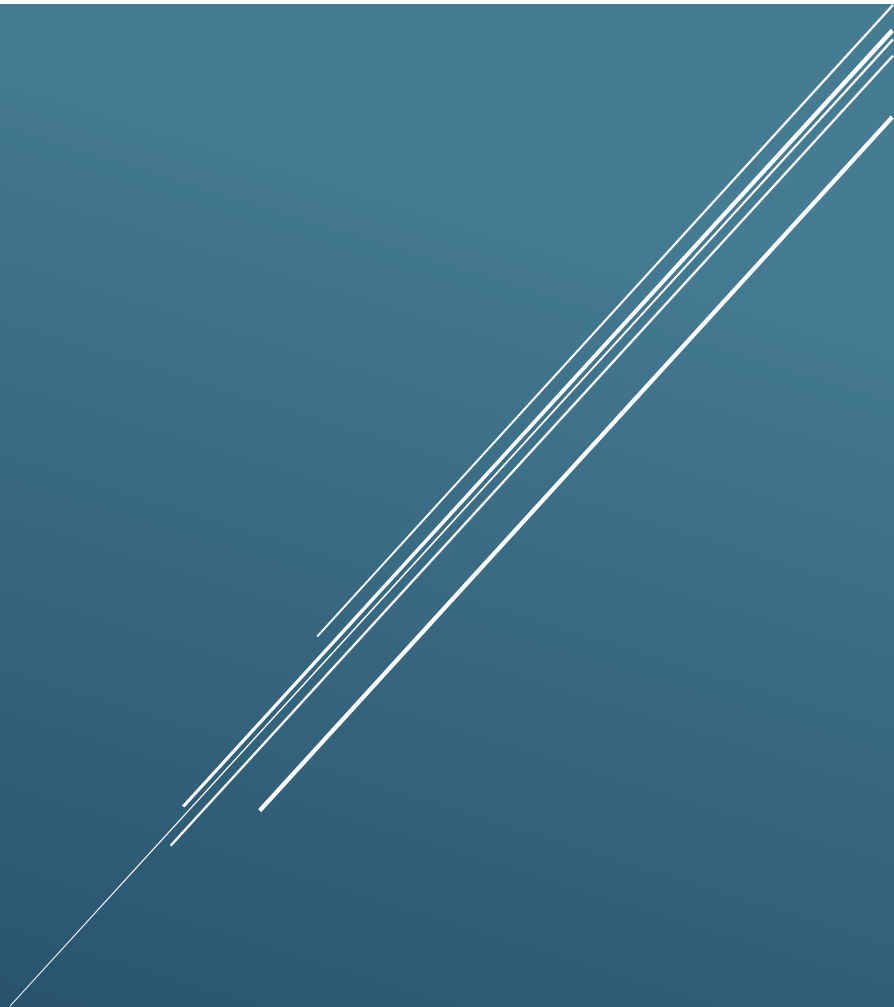




FORSVARETS SKYSTRATEGI

En sikker, skalerbar og bærekraftig skyløsning for
framtida

Metadata

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

Innhold

SKYSTRATEGIEN PÅ ÉN SIDE	2
STRATEGISK KONTEKST	3
FORSVARETS SKYLØSNING	4
FORMÅL OG VIRKEOMRÅDE	5
FORVENTEDE EFFEKTER	6
Mål 1: Sikre tilgjengelighet og motstandsdyktighet i skyløsningen	7
Mål 2: Sikre tilstrekkelig nasjonal kontroll	9
Mål 3: Muliggjøre interoperabilitet og datasentrisk arkitektur og -sikkerhet	11
Mål 4: Sikre moderne, skalerbare og fleksible IKT-tjenester	13
Mål 5: Sikre smidig og effektiv applikasjonsutvikling og produksjonssetting	15
Mål 6: Sikre økonomisk kontroll og bærekraft for skyløsningen	16
Mål 7: Sikre at skyløsningen er i tråd med NATOs sky- og digitaliseringsstrategier	17
Mål 8: Sikre en skyløsning tilpasset Forsvarets virksomhet, operative planverk og doktriner	18
Mål 9: Sikre kompetanse på skyteknologi og moderne applikasjonsutvikling	19
VEIEN MOT OPERASJONALISERING AV STRATEGIEN	20
Vedlegg	21
Vedlegg A Begrepsforklaring	21
Vedlegg B Forkortelser	23
Vedlegg C Referanser	25

SKYSTRATEGIEN PÅ ÉN SIDE

Forsvaret står overfor et sikkerhetspolitisk landskap preget av høy geopolitisk spenning, økende digital trusselaktivitet og økte krav til samvirke med NATO og allierte. For å sikre operativ handlefrihet, beslutningshastighet og utholdenhet må Forsvaret modernisere sin digitale grunnmur og etablere en sikker, skalerbar og bærekraftig *skyløsning*. Forsvarets skystrategi beskriver hvordan denne kapabiliteten skal bygges og styres.

Skystrategien beskriver mål og overordnet retning for skyløsningen. Skyløsningen er kritisk for realisering av Forsvarets fire hovedmål – operasjoner, beredskap, utholdenhet og utvikling.

Skystrategien spesifiserer ni prioriterte mål, hvorav de tre første er høyest prioritert:

- 1 Sikre tilgjengelighet og motstandsdyktighet i skyløsningen
- 2 Sikre tilstrekkelig nasjonal kontroll
- 3 Muliggjøre interoperabilitet og datasentrisk arkitektur og -sikkerhet
- 4 Sikre moderne, skalerbare og fleksible IKT-tjenester
- 5 Sikre smidig og effektiv applikasjonsutvikling og produksjonssetting
- 6 Sikre økonomisk kontroll og bærekraft for skyløsningen
- 7 Sikre at skyløsningen er i tråd med NATOs sky- og digitaliseringsstrategier
- 8 Sikre en skyløsning tilpasset Forsvarets virksomhet, operativt planverk og doktriner
- 9 Sikre kompetanse på skyteknologi og moderne applikasjonsutvikling

Figur 1 Skystrategiens ni prioriterte mål for den framtidige skyløsningen.

Forsvaret skal etablere en skyløsning med en privat *skyplattform* som kjerne, supplert med nasjonale, allierte og kommersielle skyplattformer der risikoen er akseptabel. Når målene er realisert, vil Forsvaret ha en skyløsning som sikrer høy tilgjengelighet, motstandsdyktighet og operativ handlefrihet. Data kan deles, prosesseres og utnyttes på tvers av domener, graderingsnivåer og allierte – også under påvirkning – noe som styrker situasjonsforståelse, beslutningsstøtte og tempo i operasjoner.

Skystrategien gjelder for alle som utvikler, drifter eller påvirker Forsvarets IKT – og den skal brukes som grunnlag for prioriteringer, anskaffelser og teknologivalg.

Ambisjonsnivået er høyt og krevende. Det er et gap mellom Forsvarets nåværende IKT-evne og målene i skystrategien. Likevel er dette løftet nødvendig for å sikre digital overlegenhet, robusthet og handlefrihet i møte med dagens og framtidens trusler. Skystrategien viser hvordan Forsvaret skal nå dette målet gjennom målrettet utvikling av teknologi, kompetanse og samvirke.

STRATEGISK KONTEKST

Det sikkerhetspolitiske landskapet er preget av høy geopolitisk spenning, krig i Europa – og et trusselbilde som kombinerer tradisjonelle militære virkemidler med cyberoperasjoner, påvirkningskampanjer og hybride metoder. Trusselaktører utnytter samfunnets sårbarheter og utfordrer tradisjonelle forsvars- og beredskapsstrukturer.

Forsvarets evne til å operere under alle forhold forutsetter moderne digitale kapabiliteter og evne til kontinuerlig teknologisk tilpasning. Utviklingen innen autonome systemer, elektronisk krigføring, kunstig intelligens (KI) og avanserte sensorer endrer grunnleggende hvordan operasjoner forstås, planlegges og gjennomføres, og hvilke kapabiliteter som vil forme framtidens militære styrkeforhold. Dette skaper både muligheter og avhengigheter: Forsvaret må kunne samle, prosessere, dele og analysere data raskt og sikkert, også under aktiv påvirkning, nettbrudd eller fysisk angrep.

Evnen til digital manøvrering blir sentral. De teknologiske skiftene øker kravene til Forsvarets IKT – og stiller krav til modernisering, samvirke med og mellom allierte og en kontinuerlig tilpasning for å sikre *nasjonal kontroll* og handlefrihet.

NATOs sky- og digitaliseringsstrategier (NATO, 2024a, 2024b, 2025a) fremhever at digital overlegenhet er avgjørende for alliansens evne til avskrekking, kollektivt forsvar og gjennomføring av *multidomeneoperasjoner* (MDO). Strategiene vektlegger sikker bruk av *skytenester*, *datasentrisk arkitektur*, *zero trust* og standardiserte digitale grunnmurer som muliggjør rask informasjons-delning, beslutningsstøtte og samvirke med og mellom allierte. For Forsvaret betyr dette at framtidige løsninger må være sikre, interoperable og integrerbare med NATOs digitale økosystem.

«Cloud platforms and cloud services are imperative for NATO's warfighting capabilities, and we are in a hurry»

– Mark Rutte, generalsekretær i NATO, NATOs skykonferanse 2025.

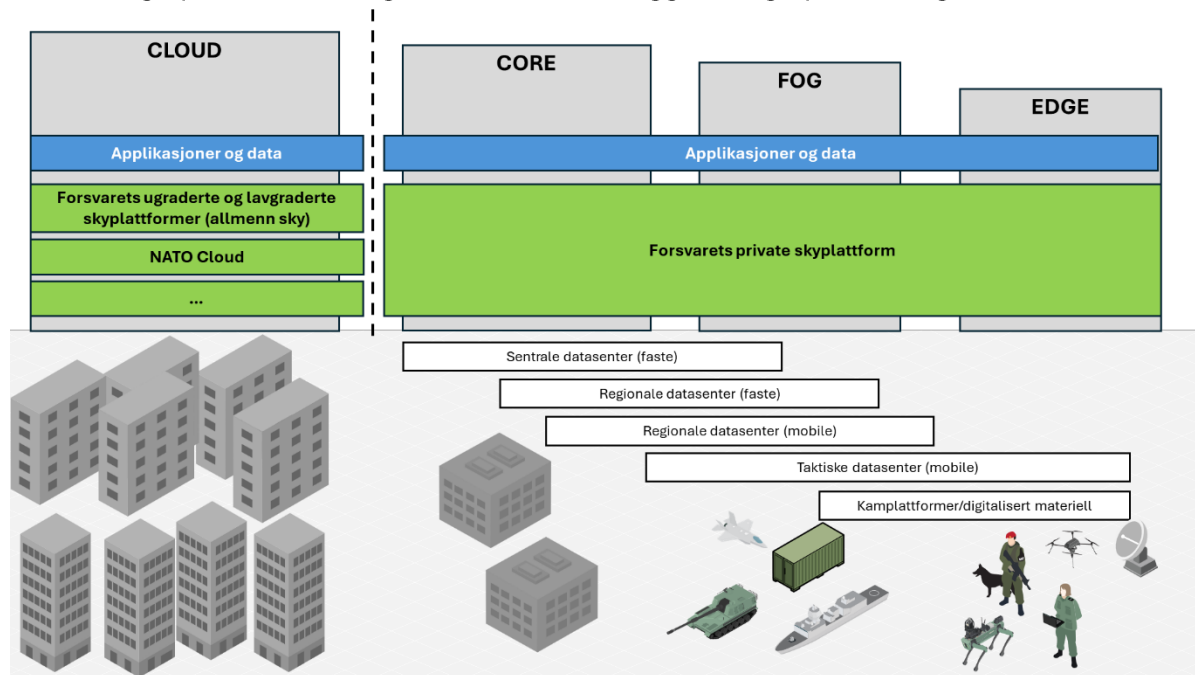
Forsvarets digitale transformasjon skal styrke situasjonsforståelse, kommando og kontroll, virksomhetsstyring og interoperabilitet. Realisering av Forsvarets fire hovedmål – operasjoner, beredskap, utholdenhet og utvikling (Forsvarsdepartementet, 2025) forutsetter en sikker, skalerbar og bærekraftig skyløsning, som en kritisk kapabilitet.

Samlet sett viser utviklingen at Forsvaret må etablere en sikker, skalerbar og bærekraftig skyløsning som understøtter operasjoner på tvers av domener og mellom allierte, og som samtidig legger grunnlaget for moderne virksomhetsstyring i et stadig mer digitalisert og uforutsigbart trusselbilde.

FORSVARETS SKYLØSNING

Skyløsning er en samlebetegnelse for skyplattformer og de nødvendige *IKT-tjenestene*, *applikasjonene* og dataene som befinner seg på disse skyplattformene. Begrepet er uavhengig av hvilken tjeneste- og *leveransemodell* som benyttes. En forenklet, konseptuell illustrasjon av *Forsvarets skyløsning* vises i figur 2 nedenfor, og beskrives nærmere i teksten.

Merk at begreper brukt i strategien er forklart i vedlegg A – begrepsforklaring.



Figur 2 En forenklet, konseptuell illustrasjon av Forsvarets skyløsning.

Skyløsningen skal understøtte Forsvarets evne til å gjennomføre operasjoner i hele konflikt-spekteret. Den vil bestå av en kombinasjon av Forsvarets private skyplattform og bruk av øvrige skyplattformer, inkludert nasjonale, allierte og kommersielle løsninger der risikoen er akseptabel. Den private skyplattformen er kjernen og bygges for kontinuitet, motstandsdyktighet og kontroll i krise og krig. *Forsvarets skyløsning* vil bestå av:

- Forsvarets private skyplattform, som omfatter:
 - *Core* – sentral kapasitet for tung prosessering og lagring
 - *Fog* – regionale noder som avlaster core og sikrer lavere latens
 - *Edge* – taktiske noder nær sensorer, våpenplattformer og brukere
- *Cloud* og øvrige skyplattformer – inkluderer framtidig *nasjonal sky*, NATO-sky og *allmenn sky* for den ugraderte og lavgraderte delen av Forsvarets skyløsning
- Applikasjoner og data, levert på tvers av disse skyplattformene

Forsvarets skyløsning er avhengig av Forsvarets kommunikasjonsinfrastruktur (FKI) for å kunne flytte applikasjoner og data. Skystrategien omfatter ikke FKI, men stiller krav til kapasitet, robusthet og funksjonell støtte for å realisere skyløsningen.

FORMÅL OG VIRKEOMRÅDE

Formålet med Forsvarets skystrategi er å etablere en tydelig retning, en strategisk intensjon, for etablering av en sikker, skalerbar og bærekraftig skyløsning for Forsvaret. Strategien er primært rettet mot etableringen av Forsvarets framtidige skyløsning. Den gir også føringer for modernisering og forbedring av eksisterende sikre plattformer og applikasjoner som er kritiske for Forsvarets operasjoner.

Skystrategien spesifiserer ni prioriterte mål for den framtidige skyløsningen. For hvert mål identifiseres et antall faktorer som er kritiske (kritiske suksessfaktorer, KSF) for å oppnå det aktuelle målet.

Skystrategien skal brukes i alle deler av *IKT-virksomhetens* styringsfunksjoner ved beslutninger som påvirker retning, utvikling og egenskaper ved den framtidige skyløsningen. Anskaffelsesmiljøene skal legge den til grunn ved kravsetting til leverandører og teknologi. Strategien er essensiell for etableringen av nye datasentre, etablering av Forsvarets sikre plattform(er) og modernisering av Forsvarets ERP (Enterprise Resource Planning).

Strategien påvirker også øvrige etater i forsvarssektoren ved å etablere føringer for plassering av Forsvarets IKT-tjenester og data. Dette skal sikre at kritiske IKT-tjenester plasseres riktig, basert på operativ betydning og risiko.

Skystrategien regulerer ikke forvaltning og styring av IKT i Forsvaret og forsvarssektoren. Dette håndteres gjennom IKT-styringsmodell for forsvarssektoren og gjeldende regelverk for Forsvaret.

Strategien komplementerer relevante nasjonale føringer, NATO-dokumenter og Forsvarets IKT-strategidokumenter (Forsvarsstaben, 2026). Den inngår i realiseringen av Langtidsplan for Forsvarssektoren 2025–2036 (LTP) (Forsvarsdepartementet, 2024), Forsvarets gjennomføringsplan (FGP) (Forsvarsstaben, 2025a) og øvrige strategiske mål.

Ved operasjonalisering skal strategien ses i sammenheng med øvrige styrende dokumenter, og justeres ved endringer i operative behov, teknologi eller sikkerhetssituasjon.

Formål og virkeområde tydeliggjør at skystrategien skal sikre en koordinert, styrt og sikker utvikling av Forsvarets skyløsning. Alle aktører som påvirker Forsvarets IKT, skal hensynta disse føringene.

FORVENTEDE EFFEKTER

Forsvarets skyløsning er en kritisk kapabilitet. Hvis målene i strategien oppnås, er de forventede effektene av skyløsningen som følger:

Høy *tilgjengelighet*, *motstandsdyktighet* og *utholdenhet* på tvers av geografiske områder forventes å gi styrket operativ evne og sikrer at kritiske IKT-tjenester fungerer i hele konfliktspennet. For å sikre handlefrihet, robusthet og redusert leverandørlåsing har skyløsningen evne til å flytte applikasjoner og data fra Forsvarets private skyplattform til nasjonale, allierte og allmenne skyplattformer, og til å motta applikasjoner og data fra allierte skyplattformer.

Forsvaret forventes å ha tilstrekkelig *nasjonal kontroll* over skyløsningen i hele livssyklusen og i alle geopolitiske situasjoner. Nasjonal kontroll baseres på retningslinjer, styringsmekanismer og kompetanse, noe som gir sikker drift og forvaltning.

Interoperabilitet og en *datasentrisk arkitektur* vil gjøre data tilgjengelige, delbare og sikre på tvers av skyplattformer og graderingsnivåer. Dette gir sømløs dataflyt, rask integrering av nye datakilder og styrket innovasjon, situasjonsforståelse og beslutningsstøtte. Enhetlig identitetsløsning og identitetsstyring etter zero trust-prinsippene vil gi sikkerhet og tilgangsstyring på tvers av lokasjoner og *informasjonssystemer*. Skyløsningen vil kunne understøtte etterlevelse av nasjonale og internasjonale lover og krav.

Gjennom *moderne, skalerbare og fleksible IKT-tjenester* kan kritiske applikasjoner og data plasseres riktig basert på risiko, *strategisk viktighet* og kritikalitet. Sluttbrukere, sensorer og effektorer vil kunne oppleve høy ytelse og tilgjengelighet, uavhengig av lokasjon. Skyløsningen vil kunne skaleres etter behov og gjenopprettes raskt ved feil.

Forsvaret vil kunne oppnå *smidig og effektiv applikasjonsutvikling* gjennom moderne utviklingsmetodikk og Development, Security and Operations (*DevSecOps*)-praksis. Dette antas å gi raskere innovasjon, hyppigere leveranser av ny funksjonalitet og økt *autonomi* i utviklings-, drifts- og vedlikeholdsteam (UDV-team).

Forsvaret vil få *økonomisk kontroll og bærekraft* i skyløsningen gjennom Financial Operations (*FinOps*)-praksis. Dette forventes å gi økt kostnadsgjennomsiktighet, mer informerte beslutninger og effektiv ressursbruk.

Forsvaret vil etterleve og understøtte *NATOs sky- og digitaliseringsstrategier*, inkludert utviklingen av føderert sky og digital grunnmur (NATO, 2024b, 2024c). Dette vil styrke samhandlingen med NATO, allierte, totalforsvaret og industrien.

Forsvaret vil oppnå bedre operativ evne ved at skyløsningen støtter Forsvarets *operative planverk og doktriner*. Dette vil kunne sikre at de digitale løsningene er integrert i operativ virksomhet.

Forsvaret vil få styrket *kompetanse* innen *skyteknologi*, dataforvaltning, programvareutvikling og digital sikkerhet. Personell vil ha forbedret kompetanse innen digitalisering og moderne applikasjonsutvikling, noe som øker Forsvarets digitale kapasitet og -kompetanse.

Mål 1: Sikre tilgjengelighet og motstandsdyktighet i skyløsningen

Dette målet skal sikre tilstrekkelig tilgjengelighet og motstandsdyktighet i skyløsningen, og er det målet som er høyest prioritert i skystrategien.



FØRINGER

Målet forutsetter at Forsvaret etablerer en privat skyplattform i egne, geografisk spredte datasentre.

Mange applikasjoner og data brukes og prosesseres ute på Forsvarets kampplattformer, sensorer, effektorer og distribuerte operasjons- og kommandostrukturer. Både de ulike delene av den private skyplattformen (core, fog og edge) og den øvrige skyløsningen trenger ulike egenskaper og kapasiteter, styrt av tydelige operative behov.

Forsvarets kritiske og strategisk viktige applikasjoner og data skal primært plasseres på Forsvarets private skyplattform. Plassering av applikasjoner og data skal baseres på helhetlige risikovurderinger. De viktigste kriteriene er operativ evne, evne til samvirke med totalforsvaret og allierte, samt tilgjengelighet og motstandsdyktighet i hele krisespekteret. I vurderingene skal Forsvaret også ta hensyn til geopolitiske forhold, teknologiske og organisatoriske avhengigheter, regulatoriske krav og kost-nytte. Dette beskrives nærmere under mål 2 om nasjonal kontroll.

Nødvendige og kritiske skytjenester skal være tilgjengelige på fog- og edge-nivå, også ved begrenset, ustabil eller manglende tilkobling til core. Dette innebærer at data skal kunne prosesseres og lagres lokalt i edge-noder, med tilstrekkelig ytelse, og med automatisk synkronisering når fog eller core igjen er tilgjengelig.

Motstandsdyktighet og håndtering av tredjepartsrisiko skal ivaretas for alle applikasjoner. Dette skal sikres gjennom dialog i tilfeller der kritiske applikasjoner inngår i Forsvarets verdikjeder, men ikke er eid eller kontrollert av Forsvaret, eller ikke er plassert i Forsvarets datasentre.

Applikasjoner og data hos understøttende etater som er kritiske for Forsvaret i krise og krig, skal følge samme plasseringsregler som Forsvarets egne.

I tillegg er evnen til portabilitet en kritisk faktor for tilgjengelighet og motstandsdyktighet, se mål 4 om moderne, skalerbare og fleksible IKT-tjenester.



KRITISKE SUKSESSFAKTORER

- 1.1 Etablere arkitektur, sikkerhet, løsninger og driftsmodeller som støtter periodevis autonomi i fog- og edge-noder
- 1.2 Etablere egenevne til å re-etablere skyløsningen under krise og krig
- 1.3 Inngå avtaler med allierte som muliggjør flytting av applikasjoner og data mellom skyplattformer ved behov
- 1.4 Regelmessig utvikle og gjennomføre øvelser som tester og videreutvikler skyløsningens digitale motstandsdyktighet
- 1.5 Sikre at modernisering av Forsvarets FKI understøtter kravene til tilgjengelighet og motstandsdyktighet i skyløsningen
- 1.6 Etablere regler og vurderingskriterier for plassering av applikasjoner og data som er kritiske for Forsvaret i krise og krig
- 1.7 Automatisere håndtering av motstandsdyktighet og tilgjengelighet, bl.a. gjennom bruk av KI

Egenskapene beskrevet i mål 1 forutsetter en moderne kommunikasjonsinfrastruktur som utnytter tilgjengelige kommunikasjonsbærere best mulig. Når Forsvaret moderniserer FKI, må det sikres at denne kommunikasjonsinfrastrukturen understøtter de kravene som stilles til motstandsdyktighet og tilgjengelighet.

Skyløsningen skal ha evne til automatisk deteksjon og håndtering av feil, uten menneskelig inngripen. Forsvaret skal vurdere redundans og teknologisk variasjon for å øke motstandsdyktigheten, men variasjonen må ikke undergrave kravene til portabilitet. I tillegg skal Forsvaret ha egenevne til å reetablere hele eller deler av skyløsningen under krise og krig, inkludert nødvendig teknisk, organisatorisk og prosessuell kapasitet.

Egenskapene som gir skyløsningen den motstandsdyktigheten som er beskrevet i dette målet skal jevnlig testes, øves og videreutvikles (for prosess, teknologi og organisasjon, PTO). Forsvaret skal utvikle planer for dette på linje med andre øvingsaktiviteter.



EFFEKT

Forsvarets skyløsning vil ha tilgjengelighet og motstandsdyktighet i hele konfliktspennet slik at IKT-tjenester i størst mulig grad opprettholdes under både digitale og fysiske angrep, nettverksbrudd og annet tilsiktet eller utilsiktet fravær av tilgang til core og/eller fog.

Tilgjengelighet, fleksibilitet og portabilitet vil være ivaretatt. *Exit-strategi* og tekniske løsninger vil gjøre det mulig å flytte applikasjoner og data raskt mellom ulike skyplattformer ved behov.

Samvirke med allierte vil være styrket. Avtaler og tekniske løsninger vil sikre at Forsvaret ved behov både kan flytte data og applikasjoner til allierte skyplattformer, og motta data og applikasjoner fra allierte skyplattformer.

Uavhengig av lokasjon og situasjon vil sluttbruker, sensor og effektor oppleve rask responstid og høy tilgjengelighet generelt, inkludert ute i edge for kritiske IKT-tjenester. Fog vil overta eller avlaste automatisk core ved behov. Tilsvarende vil skje mellom fog-noder ved behov.

Uavhengig av lokasjon vil Norges lover og folkerettslige forpliktelser etterleves, eksempelvis for sikkerhet, datalagring og personvern.

Automatisert håndtering av edge-noders tilgang til core og fog-noder som «kommer og går» vil sørge for å opprettholde evnen til å understøtte operasjoner, databehandling, prosessering og lagring samt kommunikasjons- og sikkerhetsfunksjoner, også i degraderte miljøer.

Eksterne leverandører av Forsvarets skyløsning vil tilfredsstillе minimumskrav og evalueringskriterier for sikkerhet, og er sammen med sine underleverandører vurdert med tanke på tredjepartsrisiko. Ved SaaS-*tjenestemodell* vil dette gjelde for kritiske applikasjoner. For øvrige SaaS-applikasjoner vil det gjelde så langt det er hensiktsmessig.

Mål 2: Sikre tilstrekkelig nasjonal kontroll

Dette målet skal sikre tilstrekkelig nasjonal kontroll over Forsvarets skyløsning i hele livssyklusen og i alle geopolitiske situasjoner. Tilstrekkelig nasjonal kontroll innebærer at graden av kontroll er god nok til å sikre nasjonale interesser, sikkerhet og etterlevelse. Dette målet er sammen med mål 1 høyest prioritert.



FØRINGER

Forsvaret skal benytte en risikobasert vurdering for å avgjøre hva som er tilstrekkelig nasjonal kontroll. Vurderingen skal omfatte: (1) om etablerte kontrollmekanismer, kontrakter, revisjoner og tekniske tiltak gir Forsvaret tilstrekkelig innsyn og reell påvirkningsmulighet, (2) om kritiske deler av skyplattformen er under Forsvarets kontroll, mens mindre kritiske deler kan ivaretas av eksterne eller utenlandske aktører og (3) om risikoen for uønsket påvirkning eller tap av styring er vurdert som lav og håndterbar.

Det kan være ønskelig å ha egenevne til å utvikle komplette skyplattformer, men Forsvaret vurderer risikoen ved dette som for høy til at det er et realistisk alternativ på kort sikt. Flere NATO-land, inkludert Tyskland og Storbritannia, har inngått avtaler med store teknologileverandører av risikohensyn. Behovet for å faktisk etablere en sikker skyløsning for Forsvaret veier tyngre enn behovet for å utvikle all teknologi selv. Forsvaret skal derfor realisere sin private skyplattform primært gjennom industri-samarbeid og kjøp av ferdig utviklet skyteknologi fra kommersielle aktører.

Ved evaluering av teknologileverandører skal Forsvaret inkludere nordiske og europeiske leverandører av skyteknologi. Egenutvikling skal begrenses til tilfeller der det er nødvendig av sikkerhetsmessige, kvalitetsmessige eller økonomiske årsaker, eller det ikke finnes egnet teknologi i markedet. Open source programvare kan benyttes der dette vurderes som det beste alternativet ut fra funksjonelle, sikkerhetsmessige eller økonomiske hensyn.

Teknologivalg skal tilfredsstillende krav til sikkerhet og kvalitet, og bør være økonomisk bærekraftige og forsvarlige se mål 4 – Sikre økonomisk kontroll og bærekraft.

Forsvaret skal gjennom dialog sikre at krav til nasjonal kontroll er ivaretatt for applikasjoner som er kritiske i Forsvarets verdikjeder, men som verken eies eller kontrolleres av Forsvaret, og ikke er plassert i Forsvarets datasentre.

Forsvaret skal selv ha ansvar for kontroll og drift av private skyplattformer, men kan ved behov outsource deler av dette. Kriterier for slik outsourcing må utarbeides. Teknologi fra kommersielle aktører skal vurderes ut fra blant annet hvilken grad av innsikt og kontroll Forsvaret har over anskaffelse, utvikling, drift og vedlikehold av de ulike delene av skyplattformen. Forsvaret skal



KRITISKE SUKSESSFAKTORER

2.1 Utarbeide føringer for hvordan Forsvarets private skyplattformer skal kontrolleres og driftes

2.2 Etablere mekanismer for regelmessig revisjon og evaluering av både avtaler, teknologivalg og sikkerhetsløsninger

2.3 Bygge kompetanse og kapasitet internt i Forsvaret for å sikre nødvendig uavhengighet fra eksterne leverandører

2.4 Sikre evne til å ivareta nasjonale krav til kryptologi og kontroll på informasjon og data, uansett hvor i verdikjeden de befinner seg og hvilken tilstand de er i (prosessering, lagring eller transport)

utarbeide føringer for hvordan egne datasentre skal kontrolleres og driftes. Disse retningslinjene skal sikre at Forsvaret har styring over informasjonssystemer og data, inkludert tilgangs- og sikkerhetsprosedyrer.

Norge skal i tråd med NATOs strategi benytte allmenn skyplattform for lavgradert opp til BEGRENSET. Forsvaret skal særlig vurdere nordiske og europeiske leverandører, og det skal ikke være automatikk i å kun velge blant de store hyperskalaplattformene. Hvilke applikasjoner som skal flyttes, skal vurderes for den enkelte applikasjon, basert på operative behov og driftsøkonomiske konsekvenser. Allmenn skyplattform må tilfredsstille kravene i NATO Cloud Directive (NATO, 2021), før lavgraderte applikasjoner og informasjon flyttes dit.

Forsvaret skal etablere systemer for regelmessig revisjon og evaluering av både avtaler, teknologivalg og sikkerhetsmekanismer. Dette skal gi et oppdatert beslutningsgrunnlag og fleksibilitet til å justere løsningen ved endrede behov, geopolitiske endringer eller nytt trusselbilde.

Forsvaret skal kunne ivareta nasjonale krav til kryptologi og ha kontroll på informasjon og data uansett hvor i verdikjeden de befinner seg, og uansett om de prosesseres, lagres eller transporteres.



EFFEKT

Skyløsningen vil gi Forsvaret tilstrekkelig kontroll og valgmuligheter. Forsvaret vil være i stand til å ta raske og effektive beslutninger om skyløsningen, uten å være avhengig av utenlandske aktører eller leverandører. Forsvaret vil ha kontroll med digitale verdikjeder inkludert data med tilhørende applikasjoner, prosessering, transport og lagring.

Helhetlig risikovurdering vil gi et systematisk og oppdatert beslutningsgrunnlag for hvor applikasjoner og data skal plasseres. Applikasjoner og data med strategisk betydning og som er under Forsvarets kontroll vil primært være plassert i Forsvarets private datasentre. Dette vil sikre tilstrekkelig nasjonal kontroll, datasuverenitet, styringsrett og eierskap til data gjennom hele krisespekteret.

Forsvaret vil bidra aktivt nasjonalt (inkludert med totalforsvaret) og med allierte i utvikling av digital suverenitet, interoperabilitet og kompetanse (se mål 9) på skyteknologi for å redusere avhengighet til de store teknologileverandørene. Forsvaret vil kunne drifte, kontrollere og videreutvikle egne private skyplattformer.

Mekanismer for regelmessig evaluering og revisjon av teknologi, avtaler og sikkerhetsrutiner vil sørge for at Forsvaret alltid er i forkant og kan tilpasse seg nye trusler og behov. Forsvarets digitale verdikjeder forventes å støtte både daglig drift og nasjonens beredskap på en sikker, fleksibel og bærekraftig måte.

Mål 3: Muliggjøre interoperabilitet og datasentrisk arkitektur og -sikkerhet

Dette målet er, sammen med mål 1 og 2, høyt prioritert. Målet skal sikre evne til å samle, bearbeide og utnytte data, som en avgjørende faktor for framtidig stridsevne. For å lykkes med multidomeneoperasjoner og oppnå beslutningsdominans skal data forvaltes som en varig strategisk ressurs, frigjort fra enkeltstående applikasjoner og infrastruktur. Dette garanterer at Forsvaret beholder definisjonsmakten over egne informasjonsverdier.

Realisering av ambisjonen om et datadrevet forsvar innebærer at Forsvaret skal gå fra



FØRINGER

proprietære siloer til en åpen arkitektur og åpne standarder som understøtter sømløst samvirke.

Standarder for teknisk og semantisk interoperabilitet skal identifiseres og etterleves. Interoperabilitet skal prioriteres over funksjonsrikdom, for å sikre samvirke med NATO, allierte og øvrige aktører i forsvarssektoren.

Forsvaret skal kontinuerlig tilpasse og videreutvikle digitale løsninger i tråd med gjeldende og kommende Federated Mission Networking (FMN)-spiraler. Systematisk etterlevelse av FMN skal sikre forutsigbar interoperabilitet og raskt samvirke med allierte i krise og krig.

Forsvarets skyløsning skal understøtte NATOs transformasjonsambisjon (NATO, 2024a), og sikre at skyløsningen er i tråd med NATOs sky- og digitaliseringsstrategier (se mål 7).

Sikkerhet skal knyttes direkte til dataobjektene for å muliggjøre kontrollert flyt og alliert samvirke. Dataobjekter skal verdivurderes, kontekstualiseres, beskyttes og kontrolleres uansett hvor de befinner seg. En forutsetning for alt dette er at Forsvaret etablerer en god styring og forvaltning av informasjonsarkitekturen.

Forsvarets skyplattformer og applikasjoner skal benytte datasentrisk arkitektur og *datasentrisk sikkerhet* basert på zero trust-prinsipper. Dette sikrer at tilgang styres av identitet, kontekst og behov, at arkitekturen begrenser spredning ved kompromittering, at data beskyttes uavhengig av skyplattform og lokasjon og at sikkerhet håndheves konsistent og maskinelt. Applikasjoner som ikke vurderes som kritiske i krise og krig, bør implementere zero trust-egenskaper på et tilstrekkelig og hensiktsmessig nivå.



KRITISKE SUKSESSFAKTORER

- 3.1 Etablere en felles ID-løsning i forsvarssektoren, der Forsvaret er pådriver
- 3.2 Utvikle målbilder for datasentrisk arkitektur og *datasentrisk sikkerhet*
- 3.3 Utvikle, vedlikeholde og etterleve en felles datapolicy for forsvarssektoren
- 3.4 Etablere strategisk forankret datastyring med tydelige regler for eierskap, kvalitet og tilgang
- 3.5 Bygge kultur og kompetanse for datasikkerhet og datadeling
- 3.6 Prioritere interoperabilitet over funksjonsrikdom ved valg av løsninger og standarder
- 3.7 Sikre en interoperabel skyløsning som oppfyller NATO sine krav og retningslinjer samt nasjonal ambisjon i FMN

Sømløs dataflyt og datasentrisk sikkerhet skal fungere også i degraderte miljøer med manglende eller ustabil forbindelse til core. Det skal derfor defineres hvilke egenskaper og tjenester som er nødvendige på tvers av cloud, core, fog og edge for å opprettholde operativ evne. Det legges til grunn det skal være en differensiering av hvilke IKT-tjenester og kapasitet som er nødvendig i dette plattformspennet.

En forutsetning for datasentrisk sikkerhet er entydige og verifiserte identiteter. Det skal derfor utvikles en identitetsløsning som en integrert del av skyløsningen. Løsningen skal støtte føderering av identiteter på tvers av forsvarssektoren og med allierte, basert på relevante industri- og NATO-standarder. Forsvaret skal være pådriver for å etablere en felles ID-løsning for forsvarssektoren. ID-løsningen gir kontroll med identiteten til alle brukere og roller tilknyttet skyløsningen, være seg om de tilhører forsvarssektoren eller andre aktører. ID-løsningen skal også inkludere ID for IKT (servere, applikasjoner m.m.).



EFFEKT

Data vil flyte sømløst fra sensor til effektor på tvers av ulike sikkerhetsnivåer og utnyttes fullt ut i Forsvarets virksomhet. Brukere og IKT-tjenester vil raskt og sikkert finne nødvendig informasjon, applikasjoner og IKT-tjenester. Brukerne vil få tilgang basert på felles identitetsløsning. Det vil være tillit til ivaretagelse av nødvendig tilgjengelighet, integritet og konfidensialitet. Skalerbarhet, interoperabilitet og fleksibilitet vil sikre rask integrering av nye data- og brukskilder, og Forsvaret er i stand til å utnytte data effektivt til innovasjon, situasjonsforståelse og beslutningsstøtte.

Mål 4: Sikre moderne, skalerbare og fleksible IKT-tjenester

Dette målet skal sikre at applikasjoner og IKT-tjenester bygges på en slik måte at Forsvaret kan utnytte fordelene og mulighetene som ligger i bruk av skyplattformer. Dette innebærer å bygge applikasjoner og IKT-tjenester med skyteknologi.

Skyplattformer, applikasjoner og IKT-



FØRINGER

tjenester skal utvikles basert på åpne standarder, slik at løsninger blir skalerbare, sikre, modulære og i størst mulig grad leverandøruavhengige over tid.

Mange av Forsvarets applikasjoner vil i lang tid framover være basert på arkitektur og teknologi som ikke er *cloud native*. Skyplattformene skal derfor støtte nødvendige variasjoner i kjøremiljø og andre aspekter, så lenge dette er nødvendig.

Forsvarets kritiske applikasjoner som ikke har en moderne, cloud native-arkitektur, skal transformeres. Dette arbeidet skal prioriteres høyt, og det skal utarbeides realistiske planer for hvordan denne transformasjonen skal gjennomføres.

Forsvaret skal kunne flytte, endre og integrere data, applikasjoner og infrastruktur på tvers av skyplattformer, med minst mulig behov for tilpasning. Dette for å håndtere krav til konfidensialitet, integritet, tilgjengelighet, skalerbarhet og ytelse, samt geopolitisk uforutsigbarhet og ivareta spredningsprinsippet. KI bør få dekket sitt ressursbehov, for effektivt å kunne håndtere store mengder data og komplekse beregninger.

Forsvarets applikasjoner og data skal som hovedregel utvikles og bygges for å være portable, slik at Forsvaret i minst mulig grad låses til en spesifikk løsning, leverandør eller teknologi.

Teknologistandardisering er nødvendig. *Portabilitet* og endringsdyktighet skal vektlegges i tråd med applikasjonens strategiske betydning. Dette innebærer å redusere avhengigheten til, eller unngå, proprietære løsninger og grensesnitt som hindrer ønsket portabilitet.

Ved anskaffelse eller etablering av applikasjoner og skytjenester hos eksterne aktører øker viktigheten av risikovurderinger jo høyere i tjenestemodellhierarkiet (IaaS, PaaS, SaaS) man befinner seg. Dette er særlig viktig for å sikre tilstrekkelig portabilitet, tilgjengelighet, kontroll og exit-mulighet (se også mål 1 og 2).



KRITISKE SUKSESSFAKTORER

- 4.1 Bygge skyløsningen med portabilitet som et bærende prinsipp, slik at applikasjoner og data kan flyttes på tvers av skyplattformer
- 4.2 Etablere en arkitektur som gjør at skyløsningen kan skaleres og kontinuerlig tilpasses endrede behov
- 4.3 Effektivisere og automatisere styring av arbeidslasten på tvers av skyplattformer, inkludert understøttelse av exit-strategi, sikkerhet, skalerbarhet og økonomi
- 4.4 Transformere eksisterende kritiske applikasjoner til cloud native-arkitektur



EFFEKT

Forsvarets skyløsning vil være konstruert og dimensjonert slik at den automatisk og sømløst skalerer opp og ned uten nedetid og ved belastningsendringer. Dette vil sikre tilstrekkelig ytelse under alle forhold. Gode teknologivalg vil sikre portabilitet og redusere kompleksitet og kostnader for exit fra allmenne skyplattformer.

Ved samling og fleksibel bruk av prosesserings- og lagringsressurser vil skyløsningen legge til rette for bruk av kunstig intelligens. Skyløsningen vil være en muliggjører for innovasjon ved rask og *trygg* utrulling av nye *funksjoner*.

Mål 5: Sikre smidig og effektiv applikasjonsutvikling og produksjonssetting

Dette målet skal sikre at Forsvarets skyplattform gir mulighet for moderne applikasjonsutvikling, med høy grad av automatisering og verktøyunderstøttelse i alle ledd av utviklingsprosessen.



FØRINGER

Skyplattformen skal understøtte moderne prinsipper for applikasjonsutvikling, inkludert utviklingsprosesser og teknologier for *kontinuerlig integrasjon og produksjonssetting (CI/CD)*.

Utviklingsteam skal ha tilgang til selvbetjente, standardiserte utviklingsressurser som dekker utvikling, testing, sikkerhetsharding og produksjonssetting. Sentrale stikkord er konteinerbaserte applikasjoner og standardiserte *orkestrerings-* og kjøretidsplattformer.

Skyplattformen skal støtte automatisk provisjonering av komplette DevSecOps produksjonslinjer, konfigurering og oppsett av testmiljøer basert på *Infrastructure as Code (IaC)*, samt drift av applikasjoner og IKT-tjenester.



EFFEKT

Applikasjonsutviklingen vil være smidig og effektiv – og gi hyppig og stabil produksjonssetting av applikasjoner. Produksjonssettinger vil være kjennetegnet av minimal nedetid og rask gjenoppretting ved feil. Sluttbrukerne vil oppleve en kontinuerlig forbedring av funksjonalitet og ytelse.

Utviklingsteamene vil ha høy grad av autonomi og eierskap til sine IKT-tjenester. Det vil utvikles en forståelse for brukernes behov og kan raskt tilpasse løsningene ved endrede krav for kritiske IKT-tjenester også når sentral infrastruktur ikke er tilgjengelig.

Forsvarets skyplattformer skal understøtte smidig, sikker og effektiv utvikling, test, produksjonssetting og vedlikehold av sikre applikasjoner. De skal legges til rette for regional autonom innovasjon og utvikling av applikasjoner.



KRITISKE SUKSESSFAKTORER

- 5.1 Etablere og videreutvikle en DevSecOps-kultur i Forsvaret
- 5.2 Etablere evne til kontinuerlig integrasjon og produksjonssetting (CI/CD) av applikasjoner
- 5.3 Etablere selvbetjente utviklingsteam med mulighet for autonom og geografisk redundant utvikling, produksjonssetting og drift av applikasjoner og tjenester

Mål 6: Sikre økonomisk kontroll og bærekraft for skyløsningen

Dette målet understøtter de andre målene i skystrategien ved å sikre at teknologi- og arkitekturvalg kan tas med forståelse for økonomiske konsekvenser og ressursbruk.

Forsvaret skal sikre økonomisk kontroll



FØRINGER

og bærekraft i skyløsningen ved å innføre et rammeverk og praksiser inspirert av FinOps Foundation, tilpasset Forsvarets behov.

Utvikling av Forsvarets private skyplattform og tilhørende skytjenester skal balansere krav til skytjenestene med tilgjengelige ressurser og kostnader for utvikling, drift og vedlikehold. Skalerbarhet skal være både økonomisk forsvarlig og bærekraftig. Økonomi, teknologi og drift skal ses i sammenheng, for å sikre helhetlige og informerte beslutninger.

Forsvaret skal bruke erfaringer fra både løpende drift og tidligere prosjekter til å forbedre økonomistyringen av skyløsningen. Forsvaret skal etablere mekanismer for kontinuerlig overvåkning, rapportering og analyse av kostnader for alle skytjenester. Kostnader bør være sporbare og transparente og knyttet til definerte eiere, prosjekter og kapabiliteter. Ressursbruk bør optimaliseres gjennom løpende vurdering av behov, skalering og avvikling av ubenyttede ressurser. Forsvarets skyløsning skal tilby funksjonalitet som gjør det mulig å fordele kostnader basert på faktisk bruk.



EFFEKT

Forsvaret vil ha forutsigbare, sporbare og transparente skykostnader. Ressursbruken vil være effektiv og tilpasset reelle behov. Kostnadene vil være forankret hos eiere og koblet til kapabiliteter, effekter og mål, som vil gi bedre innsikt og styring. Beslutninger vil bli tatt basert på sanntidsdata om forbruk og kostnader. Et forbedret kostnads- og forbruksbilde vil gi Forsvaret økte forutsetninger for å ivareta bærekraft i henhold til handlingsplanen i strategien for klima og miljø (Forsvaret, Forsvarsbygg, Forsvarsmateriell, & Forsvarets forskningsinstitutt, 2022; 2024).



KRITISKE SUKSESSFAKTORER

- 6.1 Etablere FinOps som en integrert del av skyforvaltningen for å sikre kontroll, transparens og forutsigbarhet i kostnader
- 6.2 Utvikle rutiner og automatiserte mekanismer for overvåkning, rapportering og analyse av skykostnader
- 6.3 Etablere prinsipper for fordeling og eierskap til skykostnader på tvers av kapabiliteter, prosjekter og enheter

Mål 7: Sikre at skyløsningen er i tråd med NATOs sky- og digitaliseringsstrategier

Dette målet skal bidra til at Forsvarets skyløsning kan samhandle og utveksle data med allierte skykapabiliteter. Dette bidrar til styrket situasjonsforståelse og bedre politiske og militære beslutninger.



KRITISKE SUKSESSFAKTORER



FØRINGER

Forsvarets skyløsning skal være i tråd med NATOs sky- og digitaliseringsstrategier (NATO, 2024a; 2025), NATO Cloud Vision 2030 (NATO, 2022a) og Cloud and Edge Computing Policy (NATO, 2024d). Forsvarets skyløsning er en sentral del av NATOs ambisjon om en felles føderert skyløsning.

I planlegging, utvikling og realisering av skyløsningen skal Forsvaret ta hensyn til planlagte leveranser av skytjenester, skyteknologi og applikasjoner i regi av Allied software for Cloud and Edge (ACE)

Programme (NATO, 2025c) – et flernasjonalt samarbeid, som starter for fullt i 2026. Norge skal være en aktiv bidragsyter på innhold og leveranser i ACE. Forsvaret skal utvikle egne planer uavhengig av ACE, men skal ta hensyn til ACE (NATO, 2025d) og NATOs Cloud Adoption Roadmap (NATO, 2025b).

Et fundament i NATOs strategi er tett samarbeid med industrien, noe som også gjelder Forsvaret. Forsvaret skal i hovedsak anskaffe teknologi fra industrien og adoptere teknologi fra NATO og allierte, framfor egenutvikling. Forsvaret skal også være tydelig på hvor industrien skal bidra, og legge til rette for at samarbeidet lykkes. Forsvaret skal utvikle en sourcingstrategi som understøtter dette.



EFFEKT

Norge vil, sammen med allierte og NATO, ha oppnådd tilstrekkelig interoperabilitet mellom nasjonale og allierte skykapabiliteter. Dette vil gi forbedret datautnyttelse, sikkerhet, samhandling og motstandsdyktighet. Forsvaret vil ha etablert et velfungerende strategisk industrisamarbeid.

7.1 Etablere sporbarhet mellom NATOs sky- og digitaliseringsstrategier og realiseringen av Forsvarets skyløsning

7.2 Etablere nødvendig styring og governance for Forsvarets skyløsning iht. NATO-krav og nasjonale føringer

7.3 Utvikle en sourcingstrategi og inngå strategiske avtaler med utvalgte industripartnere for å understøtte NATOs ambisjoner og Forsvarets behov

Mål 8: Sikre en skyløsning tilpasset Forsvarets virksomhet, operative planverk og doktriner

Dette målet skal sikre at Forsvarets skyløsning er tilpasset Forsvarets virksomhet, operative planverk, doktriner, konsepter og verdikjeder, inkludert samvirke med NATO, allierte og totalforsvaret.



FØRINGER

For å sikre at skyløsningen alltid er relevant skal det være mulig å kontinuerlig tilpasse skyløsningen til endringer som måtte skje innenfor Forsvarets mål, behov, konsepter eller verdikjeder.

Det er nødvendig med tett samarbeid mellom de ulike delene av Forsvarets virksomhet. Både operativ side og virksomhetsstyring, samt de støttende etatene, må bidra inn i utformingen av skyløsningen, for å sikre at den vil dekke de faktiske behovene.

Kontinuerlig innovasjon og rask digital utvikling er avgjørende i en moderne strid, og evne og vilje til å jobbe for kontinuerlig, behovsdrivet forbedring og innovasjon må derfor bli en del av kulturen i Forsvaret.

For å sikre ensartede IKT-tjenester på tvers av sektoren skal det etableres en felles arkitektur for IKT-tjenester for hele sektoren. I tillegg skal det etableres en felles IKT-tjenestekatalog – for å sørge for synergi og gjennomgående bruk og gjenbruk av IKT-tjenester i sektoren.



EFFEKT

Forsvarets skyløsning vil være tilpasset virksomheten, de operative behovene og konseptene, inkludert tilhørende aktiviteter, verdikjeder og interne og eksterne aktører.

Skyløsningen vil både støtte og bli utviklet i tråd med operative planverk og doktriner. Dette vil også omfatte verdikjeder og aktiviteter der øvrige etater i sektoren, totalforsvaret og det sivile samfunnet inngår.

Hele forsvarssektoren vil benytte en felles arkitektur for IKT-tjenester som sikrer ensartede og interoperable tjenester. En felles tjenestekatalog vil gjøre det mulig å finne og ta i bruk IKT-tjenester på tvers av sektoren.



KRITISKE SUKSESSFAKTORER

- 8.1 Etablere tett samarbeid på tvers av Forsvarets virksomhet, og med støttende etater, i grensesnittet mellom virksomhet, operasjoner og IKT
- 8.2 Etablere evne til å tilpasse skyløsningen til endringer i Forsvarets mål, operative behov, konsepter og verdikjeder
- 8.3 Etablere en kultur for behovsdrivet kontinuerlig forbedring og innovasjon
- 8.4 Etablere en sektorfelles arkitektur og katalog for IKT-tjenester

Mål 9: Sikre kompetanse på skyteknologi og moderne applikasjonsutvikling

Dette målet skal bidra til at Forsvaret utvikler personell, prosesser og kultur på en måte som muliggjør overgang fra en tradisjonell, applikasjonssentrisk og systemorientert arkitektur til en moderne, datasentrisk arkitektur.



FØRINGER

Forsvaret må ha nødvendig kompetanse til å anvende, forvalte og videreutvikle sky-løsningen. Dette krever at personell behersker moderne teknologier, metoder og arbeidsformer.

Forsvaret skal etablere et tankesett der data, programvare og IKT-tjenester forstås som operative kapabiliteter på linje med øvrige militære kapabiliteter. Dette innebærer et skifte fra lokal optimalisering, eierskaps-tenkning og statiske løsninger, til helhetlig verdiskaping, deling og kontinuerlig utvikling på tvers av domener, etater, allierte og totalforsvaret.

Ledere skal prioritere digital kompetanse-utvikling, og sikre nødvendig kompetanse innen arkitektur, skyteknologi og moderne systemutvikling. Tverrfaglig sammensatte team skal sikre operativ evne og helhetlige løsninger.

Forsvaret skal videreutvikle en kultur som fremmer åpenhet, deling og samarbeid, både internt og med allierte og relevante sivile aktører. Rekruttering, utvikling og sertifisering på skyteknologi, dataforvaltning, cybersikkerhet, programvareutvikling og arkitektur skal integreres i personellforvaltningen.



EFFEKT

Forsvaret vil ha tilstrekkelig personell på rett sted, som vil beherske moderne skyplattformer, dataforvaltning, cybersikkerhet, programvareutvikling og arkitektur. Tverrfaglige team vil levere effektivt på tvers av domener og etater, støttet av moderne applikasjoner og samhandlingsverktøy. Ledere vil drive digital transformasjon gjennom tydelige prioriteringer og kontinuerlig kompetansebygging. Kulturen vil preges av åpenhet, deling, læring og samarbeid – internt, og med allierte, totalforsvaret og industrien. Forsvaret vil rekruttere, utvikle og beholde nøkkelpersoner. Avhengigheten til enkeltpersoner vil være redusert. Forsvaret vil stå robust i møte med nye behov.



KRITISKE SUKSESSFAKTORER

9.1 Rekruttere, utvikle og beholde personell med kompetanse innen skyteknologi, dataforvaltning, cybersikkerhet, programvareutvikling og arkitektur

9.2 Etablere tydelig lederforankring og aktiv endringsledelse for den digitale transformasjonen

9.3 Prioritere og tilrettelegge for en kultur preget av åpenhet, deling og samarbeid

9.4 Sikre at arkitekter og utviklere sertifiseres på relevante teknologiplattformer og utviklingsmetoder

VEIEN MOT OPERASJONALISERING AV STRATEGIEN

Status og ambisjon

Det er i 2026 et tydelig gap mellom Forsvarets IKT og ambisjonene i skystrategien. Strategien angir retningen for utviklingen av en sikker, moderne og bærekraftig skyløsning som skal styrke Forsvarets operative evne i et skjerpet sikkerhetspolitisk landskap. Ambisjonsnivået er høyt og krevende, men nødvendig for å lykkes med Forsvarets digitale transformasjon.

Sentrale initiativ og avhengigheter

Forsvaret står midt i en omfattende digital transformasjon. Flere strategiske satsinger danner fundamentet for operasjonaliseringen. Tre initiativ er særlig kritiske: etableringen av nye data-sentre, utvikling av ny sikker plattform og modernisering av Forsvarets ERP-løsning. I tillegg styrker Forsvaret innovasjons- og teknologikraften gjennom etableringen av Forsvarets KI-senter og Cyberforsvarets IT-avdeling (CIT). For å realisere gevinster må FKI moderniseres og prioriterte eksisterende applikasjoner transformeres. Erfaringer fra Ukraina viser at evnen til kontinuerlig innovasjon, rask digital utvikling og skalering er avgjørende i moderne strid.

Helhetlig operasjonalisering

Skystrategien har ni mål, hvor motstandsdyktighet, nasjonal kontroll og datasentrisitet er høyest prioritert. Målene er til dels gjensidig avhengige og må realiseres i sammenheng. Strategien kan ikke forutse alle dilemmaer som vil oppstå i implementeringen. Derfor er tydelige prioriteringer, felles forståelse og enhetlig retning på tvers av Forsvarets virksomhet avgjørende. Dilemmaer og avklaringer må håndteres i etablerte styringsstrukturer og beslutningsmekanismer.

Sektoravhengigheter

Selv om skystrategien gjelder Forsvarets IKT, påvirker den hele forsvarssektoren. Når Forsvarets IKT inngår i andre etaters verdikjeder, må de ta hensyn til strategiens føringer. Strategien skal være premissgivende for beslutninger som påvirker Forsvarets IKT-kapabiliteter.

Veikart og kontinuerlig oppdatering

Digital transformasjon handler like mye om mennesker, prosess og organisasjon som om teknologi. Suksess forutsetter kulturendring, kompetanseutvikling, tydelig styring og kontinuerlig forbedring på tvers av Forsvaret. Operasjonaliseringen krever koordinert innsats på tvers av teknologi, organisasjon og prosess. Kritiske suksessfaktorer skal realiseres. Strategien skal omsettes i konkrete veikart, som synliggjør prioriteringer, risikoer og framdrift, og som oppdateres i tråd med trussel-bildet, teknologisk utvikling og erfaring fra drift, øvelser og pågående konflikter. Indikatorer for framdrift og modenhet skal etableres. Strategisk fleksibilitet og evne til justering er nødvendig for å opprettholde en digital handlekraft og relevante IKT-kapabiliteter inn i 2029 og videre.

Vedlegg

Vedlegg A Begrepsforklaring

Begrep	Forklaring
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).
Applikasjon	«Programvare som utfører en eller flere spesifikke funksjoner. Applikasjoner kan utføre eller tilby tjenester for sluttbrukere og for andre applikasjoner eller virksomhetsprosesser (Shirey, 2007).» (Forsvarsstaben, 2026). I sammenheng med sky er en applikasjon en samling av skytjenester som understøtter en eller flere virksomhetsprosesser, f.eks. ildledning, situasjonsbilde eller logistikk. Applikasjoner kan utføre eller tilby tjenester for sluttbrukere og for andre applikasjoner eller virksomhetsprosesser.
Autonomi	Evnen til å operere uavhengig og selvstendig, uten ekstern støtte eller kontroll (Forsvarsstaben, 2026).
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. (Forsvarsstaben, 2026).
Cloud native	Applikasjon designet for å utnytte egenskapene i skyteknologi fullt ut. Innebærer gjerne bruk av mikrotjenester, konteinere og orkestrering (Cloud Native Computing Foundation, 2026)
Continuous Integration/ Continuous delivery/ deployment (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)» (Forsvarsstaben, 2026).
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.» (Forsvarsstaben, 2026).
Datasentrisk tilnærming	«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.» (Forsvarsstaben, 2026).
Datasentrisk arkitektur	«En arkitektur 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 2024e)). » (Forsvarsstaben, 2026)
Datasentrisk sikkerhet	«Beskyttelsesmekanismer legges direkte på dataene uavhengig av hvor dataene befinner seg, slik at konfidensialitet, integritet og tilgjengelighet opprettholdes gjennom hele livssyklusen.» (Forsvarsstaben, 2026)
DevSecOps	«Er en forkortelse for Development, Security and Operations (utvikling, sikkerhet og drift). DevSecOps er en praksis for applikasjonsutvikling som integrerer utvikling, sikkerhet og drift i hele livssyklusen gjennom kontinuerlig testing, automatisering og rask produksjonssetting (IBM, 2025b).» (Forsvarsstaben, 2026).
Edge	«Noder helt ytterst i Forsvarets skyløsning, og ofte der data genereres, behandles og brukes. Ofte soldatnære løsninger. Bidrar til økt robusthet gjennom autonomi. Redusert nettverkstrafikk og forsinkelse. Edge omfatter ofte sensorer av ulik art og kjøretøy av ulik karakter. Kan også omfatte plattformer som en drone og ubemannede kjøretøy.» (Forsvarsstaben, 2026).
Essensielle egenskaper ved sky-tjenester	On-demand selvbetjening: setter opp og administrerer IKT-tjenester selv (On-demand self-service). Bred nettverkstilgang: IKT-tjenestene er et annet sted og du får tilgang over nettverk (Broad network access). Felles ressurser ved at datakraft og kostnader deles mellom kundene (Resource pooling). Høy elastisitet, skalerbar (Rapid elasticity). Målbare IKT-tjenester, du betaler for det du faktisk bruker (Measured service) (Direktoratet for forvaltning og økonomistyring, 2025; Mell, P., & Grance, T. (2011)).
Exit-strategi (for sky)	En teknisk, juridisk og økonomisk gjennomførbart risikobasert plan for ved behov å kunne rettidig flytte, eller kontrollert avvikle IKT-tjenester, applikasjoner, data eller infrastruktur. Planen skal hensynta både regelverk, prosess, teknologi og organisasjon (RPTO), og inkludere data og IKT-tjenester levert til Forsvaret som SaaS. Avvikling eller reduksjon i kvalitet med eventuelle tilhørende konsekvenser for Forsvarets samfunnsoppdrag og kritiske oppgaver skal spesifikt angis.

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).» (Forsvarsstaben, 2026).
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 core. Avlaster core-laget ved å filtrere, analysere og reagere på data hurtigere. Består av mange noder, typisk små datasentre eller taktiske IT-noder.
Forsvarets skyløsning	Se skyløsning.
Funksjon	«Noe som gir verdi og nytte for brukeren av IKT-tjenesten eller applikasjonen.» (Forsvarsstaben, 2026).
Informasjonssystem	«Med begrepet informasjonssystem menes 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 styringssystem (Forsvarsdepartementet, 2017).» (Forsvarsstaben, 2026).
Infrastructure as Code	Programmerbar infrastruktur, dvs. administrering og konfigurering av infrastruktur ved hjelp av kode, i stedet for manuelle prosesser (Microsoft, 2024).
Infrastructure as a Service (IaaS)	En type tjenestemodell, som omfatter grunnleggende dataressurser som nettverks-, lagrings- og behandlingskapasitet.
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.» (Forsvarsstaben, 2026).
IKT-virkosomhet	«Aktører som utvikler, drifter eller vedlikeholder (UDV) og forvalter Forsvarets IKT. Dette inkluderer interne og eksterne aktører, offentlige og private samt industri og akademia.» (Forsvarsstaben, 2026).
Konteinerbaserte applikasjoner	En konteinerbasert applikasjon er en programvare som er pakket sammen med alt den trenger for å kjøre – inkludert kode, biblioteker, konfigurasjonsfiler og kjøretid. Alt er pakket i en selvstendig, isolert enhet kalt en konteiner. Blant fordelene med <i>konteinerbaserte applikasjoner</i> er portabilitet, skalerbarhet og isolasjon.
Leveransemodell	Beskriver hvordan og hvor skytjenester distribueres og administreres, f.eks. <i>privat sky</i> og <i>allmenn sky</i> (Direktoratet for forvaltning og økonomistyring, 2025; Mell & Grance, 2011).
Multidomene operasjoner (MDO)	«NATO definerer MDO som orkestrering 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, 2022).» (Forsvarsstaben, 2026).
Nasjonal kontroll	«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 i strategien 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. (Forsvarsstaben, 2026).
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)).

Orkestrering	«Orkestrering er prosessen 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)).» (Forsvarsstaben, 2026).
Platform as a Service (PaaS)	En type tjenestemodell, med levering av driftsmiljøet (plattformen), der kunden innfører, utvikler og produksjonssetter løsninger selv.
Privat sky	Type leveransemodell. Skytjenester som er satt opp spesifikt for én virksomhet og som ikke er tilgjengelig for eksterne kunder.
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.» (Forsvarsstaben, 2026).
Software as a Service (SaaS)	En type tjenestemodell, hvor programvare driftes i ett eller flere datasentre. Leverandøren har ansvaret for drift og vedlikehold av IKT-tjenesten og alt underliggende.
Skyløsning	Samlebetegnelse for skyplattformer og de nødvendige IKT-tjenestene, applikasjonene og data som benytter disse skyplattformene. Begrepet er uavhengig av 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 <i>essensielle egenskapene</i> som gjør dem til skytjenester.» (Forsvarsstaben, 2026).
Skyteknologi	Teknologiene og de teknologiske komponentene som gjør det mulig å levere de essensielle egenskapene som gjelder for skytjenester. Dette inkluderer teknologier som kontainere, mikrotjenester, serverfrie funksjoner, cloud native-prosessorer og -infrastruktur.
Skytjenester	«En IKT-tjeneste levert fra en skyplattform ved hjelp av skyteknologi. Ifølge NIST gir skytjenester praktisk, on-demand nettverkstilgang til en delt pool av konfigurerbare dataressurser 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, P., & Grance, T. (2011). The NIST definition of cloud computing).» (Forsvarsstaben, 2026).
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).
Tjeneste-modell	Modeller som beskriver hvordan IKT-tjenestene leveres, og hvilke aktører som har ansvar for hva. NIST benytter tre tjenestemodeller: <i>Software as a Service</i> (SaaS), <i>Platform as a Service</i> (PaaS) og <i>Infrastructure as a Service</i> (IaaS) (Digitaliserings- og forvaltningsdepartementet, 2025).
Zero trust	«Sikkerhetsrammeverk basert på prinsippet om at ingen bruker, enhet eller applikasjon skal ha 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, Borchert, Mitchell & Connelly, 2020). Zero trust realiseres gjennom pilarene: bruker, enhet, nettverk, applikasjon, data, automatisering/orkestrering samt synlighet/analyse.» (Forsvarsstaben, 2026).

Vedlegg B Forkortelser

ACE	Allied software for Cloud and Edge
CI/CD	Continuous Integration/Continuous Delivery/Deployment
CIT	Cyberforsvarets IT-avdeling
CNCF	Cloud Native Computing Foundation
DCA	Datasentrisk arkitektur
DCRA	Data Centric Reference Architecture
DCS	Datasentrisk sikkerhet
DPC	Digital Policy Committee
DevSecOps	Development, Security and Operations
ERP	Enterprise Resource Planning
FinOps	Financial Operations

FGP	Forsvarets gjennomføringsplan
FKI	Forsvarets kommunikasjonsinfrastruktur
FMN	Federated Mission Networking
FSP	Forsvarets sikre plattformer
HR	Human Resources
IaC	Infrastructure as Code
IaaS	Infrastructure as a Service
ID	Identitet
IKT	Informasjon- og kommunikasjonsteknologi
KI	Kunstig intelligens
MDO	Multidomene operasjoner
NDS	NATO Digital Staff
PaaS	Platform as a Service
PTO	Prosess, teknologi og organisasjon
RPTO	Regelverk, prosess, teknologi og organisasjon
SaaS	Software as a Service
UDV	Utvikling, drift og vedlikehold

Vedlegg C Referanser

Cloud native foundation. (2026). *CNCF Cloud Native Definition v1.1*.

<https://github.com/cncf/toc/blob/main/DEFINITION.md>.

Digitaliserings- og forvaltningsdepartementet. (2025). *Nasjonal sikkerhetsplan for digital infrastruktur - Elektronisk kommunikasjon i fred, krise og krig*. Hentet fra

<https://www.regjeringen.no/contentassets/cdadcb75906d4d8f888d28306ff9e435/no/pdfs/nasjon-al-sikkerhetsplan.pdf>.

Direktoratet for forvaltning og økonomistyring. (2025). *Hva er skytjenester (cloud)*. Hentet fra

<https://markedsplassen.anskaffelser.no/veiledning/hvordan-bruke-skytjenester-etter-schrems-ii/hva-er-skytjenester-cloud>.

Elstad, A. K., Endregard, M., & Mykkeltveit, A. (2022). *Sourcing for forsvarssektorens IKT-virksomhet – skisse til rammeverk*. (FFI-rapport 22/02237). Forsvarets forskningsinstitutt. Hentet fra

<https://www.ffi.no/publikasjoner/arkiv/sourcing-for-forsvarets-ikt-virksomhet-skisse-til-rammeverk>.

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?* Hentet fra <https://www.finops.org/introduction/what-is-finops/>.

Forsvaret, Forsvarsbygg, Forsvarsmateriell, & Forsvarets forskningsinstitutt. (2022).

Forsvarssektorens klima- og miljøstrategi. Hentet fra https://www.forsvaret.no/om-forsvaret/miljo/Forsvarssektorens%20klima-%20og%20milj%C3%B8strategi_fullversjon.pdf/_attachment/inline/a218ff79-3a20-4541-bc3c-bb8c1f0c931e:94e6670c72fae916273baabb408c64e6214cdcf8/Forsvarssektorens%20klima-%20og%20milj%C3%B8strategi_fullversjon.pdf.

Forsvaret, Forsvarsmateriell, Forsvarsbygg, & Forsvarets forskningsinstitutt. (2024). *Forsvarssektorens klima- og miljøstrategi. HANDLINGSPLAN 2023–2030*. (Versjon 2, ikraftttredelse fra juni 2024).

Hentet fra https://www.fma.no/om-oss/baerekraft/Forsvarssektorens%20handlingsplan%20for%20klima%20og%20milj%C3%B8.pdf/_attachment/inline/651e771f-2d0b-4d67-a1b7-8c8a98f6bec1:8aaebbbad7c32f176659f9096ef5820a969c2ca1/Forsvarssektorens%20handlingsplan%20for%20klima%20og%20milj%C3%B8.pdf.

Forsvarsdepartementet. (2023). *Strategi for kunstig intelligens i forsvarssektoren*. Oslo. Hentet fra

<https://www.regjeringen.no/contentassets/a36197a7d69c45e68186b10117e76b5b/forsvarsdepartementet-kunstig-intelligens.pdf>.

Forsvarsdepartementet. (2024). *Forsvarsløftet – for Norges trygghet. Langtidsplan for forsvarssektoren 2025–2036*. (Prop. 87 S (2023–2024)). Hentet fra

<https://www.regjeringen.no/no/dokumenter/prop.-87-s-20232024/id3032217/>.

Forsvarsstaben. (2026). *Digital reguleringsplan*.

Forsvarsstaben. (2025). *Forsvarets gjennomføringsplan*. 1. mai 2025 (BEGRENSET).

Forsvarsdepartementet. (2025). *Tildelingsbrev for Forsvaret 2025*, 31. januar 2025, BEGRENSET.

IBM. (2025a). *What is continuous integration/continuous delivery (CI/CD)?* Hentet fra

<https://www.ibm.com/think/topics/ci-cd-pipeline>.

IBM. (2025b). *What is DevSecOps?* Hentet fra <https://www.ibm.com/think/topics/devsecops>.

Johnsen, F. T., Andersen, E. P., Langleite, R. S., & Opland, E. A. F. (2026). *Konteinerorkestrering i kampnære IKT-systemer – en innledende studie*. (FFI-rapport 26/008). Forsvarets forskningsinstitutt.

Justis- og beredskapsdepartementet. (2022). *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet*. (Meld. St. 9 (2022–2023)). Hentet fra <https://www.regjeringen.no>.

Laskey, K., Estefan, J. A., McCabe, F. G., & Thornton, D. (2009). Reference architecture foundation for service oriented architecture version 1.0. *Oasis, Committee Draft*, 2(26).

Lov om endringer i sikkerhetsloven (eierskapskontroll og lovens virkeområde), (2023).

Lov om nasjonal sikkerhet (sikkerhetsloven), (2018). <https://lovdata.no/>.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology.

Microsoft. (2024, 19.12.2024). *What is infrastructure as code (IaC)?* Hentet fra <https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code>.

Ministry of Defence. (2021). *Digital Strategy for Defence. Delivering the Digital Backbone and unleashing the power of Defence's data*. Hentet fra https://assets.publishing.service.gov.uk/media/60afae56d3bf7f435f43c7af/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf.

Nasjonal sikkerhetsmyndighet. (2023). *Nasjonal kontroll av IKT-tjenester*. Hentet fra <https://nsm.no/getfile.php/1313327-1696336231/NSM/Filer/Dokumenter/Rapporter/Nasjonal%20kontroll%20av%20IKT-tjenester.pdf>.

Nasjonal sikkerhetsmyndighet. (2024). *NSMs grunnprinsipper for IKT-sikkerhet, Versjon 2.1*. Hentet fra [NSMs Grunnprinsipper for IKT-sikkerhet v2.1.pdf](https://nsm.no/getfile.php/1313327-1696336231/NSM/Filer/Dokumenter/Rapporter/Nasjonal%20kontroll%20av%20IKT-tjenester.pdf).

NATO. (2024a). *NATO's Digital Transformation Implementation Strategy*. Hentet fra <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/17/natos-digital-transformation-implementation-strategy>.

NATO. (2025a). *Data Strategy for the Alliance*. Hentet fra <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance>.

NATO. (2023). *Federated Mission Networking: Conceptual Framework and Initiative Overview*. NATO Allied Command Transformation. Hentet fra <https://www.act.nato.int/activities/federated-mission-networking/>.

NATO. (2024b, 13.12.2024). *NATO Digital Backbone: Executive Summary*. Hentet fra <https://www.nato.int/en/news-and-events/articles/news/2024/12/13/nato-digital-backbone>.

NATO. (2024c). *NATO Digital Backbone Reference Architecture (Increment 1)*. Hentet fra https://nhqc3s.hq.nato.int/apps/DCRA_Report/id-29d4122b072148f5aaf4882ecc5d963c/elements/id-8eb04155870349879a24f358fa670fcd.html.

NATO. (2021). *Directive for the Protection of NATO Information within Public Cloud-Based CIS*, AC/322-D (2021) 0032).

NATO. (2022a). *NATO Cloud Vision 2030*. AC/322-D (2022) 0041 (INV)-NATO CLOUD vision 2030.

NATO. (2024d). *Cloud and Edge computing policy*. AC/322-WP (2024)0088-REV6-AS1.

NATO. (2025b). *NATO's Cloud Adoption Roadmap*. AC/322-WP (2025)0044-REV2-AS1.

NATO. (2025c). *Allies enhance NATO's digital posture*. Hentet fra <https://www.nato.int/en/news-and-events/articles/news/2025/07/23/allies-enhance-natos-digital-posture>.

NATO. (2024e). *Data Centric Reference Architecture for the Alliance*. Hentet fra https://nhqc3s.hq.nato.int/apps/DCRA_Report/id-29d4122b072148f5aaf4882ecc5d963c/elements/model.html.

NATO. (2022). *Multi-Domain Operations: Enabling NATO to Out-Pace and Out-think its Adversaries*. Hentet fra <https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/>.

NATO. (2025d). *Memorandum of Understanding concerning Cooperation on Development and Fielding of "Allied Software for Cloud and Edge Services (ACE)*, NDS(DPC)0008-2025, 30 June 2025.

- NOU 2016: 19. (2016). *Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. Oslo: Forsvarsdepartementet. Hentet fra <https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/>.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST special publication, 800(207)*, 1–52.
- Shirey, R. (2007, august). *Internet Security Glossary, Version 2*. Network Working Group. (RFC 4949).