakket med essensielle metadata, som er designet for å være gjenbrukbare, oppdagelige og interoperable på tvers av ulike miljøer.
Dataproduktkatalog	En søkbar oversikt over dataprodukter som gjør det mulig for konsumenter å oppdage, abonnere på og få tilgang til dataprodukter gjennom standardiserte grensesnitt
Datasentrisk arkitektur	Teknisk realisering der data er det primære organiserende elementet, strukturert som delbare, styrte og standardiserte dataprodukter innenfor en føderert modell som sikrer interoperabilitet, kvalitet og sikkerhet på tvers av informasjonssystemer og organisasjoner. (basert på NATO Data Centric Reference Architecture (NATO 2024a)).
Datasentrisk sikkerhet	Sikkerhetsmekanismer, der beskyttelsesmekanismene legges direkte på dataene uavhengig av hvor dataene befinner seg, slik at konfidensialitet, integritet og tilgjengelighet opprettholdes gjennom hele livssyklusen.
Datasentrisk tilnærming	Overordnet tilnærming, som omhandler en felles intensjon om å behandle data som en delt ressurs som kan utnyttes av alle til å gjennomføre operasjoner. Intensjonen omfatter deling, utveksling, verdsettelse og utnyttelse av data.
Datasett	En strukturert samling data som er ordnet og lagret på en måte som muliggjør effektiv behandling, analyse og videre bruk. Et datasett består typisk av flere datapunkter organisert i rader og kolonner eller andre faste formater. Datasett inneholder både selve dataene og nødvendig metadata som beskriver innhold, struktur og kontekst.
DevSecOps	Er en forkortelse for Development, Security and Operation (utvikling, sikkerhet og drift). DevSecOps er en praksis for applikasjonsutvikling som automatiserer integreringen av sikkerhet og sikkerhetspraksiser i alle faser av livssyklusen til programvareutvikling – fra innledende design til integrasjon, testing, levering og utrulling (IBM, 2025).
Digital grunnmur	Består av IT-plattform, infrastruktur og kommunikasjon. IT-plattformen omfatter felles programvare, maskinvare og kjernetjenester som gir et sikkert og fleksibelt kjøremiljø for applikasjoner. Infrastruktur omfatter maskinvare for prosessering, lagring, brannmur og datasentre. Kommunikasjon er overføring av data mellom applikasjoner og tjenester, for eksempel via Forsvarets høyhastighets transportnett, SATCOM, radiosystemer og 5G.
Digital transformasjon	Kan beskrives som: • en prosess der virksomheten endrer hvordan den utfører sine oppgaver, tilbyr bedre tjenester, jobber mer effektivt eller skaper nye tjenester ○ [...] brukeropplevelsen er selve kjernen i endringen ○ [...] baserer seg på utnyttelse av digital teknologi • en grunnleggende og omfattende endring, og ikke en mindre justering • redesign av virksomheten på alle nivå – folk, prosesser, teknologi og styring». (Digdir, 2025).
Digital verdikjede	En digital verdikjede er en sammenhengende ende-til-ende-flyt av data fra innhenting til beslutning og effekt, der sensorer, systemer, plattformer, applikasjoner og prosesser samvirker for å omdanne data til informasjon, innsikt og verdiskaping. Digitale verdikjeder bør understøtte datasentrisitet, sikkerhet, interoperabilitet, datadeling og effektiv utnyttelse av informasjonsressurser Beskriver hvordan leveranser, teknologiske komponenter og data henger sammen mellom virksomheter (Lysne, 2020, s. 10). Den omfatter sammenhengende digitale prosesser og dataflyt internt og på tvers av organisatoriske og teknologiske grenser, og viser hvordan data produseres, deles og utnyttes i ulike ledd. Verdikjeden inkluderer også avhengighetene mellom aktører og komponenter, som påvirker styring, risiko og verdiskaping.
Digitalisert materiell	Materiellsystemer der IKT utgjør en integrert del av systemets funksjon. Interoperabilitet, samvirke og dataflyt utgjør en dimensjonerende delmengde av det digitaliserte materielllets operative evne.

Edge	Noder plassert ytterst i Forsvarets skyløsning, der data genereres, behandles og brukes nær operasjonen. De muliggjør lokal databehandling tett på sensorer, plattformer og brukere, og bidrar til økt robusthet gjennom autonomi, redusert nettverkstrafikk og lavere forsinkelse.
Egenfinansiert IKT	«[...] representerer all IKT som er nødvendig, utover det som leveres gjennom Fellesfinansiert IKT, for at strukturelementet skal kunne operere både autonomt og i fellesoperasjoner. Egenfinansiert IKT må kunne samvirke med den Fellesfinansierte og inngå i en helhetlig dataflyt fra sensorer til applikasjoner som prosesserer data som grunnlag for kommando og kontroll, ildordre og logistikk. For å sikre evnen til samvirke fordrer det at IKT som innsatsfaktor følger de føringer som gis sentralt for arkitektur, sikkerhet, dataformater med mer» (Forsvarsstaben, 2025b).
Essensielle egenskaper ved skytjenester	• Bred nettverkstilgang (Broad network access): IKT-tjenestene er et annet sted og du får tilgang over nettverk. • Høy elastisitet, skalerbar (Rapid elasticity): Kapasitet kan skaleres raskt opp og ned etter behov • Ressursdeling (Resource pooling): Felles ressurser ved at datakraft og kostnader deles mellom kundene • Målbare IKT-tjenester (Measured service): Du betaler for det du faktisk bruker • On-demand selvbetjening (On-demand self-service): setter opp og administrerer IKT-tjenester selv. (Direktoratet for forvaltning og økonomistyring, 2025; Mell, P., & Grance, T. (2011)).
Exit-strategi (for sky)	En plan som beskriver hvordan IKT-tjenester, applikasjoner, data og tilhørende infrastruktur kan flyttes til en alternativ løsning eller avvikles på en kontrollert og risikobasert måte. Planen omfatter typisk tekniske, juridiske og organisatoriske forhold, og kan inkludere prosesser for flytting, avvikling, databehandling og håndtering av avhengigheter til leverandører og tjenester.
FAKTISK	Forsvarets dataprinsipper utviklet med utgangspunkt i DoDs VAULTIS-rammeverk og FAIR-prinsippene, tilpasset forsvarssektorens behov. FAKTISK beskriver egenskaper som gjør dataprodukter • Finnbare: Brukere skal kunne finne Forsvarets dataprodukter og få innsikt i hvem som er ansvarlig for dem, hva de kan forvente av dem, og hvordan de kan få tilgang til dem. • Anvendelige: Brukere skal kunne anvende Forsvarets dataprodukter, ved at de er tilgjengelige gjennom dokumenterte standard grensesnitt og via felles plattformer og tjenester. • Klare: Brukere skal ha en klar forståelse av meningsinnholdet i Forsvarets dataprodukter, ved at de bruker et felles begrepsapparat og gir tilstrekkelig kontekst. • Troverdige: Brukere skal kunne ha tillit til Forsvarets dataprodukter, gjennom at det så langt som mulig gjøres synlig hvordan produktene er produsert og hvilke kilder de tar utgangspunkt i. • Interoperable: Brukere skal enkelt kunne integrere Forsvarets dataprodukter med hverandre og med eksterne kilder, gjennom bruk av felles og standardiserte dataformater, begrepsapparat, og metadatastandarder. • Sikre: Brukere skal kunne ha tillit til at Forsvarets dataprodukter behandles på en sikker måte, der tilgang styres automatisk ut fra produktenes skjermings- og delingsbetingelser, der produktenes integritet og tilgjengelighet bevares, og der bruk og tilgang registreres og loggføres. • Koblede: Brukere skal se at Forsvarets dataprodukter er koblet sammen slik at sammenhenger og avhengigheter mellom forskjellige produkter er synlige.
Fellesfinansiert IKT	«[er] IKT-en i Forsvaret som finansieres av IKT investerings- og driftsmidler, og omfatter de tre delpordeføljene digital grunnmur (DG), operasjoner (OPS) og virksomhetsstyring (VS). DG er fundamentet for sikkert samvirke for alle forsvarrets strukturelementer og består av bl.a. kommunikasjonsinfrastruktur, sikre plattformer og kryptering. OPS understøtter direkte Forsvarets strukturer med operative systemer for kommando og kontroll, situasjonsbilde og målutvelgelse. VS understøtter Forsvaret med styringssystemer og et felles datagrunnlag for bruk i operasjoner og virksomhetsstyring.

	Fellesfinansiert IKT inkluderer dermed sentral IKT-infrastruktur som alle øvrige strukturelementer sømløst (og automatisk) kan koble seg opp til, uavhengig av om de er stasjonære eller mobile, på land, sjø eller i luften» (Forsvarsstaben, 2025b)
FinOps	En praksis og et kulturelt rammeverk. Målet er å maksimere forretningsverdien gjennom økonomisk ansvarlighet, samarbeid og datadrevne beslutninger. FinOps kombinerer prinsipper fra finans og DevSecOps, og fremmer tverrfaglig samarbeid mellom teknologiteam, økonomiavdelinger og forretningsledelse. FinOps handler ikke bare om kostnadsreduksjon, men om å skape gjennomsiktighet, eierskap og kontinuerlig forbedring. FinOps sikrer at ressursbruk er effektiv, kostnadene er forutsigbare, og at investeringene gir målbar verdi for organisasjonen (FinOps Foundation, 2025).
FMN	«[...] is a capability aiming to support command and control and decision-making in future operations through improved information-sharing. It provides the agility, flexibility and scalability needed to manage the emerging requirements of any mission environment in future NATO operations. Federated Mission Networking is based on principles that include cost effectiveness and maximum reuse of existing standards and capabilities. It consists of three elements: • Federated Mission Networking Governance, • Federated Mission Networking Framework and • Mission Networks. Federated Mission Networking will be based on trust, willingness and commitment. Federated Mission Networking is built on lessons learned from the Afghanistan Mission Network (AMN) implementation and on the NATO Network Enabling Capability Programme» (NATO, 2022b).
Fog	Et distribuert mellomlag mellom cloud-kjernen (core) og edge noder. Fog-laget ligger nærmere operasjonsområdet for å redusere latenstid. Behandler data lokalt før de eventuelt sendes videre til sentral sky. Avlaster core-laget ved å filtrere, analysere og reagere på data hurtigere. Består av mange noder, typisk små datasentre, rutere, aksesspunkter eller taktiske IT-noder.
Forsvarets IKT	Samlebetegnelse for all Forsvarets IKT, alt fra applikasjoner, informasjonssystemer, kommunikasjonsinfrastruktur til IKT i digitalisert materiell.
Forsvarets IKT-virksomhet	Aktører som utvikler, drifter eller vedlikeholder og forvalter Forsvarets IKT. Dette inkluderer interne og eksterne aktører, offentlige og private samt industri og akademia.
Forsvarets sikre plattformer (FSP)	Samlebetegnelse for felles programvare og maskinvare som skaper kjøremiljøer for applikasjonene. Forsvaret benytter FSP på alle relevante graderingsnivåer, og omfatter administrativ saksbehandling samt operativ bruk på både ugradert og gradert nivå.
Forsvarets skyløsning	Samlebetegnelse for skyplattformer og de nødvendige IKT-tjenestene, applikasjonene og data som benytter disse skyplattformene. Begrepet er uavhengig av tjeneste- og leveransemodell som benyttes.
Funksjon	Noe som er av verdi og nytte for brukeren av funksjonen (Elstad et al., 2022).
Føderert identitet	En identitet som administreres av én betrodd identitetsleverandør og brukes på tvers av flere systemer eller organisasjoner, slik at brukeren kan autentiseres uten å ha separate kontoer i hvert system.
Føderert styringsmodell	En styringsmodell der sentrale, obligatoriske policyer og kontrollkrav håndheves felles, mens identiteter, tilgang og ressurser forvaltes lokalt innen definerte tillits- og ansvarsgrenser.
Grunndata	Autorative data om kjerneentiteter (som personell, materiell og geografi) som forvaltes som en felles sannhet og gjenbrukes på tvers av hele organisasjonen for å sikre konsistens. Kalles også masterdata eller stamdata.
Hyperskalerbare skyplattformer	Skytjenester levert av globale tilbydere med svært stor, distribuert infrastruktur som gir tilgang til omfattende datakraft, lagring og nettverksressurser på tvers av datasentre. De er utformet for å skalere raskt og elastisk i takt med etterspørsel, slik at virksomheter kan håndtere store og varierende arbeidslaster uten å redusere ytelse eller tilgjengelighet (Oracle, 2026).
IKT-system	Maskinvare, programvare og tilknyttet infrastruktur (NSM, 2024)»

IKT-tjeneste	Generelt begrep for en funksjon som leveres av programvare (Laskey et al., 2009), hvor en funksjon er noe som er av verdi og nytte for konsumenten av IKT-tjenesten (Elstad et al. 2024). Konsumenten av en IKT-tjeneste kan være en sluttbruker eller en annen IKT-tjeneste.
Informasjon	Data som er velformet (syntaks) og gjennom en dekodings- og fortolkningsprosess gir en mening (semantikk) (Elstad et al., 2022).
Informasjonssystem	« [...] systemer som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker. Informasjonssystem skal i sikkerhetsloven forstand forstås vidt. Begrepet omfatter både manuelle og digitale informasjonssystemer, og favner alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer» (Forsvarsdepartementet, 2017).
Infrastructure as a Code	Programmerbar infrastruktur, dvs. administrering og konfigurering av infrastruktur ved hjelp av kode, i stedet for manuelle prosesser (Microsoft, 2024).
Infrastructure as a Service	En type tjenestemodell, som omfatter grunnleggende dataressurser som nettverkslagrings- og behandlingskapasitet.
Innkapsle informasjonssystem	Å lage et moderne grensesnitt rundt et gammelt (legacy) informasjonssystem, slik at det kan levere data i nye formater og brukes i moderne informasjonsutveksling – uten å endre selve det gamle informasjonssystemet.
Innsatsområde	Tematisk gruppering av prinsipper innenfor områder som er kritiske for å lykkes med transformasjonen.
Interoperabilitet	« [...] the ability of the entities of an organisation to work together, and it covers aspects ranging from technical to business concerns» Liu et al. (2020 s. 2). I følge Liu et al. (2020) kan interoperabilitet defineres på ulike nivåer: • Fysisk interoperabilitet innebærer at det kan overføres elektroniske signaler mellom avsender og mottaker uten tap av fysiske egenskaper. • Empirisk interoperabilitet gjør at mottakeren kan rekonstruere det samme innholdet, bortsett fra eventuelle problemer som oppstår fra det fysiske nivået. • Syntaktisk interoperabilitet er knyttet til om datastrukturer og filformater er lesbare både hos mottaker og sender, slik at for eksempel informasjon eller språk gjenkjennes av forskjellige samarbeidende informasjonssystemer. • Semantisk interoperabilitet sikrer at den samme betydningen av innhold utveksles mellom informasjonssystemene. Det vil si at dette nivået ikke bare beskriver om dataene er universelt tilgjengelige og gjenbrukbare, men at det også adresserer mangelen på felles forståelse forårsaket av bruk av forskjellige semantiske representasjoner grunnet ulik kontekst eller syntaksavhengige tilnærminger. • Pragmatisk interoperabilitet sikrer at forretningsprosesser, støttet av informasjonssystemene, i hver enkelt kontekst kan aggregeres for å oppnå den generelle intenderte hensikten ved justering av forretningsarbeidsflyter, prosesser og regler. • Sosial interoperabilitet handler om at det er samsvar i tradisjoner, policies, kultur, etikk og lederstil."
Interoperability by Design	Applikasjoner og informasjonssystemer utvikles med innebygde krav til samhandling og gjenbruk fra starten av, slik at de kan utveksle data og fungere sømløst med andre systemer uten behov for senere tilpasninger. Dette innebærer at interoperabilitet og gjenbruk er grunnleggende premisser i designfasen.
Kapabilitet	Evnen til at et system eller en organisasjon kan utføre en funksjon på et gitt prestasjonsnivå for å oppnå strategiske eller operative mål. Den realiseres gjennom kombinasjoner av mennesker, prosesser, organisasjon, informasjon og teknologi. (NATO, 2020). For Forsvarets IKT vil elementer som mennesker, prosess, kompetanse, applikasjoner, data, informasjonssystemer og kommunikasjonsinfrastruktur inngå.
Kapabilitetsbasert utvikling	En planleggingsmetode der man identifiserer hvilke kapabiliteter (evner), som kompetanse, prosesser og teknologi Forsvaret trenger for å nå ønskede mål, og vurderer gapet mellom eksisterende og nødvendige kapabiliteter.
Kapabilitetskart	Oversikt over kapabiliteter og relasjoner mellom disse.

Kjøremiljø	Den tekniske plattformen et program eller en IKT-tjeneste kjører på, som nødvendig programvare, konfigurasjon.
Kunnskapsgraf	En strukturert representasjon av entiteter og relasjonene mellom dem.
Leveransemodell	Beskriver hvordan og hvor skytjenester distribueres og administreres, f.eks. privat sky og allmenn sky (Direktoratet for forvaltning og økonomistyring, 2025; Mell, P., & Grance, T. (2011)).
Metadata	Data som beskriver andre data (f.eks. opprinnelse, struktur og format).
Metamodell	En modell av en modell – altså et abstrakt rammeverk som definerer hvilke begreper, relasjoner og regler som brukes for å beskrive arkitekturen. Den spesifiserer strukturen og semantikken som ulike arkitekturmodeller skal følge, slik at arkitekturarbeidet blir konsistent, forståelig og sammenhengende.
Modulær arkitektur	En arkitektur hvor et system er bygget opp av uavhengige moduler med klart definerte grensesnitt, slik at hver modul kan utvikles, vedlikeholdes og videreutvikles uten å påvirke hele systemet.
Multidomene-operasjoner	<i>orkestrering</i> av militære aktiviteter på tvers av alle domener og miljøer, synkronisert med ikke-militære aktiviteter, for å gjøre alliansen i stand til å levere konvergerende effekter til rett tid (NATO, 2022a).
Nasjonal kontroll	«[...] innebærer styringsevne til å ta effektive beslutninger gjennom for eksempel regulering, eierskap eller avtaler, og handlefrihet til å gjennomføre beslutninger mest mulig uavhengig av utenlandske aktører og innsatsfaktorer.» Begrepet brukes for å beskrive en tilstand der Forsvaret kan ivareta sin handlefrihet og styringsevne gjennom hele krisespekteret. Et fravær av egenkontroll kan kjennetegnes ved at Forsvaret står i et avhengighetsforhold til en ekstern aktør. (Digitaliserings- og forvaltningsdepartementet, 2025; Nasjonal sikkerhetsmyndighet, 2023). Tilstrekkelig nasjonal kontroll innebærer at Forsvaret ikke nødvendigvis har full kontroll, men at graden av kontroll er god nok til å sikre nasjonale interesser, sikkerhet og etterlevelse. Dette vurderes risikobasert og kan innebære at: • Kontrollmekanismer, kontrakter, revisjoner og tekniske tiltak gir Forsvaret tilstrekkelig innsyn og påvirkning. • Kritiske deler er under Forsvarets kontroll, mens mindre kritiske deler kan ligge hos eksterne eller utenlandske aktører. • Risikoen for uønsket påvirkning eller tap av styring er vurdert som lav og håndterbar.
Nasjonal sky	«En nasjonal skytjeneste for å sikre økt nasjonal kontroll over kritisk IKT-infrastruktur og å beskytte viktig informasjon.» (Meld. St. 9 (2022–2023)).
Observerbarhet («observability»)	Evnen til å overvåke dataflyt og måle data- og leveranse kvalitet, inkludert forsinkelser, volum og feilrater, for å sikre operativ presisjon og proaktiv feilretting.
Ontologier	Et felles og delt, maskinlesbart vokabular for en virksomhet eller kunnskapsområde. En ontologi er mer enn et begrepsapparat, og beskriver både hvilke begreper som finnes, hvordan de henger sammen og hvilke relasjoner og regler som gjelder mellom dem. Dette gjør sammenhenger logiske og entydige, slik at både mennesker og maskiner kan forstå, dele og gjenbruke data på samme måte. Der begrepsapparat forklarer hva et begrep betyr, viser en ontologi også hvordan begrepet er koblet til andre begreper – f.eks. hvordan «avdeling» relaterer til enhet, styrke, oppdrag og lokasjon – og hvilke regler som gjelder.
Opphav («data provenance»)	Informasjon om et dataprodukts kilder, produksjonsprosess og transformasjoner, som gjør det mulig å forstå og etterprøve hvordan produktet er fremstilt.
Orkestrering	Prosessten med å administrere og koordinere flere programvarekomponenter (konteinere) for å sikre at de fungerer effektivt sammen, skaleres dynamisk og håndteres automatisk (Johnsen, Andersen, Langleite & Opland, 2026).
Platform as a Service	En type tjenestemodell, med levering av driftsmiljøet (plattformen), der kunden innfører, utvikler og produksjonsetter løsninger selv.
Policy-as-code	Tilnærming til å administrere og håndheve sikkerhetspolicyer ved å uttrykke dem ved hjelp av programmerings- eller konfigurasjonsspråk.

Portabilitet	Teknisk, juridisk og økonomisk evne til å flytte applikasjoner, data og IKT-tjenester mellom leverandører eller andre skyløsninger. Begrepet inkluderer evne innen dimensjoner som prosess, teknologi og organisasjon.
Prinsipp	Retningsgivende og intensjonsbaserte føringer for IKT-virksomheten. Noen av prinsippene er ambisiøse og krever tid å etterleve, samtidig er disse nødvendige for å bidra til at Forsvaret lykkes med den digitale transformasjonen.
Privacy by design	Innebygd personvern innebærer at man integrerer personvern i utviklingen av systemer, tjenester og prosesser fra starten av, i stedet for å legge det på som et tillegg etter at systemet er ferdigstilt. Det handler om å minimere risikoen for den registrerte gjennom hele livssyklusen til løsningen. Datatilsynet.no (Veiledning om innebygd personvern)/ Artikkel 25 i Personvernforordningen (GDPR)
Replikering	Opprettelse og vedlikehold av flere kopier av data på tvers av geografisk adskilte noder eller applikasjoner for å sikre tilgjengelighet, redundans og konsistens.
Security by Design	En prosess, som omfatter at sikkerhetstiltak ivaretas i riktig utviklingsfase. Sikkerhet bygges inn i applikasjoner og informasjonssystemer fra starten av designprosessen, i stedet for å legges til i etterkant. Dette innebærer at sikkerhetskrav, risikoreduserende tiltak og arkitektoniske prinsipper blir integrert i utforming, utvikling og drift, slik at systemet er robust og motstandsdyktig mot angrep allerede fra grunnstrukturen.
Separation of concern	Sørge for tydelig ansvarsfordeling mellom moduler. Hver modul har ett tydelig ansvarsområde – ikke flere. Data, logikk og ansvar som hører sammen, holdes samlet. Endringer i én del av systemet krever ikke endringer i mange andre deler.
Skyløsning	Samlebetegnelse for skyplattformer og de nødvendige IKT-tjenestene, applikasjonene og data som benytter disse skyplattformene. Begrepet er uavhengig av tjeneste- og leveransemodell som benyttes.
Skyplattform	Teknologisk plattform som tilbyr kapabiliteter for utvikling, utrulling, drift og skalering av digitale løsninger i skyen, basert på automatiserte IKT-tjenester for infrastruktur, sikkerhet, datahåndtering og applikasjonshåndtering. En skyplattform sørger for at IKT-tjenestene får de essensielle egenskapene som gjør dem til skytjenester.
Skyteknologi	Teknologiene og de teknologiske komponenter som gjør det mulig å levere de essensielle egenskapene som gjelder for skytjenester. Dette inkluderer teknologier som containere, mikrotjenester, serverless funksjoner, cloud native-prosessorer og -infrastruktur.
Skytjeneste	En IKT-tjeneste levert fra en skyplattform ved hjelp av skyteknologi. Ifølge NIST gir sky-tjenester praktisk, on-demand nettverkstilgang til en delt pool av konfigurerbare data-ressurser som raskt og effektivt leverer IKT-tjenester til virksomheten. Bruk av skytjenester muliggjør kostnadsmodeller basert på faktisk forbruk i motsetning til tradisjonelle tjenestemodeller. Mer formelt definerer NIST skytjenester som bestående av fem essensielle egenskaper, tre tjenestemodeller og fire leveransemodeller (Mell, & Grance, 2011).
Software as a Service	En type tjenestemodell, hvor programvare driftes i ett eller flere datasentre. Leverandøren har ansvaret for drift og vedlikehold av IKT-tjenesten og alt underliggende.
Sourcing	«[...] en strategisk beslutning om hvorvidt en tjeneste skal utføres med interne ressurser eller om hele eller deler av tjenesten skal leveres som et tjenestekjøp eller samarbeid med ekstern virksomhet.» (Elstad et al., 2022).
Sporbarhet	«[...] en egenskap ved en prosess eller et produkt [informasjon] som gjør det mulig å finne tilbake til opprinnelsen og i ettertid følge forløpet i alle ledd av prosessen eller historien til produktet [informasjonen]. Sporbarhet oppnås ved at alt som har skjedd i en hendelseskjede blir målt og registrert, og at dette blir dokumentert og oppbevart for ettertiden» (Hofstad, 2017; Elstad et al., 2022).
	Sporbarhet for data («data lineage»): Evnen til å følge et dataprodukts reise fra kilde til konsument, inkludert alle transformasjoner, tilganger og endringer gjennom livssyklusen.
Strategisk viktig	Prosesser og tjenester som er essensielle for Forsvarets kjernevirksomhet (primæraktiviteter), som er direkte knyttet til Forsvarets eksistens. En mangelfull håndtering av strategisk viktige prosesser og tjenester vil få store konsekvenser for virksomheten (Elstad et al., 2022).

Strong cohesion	Alt innhold i en modul hører tett sammen og bidrar til samme funksjon. Sørge for at hver modul er solid og konsistent innad. En modul inneholder kun logikk og data som naturlig hører sammen. Modulen har høy indre sammenheng, og en ser tydelig hva modulen gjør og hvorfor den finnes.
Strukturelement	Et organisasjonsledd (uansett nivå, størrelse eller kapasitet) som er en selvstendig operativ enhet. Et strukturelement (SE) kobles sammen med andre SE på høyere og/eller lavere nivå til en organisasjonsstruktur. Et SE kan for eksempel være et lag, seksjon, tropp, skvadron, fartøy eller en divisjon. Et SE er et hjemmelsgrunnlag, og består av kapasitetsbeskrivelser, stillinger med tilhørende stillingsbeskrivelse, materiellhjemler, økonomistruktur og fagstruktur med logistikkrelasjoner (Forsvarsstaben, 2025b).
Systemeier	Den som har ansvar for oppnåelse og opprettholdelse av forsvarlig sikkerhetsnivå på alle sine informasjonssystemer (Sikkerhetsdirektivet).
Tjenestemodell	Modeller som beskriver hvordan IKT-tjenestene leveres, og hvilke aktører som har ansvar for hva. NIST benytter tre tjenestemodeller: Software as a Service (SaaS), Platform as a Service (PaaS) og Infrastructure as a Service (IaaS) (Digitaliserings- og forvaltningsdepartementet, 2025).
Tjenester	En funksjon som leveres av et informasjonssystem, som skaper verdi og nytte for brukeren av tjenesten (Laskey et al., 2009; Elstad et al, 2022).
Triage, isolasjon, respons og gjenoppretting	• Triage: Innledende vurdering og prioritering av hendelser basert på alvorlighetsgrad, påvirkning og hastegrad. • Isolasjon: Tiltak for å begrense eller stoppe spredning av en hendelse ved å skille berørte systemer, kontoer eller nettverk fra resten av miljøet. • Respons: Koordinerte handlinger for å håndtere og redusere konsekvensene av en hendelse etter at den er identifisert. • Gjenoppretting: Prosessen med å gjenopprette normal drift og sikre at systemer, data og tjenester fungerer som forventet etter en hendelse.
Verifisert identitet	En identitet som er kontrollert og bekreftet gjennom pålitelige kilder eller godkjente metoder, slik at det er høy tillit til at personen eller enheten er den den utgir seg for å være.
Virksomhetsdrevet IKT-utvikling	Planlegging, prioritering og gjennomføring av IKT-tiltak tar utgangspunkt i virksomhetens strategiske mål og behov, slik at teknologi brukes som et virkemiddel for verdiskaping (Ward & Peppard, 2016). Omfatter en helhetlig håndtering av prosessforbedringer, kontroll over informasjonsbehovet, applikasjonsforbedringer, teknologianvendelse og samhandling.
Virtuell datatilgang	Tilgang til data og dataprodukter direkte fra kildesystemene uten at data fysisk flyttes eller kopieres, slik at data fremstår som tilgjengelig fra ett sted for konsumenten uavhengig av hvor de faktisk befinner seg.
Zero trust	Sikkerhetsrammeverk basert på prinsippet om at ingen bruker, enhet eller applikasjon har implisitt tillit, uansett om de befinner seg innenfor eller utenfor organisasjonens nettverk. All tilgang må verifiseres eksplisitt, basert på identitet, kontekst og enhetens tilstand, og gis kun med minste privilegium. Zero trust antar at brudd kan skje og krever kontinuerlig autentisering, autorisasjon og overvåking av alle forespørsler (Rose et al., 2020). Zero trust realiseres gjennom pilarene: bruker, enhet, nettverk, applikasjon, data, automatisering/orkestrering samt synlighet/analyse.
Åpen standard	Data lagres i et format som alle aktører kan bruke, forstå, lese og bygge videre på – uten å måtte kjøpe eller benytte en bestemt programvare eller betale lisens.
Åpent format	Konkret filformat basert på en åpen standard.

5 Forkortelser

ABAC	Attribute-Based Access Control
API	Application Programming Interface
APP	Applikasjoner og applikasjonsutvikling
ARK	Kapabilitetsbasert utvikling av IKT
CI/CD	Continuous Integration / Continuous Delivery eller Deployment

CYFOR	Cyberforsvaret
DAT	Datadrevet forsvar og KI
DDIL	Disconnected/disrupted, Degraded, Intermittent and Limited/Low-Bandwidth (kommunikasjonsmiljøer)
DevSecOps	Development, Security and Operations
DG	Digital grunnmur
DIM	Arkitektur og sikkerhet i digitalisert materiell
DoD	Department of Defense (USA)
DRP	Digital reguleringsplan
ERP	Enterprise Resource Planning
FAIR	Findable, Accessible, Interoperable, Reusable
FAKTISK	Finnbare, Anvendelige, Klare, Troverdige, Interoperable, Sikre, Koblede
FDSA	Forsvarets datasentriske arkitektur
FGP	Forsvarets gjennomføringsplan
FinOps	Financial Operations
FMN	Federated Mission Networking
FoU&I	Forskning og Utvikling og Innovasjon
FSL	Forsvarets skyløsning
FSP	Forsvarets sikre plattformer
FST	Forsvarsstaben
GNF	Grunnleggende nasjonale funksjoner
HR	Human Resources
IKT	Informasjons- og kommunikasjonsteknologi
KI	Kunstig intelligens
KIT	Konfidensialitet, integritet og tilgjengelighet
MDO	Multidomeneoperasjoner
MEO	Menneske og organisasjon
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSM	Nasjonal sikkerhetsmyndighet
OPS	Operasjoner
PSM	Forsvarssjefens porteføljestyre
SAM	Samvirke med allierte, totalforsvaret og andre relevante aktører
SE	Strukturelement
SIK	Sikker IKT i Forsvaret
TCI	Teknologi, cyber og IKT
UDV	Utvikling, drift og vedlikehold
VAULTIS	Visibility, Accessibility, Understandability, Lineage, Trustworthiness, Interoperability, Security
VS	Virksomhetsstyring

6 Referanser

Litteratur

- Cloud Native Computing Foundation. (2026). *CNCF cloud native definition v1.1*.
<https://github.com/cncf/toc/blob/main/DEFINITION.md>
- Digdir. (2025). *Hva er digital transformasjon?* <https://www.digdir.no/innovasjon/hva-er-digital-transformasjon/1589>
- Digitaliserings- og forvaltningsdepartementet. (2025). *Nasjonal sikkerhetsplan for digital infrastruktur: Elektronisk kommunikasjon i fred, krise og krig*.
<https://www.regjeringen.no/contentassets/cdadcb75906d4d8f888d28306ff9e435/no/pdfs/nasjonal-sikkerhetsplan.pdf>
- Direktoratet for forvaltning og økonomistyring. (2025). *Hva er skytjenester (cloud)*.
<https://markedsplassen.anskaffelser.no/veiledning/hvordan-bruke-skytjenester-etter-schrems-ii/hva-er-skytjenester-cloud>
- Elstad, A. K., Lund, K., Kristiansen, S., & Bloebaum, T. H. (2022). *Informasjonsdeling i Forsvarets beslutningsprosesser – kritiske suksessfaktorer* (FFI-rapport 22/00146). Forsvarets forskningsinstitutt.
- Elstad, A. K., Lund, K., Solheim, Å. G., Endregard, M., & Mykkeltveit, A. (2024). *Forsvarets moderne og motstandsdyktige digitale grunnmur – kritiske suksessfaktorer* (FFI-rapport 24/00074). Forsvarets forskningsinstitutt.
- FinOps Foundation. (2025). *What is FinOps?* <https://www.finops.org/introduction/what-is-finops/>
- Floridi, L. (2002). *Philosophy and computing: An introduction*. Routledge.
- Forsvarsdepartementet. (2017). *Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet (sikkerhetsloven)*. <https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/>
- Forsvarsdepartementet. (2024, 18. januar). *Fremtidens IKT-virksomhet i Forsvaret: Oppdrag F24 IKT*.
- Forsvarsstaben. (2025a, 1. mai). *Forsvarets gjennomføringsplan* [BEGRENSET].
- Forsvarsstaben. (2025b, 1. mai). *Forsvarets gjennomføringsplan: Delplan IKT* [BEGRENSET].
- Hofstad, K. (2017). Sporbarhet. I *Store norske leksikon*. <https://snl.no/sporbarhet>
- IBM. (2025). *What is DevSecOps?* <https://www.ibm.com/think/topics/devsecops>
- Justis- og beredskapsdepartementet. (2022). *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet (Meld. St. 9 (2022–2023))*.
<https://www.regjeringen.no/no/dokumenter/meld.-st.-9-20222023/id2950130/>
- Johnsen, F. T., Andersen, E. P., Langleite, R. S., & Opland, E. A. F. (2026). *Kontainerorkestrering i kampnære IKT-systemer – en innledende studie* (FFI-rapport 26/008). Forsvarets forskningsinstitutt.
- Kristiansen, S., & Elstad, A. K. (2022). *Bruk av SharePoint for å styrke kvalitet i beslutningsprosesser i Forsvaret – med eksempler fra operations assessment* (FFI-rapport 22/00113). Forsvarets forskningsinstitutt.
- Laskey, K., Estefan, J. A., McCabe, F. G., & Thornton, D. (2009). *Reference architecture foundation for service oriented architecture version 1.0* (OASIS Committee Draft 02). OASIS.
- Liu, L., Li, W., Aljohani, N. R., Lytras, M. D., Hassan, S. U., & Nawaz, R. L. (2020). A framework to evaluate the interoperability of information systems – Measuring the maturity of the business process alignment. *International Journal of Information Management*, 54, 1–13.

- Lysne, O. (2020). *Risikostyring i digitale verdikjeder: Rapport fra en arbeidsgruppe ledet av professor Olav Lysne*. Direktoratet for samfunnssikkerhet og beredskap.
<https://www.dsbinform.no/DSBno/2020/rapport/risikostyring-i-digitale-verdikjeder/>
- Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology.
- Microsoft. (2024). *What is infrastructure as code (IaC)?* <https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code>
- Nasjonal sikkerhetsmyndighet. (2024). *NSMs grunnprinsipper for IKT-sikkerhet* (Versjon 2.1).
<https://nsm.no/getfile.php/1313975-1717589722/NSM/Filer/Dokumenter/Veiledere/NSMs%20Grunnprinsipper%20for%20IKT-sikkerhet%20v2.1.pdf>
- NATO. (2020). *NATO architecture framework*. Architecture Capability Team Consultation, Command & Control Board.
https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/NAFv4_2020.09.pdf
- NATO. (2022a). *Multi-domain operations: Enabling NATO to out-pace and out-think its adversaries*. <https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/>
- NATO. (2022b). *Federated mission networking*. <https://www.act.nato.int/activities/fmn>
- NATO. (2024a). *A data centric reference architecture for the Alliance*.
https://nhqc3s.hq.nato.int/apps/DCRA_Report/id-29d4122b072148f5aaf4882ecc5d963c/elements/model.html
- NATO. (2026). *NATO architecture framework version 4.1* (Document version 2026.03). Architecture Capability Team Digital Policy Committee.
<https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/NATO-Architecture-Framework-v4-1-en.pdf>
- Oracle. (2026). *What is a hyperscale cloud?* <https://www.oracle.com/cloud/hyperscaler-cloud/>
- Peppard, J., & Ward, J. (2016). *The strategic management of information systems: Building a digital strategy*. John Wiley & Sons.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology.
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420
- Shirey, R. (2007). *Internet security glossary, version 2* (RFC 4949, FYI 36). RFC Editor.
<https://www.rfc-editor.org/info/rfc4949>
- Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., ... Mons, B. (2016). The FAIR guiding principles for scientific data management and stewardship. *Scientific Data*, 3, 160018.
- U.S. Department of Defense. (2020). *DoD data strategy*.
<https://media.defense.gov/2020/Oct/08/2002510959/-1/-1/0/DOD-DATA-STRATEGY.PDF>

Lover og direktiver

Personopplysningsloven. (2018). *Lov om behandling av personopplysninger* (LOV-2018-06-15-38).

Sikkerhetsdirektivet. (2024). *Direktiv for sikkerhetstjeneste* [Tjenstlig].

Sikkerhetsloven. (2018). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24).