



POLITIET

Strategi for fremtidig IKT-funksjon i politiet

Hoveddokument

Version 1.0

Dato: 25.05.2018



Innhold

1	Innledning	3
2	Politiets behov	5
2.1	Politiets overordnede mål og strategier	5
2.2	Noen viktige områder for politiet	6
2.3	Hvordan skal IKT-funksjonen bidra til at politiet lykkes?	8
2.4	Sikkerhetsmessige rammer for IKT-funksjonen	9
3	Fremtidige digitale løsninger	10
3.1	Fremtidige digitale løsninger vil drive utviklingen av politiet	10
3.2	Fremtidig informasjonslandskap	11
3.3	Fremtidig applikasjonslandskap	12
3.4	Fremtidig teknologi- og infrastrukturlandskap	13
3.5	Fremtidig sikkerhetsarkitektur	15
4	Fremtidig leveransemodell	16
4.1	Fremtidig leveransemodell for IKT	16
4.2	Sikker utvikling, testing og drift	18
5	Styring av IKT-funksjonen	19
5.1	Hensikt, mål og prinsipper for fremtidig IKT-funksjon	19
5.2	Styring av IKT	20
5.3	Oppgavefordeling for IKT-løsninger	21
5.4	Samhandling	22
5.5	Finansiering av IKT	23
5.6	Måling av IKT	23
6	Bruk av leverandørmarkedet	24
6.1	Strategiske betraktninger	24
6.2	Vurdering av tjenestekjøp innen politiets virksomhetsområder	24
6.3	Vurdering av tjenestekjøp innen politiets IKT-funksjon	26
6.4	Sikkerhetsmessige vurderinger i forbindelse med tjenestekjøp	27
6.5	Sikkerhetsmessige betraktninger om bruk av skytjenester	28
7	Organisering og kompetanse	30
7.1	Organisering av IKT-funksjonen	30
7.2	Kompetansebehov i fremtidig IKT-funksjon	30
8	Begrepsliste	32
9	Figuroversikt	36
10	Oversikt over vedlegg	37

1 Innledning

IKT-funksjonen¹ i politiet har gjennomgått store endringer de siste årene. Det er gjennomført en profesjonalisering gjennom etablering av IKT-avdelingen i Politidirektoratet og Politiets IKT-tjenester (PIT) som felles leverandør av IKT-tjenester. Lokale IKT-medarbeidere og IKT-løsninger i distriktene er overført til PIT for å gi bedre organisering og styring av hele IKT-funksjonen. Dagens IKT-funksjon er imidlertid fortsatt organisert som en tradisjonell IKT-virksomhet og anvender tradisjonelle metoder for prosjektgjennomføring og utvikling og forvaltning av politiets IKT-løsninger.

De siste årene er det gjennomført store og viktige tiltak for sikre og forbedre politiets IKT-infrastruktur og tilpasse IKT-løsningene til ny distrikts- og organisasjonsstruktur som følge av Nærpolitireformen. I hele perioden er det også levert endringer og ny funksjonalitet både via prosjekter og løpende forvaltning. Som Digitaliseringsstrategien påpekte er det imidlertid fortsatt et stort behov for å modernisere politiets eksisterende IKT-løsninger (ta inn etterslepet fra 2000-tallet) og for å utvikle nye digitale løsninger for å forbedre og effektivisere politiets oppgaveløsning.

De siste 20 årene har ikke utviklingen av politiets IKT-løsninger fulgt noen helhetlig plan eller arkitektur basert på en samlet forståelse av politiets behov for IKT-løsninger. Utviklingen har vært preget av at større og mindre funksjonelle behov har blitt løst ved å videreutvikle eksisterende applikasjoner eller ved å etablere nye enkeltløsninger. Dette har ført til at politiet nå har et fragmentert informasjons-, applikasjons- og teknologi- og infrastrukturendskap som ikke støtter morgendagens behov.

Politiet har etablert en virksomhetsstrategi "Politiet mot 2025" og en tilhørende digitaliseringsstrategi som stiller store krav til politiets utnyttelse av informasjon og teknologi. Virksomhetsstrategien uttrykker at forebygging og etterretning er sentralt og skal gjennomsyre politiets måte å jobbe på, i tillegg til at politiet i større grad skal være tilstede i det digitale rom. Disse behovene stiller helt andre krav til politiets digitale løsninger enn hva mange andre virksomheter står overfor. Rask utvikling av sikre digitale løsninger vil være svært viktig for politiets evne til å realisere virksomhetsstrategien. Vi vil ikke kunne realisere disse ambisjonene hvis vi fortsetter vår IKT-utvikling slik vi gjør i dag, politiets behov krever en helhetlig plan og tilnærming for utvikling av våre digitale løsninger. Dette gjelder både hva politiet skal ha av digitale tjenester i fremtiden og hvordan IKT-funksjonen skal levere disse. Fremover vil utvikling av digitale løsninger være enda tettere koblet mot virksomhetsutvikling i politiet enn i dag. "Strategi for fremtidig IKT-funksjon i politiet" er utformet for å gi en tydelig retning for politiets utvikling av digitale løsninger fremover og derigjennom bidra til raskere digitalisering og oppnåelse av virksomhetsstrategiens mål.

Dette dokumentet dekker syv hovedområder. I kapittel 2 omtales politiets behov som grunnlag for digitalisering. Kapittel 3 beskriver et overordnet målbilde for de digitale løsningene som skal dekke behovene i fremtiden. I kapittel 4 foreslås en ny modell for hvordan vi skal levere digitale tjenester i fremtiden for å bidra til raskere digitalisering av politiet. De videre kapitlene omhandler forutsetninger og rammer som må være tilstede for å lykkes med strategien. Kapittel 5 omhandler styring av IKT-funksjonen og kapittel 6 beskriver strategi for hvordan leverandørmarkedet skal anvendes bedre for å gi raskere digitalisering. Organisering av IKT-funksjonen og kompetanse som er nødvendig for å realisere strategien er omtalt i kapittel 7. Informasjonssikkerhet og personvern er tema som angår alle hovedområdene og er derfor omtalt i flere av kapitlene i dokumentet.

Politiets behov handler om å ivareta etatens samfunnsoppdrag og realisere de strategiske retningsvalg mot 2020 og 2025 som er gjort i virksomhetsstrategien. Det må tilrettelegges for et politi som jobber proaktivt ved å styrke politiets kunnskap om kriminaliteten basert på bedre utnyttelse av informasjon² og med notoritet på hva politiet foretar seg. Økt tilgjengelighet og kvalitet i tjenester stiller større krav til automatisering og selvbetjening. Politiets må også ha verktøy for å kunne være tilstede og skape trygghet i det digitale rom.

¹ Med "IKT-funksjon" menes "de deler av politiet som er involvert i utforming, utvikling, videreutvikling, forvaltning og drift av politiets IKT-løsninger", dette inkluderer også prosesseiere og fagmiljøer i politiet

² Begrepe "Opplysninger" og "Informasjon" brukes om hverandre

Politiets fremtidige digitale løsninger må utvikles med en helhetlig tilnærming til hvordan prosesser, informasjon og applikasjoner skal fungere i sammenheng. Politiets løsninger må legge til rette for samhandling mellom ulike arbeidsprosesser og funksjoner i politiet. Informasjonslandskapet må struktureres og forvaltes på en måte som gjør opplysningene tilgjengelige og bidrar til kunnskap om kriminaliteten. Applikasjonslandskapet må gi retning til hvordan eksisterende applikasjoner kan moderniseres og støtte arbeidsprosessene og informasjonsdelingen i politiet. Teknologiplattformene må legge til rette for raskere utviklingsprosesser, god informasjonssikkerhet, samhandling og bruk av ny teknologi.

Politiets leveransemodell for digitale løsninger skal optimaliseres for hyppigere og mindre leveranser og fokus på verdien disse skaper for politiet. Det skal legges til rette for tettere brukerinvolvering og tverrfaglige, autonome team som gis ende-til-ende leveranseansvar for digitale løsninger.

Leveransemodellen må både støtte prosesser for utvikling basert på ny teknologi gjennom DevOps³ og samtidig kunne ivareta initiativ som krever tradisjonell prosjektgjennomføring. Etterlevelse av lovverk og sikkerhet skal bygges inn i alle leveranseprosesser.

Styring av IKT-funksjonen skal baseres på prinsipper som bidrar til raskere digitalisering av politiet gjennom økt utnyttelse av teknologi og innovasjon, raskere leveranseprosesser, bruk av markedet, forutsigbar finansiering og stabil og sikker drift. Styringsmodellen skal omfatte alle aspekter av IKT i politiet, både det som er felles og det som er spesielt. En risikobasert tilnærming skal legges til grunn for all utvikling, forvaltning og drift av IKT-løsninger, enten politiet gjør det selv eller kjøper tjenester.

Politiets skal ivareta en styrt, effektiv og trygg **bruk av leverandørmarkedet** for å styrke sin leveranseevne. Vi foretar et strategisk valg om å styrke politiets egen evne til å utvikle og forvalte digitale løsninger som inngår i politiets kjernevirksomhet, og dreier bruken av leverandørmarkedet mot løsninger som bedre kan ivaretas med kompetanse og kapasitet utenfor politiet.

³ DevOps er en metodikk som fremhever kommunikasjon, samarbeid og integrasjon mellom utvikling og drift og som har fokus på flyt (effektive verdikjeder og hurtige leveranser), tilbakemelding (monitorering og feilhåndtering) og eksperimentering (prototyping og læring).

2 Politiets behov

2.1 Politiets overordnede mål og strategier

Virksomhetsstrategien "Politiet mot 2025" og Digitaliseringsstrategien er overordnede strategidokumenter for Politi- og lensmannsetaten. Her blir politiets samfunnsoppdrag, visjon og mål nærmere beskrevet. Virksomhetsstrategien henviser til politiets samfunnsoppdrag som uttrykker at politiet skal handle forebyggende, håndhevende og hjelpende for å ivareta borgernes rettsikkerhet, trygghet og alminnelige velferd.

Strategien for fremtidig IKT-funksjon legger virksomhetsstrategien til grunn som uttrykk for de overordnede behovene for endring i politiet, som IKT-funksjonen skal bidra til å realisere med utvikling av politiets digitale løsninger. Fremtidsbildet for politiet i 2025 beskrives i fire strategiske temaer med 12 strategiske mål mot 2020.



Figur 1: Strategiske temaer og mål for politiet

Virksomhetsstrategien har et særlig fokus på å styrke den forebyggende evnen til politiet. Dette krever innsats fra alle virksomhetsområder i politiet. Det stiller også spesielle krav til politiets digitale løsninger som skiller seg fra øvrige behov for videreutvikling av politiets funksjoner. Kriminelle nettverk og miljøer er innovative og med nye digitale muligheter har dette akselerert. Dette er en kontinuerlig utfordring for politiet. For å ligge i forkant må politiet derfor også være nytenkende og innovative.

Målene i virksomhetsstrategien berører alle funksjoner og virksomhetsområder i politiet, og det er behov for videreutvikling av politiets digitale løsninger på alle områder. Spesielt stiller de strategiske temaene "I forkant av kriminaliteten" og "Trygghet i det digitale rom" store krav til politiets digitale løsninger. Dette er også behov som det i liten grad kan kjøpes ferdige IKT-løsninger til i markedet og som markedet generelt har lite kompetanse på. "Tilgjengelige polititjenester med høy kvalitet" og "Et moderne og kompetent politi" er også utfordrende, men behovene her minner mer om behovene hos andre virksomheter og er også bedre kjent i markedet.

Politiets virksomhet og oppgaver er komplekse og skiller seg fra mange andre virksomheter, det finnes ikke enkle løsninger for å imøtekomme disse behovene. Vi må derfor sørge for et langsiktig og tett samarbeid mellom prosesseiere, fagmiljøer og brukere og "det digitale leveranseapparatet", for å skape fremtidige løsninger som gjør politiet i stand til å være i forkant av kriminaliteten, styrker politiets evne til å ivareta trygghet i det digitale rom og sikrer tilgjengelige polititjenester med høy kvalitet.

Gjennom temaet "Et moderne og kompetent politi" konkretiseres målet om å styrke politiets evne til digitalisering. For å møte dette behovet må IKT-funksjonen endre sine leveransemodeller, jobbe tettere med prosesseiere og brukere og levere IKT-tjenester i hurtigere tempo enn tidligere.

I forkant av kriminaliteten

Virksomhetsstrategien uttrykker at hovedstrategien skal være å forhindre kriminalitet. Å forhindre kriminalitet forutsetter at vi kjenner til kriminaliteten og de kriminelle. At vi har kunnskap om hvem de er, om deres egenskaper og hvordan vi kan bekjempe dem. Med andre ord, et forebyggende politi er et politi som handler proaktivt basert på kunnskap om trusselbildet og som har en risikobasert tilnærming til hendelser, fenomener, grupper eller personer. Det proaktive arbeidet forutsetter at politiet må ha oppdatert kunnskap til en hver tid. Politiet må kontinuerlig samle og analysere informasjon og utvikle og dele kunnskap som er relevant for en gitt kontekst – Etterretningsdoktrinen sier at politiet skal være i stand til å utarbeide tidsrelevant etterretningsinformasjon. Politiet jobber tradisjonelt erfaringsbasert med stor bruk av implisitt kunnskap. Ved å berike dette med eksplisitt kunnskap om kriminaliteten gjennom informasjon, kan vi styrke politiets evne som en lærende kunnskapsvirksomhet.

Et forebyggende politi har tilgjengelige tjenester med høy kvalitet og skaper trygghet i det digitale rom. Dagens polititjenester, handlingsmønster og IKT-tjenester støtter en reaktiv arbeidsform. Overgangen fra reaktiv til proaktiv krever at vi innoverer og endrer måten vi jobber på og tjenestene vi tilbyr. Vi må vurdere hvordan politiet jobber med sine samarbeidspartnere, vi må vurdere om det er noen andre vi kan trekke mer med for å øke vår evne på kjerneområder og ikke minst hva vi kan tilby andre. Vi må med andre ord tenke helhetlig om våre brukere, samarbeidspartnere og leverandører med mål om å kunne handle proaktivt for å være i forkant av kriminaliteten og skape verdi i tråd med politiets virksomhetsstrategi.

Realisering av behovene for endring gjennom digitalisering er derfor en hovedoppgave for IKT-funksjonen sammen med prosesseierne.

Digitalisering krever innovasjon og tverrfaglig samarbeid

For å lykkes med digitalisering og realisering av målene som uttrykkes i virksomhetsstrategien, kreves en sterkere innovasjonsevne. Virksomhetsstrategien etterlyser nye typer tjenester og økt brukerfokus. I arbeidet med "Strategi for fremtidig IKT-funksjon for politiet" har vi identifisert flere innovasjonstyper og grep politiet bør gjøre for å kunne forbedre det forebyggende arbeidet gjennom nye tjenester og økt brukerfokus. Interne forhold som nettverk, struktur og prosesser er grunnleggende innovasjonstyper politiet må fokusere på for å øke samhandling og utnyttelse av kunnskap.

Tverrfaglig samarbeid er viktig i prosessen for digitalisering av politiets tjenester. Denne type samhandling sikrer både at nødvendig kompetanse er til stede for å kunne løse oppgaven effektivt og nødvendig kunnskapsdeling med organisasjonene vi samarbeider med. Flere aktører gir flere perspektiver og involvering av aktuelle aktører må gjøres i en tidlig fase. Aktørene kan være både eksterne og interne. Vi skal tenke langsiktig, men handle med hurtige steg, for å få hele organisasjonen med på endringsreisen og for å kunne justere kursen underveis.

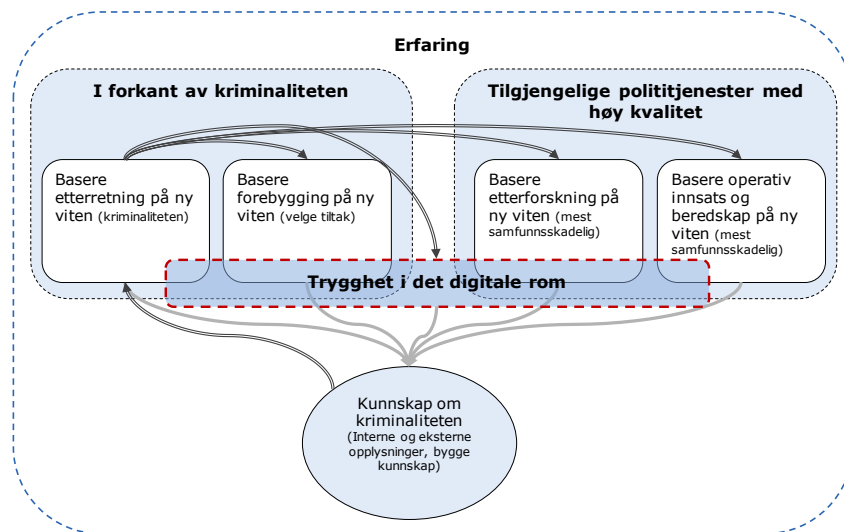
2.2 Noen viktige områder for politiet

Virksomhetsstrategien uttrykker at politiet skal være i forkant av kriminaliteten, levere tilgjengelige polititjenester med høy kvalitet og være tilstede og skape trygghet i det digitale rom. For å klare dette må vi være et moderne og kompetent politi. Av disse strategiske temaene kan vi avlede at politiet må styrke seg på noen viktige områder.

Kunnskap om kriminaliteten

Grunnleggende for å realisere politiets mål og strategier er evne til å håndtere informasjon, skape og utnytte kunnskap om kriminaliteten. Kunnskapsbasert arbeid handler om å ta faglige avgjørelser på grunnlag av den beste kunnskapen som til enhver tid er tilgjengelig. Kunnskap om kriminaliteten etableres ved å bruke nye og historiske opplysninger som grunnlag for enkeltvis eller løpende analyse. Systematisk innhenting av nye og mer detaljerte opplysninger gir grunnlag for bedre analyser. Her vil borgere, organisasjoner og samarbeidspartnere være nyttige kilder, men ikke minst etterforskning og operativ

tjeneste. Mengden informasjon som kan benyttes er enorm og stadig økende, manuelle analyser vil derfor ikke være praktisk. Automatisering må støtte politiets bearbeiding og bruk av informasjon.



Figur 2: Sammenheng mellom strategiske temaer og informasjon

Manuelle oppgaver for innhenting bearbeiding og analyse av informasjon skal automatiseres for å øke kapasitet og evnen til å løse politiets oppgaver. Kunnskap om kriminaliteten som er lett tilgjengelig bidrar til å utvikle kunnskap om trusler og risikoreduksjon for å dele med aktører som har behov for det. Kunnskapen som skapes må være aktuell og relevant da det er grunnlag for beslutninger.

Risikobasert tilnærming til politiarbeid

En risikobasert tilnærming til politiarbeidet er grunnleggende for å være proaktive og kunne hindre kriminalitet. En slik tilnærming er felles for målrettet arbeid i alle virksomhetsområder.

- Etterretning bidrar med kontinuerlige risikovurderinger og etterretningsinformasjon
- Etterforskningen vil kunne rettes mot den mest samfunnsskadelige kriminaliteten
- Forebygging vil ha bedre grunnlag for å velge de riktige tiltakene
- Operativ tjeneste og beredskapsfunksjonen vil tilsvarende være rettet mot prioritert områder.

Ivareta informasjonssikkerhet og personvern

Politiet er en etat som eier og benytter mye informasjon både åpen og sensitiv, som må beskyttes. I det ligger det krav om ivaretagelsen av høy kvalitet på informasjon, informasjonssikkerhet og personvern i digitale løsninger vi utvikler, både for intern og ekstern bruk. I tillegg skal politiet bidra til effektiv og sikker ID-forvaltning.

Ivareta etterlevelse av dokumentasjonskrav og -behov

En rekke lover og regler stiller krav til at politiet dokumenterer sin myndighetsutøvelse, og sikrer at denne er tilgjengelig enten internt, for parter eller offentligheten. IKT-løsningene må gi både støtte for tilstrekkelig notoritet i prosessene (fangst); og at dokumentasjonen (uavhengig av format) beholder sin autentisitet (bevisverdi) og er lesbar (tilgjengelig) i tråd med krav om oppbevaringstid (langtidslagring) for det enkelte prosessområdet. Politiet må utvikle tjenester som ivaretar dette for å få forbedret styringsinformasjon, rettsikkerhet for borgerne og demokratisk kontroll.

Engasjere borgere og organisasjoner

Politiet skal yte god service til borgere og organisasjoner både gjennom fysisk og digital samhandling. Digital samhandling må etableres for tradisjonelle tjenester som søknader o.l., men borgere og organisasjoner skal også møte, dele informasjon med og samhandle med politiet i det digitale rom, bl.a. gjennom informasjon, råd, kontaktmuligheter og patruljering.

Kontinuerlig forbedring

For å forbedre oss må vi måle om tiltakene vi gjør virker og bidrar til at politiets mål oppnås. Måling vil også vise om vi har behov for å endre og tilpasse praksisen vår. Måleparametere bør settes opp i

samarbeid med de som skal arbeide med tiltakene knyttet til de strategiske temaene i virksomhetsstrategien. Målinger må kunne summeres på effektnivå, enten det gjelder samfunns- og brukereffekter eller effekter for samarbeidspartnere og interne brukere.

2.3 Hvordan skal IKT-funksjonen bidra til at politiet lykkes?

På et overordnet nivå kan vi si at IKT-funksjonen skaper verdi for politiet langs to akser. Den første akse handler om hva vi leverer av digitale tjenester til politiet og den andre akse handler om hvordan disse tjenestene leveres. Hvordan vi leverer påvirker også hva vi til slutt leverer. Rask utvikling av fremtidsrettede, sikre digitale løsninger vil være svært viktig for at politiet skal lykkes med å realisere virksomhetsstrategien.

2.3.1 Hva vi leverer av digitale tjenester

De fremtidige digitale løsningene i politiet skal dekke behovene som uttrykkes gjennom politiets virksomhetsstrategi. De digitale tjenestene som er nødvendige for at politiet skal være i forkant av kriminaliteten, ha tilgjengelige polititjenester med høy kvalitet og skape trygghet i det digitale rom krever noe helt annet enn det politiet har i dag. Spesielt det å være i forkant av kriminaliteten og å skape trygghet i det digitale rom er dimensjonerende for hvordan vi organiserer informasjonen vår, deler inn og integrerer applikasjonene våre og etablerer infrastruktur for å utvikle, drifte og anvende våre digitale løsninger. Det stiller også krav til hvordan vi sikrer informasjonen og våre digitale tjenester, både med hensyn på konfidensialitet, integritet og tilgjengelighet.

Det er mulig å fortsette den praksisen vi har drevet siden tidlig på 2000-tallet med å videreutvikle eksisterende applikasjoner og anskaffe nye for å dekke nye funksjonelle behov, og på 3-5 års sikt lykkes med å tilby nyttig funksjonalitet til våre ansatte og tilsynelatende digitalisere politiets arbeid. Men dette vil ikke være en farbar vei på lengre sikt, noe som gradvis vil bli mer og mer tydelig ettersom nye behov og krav enten ikke lar seg løse eller krever veldig stor innsats. En kortsiktig tilnærming vil bare øke det teknologiske etterslepet.

Skal vi klare å etablere og levere de riktige digitale tjenestene til politiet innenfor de ressursmessige rammene som politiet har, må vi ha helhetlige målbilder for prosesser, informasjon, applikasjoner, teknisk infrastruktur og sikkerhet som setter retning for det vi skal etablere – det har vi ikke i dag. Vi må også evne og styre alle utviklingsaktivitetene i retning av målbildene og ikke bare fortsette dagens praksis.

Begrensede ressurser (både mennesker og økonomi) og behov for kontinuitet i politiets tjenester og IKT-løsninger, tilsier at vi må modernisere "arven" og etablere nye digitale løsninger over tid. Samtidig har politiet et høyt ambisjonsnivå mot 2025, noe som ikke gir rom for store prosjekter som mislykkes eller går i feil retning. Vi må altså utvikle våre digitale løsninger etter en "Reguleringsplan for digitale løsninger" (se kapittel 3 Løsning) og vi må gjøre det på en annen måte enn i dag.

2.3.2 Hvordan vi leverer digitale tjenester

Det strategiske temaet "Et moderne og kompetent politi" i virksomhetsstrategien, uttrykker mål som også er drivende for hvordan politiets IKT-funksjon må levere sine tjenester i fremtiden, herunder strategisk mål 12 om å "styrke evnen til digitalisering". Dagens måte å utvikle politiet og digitale løsninger på vil ikke gi de effektene virksomhetsstrategien legger opp til og den utnytter heller ikke de mulighetene teknologiutviklingen har gitt for å etablere og levere digitale løsninger på nye og mer effektive måter.

For å bidra til at politiet lykkes må vi klare å styre og levere digitale tjenester på en mer målrettet måte innen de begrensede økonomiske rammene politiet har. Vi må sikre en tett knytning mellom virksomhetsstrategien, etablerte målbilder og de utviklingstiltakene vi faktisk gjennomfører. Vi må klare å utnytte de mulighetene som ligger i den utviklingen som skjer i leveranseprosessene på teknologiområdet (små og hyppige leveranser, DevOps), vi må omstille vår organisasjon til å levere mer selv på strategisk viktige områder og vi må bli bedre til å utnytte leverandørmarkedet på en styrt, effektiv og trygg måte. Disse temaene er nærmere beskrevet i kapittel 4 til 7.

2.4 Sikkerhetsmessige rammer for IKT-funksjonen

IKT-funksjonen i politiet må kjenne til og etterleve de krav og behov som gjelder for informasjonsforvaltning, informasjonssikkerhet og personvern. De sikkerhetsmessige rammer er drøftet nærmere i vedlegg 4: *"Sikkerhet i IKT-funksjonen i politiet – rammer for sikkerhet i IKT-funksjonen i politiet"*. Rammene kan deles inn i følgende fire områder:



Figur 3: Sikkerhetsmessige rammer for politiets IKT-funksjon

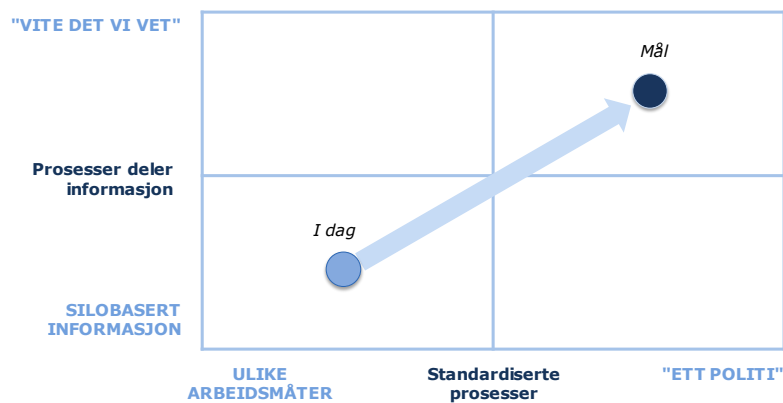
1. Alle regjeringens føringer angir at riktig ivaretagelse av informasjonssikkerhet og personvern er forutsetninger for digitalisering, og at tilnærmingen til dette skal være risikobasert med gode og strukturerte mekanismer for styring og kontroll.
2. Av lover og regler som spesielt gjør seg gjeldende, og vil være dimensjonerende for politiets arbeid med sikkerhet og personvern, er eksisterende og ny sikkerhetslov, samt politiregisterloven og den nye europeiske personvernforordningen (GDPR). I tillegg kommer en rekke andre lover som har betydning for IKT-funksjonen i politiet (eksempelvis arkiv- og forvaltningslov)
3. Politiets egne krav og sikkerhetsmessige behov er svært førende for IKT-funksjonen. Politiet må ha tillit til at informasjonen blir behandlet slik at det ikke får konsekvenser for eget og andres personell eller hvordan politiet jobber og samarbeider med andre aktører både nasjonalt og internasjonalt.
4. Samfunnets tillit til hvordan politiet og rettsapparatet behandler informasjon om borgerne gir også tydelige forvaltnings- og sikkerhetsmessige rammer for IKT-funksjonen, eksempelvis for å ivareta riktig personvern og for å ivareta sikkerheten til politiet og dets samarbeidsaktører.

3 Fremtidige digitale løsninger

3.1 Fremtidige digitale løsninger vil drive utviklingen av politiet

For å kunne realisere de mål og behov som uttrykkes i politiets virksomhetsstrategi kreves en helhetlig tilnærming til hvordan fremtidige digitale løsninger i politiet skal utformes og samhandle. Vi klarer ikke å komme i forkant av kriminaliteten og skape trygghet i det digitale rom ved å utvikle de digitale løsningene hver for seg. Politiet må klare å utnytte datamaskiner til det de er gode til i dag (f.eks. mønster-gjenkjenning), ikke bare det de var gode til for 20 år siden. Teknologianvendelsen skal være innrettet mot å forbedre politiets arbeidsprosesser og hvordan informasjon behandles, og den skal baseres på de overordnede behovene som uttrykkes i politiets virksomhetsstrategi.

Et av de viktigste bidragene fra IKT-funksjonen i politiet er å understøtte ønsket om "Ett politi" som løser like oppgaver på samme måte og som har tilgang til politiets samlede kunnskap i oppgaveløsningen.



Figur 4: Retning for digitale løsninger i politiet⁴

Felles digitale løsninger bidrar til standardisering av politiets prosesser og til å gjøre politiets tjenester mer tilgjengelige for innbyggere og virksomheter. Deling av informasjon på tvers av arbeidsprosesser, virksomhetsområder og enheter i politiet skal bidra til at vi kan jobbe enda mer kunnskapsbasert⁵, evner å ligge i forkant av kriminaliteten og etterforsker og oppklarer kriminelle forhold.⁶ Samtidig skal vi også sørge for at politiets behov for til dels meget spesialiserte digitale løsninger lar seg levere på en hensiktsmessig måte. Dette angir en retning for hvordan vi må bygge våre fremtidige digitale prosesser og løsninger fremover.

Viktige egenskaper i politiets digitale løsninger

Politiets fremtidige digitale løsninger må ha innebygd noen viktige egenskaper som er sentrale for å møte behovene og målene som uttrykkes i politiets overordnede strategier og føringer. Vi skal:

- Tilrettelegge våre løsninger for samhandling på et **felles sett av opplysninger** som kan anvendes på tvers av arbeidsprosesser
- Anvende **prosessautomatisering** til å effektivisere politiets oppgaveløsning og frigjøre tid til oppgaver som krever politikompetanse og tilstedeværelse
- Bruke **mønster-gjenkjenning** og kognitive teknologier til å styrke vår evne til å ligge i forkant og avklare kriminalitet
- Tilby politiet **mobile løsninger** for å kunne utføre oppgaver der politiet er tilstede med de opplysningene som behøves
- Styrke **selvbetjening** og **digital samhandling** i politiets tjenester
- Skape **notoritet** og ivareta **etterlevelse, informasjonssikkerhet og personvern** i vår behandling av opplysninger.

⁴ Modell fra Weill & Ross, Enterprise architecture as strategy (2006)

⁵ Et mer "informasjonsdrevet" politi

⁶ Iht. de lover og regler som gjelder for deling av opplysninger

"Reguleringsplan for digitale løsninger"

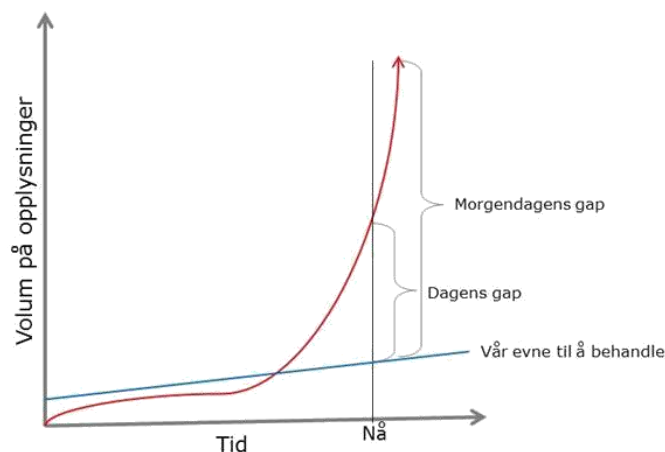
For å kunne lage fremtidsrettede, gode digitale løsninger må vi begynne å se alle delene av IKT-løsningene våre i sammenheng – ikke fortsette å løse behovene hver for seg. Dette dreier seg om å styre mer målrettet:

- Hvordan vi organiserer og forvalter **informasjonen** vår
- Hvordan vi deler inn, integrerer og utformer brukerflater for **applikasjonene** våre
- Hvilken **infrastruktur** vi etablerer
- Hvordan vi **sikrer** informasjonen og de digitale løsningene våre.

Dette kapittelet sammenfatter mål og strategier IKT-funksjonen vil følge for å realisere politiets fremtidige informasjons-, applikasjons- og teknologi- og infrastrukturlandskap, samt sikkerhetsarkitektur. Disse perspektivene på virksomheten fungerer sammen i å realisere de egenskapene vi ønsker i våre digitale løsninger – en "Reguleringsplan for digitale løsninger".

3.2 Fremtidig informasjonslandskap

Behovene fra virksomhetsstrategien uttrykker tydelig at politiet trenger felles tilgang til og utnyttelse av opplysninger på tvers av virksomhetsområder og arbeidsprosesser. Politiet må øke sin evne til å behandle disse opplysningene digitalt slik at arbeidsprosesser i enda større grad baseres på kunnskap om kriminaliteten og for å øke samhandling internt og eksternt. Videre vet vi at den enorme informasjonsmengden som allerede eksisterer i dag vil øke eksponentielt i årene som kommer. Dette vil skape et stort gap mellom hva politiet evner å håndtere og hva vi forventes å håndtere, hvis ikke politiets behandling av informasjon digitaliseres ende til ende.



Figur 5: Forventet utvikling av opplysningsmengde og dagens evne til å behandle disse

Økningen i mengder og tolkninger av disse opplysningene vil også medføre et behov om å mestre økende kompleksitet. Nye og utvidede føringer stiller krav til kontroll med alle opplysninger og notoritet til politiets behandling av disse – på tvers og på alle nivå. Eksempelvis er det er for øyeblikket aktuelt med endringer i personopplysningslov (som en følge av GDPR) som stiller nye krav til politiets evne til å holde oversikt over og ivareta informasjonssikkerhet i behandling av personopplysninger.

Politiets målbilde for behandling av opplysninger beskriver en generell og grunnleggende prosess for behandling av opplysninger i tre steg – målet er at tiden vi benytter for å fange, bearbeide og bruke opplysninger gjennom denne kontinuerlige arbeidsprosessen skal gå mot null, for oppgaver som ikke krever manuell behandling og vurdering.

Vi skal etablere en helhetlig informasjonsforvaltning for informasjonslandskapet i politiet som skal jobbe for å tilrettelegge for å fange, bearbeide og bruke de opplysningene som politiet trenger på en effektiv måte.

Hvilke opplysninger skal behandles i politiets digitale løsninger?

I forbindelse med denne strategien er det utformet en beskrivelse av informasjonslandskapet til politiet og utvalgte begreper som inngår i politiets arbeidsprosesser og digitale løsninger. Kartleggingen av informasjonslandskapet danner grunnlag for å etablere løsninger som "snakker sammen" og bidrar til å forme fremtidige applikasjoner med utgangspunkt i opplysningene de behandler.

I beskrivelsen av informasjonslandskapet er politiets virksomhetsområder og kjerneprosesser sentrert rundt det som betraktes som sentrale opplysninger som angår alle områdene. Hensikten er å tydeliggjøre at ulike virksomhetsområder arbeider inn mot et felles sett av opplysninger. Disse skal kunne fanges og bearbeides i én arbeidsprosess (eksempelvis på en operasjonssentral) og anvendes i en annen arbeidsprosess (eksempelvis innen etterretning). Et utvalg begreper er brukt for å beskrive våre felles opplysninger:

- *Hendelser* representerer "noe som har skjedd" og som er blitt fanget. Hendelser kan knyttes til tid, sted, personer og objekter. En serie av hendelser som antas å ha en sammenheng inngår i et *hendelsesforløp*.
- *Oppgaver* representerer konkrete gjøremål som utgjør politiets behandling og kan være et predikert sett av aktiviteter i en prosess som utføres etter satte regler. Disse kan utføres manuelt eller maskinelt og kan være knyttet mot hendelser. Oppgaver følger hverandre i *oppgaveforløp*, og kjeden skal bidra til å gi notoritet på politiets behandling. En oppgave kan eksempelvis være å gjennomføre et avhør eller foreta en passkontroll.
- *Mønster* anvendes for å generalisere sammenhenger som gjentar seg innen hendelser og oppgaver. Mønstre vil både kunne bidra til at politiet er i forkant og forstår situasjoner før de oppstår, og til å styrke politiets avklaring og etterforskning av hendelser. De kan også bidra til å avdekke og foreslå beste praksis innen politiets oppgavebehandling.
- *Person* omfatter de begreper som anvendes for å representere en identifisert eller uidentifisert person eller foretak, med eventuelle tilhørende identifiserende opplysninger.
- *Objekt* representerer logiske og fysiske ting (og dyr) som politiet behandler i sin oppgaveløsning.

Informasjonslandskapet består av mange flere begreper utover de som er nevnt over. Politiet har delvis tidligere også systematisert og dannet felles oversikt over informasjonen som behandles i informasjonssystemer i politiet. Vi skal kontinuerlig forbedre dette arbeidet ved styrt og strukturert forvaltning av dette informasjonslandskapet (ontologien). Dette for å kunne styre våre aktiviteter for tilrettelegging for gjenbruk og fellesforståelse av opplysninger på tvers av alle våre arbeidsprosesser og digitale løsninger.

3.3 Fremtidig applikasjonslandskap

Digitale arbeidsprosesser og behandling av opplysninger realiseres gjennom politiets applikasjoner. Politiet har i dag mange applikasjoner med vesentlig behov for modernisering både funksjonelt, sikkerhetsmessig og teknisk – det er et mål å sikre kontinuitet for sentrale digitale tjenester og applikasjoner og således kontinuitet for politiets tjenester. Det er også en rekke nye forretningsbehov som krever ny og forbedret digital støtte, blant annet for å realisere virksomhetsstrategien. For å sikre kontinuitet og at politiet kan utvikle sine tjenester videre trengs en helhetlig plan for utvikling av politiets applikasjonslandskap. Som del av strategien er det derfor tatt frem en første versjon av et fremtidig applikasjonslandskap.

Formålet med applikasjonslandskapet er både å angi en langsiktig retning samt konkrete steg som kan tas på kort sikt gjennom IKT-funksjonens leveransemodell. Videre konkretiserer beskrivelsen av applikasjonslandskapet hvordan politiets eksisterende applikasjoner over tid skal fornyes, herunder hvilke applikasjoner som er tenkt faset ut og erstattet eller videreutviklet. Over tid må alle dagens applikasjoner skiftes ut. Applikasjonslandskapet er også et viktig grunnlag for å planlegge bidrag fra leverandørmarkedet.

Mål for applikasjonslandskapet

Det fremtidige applikasjonslandskapet skal støtte politiets fremtidige arbeidsprosesser og realisere informasjonslandskapet. Et viktig prinsipp for realisering av applikasjonslandskapet er at vi ikke tar bort funksjonalitet eller systemer før de kan erstattes med alternativer som fungerer minst like bra.

Fremtidig IKT-funksjon i politiet skal bidra til raskere digitalisering av politiet. For å lykkes med ny leveransemodell kreves applikasjoner som er enklere å utvikle og forvalte med reduserte avhengigheter. Flere av politiets applikasjoner har vært utviklet over lang tid med stadig påbygging av ny funksjonalitet, uten en helhetlig plan for fordeling av informasjon og funksjonalitet mellom applikasjonene. Dette gjør det krevende å levere raske forbedringer da en endring kan ha vesentlig påvirkning på andre deler av løsningen. Det gjør også at det eksisterende applikasjonslandskapet i liten grad støtter politiet i å komme i forkant av kriminaliteten. I det fremtidige applikasjonslandskapet vil derfor applikasjonene brytes opp i mindre applikasjoner med mer avgrenset informasjon og funksjonalitet, i tråd med beste praksis. En slik arkitektur er også nødvendig for å ta fatt på de store moderniseringsoppgavene politiet står overfor innenfor eksisterende rammer for finansiering. Den vil også bidra til at politiet er friere til å kunne kjøpe tjenester i markedet med mindre avhengighet til enkeltleverandører.

Et viktig prinsipp for det fremtidige applikasjonslandskapet er at brukeropplevelsen skal stå sentralt i utviklingen av politiets applikasjoner og at flere underliggende applikasjoner skal sys sammen i ett brukergrensesnitt. Dermed slipper brukere å bytte mellom ulike applikasjoner for å utføre sine arbeidsprosesser. Funksjonaliteten vil også kunne gjøres tilgjengelig i nye typer brukergrensesnitt, eksempelvis talebaserte.

Et annet viktig prinsipp er å skille mellom opplysninger på den ene siden og politiets behandling av dem på den andre siden. En stor og gjennomgripende endring i politiets applikasjonslandskap handler om å legge til rette for samhandling omkring et felles sett av opplysninger. Dette krever en gjennomtenkt og helhetlig arkitektur som legger til rette for at opplysninger som innhentes i en kontekst skal kunne utnyttes i en annen, og påvirker mange av våre applikasjoner. Vi skal løse dagens utfordringer med håndtering av personer og identiteter, og gjøre det mulig å behandle personer av ukjent identitet i våre løsninger – som igjen er helt sentralt for etterforsknings- og ID-arbeid i politiet.

Applikasjonslandskapet skal bidra til å gi retning til arbeidet og det skal etableres en kontinuerlig prosess for forvaltning og revisjoner av applikasjonslandskapet. Det overordnede målet for styring av applikasjonsarkitektur er "Rask og kostnadseffektiv utvikling og forvaltning av applikasjoner, tilgjengelige for alle hele tiden."

3.4 Fremtidig teknologi- og infrastrukturelandskap

For å kunne realisere fremtidig informasjons- og applikasjonslandskap gjennom en ny leveransemodell for IKT-funksjonen, må politiet ha en teknisk infrastruktur som gjør det mulig med kontinuerlig utvikling og produksjonssetting av ny funksjonalitet. Dette fordrer evne til å utnytte moderne plattformtjenester og skyteknologi som også er avhengig av at politiets applikasjoner utvikles etter prinsipper som er angitt i fremtidig applikasjonslandskap. Politiet klarer ikke å utnytte de fordelene teknologien gir i utvikling og drift med applikasjoner på gammel teknologi og arkitektur – det representerer også en sikkerhetsrisiko.

I tillegg må politiet ha en moderne infrastruktur for å kunne samhandle effektivt og benytte applikasjoner på tvers av arbeidssteder og ulikt klientutstyr.

Fremover må IKT-funksjonen tilby flere ulike typer infrastrukturetjenester. Vi skal:

- Modernisere infrastrukturen for samhandling og tilgjengeliggjøring av applikasjoner til sluttbrukere
- Etablere en skybasert infrastruktur for utvikling og drift av applikasjoner
- Etablere infrastruktur for bruk i etterforskning og oppgaver. Infrastrukturetjenester som skal leveres *direkte* til sluttbrukerne. Dette er en type tjenester som IKT-funksjonen i dag ikke leverer, politidistrikter og særorgan løser det selv. Det foreligger ikke en sammenhengende plan for utviklingen av slike tjenester.
- Fortsette med å etablere basis infrastruktur for oppbevaring og sikring, nettverk, prosessering og lagring av applikasjoner og informasjon, både i privat, offentlig og allmenn sky.

Politiets infrastruktur skal ivareta krav som stilles til sikkerhet og tilby støtte for håndtering av ugraderte, lavgraderte og høygraderte applikasjoner. Infrastrukturtenester til sluttbrukere er underlagt de samme lovkrav som politiets systemer for øvrig.

Infrastrukturtenester for samhandling og tilgjengeliggjøring av applikasjoner til sluttbrukere

Dagens Origo-løsning dekker ikke politiets behov for samhandling, bruk av Internett og tilgjengeliggjøring av applikasjoner og må moderniseres.

Infrastrukturtenester for utvikling og drift av applikasjoner til sluttbrukerne

PIT har under etablering en moderne plattform basert på skyteknologi – Organa. Plattformen skal støtte utvikling og modernisering av applikasjoner, og all utvikling av nye applikasjoner i politiet skal derfor baseres på denne plattformen.

Skyteknologi i eget datasenter tar ikke bort investeringskostnadene og begrensningene som ligger i kontinuerlig håndtering og utskifting av egen maskinvare, og utnytter ikke fullt ut evnen til å skalere lagrings- og prosesseringskraft som ligger i allmenne skyløsninger⁷.

- Politiet skal derfor fortsette og utforske muligheter og strategier som kan tilby en sikker offentlig skyplattform. Politiet skal samarbeide med forsvarssektoren og eventuelle andre offentlige aktører om etablering av en slik plattform.
- Tjenester som kan tilbys i markedet for etablering av privat skyplattform for politiet skal også vurderes
- Politiet skal også vurdere bruk av allmenne skyløsninger.

Politiets infrastruktur må gi støtte for nye teknologikomponenter som kreves av fremtidige arbeidsprosesser og applikasjoner. Det fremtidige applikasjonslandskapet legger opp til vesentlig utnyttelse av kunstig intelligens, automatisering, samt teknologier for håndtering av store mengder data. Politiet vil ha behov for en plattform for tingenes internett⁸ for å håndtere store mengder data fra sensorer og utstyr. Videre skal politiet kunne anvende teknologier for talestyring som alternativt brukergrensesnitt for oppgaver hvor skjerm er mindre egnet som grensesnitt (patruljer m.m.).

Infrastrukturtenester for bruk i etterforskning og oppgaver

Etterforskere og operativt personell har et stort udekket behov for infrastrukturtenester hvor de kan behandle og dele digitale spor, beslag og annen dokumentasjon i et sikkert miljø. De har også behov for anonym og uniformert tilgang til Internett for oppgaver knyttet til patruljering og spaning i det digitale rom. Disse tjenestene vil derfor være en viktig del av løsningen for å styrke politiets evne til fange, bearbeide og bruke opplysninger, samt utføre andre politioppgaver i det digitale rom, som understøtter målene i virksomhetsstrategien.

Det pågår flere initiativ for å tilby etterforskere og operativt personell støtte til å håndtere digitale spor, beslag og annen dokumentasjon som hentes eksternt. Ved å innføre standardiserte tjenester vil det være mulig å se de ulike initiativene i sammenheng og gi utviklingen en god retning.

Basis infrastrukturtenester

Dette omfatter oppbevaring og sikring, nettverk, prosessering og lagring av applikasjoner og informasjon.

Vi skal:

- Videreføre etablering av nytt datasenter
- Benytte infrastruktur i privat ekstern sky, offentlig sky og allmenn sky der det er hensiktsmessig
- Fortsette samarbeidet med forsvarssektoren.

⁷ "Public Cloud" på engelsk

⁸ Tingenes internett (Internet of Things (IoT) på engelsk) vil si at hverdagslige gjenstander som lyspærer, døråser, biler o.l. kobles til internett

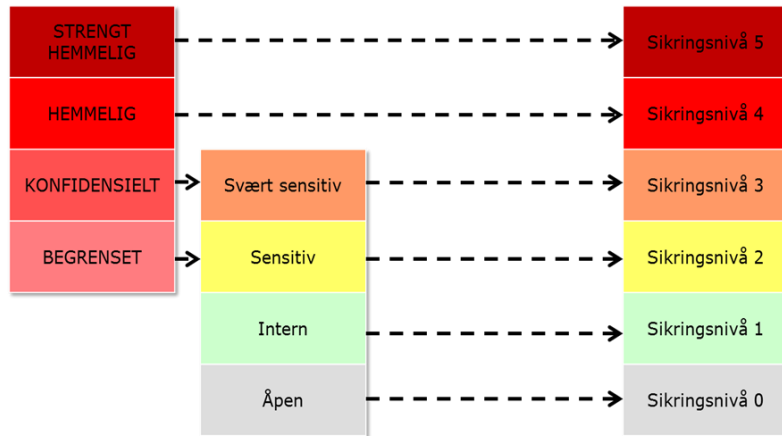
3.5 Fremtidig sikkerhetsarkitektur

En god sikkerhetsarkitektur skal sørge for evnen til å motstå digitale angrep og legger til rette for at sikkerhet blir ivare tatt på en balansert og riktig måte gjennom hele IKT-livssyklusen som vist i figur nedenfor.



Figur 6: Sikkerhet i hele IKT-livssyklusen

Politiets tekniske sikkerhetsarkitektur må gjenspeile *policy for klassifisering og verdivurdering*, både dagens og fremtidige versjoner av denne. Når informasjonen har blitt verdivurdert og klassifisert skal den sikres. En teknisk sikkerhetsarkitektur må etableres for å ivareta krav knyttet til ulike sikringsnivå. Et sikringsnivå defineres ut fra risikonivå og da hovedsakelig basert på verdinivå.



Figur 7: Sikringsnivå for de ulike verdinivåene

Et sett av sikringsnivåer må utarbeides hvor minimumskrav til sikkerhet på hvert nivå er gitt. Dette skal være krav til behandling både elektronisk og fysisk, oppbevaring, lagring og forsendelse av informasjon.

En teknisk sikkerhetsarkitektur innebærer inndeling i ulike sikkerhetssoner, definere grensnitt mellom dem og hvilke tiltak som må ivaretas innenfor hvert sikringsnivå. Tiltakene vil defineres i flere dimensjoner, både menneskelige, organisatoriske og teknologiske. Gjeldende avtaler, sertifiserte løsninger, bruk av offentlige felleskomponenter som Altinn, lovkrav med forskrifter og veiledninger bør defineres inn i de relevante sikringsnivåene. I tillegg kan sikringsnivåene defineres i henhold til politiets egen risikoaksept. NSM har utarbeidet ulike teknologiske veiledninger som kan vurderes bruk for de høyeste sikringsnivåene (G-veiledningene). Arkitektur og sikkerhetsprosesser må ivareta grunnprinsippene for IKT-sikkerhet ved å gå inn i de definerte områdene som er skissert av NSM.

4 Fremtidig leveransemodell

4.1 Fremtidig leveransemodell for IKT

I dag leveres IKT-løsninger og funksjonalitet gjennom tradisjonelle prosjekter eller gjennom mindre endringer og forbedringer i forvaltning av IKT-løsningene. Begge leveransemåtene har en sekvensiell tilnærming⁹ med siloer og overleveringssteg mellom behovsspesifisering, utvikling, testing, lansering og drift – dette er ressurskrevende og tar lang tid.

Politiet har et stort innovasjonspress der vi raskt må reagere på endringer og trender både i det fysiske og i det digitale rom. For å realisere politiets komplekse behov og bygge fremtidsrettede digitale løsninger som beskrevet i kapittel 2 og 3, må veien fra idé til utvikling og utprøving derfor være kort og gjennomføres kontinuerlig, slik at vi raskt kan dra nytte av den læringen som gjøres.¹⁰ Med dagens teknologi og metoder er det nå mulig å levere funksjonalitet kontinuerlig gjennom mindre og hyppigere leveranser, slik det også gjøres i virksomheter som lykkes med digitalisering.

Dette krever en endring i hvordan politiet utvikler og leverer digitale løsninger. For å levere digitale løsninger på en måte som er best tilpasset den enkelte oppgavens størrelse, egenart og kompleksitet må politiet ha en leveransemodell som omfatter både kontinuerlige leveranser og dagens mer tradisjonelle prosjekter. Over tid skal stadig mer leveres som kontinuerlige leveranser iht. DevOps-modellen. Denne måten å levere på gjelder ikke bare for IKT-løsningene – det strekker seg langt inn i hvordan politiet utvikler sine tjenester og arbeidsprosesser og har stor betydning for samarbeidet mellom brukerne, prosesseier og IKT-funksjonen. Dette har også konsekvenser for hvordan vi sikrer arbeidstakernes medbestemmelse i den utviklingen som skjer. Vi vil ta utgangspunkt i dagens modell for forvaltningsleveranser når vi utvikler en modell for kontinuerlige leveranser i politiet.¹¹ Ved å gå mot en leveransemodell basert på DevOps ønsker vi å oppnå følgende effekter:

- Kortere tid fra identifisert behov til levert verdi for bruker
- Økt fokus på brukernes reelle behov
- Bedret kvalitet på digitale løsninger
- Økt evne til å respondere på behov fra samfunnet
- Mindre administrasjon og mer verdi for brukerne for hver investert krone
- Redusert risiko

Produktutvikling og kontinuerlige leveranser basert på DevOps skal være førstevalget for utvikling av digitale løsninger i politiet. Det vil likevel finnes områder der tradisjonelle prosjekter iht. politiets prosjektmodell kan benyttes. Dette kan gjelde midlertidige arbeidsoppgaver hvor 1) oppgaven er stor og det er mulig å designe løsningen i tidligfase (f.eks. infrastruktur), 2) koordineringsoppgaven er særlig stor (f.eks. PNP IKT) eller 3) mange IKT-systemer og produktteam blir berørt. Også tradisjonelle prosjekter skal ha en smidig tilnærming i gjennomføringsfasen med en aktiv produkteier. Prosjektene skal planlegges for å levere et minimumsprodukt raskt, og videreutvikling av funksjonalitet skal skje iht. smidig utvikling i produksjonslinjen.

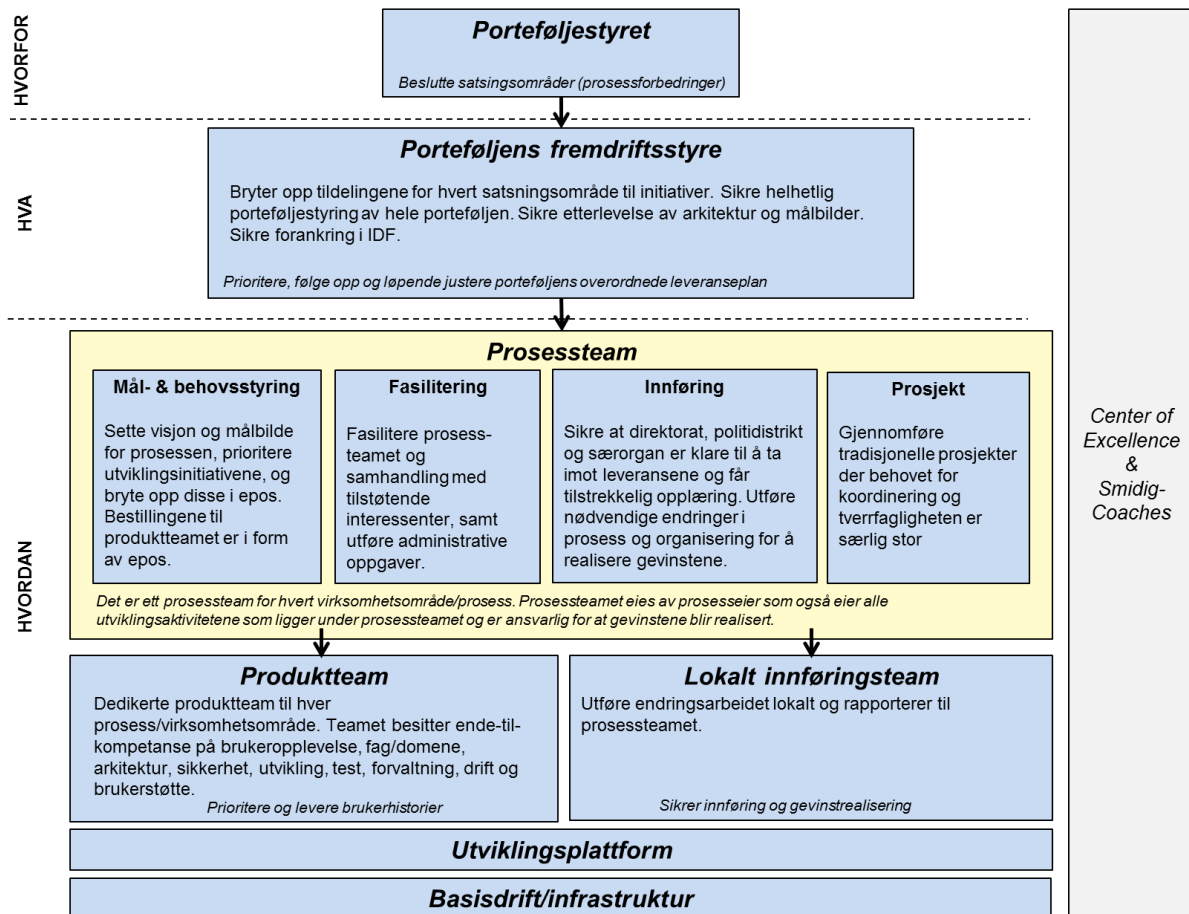
Fremtidig leveransemodell deles inn i tre nivåer: 1) Et *porteføljestyre* som beslutter satsingsområder og tildelinger, 2) Et *fremdriftsstyre* som bryter opp tildelingene i initiativer og følger opp den samlede porteføljen, 3) Et praktisk nivå bestående av *prosessteam*, *produktteam* og *lokale innføringsteam* for den enkelte prosess¹² som definerer og leverer konkrete tiltak..

⁹ Også kalt en "plan-build-run"-leveransemodell

¹⁰ Denne leveransemodellen heter DevOps. DevOps skiller seg fra tradisjonelle prosjekter ved at det gjennomføres mindre og hyppigere leveranser og med en tett dialog mellom brukere, utviklere og de som drifter IKT-løsningen. I en DevOps-modell gis et helhetlig leveranseansvar til ett tverrfaglig produktteam som spesifiserer, utvikler, tester og drifter en løsning.

¹¹ Denne DevOps-baserte leveransemodellen vil måtte utvikles over tid i tråd med metodeutviklingen på IKT-området

¹² Med "prosess" menes her en overordnet arbeidsprosess i virksomheten, eksempelvis Straffesaksbehandling



Figur 8: Illustrasjon av fremtidig leveransemodell

Hver prosess har sine produktteam og lokale innføringsteam. Hvert nivå skal sikre at de fatter beslutninger som medfører at pengene blir investert i det som gir størst verdi for brukerne og samtidig støtter opp under virksomhetens strategi. For å sikre målrettet utvikling av politiets digitale løsninger skal prosessteam og produktteam sørge for at "Reguleringsplan for digitale løsninger" etterleves og utvikles.

Superbrukerne og fagmiljøene involveres i ny leveransemodell helt fra idé/behovsspesifisering i arbeidet sammen med prosess-teamet og gjennom detaljering, utvikling og kontinuerlig avsjekk/testing sammen med produktteamene. For å sikre vellykket virksomhetsutvikling og innføring i direktoratet, distriktene og særorgan som følge av leveransene fra produksjonslinjene, opprettes det innføringsteam som tar ansvar for opplæring/kompetansebygging, gevinstrealisering, og nødvendige endringer i organisering og prosess. De som driver brukerservice involveres også, både i formidling av behov og støtte i lokal innføring.

Prinsipper for ny leveransemodell

- | | |
|---------------------------------------|---|
| 1. Brukeren i sentrum | Brukerne er først og fremst de som mottar politiets tjenester, dernest de ansatte som tar i bruk leveransene fra produktutviklingen og prosjektene for å yte tjenestene til samfunnet. Vi skal alltid ta utgangspunkt i brukernes behov, og videreutvikle våre produkter og tjenester for å gi dem høyest grad av nytte. Vi må redusere til et minimum alle aktiviteter som ikke er nødvendig for å skape verdi for brukeren. |
| 2. Beslutninger fattes på riktig nivå | Kunnskapsbaserte beslutninger fører til høyere kvalitet på tjenestene vi leverer. For å sikre at de med riktig kompetanse tar beslutninger innen sitt område er det viktig at myndigheten for å fatte beslutninger delegeres til der kompetansen sitter. Dette gjelder også de ansattes medbestemmelse. Dette krever en kultur preget av gjensidig tillit på tvers av organisatoriske enheter og rapporteringslinjer. |

3. Fokus på flyt	For å redusere ledetiden fra bestilling til verdi er levert for brukeren er det nødvendig at alle ledd i verdikjeden prioriterer aktiviteter som er verdiskapende for produktet og fjerner hindringer som kan forlenge ledetiden. Det er derfor viktig at enhver i verdikjeden har nødvendig myndighet og fokus til å ferdigstille sine arbeidsoppgaver.
4. Innebygd kvalitet	Kvalitet bygges inn i løsningene så tidlig som mulig og står i hovedfokus på alle nivåer i verdikjeden fra behovet oppstår til løsningen er i produksjon. Hver delleveranse som sendes videre i verdikjeden skal være av riktig kvalitet før den sendes til neste ledd eller fase.
5. Kontinuerlig læring og utprøving	For å oppnå det beste resultatet skal vi pilotere så tidlig som mulig og forbedre produktet gjennom flere iterasjoner. Vi må ha en kultur hvor vi løpende lærer av vår suksess og feil, og hvor det er akseptert å ikke lykkes på første forsøk.
6. Innebygd sikkerhet og personvern	Sikkerhet og personvern bygges inn i løsningene så tidlig som mulig. Ved å tenke personvern tidlig i utviklingsprosesser kan systemet designes slik at det tar hensyn til viktige personvernprinsipper. God informasjonssikkerhet må være en del av løsningen. Risikovurderinger må gjøres for helhetlige løsninger og i hver delleveranse, slik at riktige tiltak blir iverksatt. Risikostyringsprosessen er en kontinuerlig forbedringsprosess, som ivaretar strukturerte risikovurderinger der dette er nødvendig.

4.2 Sikker utvikling, testing og drift

Sikkerhet må bygges inn utviklings- og testprosesser som brukes av politiet og underleverandører. Der DevOps benyttes som leveransemodell er det hensiktsmessig at dette forstås som "DevSecOps" slik at sikkerhet blir en integrert del i hele utviklingsprosessen hvor sikkerhetskompetanse, metoder og verktøy er representert i utviklingsteamene. Sikkerhetstesting/sårbarhetstesting vil være en integrert del av utviklingen. Security Development Lifecycle (SDL) er en anerkjent standard som er etablert av Microsoft for å utvikle produkter med færre sårbarheter. Denne metoden kan brukes både i smidig utvikling og for plan-build-run prosesser.

NSM gir flere anbefalinger rundt test i sine grunnprinsipper for IKT-sikkerhet som bør vurderes som et ledd i sikker utvikling og testing. Et hovedbudskap i disse prinsippene er å unngå at sensitiv informasjon kommer på avveie, at produksjonsdata forblir tilgjengelige og upåvirket av utvikling og test.

Sikkerhet i drift handler om å ivareta sikkerheten i henhold til bestemt sikkerhetsarkitektur som å vedlikeholde sikringsnivå, opprettholde motstandsdyktighet mot digitale angrep, og å kunne oppdage og håndtere digitale angrep.

Innebygd personvern

Vi skal ivareta innebygd personvern i utvikling av politiets digitale løsninger. Datatilsynet har gitt ut en egen veileder som skal hjelpe norske virksomheter å forstå og etterleve kravet om innebygd personvern i de nye personvernreglene. Den er utarbeidet i samarbeid med sikkerhetsekspertene og programutviklere i privat og offentlig sektor. Veilederen beskriver syv aktiviteter i en kontinuerlig prosess og hva som inngår i hver aktivitet, herunder krav, design, koding, test, produksjonssetting, forvaltning og opplæring.

Sikkerhetsgodkjenning eller annen sikkerhetsakkreditering

Dersom politiets informasjonssystemer blir definert som sikkerhetsgraderte skal de sikkerhetsgodkjennes av en godkjenningsmyndighet før de tas i bruk. Dersom informasjonssystemer ikke inneholder gradert informasjon, men like fullt er å anse som viktige for nasjonale sikkerhetsinteresser/grunnleggende nasjonale funksjoner blir de definert som skjermingsverdige informasjonssystemer. Også disse systemene blir da gjenstand for sikkerhetsgodkjenning.

For andre systemer kan en sikkerhetsakkrediteringsprosess gjennomføres som et ledd i å ivareta etterlevelse av annet regelverk.

5 Styring av IKT-funksjonen

5.1 Hensikt, mål og prinsipper for fremtidig IKT-funksjon

Hensikten med utviklingen av fremtidig IKT-funksjon og leveransemodell er å oppnå "**Raskere realisering av digitale løsninger for politiet**". Dette skal vi gjøre på en måte som sikrer at personvern, sikkerhet og andre krav til etterlevelse blir bygd inn i løsningene fra start og løpende ivarettatt gjennom hele livssyklusen. Raskere realisering av sikre digitale løsninger vil bidra til at politiet kan utnytte mulighetene og møte utfordringene som ligger i den voldsomme innovasjonen som skjer på teknologiområdet, og derigjennom realisere politiets virksomhetsstrategi både på kort (2020) og lang sikt (2025). Stabil og sikker drift av politiets IKT-løsninger vil fortsatt være sentralt for IKT-funksjonen.

Basert på hensikten har vi definert seks viktige mål med tilhørende prinsipper¹³ for IKT-funksjonen fremover:

1. **Forbedre politiets tjenester gjennom økt utnyttelse av innovasjon innen teknologi**
Politiet må etablere en systematisk tilnærming til utnyttelse av teknologidrevet innovasjon. Vi må bygge kompetanse på innovasjonsledelse, dataanalyse og innsikt og vi må samarbeide med leverandører og andre virksomheter for å styrke vår egen kompetanse. Mye av teknologiutviklingen skjer som skytjenester så det er viktig at politiet kan nyttiggjøre seg disse.
2. **Øke tempo i etablering av digitale løsninger i politiet**
For å kunne levere mindre leveranser hyppigere til brukerne enn i dag må politiet etablere en leveransemodell basert på produktutvikling, brukerinvolvering, smidige prinsipper og DevOps med innebygd personvern og sikkerhet. Allokering av ressurser til utvikling funksjonalitet må i større grad styres og baseres på effekter som skal oppnås. Leveransemodellen må veiledes og støttes av målbilder, arkitektur og moderne skybasert infrastruktur. Vi skal også øke politiets interne utviklingskapasitet. Vi ønsker også å samarbeide tettere med forsvarssektoren for å dra nytte av hverandres kompetanse og kapasitet.
3. **Sikre kapasitet, kompetanse og fleksibilitet til å håndtere politiets behov**
Vi skal bygge opp egen kompetanse og kapasitet på det som er politispesifikk kjernevirksomhet, og vi skal bruke markedet på det som ikke er spesifikt for politiet. Vi er også nødt til å bruke markedet på teknologiområder som utvikler seg fortere enn vi klarer å følge med. Vi skal bygge egen kompetanse på å integrere og følge opp tjenester fra eksterne leverandører.
4. **Redusere politiets investeringsbehov og øke forutsigbarheten på kostnadsutviklingen**
Der det er mulig og hensiktsmessig ønsker vi å benytte markedet til å jevne ut behovet for reinvesteringer slik at det blir mer forutsigbart, og redusere behovet for pukkelinvesteringer slik at det blir mer håndterbart. Dette kan bl.a. gjøres ved å inngå langsiktige tjenesteavtaler for digitale løsninger som ikke er i politiets kjernevirksomhet og å utnytte storskalafordeler og abonnementsbaserte tjenester i markedet. Vi ønsker også å utnytte konkurransen i markedet bedre for å oppnå gode vilkår.
5. **Sikre en styrt, effektiv og trygg bruk av markedet**
All bruk av markedet skal vurderes med hensyn på hensiktsmessighet, kostnadseffektivitet og informasjonssikkerhet, og bruk av markedet skal skje i tråd med relevant regelverk herunder regelverk for sikkerhet og personvern. Vi må styrke vår styring og oppfølging av de som har tilgang til politiets informasjon og digitale løsninger. Det er også nødvendig å utarbeide en strategi for bruk av ulike typer skytjenester.
6. **Ivareta stabil og sikker drift av digitale løsninger også i fremtidig IKT-funksjon og leveransemodell**
Vi skal sikre etterlevelse av relevant regelverk herunder regelverk for sikkerhet og personvern, i utvikling, forvaltning og drift av IKT-løsninger. Vi skal ha en risikobasert tilnærming til utvikling, drift og forvaltning og det skal være tydelige krav til tilgangsstyring og kontroll i dette arbeidet. For å sikre gode tjenester må vi etablere helhetlig ansvar og kapasitet for å styre og integrere IKT-tjenester og -

¹³ Teksten under målene er et sammendrag av de prinsippene som er definert for hvert mål. Den komplette teksten finnes i vedlegg 1.

løsninger ende til ende. Vi ønsker også å bruke markedet til bygge standardiserte infrastrukturtenester.

5.2 Styring av IKT

5.2.1 Styringsmodell for IKT

Styringsmodellen¹⁴ for IKT i politiet omfatter all etablering, videreutvikling, forvaltning, drift, support, bruk, avvikling og oppfølging av digitale løsninger som er innenfor politiets/politidirektørens ansvarsområde. Dagens styringsmodell bestående av styringsområder¹⁵, beslutningsmodell, styringsstruktur, styringsprosesser og styringsdokumenter ble sist revidert helhetlig i 2014/15 bl.a. basert på de endringene som ble gjort i Politidirektoratet og etableringen av PIT. Styringsmodellen må nå revideres som følge av denne strategien. I kapittel 5.2.2 beskrives risikostyring innenfor informasjonssikkerhet nærmere, det vil tas inn i revideringen av styringsmodellen.

Noen viktige prinsipper for styringsmodellen er gjengitt nedenfor:

- Understøtte ett politi og utvikling av fellesløsninger
- Omfatte både det som er felles, det som er spesielt, det som er saksspesifikt og det som er særskilt (se kapittel 5.3)
- Sørge for størst mulig grad av felles IKT-infrastruktur
- Politidistrikt, særorgan etc. er brukere av politiets digitale tjenester, ikke kunder
- Ikke internhandel og internfakturering for digitale tjenester
- Ivareta de til enhver tid gjeldende rammer for informasjonssikkerhet og personvern

5.2.2 Risikostyring innenfor informasjonssikkerhet

Politidirektoratet skal legge til rette for god sikkerhetsstyring i direktoratet og politidistriktene for øvrig.¹⁶ Sikkerhetsstyring tilrettelegger for at politiets egne viktige verdier beskyttes gjennom risikobasert og strukturert arbeid preget av kontinuerlig forbedring. Sikkerhetsstyring er det samme som risikostyring innenfor sikkerhetsområdet.

Risikostyring skal sikre at den risikoen virksomhetens informasjonsverdier utsettes for er på et akseptabelt nivå. Risikostyring av informasjonssikkerhet i virksomhetene skal være en gjentakende prosess som innebærer:

- Fastsettelse av risikoaksept
- Analyse av risiko
- Håndtering av risiko
- Beslutning om gjenværende risiko er akseptabel

Politidirektørens risikoaksept

Politidirektørens risikoaksept definerer på hvilket nivå risikoaksepten ligger for hvert definert konsekvensområde. I tillegg til nivå for risikoaksept vil det være opp til politidirektøren og vurdere hvilke konsekvensområder som er riktige å bruke for politiet. Konsekvensområder kan for eksempel være konsekvenser for politiets evne til å løse samfunnsoppdraget, omdømme/tillit, personell, økonomi, borgere.

Risikostyring i politiets IKT-funksjon

Risikostyring innen IKT-funksjonen gjør seg gjeldende på flere områder. Politidirektoratet har den overordnede IKT-styringen, og må derfor også ha den overordnede risikostyringen innenfor IKT-funksjonen. Prosesseiere setter premisser for IKT-funksjonen og må ha et forhold til lover og regler som

¹⁴ [En styringsmodell] er en forenklet fremstilling av hvordan styringen er organisert, og (...) viser sammenhenger mellom styringsaktiviteter, hvem som tar formelle beslutninger, hvem som realiserer mål og utfører aktiviteter, samt knytter styringsaktivitetene til verktøy og virkemidler som benyttes, Senter for statlig økonomistyring (2011) En beskrivelse av styringsmodellen i et departement, s. 8

¹⁵ Styringsområder i dagens styringsmodell er: Mål og strategi for IKT i politiet, Økonomistyring, Portefølje- og prosjektstyring, Arkitekturstyring, Virksomhetsstyring av PIT, Tjenesteleveransestyring og Tjenesteforvaltning

¹⁶ Tildelingsbrev 2018 Politidirektoratet, 5.2.1 Mål 1

gjelder deres arbeidsprosesser hvordan informasjonssikkerhet og personvern ivaretas i disse. Politiets IKT-tjenester skal levere sikre digitale løsninger i tråd med prosesseiers behov og krav, både i utvikling, drift og forvaltning av løsningene. Dette gjøres gjennom en risikobasert tilnærming. Dette gjelder for alle ledd i verdikjeden, både for egenproduserte tjenester og for tjenester som kjøpes av andre.

Der særorgan, politidistrikt eller andre aktører i politiet utøver tilsvarende roller som ovenfor vil det samme ansvaret for risikostyring gjelde for dem. Grensesnitt mellom virksomhetene må avklares, og tydelig ansvar og myndighet defineres for de ulike virksomhetene i politiet.

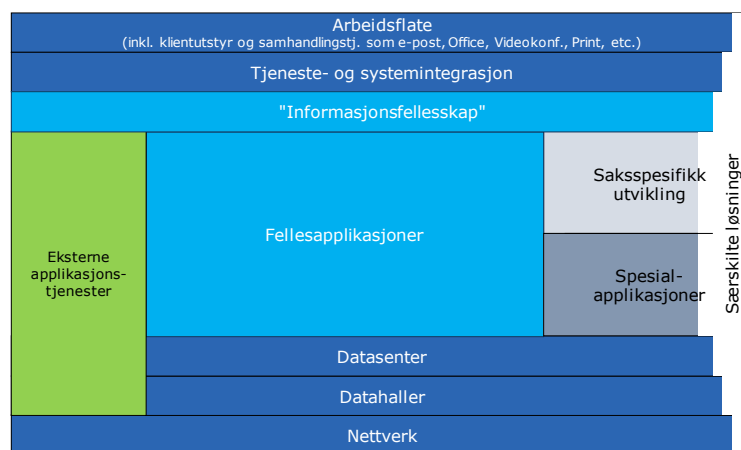
Beslutningsnivåer for risikoeierskap og risikoaksept i politiet knyttet til IKT-funksjonen

For å kunne ivareta god risikostyring, må det tydelig fremkomme hvem som har ansvar for hvilke områder og hvem som har myndighet til å akseptere risiko innenfor de ulike områdene. En tydelig nivåinndeling vil kunne rydde opp i uklare ansvarsforhold knyttet til sikkerhet og risikoaksept, men også knyttet til premissgivelse og styring i IKT-funksjonen.

I vedlegg 4 er det utarbeidet et forslag til nivåer for risikoaksept knyttet til de prosessene som er nødvendig å ivareta i IKT-funksjonen. En slik nivåinndeling vil medføre avklaringer innad i POD og mellom POD og underliggende virksomheter, både PIT, PFT, politidistrikt og særorgan.

5.3 Oppgavefordeling for IKT-løsninger

De digitale løsningene i politiet kan grovt sett deles inn som vist i figuren under. Alle delene er viktige for politiets oppgaveløsning.



Figur 9: Grovinndeling av IKT-løsninger

Oppgavene på de ulike områdene i figuren fordeles i utgangspunktet på følgende måte:

Område	Oppgavefordeling
1. Arbeidsflate, Tjeneste- og systemintegrasjon	- PIT leverer de arbeidsflatene med tilhørende klientutstyr som er nødvendig for å bruke politiets IKT-tjenester på en hensiktsmessig måte der våre ansatte trenger det - PIT integrerer politiets IKT-tjenester og IKT-løsninger slik at de fremstår som helhetlige for våre brukere, både innenfor og utenfor politiet
2. "Informasjonsfellesskap"	Det er et mål at informasjon skal kunne deles på tvers av eksterne applikasjonstjenester, felles- og spesialapplikasjoner og konkrete saker/etterforskninger/oppgaver.
3. Basis infrastruktur (Nettverk, Datahaller og Datasenter)	- PIT leverer WAN som realiserer de nettverk som er nødvendig for politiets bruk og kobling mot internett for hele politiet - PIT leverer datahaller for politiets prosesserings-, lagrings- og

	nettverkskomponenter • PIT leverer datasenter (prosessering, lagring etc.) både tradisjonelt og skybasert, på tvers av eget datasenter, datasenter hos leverandører og fra allmenn sky
4. Fellesapplikasjoner	De standardiserte, felles applikasjonene som støtter prosessene i alle politiets virksomhetsområder på tvers av alle politidistrikter og særorgan samt POD, PFT og PIT. Fellesapplikasjoner etableres, videreutvikles og driftes av PIT i tett samarbeid med brukerne av applikasjonene og evt. underleverandører. Eksempel på fellesapplikasjoner er BL, Indicia og PO.
5. Spesialapplikasjoner	De spesielle applikasjonene som i tillegg (til 4) er nødvendige for prosesser og arbeidsoppgaver som kun utføres ett sted, av én organisasjon, i én metode eller i én spesialistfunksjon i politiet. Spesialapplikasjoner skal kun tilgjengeliggjøres for et lite antall brukere. Spesialapplikasjoner kan etableres, videreutvikles og driftes av brukerne sin organisasjon, evt. i samarbeid med PIT. Hvis en spesialapplikasjon skal breddes videre i politiet skal applikasjonen overføres til PIT som en fellesapplikasjon. Eksempel på spesialapplikasjoner er Argus og LIMS.
6. Saksspesifikk utvikling	Den spesielle utvikling og anvendelse av funksjonalitet/applikasjoner som i tillegg (til 4 og 5) er nødvendige for arbeidsoppgaver knyttet til én sak/etterforskning/oppgave. Saksspesifikke løsninger benyttes av de som jobber med saken/etterforskningen/oppgaven. Saksspesifikke løsninger kan etableres, videreutvikles og driftes av brukerne sin organisasjon, evt. i samarbeid med PIT. Det er et mål at så mye som mulig av det som gjøres av saksspesifikk utvikling over tid kan gjøres om til felles- eller spesialapplikasjoner eller utvide det som tilbys gjennom infrastrukturen – dette vil være et meget viktig bidrag for å utvikle de standardiserte IKT-tjenestene til politiet.
7. Særskilte løsninger	IKT-løsninger som dekker helt særskilte behov i politiet og som av ulike grunner kan avvike fra politiets felles infrastruktur
8. Eksterne applikasjons-tjenester	Applikasjoner som politiet benytter for å løse sine oppgaver som leveres av eksterne leverandører, enten skybasert som Software as a Service (SaaS) eller som tradisjonelle applikasjonstjenester. En ekstern applikasjonstjeneste kan anvendes enten som en fellesapplikasjon eller som en spesialapplikasjon og vil styres som disse. Eksempel på dette er Webcruiter, CIM, SAP og SIAN.

Fellesapplikasjoner, spesialapplikasjoner, saksspesifikke løsninger og særskilte løsninger kan være egenutviklet, hyllevare eller SaaS/applikasjonstjenester.

Etablering og videreutvikling av fellesapplikasjoner og spesialapplikasjoner skal følge politiets applikasjonslandskap.

Fellesapplikasjoner, spesialapplikasjoner og saksspesifikke løsninger med tilhørende maskinvare skal som hovedregel plasseres i, utvikles og produseres på, integreres med og tilgjengeliggjøres via politiets felles basis infrastruktur, arbeidsflate og tjeneste- og systemintegrasjon. Kun for særskilte løsninger vil det gis adgang til å avvike fra dette på ett eller flere områder.

5.4 Samhandling

Innovasjon og utvikling i politiet gjennom digitalisering avhenger av tverrfaglig samarbeid. Det må etableres samarbeid og samhandling for all virksomhetsutvikling i politiet. I tillegg til roller og funksjoner som er beskrevet i leveransemodellen kreves et tverrfaglig samarbeid for å:

- Identifisere, beskrive og prioritere behov for å ivareta en helhetlig tilnærming til virksomhetsutvikling
- Drive innovasjon og identifisere mulighetsrom for digitalisering av arbeidsprosesser
- Lage målbilder, veikart og langtidsplaner for å etablere forutsigbarhet
- Utforme beslutningsgrunnlag slik at porteføljestyret kan ta gode beslutninger

5.5 Finansiering av IKT

Kostnadene til IKT i politiet utgjør litt over 10 % av etatens budsjett.¹⁷ Mye av kostnadene går til eksterne leverandører, nesten 1,4 mrd. NOK i 2017.¹⁸ IKT-kostnadene i politiet fordeler seg på to hovedgrupper:

- Sentrale IKT-kostnader som omfatter den strategiske utviklingsporteføljen inkl. politiets frie utviklingsmidler og øremerkede midler fra JD, og PIT's budsjett som omfatter drift og minimumsforvaltning, endring og forbedring av eksisterende IKT-løsninger og administrasjon og egen virksomhetsutvikling
- Lokale IKT-kostnader i politidistrikt og særorgan

Til tross for at det vil være et stort investeringsbehov knyttet til fornyelse av politiets digitale løsninger, er vurderingen at mye av denne utviklingen kan la seg realisere over tid ved omdisponering av eksisterende rammer slik at politiet får mer IKT for pengene. Det er heller ikke ønskelig å etablere en strategi som har for store avhengigheter til satsingsforslag og tilførsel av ytterligere midler – dette er også i tråd med politiets virksomhetsstrategi. Den største utfordringen med finansiering er det etterslepet politiet har på IKT-området som gjør at politiet fortsatt er avhengig av tilførsel av ekstra midler for å realisere applikasjonslandskapet på viktige områder som f.eks. Straffesak – hvis ikke vil moderniseringen ta for lang tid.

Et grep vi ønsker å videreføre er å erstatte innleide konsulenter i PIT og POD med egne ansatte. Det vil øke antall ansatte, men redusere kostnadene. Der det er mulig og hensiktsmessig ønsker vi å benytte markedet til å jevne ut behovet for reinvesteringer slik at det blir mer forutsigbart, og redusere behovet for pukkelinvesteringer slik at det blir mer håndterbart. Vi skal fortsette med å budsjettfinansiere PIT og ikke innføre tjenestepricing og internfakturerings. Dagens praksis med underfinansiering av PIT må avsluttes. De store eksterne IKT-kostnadene i politidistrikter og særorgan¹⁹ gjør at vi må vurdere om det skal etableres flere felles IKT-tjenester til politiet for bedre å møte behovet ute i etaten. Felles IKT-tjenester kan også gi stordriftsfordeler og bidra til mer enhetlig oppgaveutførelse og redusert behov for at hvert distrikt og særorgan skal bygge den samme kompetansen.

5.6 Måling av IKT

Politiet er avhengig av en effektiv IKT-funksjon og det er derfor nødvendig å måle hvilken effekt, kvalitet og verdi IKT-funksjonen bidrar med til politiets måloppnåelse. Målene for politiet er gitt i virksomhetsstrategiens 12 strategiske mål for 2020 og det er ønskelig å kunne knytte målingen av IKT helt tilbake til disse.

I tråd med kapittel 2.4, kapittel 3 og kapittel 5 må vi måle IKT-funksjonen på:

- Hva vi leverer av IKT-løsninger
- Hvordan vi leverer IKT-løsninger
- Økonomisk utvikling
- Stabil og sikker drift.

Dette må gjøres om til detaljerte måleparametere med beskrivelse av konkrete målinger på hvilken effekt, kvalitet og verdi IKT bidrar med til virksomheten.

¹⁷ Dette er høyere enn hva som disponeres innen enkelte andre offentlige etater (helsesektoren, Nav, m.fl.)

¹⁸ 1364 MNOK iht. PFT sin spend-analyse for 2017 på kategorien IKT

¹⁹ 648 MNOK inkl. Nødnett iht. PFT sin spend-analyse for 2017 på kategorien IKT

6 Bruk av leverandørmarkedet

6.1 Strategiske betraktninger

Det er ikke hensiktsmessig, gjennomførbart eller kostnadseffektivt for politiet å ha full kapasitet og kompetanse innenfor alle områder av IKT-funksjonen, og politiet anvender i dag leverandørmarkedet i utstrakt grad for å levere digitale tjenester. Det er mulig å utnytte leverandørmarkedet bedre enn det politiet gjør i dag. Tidligere analyser²⁰ viser at bruken av markedet innen applikasjonsutvikling og -forvaltning i stor grad er timebaserte ressurskjøp, noe som indikerer et potensial knyttet til storskaladrift, partnertankegang og større deling av kommersiell risiko. Videre viser analysene at dagens IKT-funksjon har relativt sett mye kapasitet og kompetanse innen ikke-strategiske funksjoner og arbeidsoppgaver og for lite kapasitet knyttet til digital innovasjon, systemutvikling, tjenesteintegrasjon, prosjektledelse, leverandørstyring, virksomhetsarkitektur, kognitive teknologier, dataanalyse og sikkerhet. Det er også muligheter for konsolidering av avtaler og leverandører.²¹

Områder hvor leverandørmarkedet kan gi et strategisk fortrinn for politiet omfatter støtte på innovasjon og kompetanse innen anvendelse av ny teknologi. Videre behøves kapasitet og kompetanse som øker politiets fleksibilitet til å skalere og nedskalere utviklingsinnsats etter behov. Langsiktige partnerskap på et færre sett av leverandører kan styrke denne evnen. Videre bør bedre bruk av leverandørmarkedet utnyttes for å redusere politiets investeringsbehov og øke forutsigbarhet på finansiering, eksempelvis ved at markedet kan bidra med investeringer og storskalafordeler på infrastruktur og applikasjoner.

Så langt som mulig skal politiet unngå å komme i uhensiktsmessige avhengighetsforhold til enkeltleverandører. For tjenester og løsninger som kjøpes i markedet skal det kunne etableres reelle konkurransesituasjoner.

Konkrete tiltak for bruk av leverandørmarkedet er beskrevet nærmere i vedlegg 5.

6.2 Vurdering av tjenestekjøp innen politiets virksomhetsområder

Som del av denne strategien er det et uttalt mål at politiet skal gjøre mer av IKT-utviklingen selv på løsninger som benyttes i politiets kjernevirksomhet, og fortsette å anvende leverandørmarkedet på mindre strategiske oppgaver og for å styrke politiets egenutvikling med kapasitet og kompetanse. Det er gjennomført en analyse av hvilke applikasjons- og tjenestekområder som er egnet for tjenestekjøp og hva politiet bør ivareta med egen kapasitet og kompetanse, i henhold til mål for fremtidig IKT-funksjon som beskrevet i kapittel 5.1. Det er anvendt en evalueringsmodell som består av kriterier knyttet til tjenestenes egenart (standardiserte vs. spesialiserte), kompetansetilgang, strategisk verdi av tjenestene m.m. I tillegg er det tatt hensyn til politiets antatte kapasitet og evne til å levere tjenester med eget personell. Vurderingen²² er nærmere beskrevet i vedlegg 5 – Bruk av leverandørmarkedet og oppsummert nedenfor. Vurderingen tar utgangspunkt i de endringer på applikasjonene som er foreslått i fremtidig applikasjonslandsskap og som angir omfanget av nye løsninger, samt hvilke eksisterende løsninger som er tenkt videreutviklet, erstattet eller på sikt faset ut.

Styring og ledelse

Styring og ledelse er et strategisk virksomhetsområde hvor politiet skal sitte i førersetet for styring, kontroll og utførelse. De digitale løsningene som støtter oppunder dette virksomhetsområde er i stor grad standardiserte med begrenset behov for politispesifikk kompetanse. Større grad av tjenestekjøp kan være hensiktsmessig på dette området sammenlignet med mer politispesifikke virksomhetsområder.

Opparbeide kunnskap

Etterretning er et politispesifikt område som er høyt prioritert i politiets virksomhetsstrategi. Dette er et område hvor politiet i stor grad bør utvikle løsningene selv (eksempelvis ny etterretningsapplikasjon), med

²⁰ Bla. gjeldende IKT Sourcingstrategi (2013) og realiseringsplaner og mulighetsstudien for IKT Sourcing og finansiering (2017)

²¹ Ifm. HSO-fase 1 er applikasjonene som PIT har tatt over fra politidistriktene ikke konsolidert

²² Vurderingen har ikke omfattet en risikoanalyse med hensyn til sikkerhet. Før evt. tjenestekjøp vil dette i tillegg måtte gjøres for de aktuelle områdene.

bruk av strategiske leverandører for å sikre tilstrekkelig kompetanse og kapasitet. For Legacy-applikasjoner som skal fases ut innenfor etterretning, bør tjenesteaftaler med leverandører videreføres. De andre områdene innenfor opparbeide kunnskap (personer, miljøer og fenomener, sammenhenger og mønster, formidle kunnskap internt og eksternt, informasjonsinnhenting) er også politispesifikke virksomhetsområder med stor grad av strategisk kompetanse, men har et potensial for tjenestekjøp av enkelte applikasjoner. Det bør også utredes muligheter for bruk av hyllevareprodukter for noen av behovene.

Forebygging og beredskap

Forebygging og beredskap mangler vesentlig digital støtte i dag og ny applikasjon for forebygging er definert i fremtidig applikasjonslandskap. Det anbefales at nye applikasjoner innen dette området utvikles av politiet selv. Beredskap krever også god materiellstyring og -forvaltning for å holde oversikt over politiets materielle ressurser. På dette området vil hyllevare kunne anvendes og baseres på eksisterende ERP-plattform som kan ruller ut til distriktene. Det er tydelige sikkerhetsbehov knyttet til materiellstyring og -forvaltning innenfor enkelte områder (alvorlig/organisert kriminalitet, terror). Slik informasjon vil kunne avsløre politiets kapasiteter, kapabiliteter og metoder. Vurderinger må derfor gjøres om disse behovene skal dekkes i særskilte løsninger eller gjennom fellesløsninger.

Politioperativt

Innen operativt politiarbeid foreligger et stort behov for modernisering, og det er pågående initiativ for å utrede forbedringer. Det skal både etableres nye applikasjoner og gjennomføres transformasjoner av eksisterende applikasjoner på dette området. Noen funksjoner er forholdsvis standardiserte og kan støttes av tjenester i markedet, mens andre krever politispesifikk kompetanse i IKT-utvikling. Av hensyn til prioritering av utviklingskapasitet i politiet anbefales anvendelse av leverandørmarkedet i større grad gjennom kjøp av hyllevare og utviklingstjenester, enn for andre politispesifikke områder. Politioperativt har et tydelig sikkerhetsbehov knyttet til områder som berører alvorlig kriminalitet og terror som må tas i betraktning ved vurdering av tjenestekjøp.

For spesielle situasjoner har operativt politiarbeid et særskilt behov for gode og sikre digitale løsninger i form av kommando- og kontroll systemer, og kommunikasjonsløsninger. Her er det aktuelt å inngå et sivilt-militært samarbeid i tillegg til å ta i bruk sikre fellesløsninger.

Straffesaksbehandling

Innen etterforskning, påtale og irettføring må det gjennomføres gjennomgripende endringer for å modernisere og fornye applikasjonsstøtten. Med ny straffeprosesslov følger også mange funksjonelle behov som skal realiseres, med få muligheter for å anvende standardiserte IKT-tjenester i markedet. Anbefalingen er at denne transformasjonen primært realiseres ved egenutvikling i politiet, med kjøp av tjenester i markedet til å støtte med kapasitet og kompetanse.

Forvaltning

Mange av politiets publikumstjenester ligger innen området forvaltning. Disse tjenestene består i stor grad av funksjonalitet som er svært standardisert i markedet (søknader, saksbehandling og selvbetjening). Det er også et område med stort potensiale for effektivisering gjennom digitalisering. Anbefalingen er at politiet vurderer stor grad av tjenestekjøp av IKT-tjenester innenfor dette området, gjennom avtaler med ende-til-ende ansvar hos strategiske leverandører i markedet. Finansiering av dette bør knyttes til gevinst- og effektuttak av digitaliseringen. Merk at håndtering av person og ID ifm. pass og grensekontroll ikke inngår i dette området, men er plassert under området "opparbeide kunnskap".

Sivil rettspleie

Sivil rettspleie er et område hvor politiet i stor grad kjøper IKT-tjenester fra Skatteetaten (Statens innkreivingsentral). Politiet skal videreføre samarbeid med Skatteetaten på dette området. Det foreligger planer i politiet for omfattende digitalisering av tjenester innen sivil rettspleie.

Støtte

Administrative støttefunksjoner er et område med potensial for å finne gode pakkeløsninger/hyllevare i markedet, og politiet bør i så stor grad som mulig anvende tjenestekjøp innen administrative støttefunksjoner. Eksempelvis med etablering og utrulling av en felles ERP-plattform innen innkjøp, materiell og logistikk for politiet basert på hyllevare. DFØ er en sentral leverandør for politiet som også

leverer lønn- og regnskapstjenester som også omfatter applikasjoner som skal anvendes i politiet. Merk at det eksisterer tydelige sikkerhetsbehov knyttet til slike løsninger innenfor enkelte områder (alvorlig/organisert kriminalitet, terror). Slik informasjon kan si noe politiets kapasiteter, kapabiliteter og metoder. Vurderinger må derfor gjøres om disse behovene skal dekkes i særskilte løsninger eller gjennom fellesløsninger.

Felleskomponenter

Felleskomponenter omfatter applikasjoner og funksjonalitet som anvendes innenfor flere virksomhetsområder. Enkelte løsninger kan vurderes som strategiske (brukergrensesnitt m.m.) men kan dra stor fordel av kompetanse som er tilgjengelig i markedet. Enkelte løsninger er også anskaffet som hylleware. Det vil også være felleskomponenter politiet bør utvikle selv. For felleskomponenter må prioritering av egen utviklingskapasitet avveies mot utvidet bruk av leverandørmarkedet.

6.3 Vurdering av tjenestekjøp innen politiets IKT-funksjon

Det er gjort en analyse av oppgavene i politiets IKT-funksjon og hvilke typer av tjenestekjøp som er fornuftig å gjøre til denne. Analysen er basert på funnene fra mulighetsstudien, referansecase, beste praksis i markedet og sett opp mot politiets mål og retning for fremtidig IKT-funksjon.

Strategi og styring

Politiet må selv ha kapasitet og kompetanse til å utøve strategi og styring av IKT-funksjonen. Dette krever at politiet må styrke egen kompetanse og kapasitet til å drive tjeneste- og leverandørstyring i tillegg til informasjonssikkerhet, herunder ivareta sikkerhetsmekanismer. Politiet bør vurdere å benytte innovasjonspartnerskap og støtte fra markedet til å bygge funksjoner innen strategi og styring. Politiet bør samarbeide med internasjonale politiorganisasjoner og andre offentlige virksomheter der det er mulig.

Tjeneste- og systemintegrasjon

Politiet skal selv ivareta funksjonen for tjenesteintegrasjon, som er ansvarlig for at ulike IKT-tjenester fungerer i sammenhengende arbeidsprosesser for brukerne. Markedet bør brukes som hjelp til å bygge opp funksjonene gjennom beste praksis på prosesser, verktøy og metode. Dette bør gjøres sammen med strategiske leverandører som inngår som en del av politiets styringsmodell. Verdikjedeovervåkning²³ krever stor forståelse for virksomhetsprosessene og sammenheng med applikasjonene. Kompetanse bør derfor bygges internt.

Tjenestestøtte

For sentral og lokal 1. linje brukerstøtte skal politiet ha nærhet til sine brukere med eget personell og det anbefales ikke å etablere en brukerstøtte hos ekstern leverandør. Feilhåndtering og 2.-3. linje brukerstøtte vil, avhengig av virksomhetsområde, leveres av produktteamene i et ende-til-ende perspektiv. Politiet må derfor selv besitte spesialkompetanse på fagsystemer (2.-3. linje i brukerstøtte) som forvaltes av politiets egne ansatte, ellers skal leverandører benyttes på 2. og 3-linje supporttjenester for brukerne av løsninger som ivaretas av leverandører.

Sluttbrukertjenester

Ende-til-ende tjenester for klient og arbeidsflate blir i tidligere utredninger identifisert som konkrete eksempler på tjenester som er aktuelle for tjenestekjøp. Politiet (PIT) er i gang med en utredning for tjenestekjøp av klientadministrasjon inkludert arbeidsflate i et 2-års perspektiv.

Infrastruktur

Politiet har nylig ferdigstilt utbygging av ett datasenter og jobber med utbygging av ytterligere ett. Målet er at politiet på sikt også skal benytte infrastruktur i offentlig sky og i allmenn sky. Infrastruktur vurderes som en god kandidat for tjenestekjøp i evalueringsmodellen, med unntak av særskilte hensyn til informasjonssikkerhet. Innen dette området er det behov for videre utredninger i tråd med vurderinger av skystrategi og aktuelle samarbeidspartnere.

²³ Overvåke at alle komponentene/applikasjonene i en verdikjede/prosess fungerer slik at hele verdikjeden/prosessen fungerer

6.4 Sikkerhetsmessige vurderinger i forbindelse med tjenestekjøp

Politiet har en kritisk funksjon i samfunnet og mange av politiets tjenester skal være tilgjengelige når mye annet i samfunnet ikke fungerer, det gjelder også politiets digitale løsninger og informasjon. Disse må derfor sikres godt. De fleste overordnede føringer beskriver at tjenestekjøp kan gi sikkerhetsmessige gevinster, men at risikovurderinger er nødvendig å gjennomføre ved hvert kjøp. En grunnpilar i en risikovurdering er å gjennomføre en grundig vurdering av hvilken informasjon det dreier seg om og hvilke konsekvenser det kan få for samfunnet, politiets oppgaveløsning, personer som er registrert i politiets systemer og eget personell dersom informasjonen blir tilgjengeliggjort for eksterne leverandører. Ulike lovverk gir føringer for hva som må tas hensyn til der eksterne leverandører skal behandle sensitiv informasjon. Politiet kan i tillegg gi egne føringer utover dette i forbindelse med egen risikostyring og risikoaksept.

I utgangspunktet bør politiets informasjonssystemer befinne seg i Norge, både på grunn av politiets behandling av store mengder sensitiv informasjon og med hensyn til politiets rolle i Totalforsvaret. Den samme anbefalingen er gitt av NSM i rapporten om "sikker sky".

Justis- og beredskapsdepartementets føringer knyttet til tjenesteutsetting

JD har gitt Politidirektoratet føringer knyttet til tjenesteutsetting av IKT i justissektoren.²⁴ JD stiller seg i utgangspunktet positive til at tjenesteutsetting kan være et godt virkemiddel for å oppnå bedre sikkerhet, mer tilgjengelige og innovative tjenester, lavere kostnader, økt kompetanse og leveransedyktighet. De forventer at gode og dokumenterte vurderinger av risiko og sårbarhet blir gjennomført i forkant av eventuell tjenesteutsetting.

JD oppfordrer direktoratet til å se til de anbefalinger som NSM gir rundt tjenesteutsetting i deres grunnprinsipper for IKT-sikkerhet. I tillegg viser de til Kommunal- og moderniseringsdepartementets (KMD) Nasjonal strategi for bruk av skytjenester og Digitaliseringsrundskrivet.

NSMs råd ved tjenesteutsetting

NSM har skissert noen grunnprinsipper for IKT-sikkerhet. Virksomheten må sørge for at sikkerhetsnivået opprettholdes eller forbedres i forbindelse med tjenesteutsetting. Kravene til sikring av tjenester satt ut til tredjepart vil i prinsippet ikke være annerledes enn når de leveres av virksomheten selv. De samme kravene må innfris og må reguleres i kontrakter, følges opp og kontrolleres, slik at de ivaretas av tjenesteleverandøren. De tjenester som settes ut må også inkluderes i den resterende porteføljen til virksomheten. Virksomheten må etablere en helhetlig arkitektur og må forstå hvilke funksjoner i det totale systemet som ivaretas hvor i arkitekturen og av hvem. NSMs grunnprinsipper for IKT-sikkerhet bør følges, uavhengig av om tjenesten leveres internt eller av en tjenesteleverandør.

NSM har i sin rapport "Helhetlig IKT-risikobilde 2017" beskrevet behovet for bestillerkompetanse som dekker områder som virksomhetskompetanse, sikkerhetskompetanse, integrasjonskompetanse, kompetanse om anskaffelser og juridisk kompetanse.

Politidirektoratets "føre var"-prinsipper

Politidirektoratet har utarbeidet et sett med "føre var"-prinsipper, som skal være et utgangspunkt for mer detaljerte verdi- og risikovurderinger bl.a. ved konkrete tjenestekjøp knyttet til utvikling, drift og forvaltning av politiets IKT-løsninger. "Føre var"-prinsippene tar utgangspunkt i egen risikoaksept og har ikke lagt merkantile eller juridiske vurderinger til grunn:²⁵

1. De samme sikkerhetsmessige rammene som gjelder for politiet vil gjelde for hele leverandørkjeden
2. Alle politiets data skal lagres og prosesseres i Norge
3. All utvikling, forvaltning og drift av politiets IKT-løsninger skal skje fra Norge
4. Alle som har tilgang til data, drifter, utvikler eller forvalter IKT-løsninger som ansatt i eller etter avtale med politiet, skal ha taushetsplikt, uttømmende og utvidet politiattest og nødvendig sikkerhetsklarering avhengig av hva slags informasjon de har tilgang til

²⁴ Brev fra JD (DL 201705167-1)

²⁵ Risikovurderinger som foretas for det enkelte tjenestekjøp kan tilsi at prinsippene kan avvikes (eksempelvis ved kjøp av skytjenester) dersom restrisiko kan aksepteres

5. Leverandører til politiet på IKT-området kan kun ha ett nivå med underleverandører
6. Dersom det benyttes underleverandører skal de underlegges tilsvarende begrensninger og sikkerhetsregime som leverandøren
7. Alle leverandører som leverer tjenester til politiet kan underlegges tilsynsvirksomhet og kontroll fra politiet. Dette avgrenses ikke bare til tekniske eller sikkerhetsinspeksjoner. Revisjon kan gjennomføres av politiet selv eller av avtalt tredjepartsrevisor.
8. Alle leverandører skal forpliktes til å kunne fremlegge oppdaterte lister av personell med tilgang eller sannsynlig tilgang til politiets data. Dette personellet skal etterleve punkt 4.
9. Dersom det oppstår hendelser eller avvik fra regulær trafikk/oppdragshåndtering skal dette varsles til egen og egnet kanal hos politiet
10. Politiet og leverandør/underleverandør skal jevnlig sammen vurdere den tekniske løsningen i den hensikt å verifisere at dette er den mest optimale løsningen hva angår de truslene og sårbarhetene som er mot den valgte teknologiske plattform og komponenter. Dersom det avdekkes avvik fra optimal løsning eller krav (herunder sikkerhet mm.) skal dette utbedres uten opphold.

6.5 Sikkerhetsmessige betraktninger om bruk av skytjenester

Ved bruk av skytjenester gir digitaliseringsrundskrivet føringer om at *"Når det ikke foreligger spesielle hindringer for å ta i bruk skytjenester, og slike tjenester gir den mest hensiktsmessige og kostnadseffektive løsningen, bør en velge slike tjenester. Spesielle hindringer kan for eksempel være særlige krav til sikkerhet og sårbarhet."*

Nasjonal strategi for bruk av skytjenester angir at bruk av skytjenester kan gi bedre sikkerhet da leverandørene kan ha bedre sikkerhetskompetanse- og ressurser enn kunden. Strategien stiller krav til risikovurderinger rundt områder som har spesielle sikringsbehov, om *det er økonomiske, konkurransemessige eller andre årsaker*. Sikkerhetspolitiske konsekvenser skal også vurderes der skytjenester befinner seg utenfor EU/EØS-området. Andre lands regler for innsyn skal tas hensyn til i vurderingen.

Personopplysningsloven sier at overføring av personopplysninger bare kan skje til stater som sikrer en forsvarlig behandling av opplysningene. Landene innenfor EU/EØS-området er anerkjent som stater som sikrer at personopplysninger behandles forsvarlig, og derfor kan man overføre personopplysninger til disse statene forutsatt at personopplysningslovens øvrige vilkår er oppfylt. Det samme gjelder land som Europakommisjonen har godkjent. Personopplysninger kan også overføres til USA dersom mottakervirksomheten har sertifisert seg etter *Privacy Shield-avtalen*.

Der tverrsektorielle løsninger finnes eller planlegges som er tilpasset de sikkerhetsbehov som politiet har bør disse brukes. Dette gjelder for sikkerhetsbehov både i form av sin rolle i Totalforsvaret ved tilspissede situasjoner og i form av sin daglige rolle hvor store mengder sensitiv informasjon behandles. Noen initiativ er angitt nedenfor som brukes, eller bør vurderes brukt eller videreutviklet. En samordning og koordinering mellom initiativene bør gjennomføres av justisdepartementet.

Sikker sky

NSM har på oppdrag fra JD utredet muligheten for etablering av en statlig driftet skytjeneste med et høyt sikkerhetsnivå slik at også sentrale myndigheter med særskilte sikkerhetsbehov kan utnytte mulighetene til effektivisering som skytjenester gir. Høyt sikkerhetsnivå gjelder her både for lavgradert (BEGRENSET) og ugradert men sensitiv informasjon. Utredningen ble gjennomført i samarbeid med Difi. Arbeidet går gjennom ulike løsnings- og eierskapsmodeller, og belyser viktige sikkerhetsmessige problemstillinger knyttet til disse alternativene. En samlet anbefaling av dette arbeidet er at det etableres en "sikker sky"-løsning for BEGRENSET og SENSITIV.

Da politiet behandler store mengder sensitiv informasjon og noe gradert informasjon er det nærliggende å konkludere at der politiet ønsker å benytte seg av de fordeler bruk av skytjenester gir, må «sikker sky» benyttes.

Der politiet har behov for å ta i bruk allmenne skytjenester, skal alltid risikovurderinger gjennomføres før slike tjenester tas i bruk. Tiltak etter risikovurderinger kan være anonymisering av data, kryptering, eller unngå å ta i bruk allmenne skytjenester for det vurderte området.

Samhandling innenfor totalforsvaret – Infrastructure as a service

Prop. 151 S (2015-2016) gir politiske føringer om samarbeid mellom Forsvaret og politiet innenfor IKT-området for å *understøtte samhandlingen innenfor totalforsvaret og bidra til effektiv utnyttelse av de samlede IKT-ressursene*. I første omgang er et arbeid startet for å se på mulighetene for et samarbeid innenfor "Infrastructure as a service" mellom politiet og Forsvarets Materielltjenester (FMA). Dette arbeidet skal videreføres.

Nasjonalt BEGRENSET Nett (NBN)

NBN er en gradert plattform som er etablert for å tilby muligheter for lavgradert informasjonsutveksling mellom departementene og statlige virksomheter. Politiet skal ta i bruk NBN i tråd med oppdrag fra JD og vurdere ytterligere bruk av NBN i politiet.

7 Organisering og kompetanse

Vi skal utvikle og levere fremtidsrettede digitale løsninger til politiet og vi skal gjøre det på en annen måte enn vi tradisjonelt har gjort – politiet skal gjøre mer selv, utnytte leverandørmarkedet bedre og ta i bruk kontinuerlige leveranser basert på DevOps som leveransemodell. For å lykkes med dette må vi også se på hvordan vi organiserer IKT-funksjonen og hvilken kompetanse IKT-funksjonen og politiet generelt må ha.

7.1 Organisering av IKT-funksjonen

Organiseringen med Politidirektoratet som premissgiver for IKT-funksjonen og Politiets IKT-tjenester som politiets felles tjenesteleverandør på IKT-området videreføres. Gjennom prosjekt HSO²⁶-fase 1 ble lokale IKT-medarbeider og IKT-løsninger i politidistriktene overført til PIT. HSO-fase 2 som omfatter særorganene skal gjennomføres.

Ved overgang til en leveransemodell basert på kontinuerlig produkt-/tjenesteutvikling og DevOps er det nødvendig at POD og PIT vurderer sin organisering mhp. hva som bør være funksjonsorganisert og hva som bør være produktorganisert, for å sikre raskere digitalisering av politiet. Dette gjelder for hele verdikjeden fra digitaliseringsbehov oppstår til det er dekket. Kapittel 4.1 skisserer organisering av arbeidet for å kunne levere løsninger fortløpende. Det vil være viktig å bygge et kompetansemiljø (Center of Excellence) for utviklingsarbeid som støtter en helhetlig tilnærming til utvikling av politiet fra porteføljestyring til DevOps.

IKT-funksjonen må etablere en kapasitet som skal sørge for at politiet har en systematisk tilnærming til utnyttelse av teknologidrevet innovasjon i politiets oppgaveløsning.

For å støtte opp under og forenkle politiets bruk av intern og ekstern informasjon samt sikre etterlevelse av lover og regler, må politiet vurdere organisering av sin informasjonsforvaltning og dataanalyse. Politiet må øke sin evne til å behandle informasjon digitalt slik at arbeidsprosesser i enda større grad baseres på kunnskap om kriminaliteten og for å øke samhandling internt og eksternt.

Det må etableres en kapasitet for sikkerhetsovervåking av politiets digitale løsninger (SOC²⁷-funksjon) som sikrer evne til raskt å oppdage sikkerhetshendelser/angrep og til raskt å håndtere hendelser for å redusere/minimalisere skadeomfanget. En slik funksjon er et viktig hjelpemiddel i risikostyringen da den gir et dag-til-dag bilde av hvor sårbarhetene ligger. En slik funksjon må sees i sammenheng med politiets oppgave i etablering og drift av Justis-CERT²⁸-funksjonen for hele justissektoren. Justis- og beredskapsdepartementet har gitt ut et eget rammeverk for håndtering av IKT-hendelser. Rammeverket må legges til grunn i etableringen av SOC og Justis-CERT-funksjonen.

7.2 Kompetansebehov i fremtidig IKT-funksjon

Kompetanseområdene som er beskrevet nedenfor er de som anses som spesielt viktige for å realisere fremtidig IKT-funksjon og leveransemodell. For å lykkes med digitalisering er vi i tillegg helt avhengig av tverrfaglig samarbeid mellom disse "digitale" kompetanseområdet og dyp kompetanse på politiets arbeidsprosesser og bruk av informasjon og teknologi.

I tillegg til å beskrive kompetansebehov som er utledet fra denne strategien beskriver også rapporten *"Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende tiårene, POD 2017"* kompetansebehov som er relevante for IKT-funksjonen. Av det som er spesielt relevant for fremtidig IKT-funksjon er teknologiutviklingen, kriminalitets- og trusselutviklingen, og effektivisering.

²⁶ "Helhetlig styring og organisering av IKT i politiet"

²⁷ Security Operations Centre

²⁸ Computer Emergency Response Team

Digital kompetanse i politiet generelt

I henhold til *Meld. St. 27 Digital agenda* kjennetegnes digitalt modne virksomheter gjerne ved at de har en ledelse med høy digital kompetanse og god IKT-strategisk forståelse. Digital kompetanse og overordnet IKT-strategisk forståelse er vesentlig å ha både for ledere i politiet og for de som representerer politifaglige og administrative prosesser i Politidirektoratet, politidistrikt og særorgan.

Fremtidig leveransemodell

For å kunne implementere fremtidig leveransemodell må alle nivåer fra porteføljestyret og ned til det enkelte produktteamet ha tilførsel av kompetanse. Først og fremst må alle involverte medarbeidere få en forståelse av de grunnleggende prinsippene for leveransemodellen og hva prinsippene betyr for den enkelte og deres hverdag.

Innovasjon og tjenesteutvikling

IKT-organisasjonen skal styrke kompetanse innen innovasjon og tjenesteutvikling gjennom økt samarbeid med distrikter og særorgan.

Informasjonsforvaltning, dataanalyse og innsikt

Politiet må videreutvikle sin kompetanse på informasjonsforvaltning, dataanalyse og innsikt til bruk bl.a. i forebygging av kriminalitet, politioperativt arbeid og virksomhetsstyring.

Skytjenester og kognitive teknologier

Politiet skal styrke sin egen kompetanse på bruk av skytjenester og kognitive teknologier slik at politiet kan dra nytte av dette i sin oppgaveløsning.

Systemutvikling

Politiet skal styrke egen utviklingskapasitet der det bidrar til bedre og raskere oppfyllelse av virksomhetsstrategien og der løsninger ikke er lett tilgjengelig i leverandørmarkedet.

Bestiller- og leverandørstyringskompetanse

Politiet må selv ha styring, kontroll og i stor grad utøve IKT-funksjonen. Der det er relevant å bruke eksterne tjenesteleverandører må politiet styrke egen kompetanse og kapasitet til å drive tjeneste- og leverandørstyring. Tjenestekjøp krever gode risikovurderinger og høy bestillerkompetanse. Politiet må besitte nødvendig kompetanse til blant annet å gjennomføre selve anskaffelsen, følge opp i produksjonsfasen og gjennomføre en eventuell avvikling av kontrakten eller tjenesten.

Tjeneste- og systemintegrasjon

For å sikre en styrt, effektiv og trygg bruk av markedet må politiet bygge kompetanse på å integrere og følge opp tjenester fra eksterne leverandører i henhold til mål og prinsipper for fremtidig IKT-funksjon.

Kompetanse innenfor informasjonssikkerhet og IKT-sikkerhet

Samtidig som alle nivåer i leveransemodellen må ha digital kompetanse, er det også viktig med sikkerhetskompetanse på de ulike nivåene. Alle nivåene må kjenne til hva som ligger i begrepet risikostyring og hvilke sikkerhetsmessige rammer politiet må forholde seg til. I tillegg vil det være behov for ytterligere kompetanse innenfor de ulike nivåene:

- Politiets ledelse må ha kompetanse om sammenhengen mellom IKT-funksjonen og nivåer for risikoaksept.
- Sikkerhetsfunksjonen må ha kompetanse rundt premissgivelse og kontroll
- Behandlingsansvarlige må ha kompetanse om risikoaksept og databehandleravtaler knyttet til personopplysninger og politiregisterinformasjon
- Prosesseiere må ha kompetanse om verdivurdering og risikoaksept innenfor sine arbeidsprosesser
- IKT-funksjonen må ha kompetanse om digitale trusler og sårbarheter og hvordan de skal kunne etterleve de krav som ligger under de sikkerhetsmessige rammene. IKT-sikkerhetskompetanse må ivaretas i alle ledd og prosesser i IKT-funksjonen, både for interne og eksterne tjenesteleverandører.

8 Begrepsliste

Begrep	Beskrivelse
Applikasjon	Programvare bestående av funksjoner som fyller behovene til en IKT-tjeneste. Hver applikasjon kan være del av mer enn én IKT-tjeneste. En applikasjon kjøres på en eller flere servere eller klienter som er en del av infrastrukturen.
Arbeidsflate	Består av et standardisert operativsystem, sentrale applikasjoner, personlige innstillinger med egne applikasjoner og data og kontroller for å håndheve aksess og rettigheter. Arbeidsflaten kan aksesseres fra en offentlig stasjonær eller privat pc. Er meningslikt med brukergrensesnitt og bruker flate
Bruker	Mottaker av og kravstiller til tjenester som ytes av leverandøren. Med bruker forstår vi her sluttbrukere og/eller brukerorganisasjon. Digitaliseringsstrategien definerer tre overordnede brukergrupper: innbyggere og ansatte i virksomheter, medarbeidere, samhandlere
CERT	Computer Emergency Response Team
DevOps	Utviklingsmetodikk som forener utvikling og drift av programvare. Kommer av sammensettingen av Development og Operations, fritt oversatt til norsk, metodikk for samlet utvikling og drift
DevSecOps	Implemterer sikkerhetsprinsipper i DevOps-tilnærmingen med større fokus på hurtighet og operasjonell ytelse.
Digitale rom	Omfatter digitale elementer og innhold som enten er egenutviklet eller levert av andre. Begrepet dekker både fysiske eller logiske sammenkoblinger av informasjonssystemer.
Digitaliseres	Transformativ prosess der noe går fra å være litt digitalt til å bli mer digitalt modnet. Til eksempel kriminaliteten i det digitale rom er digital fra start og vil følge andre angrepsvektorer en analog kriminalitet.
Digitalisering	Transformativ prosess der noe gjerne går fra å være analogt til å bli digitalt ved å ta i bruk teknologi for å endre en tradisjonell prosess eller gjenstand. Fra et teknisk perspektiv gjenskaper man en fysisk prosess eller gjenstand i form av tallverdier, logikk og matematiske modeller.
Fellesløsninger	Løsninger som er til for fellesskapet og som kan benyttes når virksomhetene skal utvikle brukerrettede digitale tjenester på tvers.
Hurtige leveranser	Smidig utviklingsmetodikk for å svare på høy endringstakt og økte brukerbehov. Korte innovasjonssykluser med hurtig prosessdrevet utvikling, testing og forkasting.
IKT-funksjon	Omfatter organisatorisk de delene av politiets virksomhet som utfører arbeidsprosesser som utvikler IKT-løsninger og leverer digitale tjenester. Dette er organisatorisk nå IKT-avdelingen i POD, politidistriktene IKT-funksjon, særorganenes IKT-funksjon og Politiets IKT-tjenester. Inneholder også oppgaver, prosesser, roller og ansvar som er relatert til digitalisering av politiet.
IKT-sikkerhet	IKT-sikkerhet innebærer å være bevisst hele spekteret av digitale sårbarheter. IKT-sikkerhet omfatter både tekniske og administrative sikringstiltak og innebærer beskyttelse av både IKT-systemer og informasjonen i disse. IKT-sikkerhet handler derfor om beskyttelse av "alt" som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. (Meld. St.38)
Informasjon	<u>En</u> samling data som er strukturert/tilført mening (tolket)

Begrep	Beskrivelse
Informasjonsarkitektur	Modell eller konsept for informasjon og benytter diagram for å visualisere detaljene i sammensatte informasjonssystemer.
Informasjonsforvaltning	Informasjonsforvaltning betyr et helhetlig syn på aktiviteter, verktøy og andre tiltak for å sikre best mulig kvalitet, utnytting og sikring av informasjon i en virksomhet. Organiseringa av informasjonen skal være systematisk og henge sammen med virksomhetens arbeidsprosesser. (Difi-rapport 2013:10)
Informasjonslandskap	Visning av sammensetting av opplysninger. Kan også omtales som politiets ontologi. Informasjonslandskapet formes av faktorene bak "big data": økt informasjonsproduksjon og økt deling av informasjon samt økt variasjon på opplysninger.
Informasjonssikkerhet	Informasjonssikkerhet handler om å beskytte informasjon, informasjonsbærere og miljøet hvor informasjonen behandles, mot uønskede hendelser og handlinger. Dette innebærer at informasjon beskyttes mot uautorisert innsyn (konfidensialitet), uautorisert endring (integritet) og at den er tilgjengelig når det er behov for den (tilgjengelighet).
Infrastructure as a Service (IaaS)	Infrastruktur levert over internett av en ekstern leverandør.
Kanban	Utviklingsmetodikk som håndterer og styrer arbeidsflyt
KPI	Ytelsesindikator for å måle effektiviteter i en prosess
Leveransemodell	Gjengivelse av samspillet mellom mennesker og digitale løsninger for å oppnå ønskede gevinster.
Leveranseprosesser	Fasene som inngår i en leveranse slik at man til en hver tid vet hva man får.
Løsningsarkitektur	En beskrivelse av en selvstendig og fokusert forretningsoperasjon eller aktivitet, og hvordan IS/IT understøtter denne operasjonen. En løsningsarkitektur gjelder vanligvis for et enkelt prosjekt eller en prosjektleveranse, og bidrar til å oversette krav til en løsningsvisjon, overordnede forretningspesifikasjoner og/eller IT-systemspesifikasjoner, og en portefølje av implementeringsoppgaver. (TOGAF)
Minimumsprodukt	Minste enhet som kan leveres i produksjon som gir verdi
Multimodal	Ha eller involvere ulike aktivitets- eller hendelsesmoduser
Notoritet	At noe er etterviselig og kontrollerbart.
Opplysninger	Omfatter en sammensettinga av data, informasjon, kunnskap, regler og intelligens. Slik behandling ved bygging og beriking av opplysninger omtales også som informasjonsforvaltning.
Personvern	Retten til et privatliv og retten til å bestemme over egne personvernopplysninger. Det er ikke alle verdier en virksomhet besitter som det bare er opp til virksomheten å avgjøre om skal beskyttes. Også verdier som må sikres pga. f. eks. offentlige krav, avtaler med andre eller symbolverdier som kan være attraktive terrormål, må derfor identifiseres (NSM).
Plan-Build-Run	Driftsmodell for langsiktig implementering på tvers av teknologidomener for å øke prestasjon
Platform as a service (PaaS)	Platform as a Service referer til å tilby skytjenester hvor man kan utvikle, kjøre og styre applikasjoner uten å måtte bygge og drifte infrastruktur lokalt
Prosjekt	En midlertidig organisasjon som skal levere ett eller flere produkter i den hensikt å oppnå spesifiserte mål og gevinster.
Risikoaksept	Definerer hvilket nivå risikoaksepten ligger for ulike konsekvensområder. Eksempler på konsekvensområder kan være omdømme, liv og helse til borgere og personell, økonomi, mm.

Begrep	Beskrivelse
Risikostyring	Styring ved å utføre risikovurderinger og som skal sikre at den risikoen virksomhetens verdier utsettes for er på et akseptabelt nivå. Risikostyring av informasjonssikkerhet i virksomhetene skal være en gjentakende prosess som innebærer fastsettelse av risikoaksept, analyse av risiko, håndtering av risiko og beslutning om gjenværende risiko er akseptabel
Samhandling	Annet ord for interoperabilitet. I europeisk sammenheng (EIRA) skiller man på teknisk, semantisk, juridisk, og strategisk samhandling
Samhandlingsløsning	En løsning som kan integrere og samle flere former for samhandling. En samhandlingsløsning forbedrer forretningsprosesser ved å gjøre det mulig å samhandle effektivt uten å være fysisk på samme sted. Samhandlingsløsninger omtales også om "Collaboration" eller "Unified Communication"
Scrum	Scrum er et rammeverk laget med henblikk på å utvikle komplekse informasjonssystemer. Det brukes i hovedsak til å utvikle programvarebaserte systemer og benyttes gjerne i kombinasjon med Extreme Programming (XP), men kan i prinsippet brukes til å håndtere alle slags prosjekter av en viss kompleksitet. Teorien er basert på empirisk prosesskontroll og fordrer at man jobber inkrementelt og iterativt og at selve utviklingsjobben utføres av tverrfaglige, selvstyrte team (Wikipedia).
Skyplattform	Felles plattform i skyen bestående av flere sammensatte produkter.
Skyteknologi	Teknologi som gjør det mulig å prosessere og lagre opplysninger virtuell og derav hvor som helst (~ i skyen), kan også inkludere infrastrukturen for å flytte opplysningen til og fra lagring samt prosessering.
SLA (står KPI/SLA)	Service Level Agreement – se tjenesteavtale.
Smidig	Smidig (Agile på engelsk) er et fellesnavn på systemutviklingsmetoder som legger vekt på fleksibilitet og hyppige delleveranser samt tett kommunikasjon mellom de som utvikler systemet og de som skal bruke det.
Smidig prosjekt	Et prosjekt som følger en Plan-Build-Run-tilnærming, men som leverer smidig innen hver fase
SOC	Security Operations Center
Sourcing	Engelsk ord som brukes om den norske betydningen av forholdet mellom det man skal kjøpe inn av- og bygges selv, av løsninger og tjenester.
Sourcingstrategi	Definerer hvilke oppgaver og kompetanse innenfor drift, forvaltning og utvikling som skal ivaretas internt og hva som skal kjøpes eksternt samt hvordan det skal kjøpes.
Styring	Utførte handlinger som gjør at man ender dit man søker.
Styringsmodell	Modell som dokumenterer styringsstruktur, styringsområder med tilhørende styringsprosesser og de fullmakter som er nødvendig for helhetlig styring av politiet.
Superbruker	Rolle som har inngående kunnskap om IKT-systemet og bruker det til daglig. Bistår ved innføring av nye versjoner og oppdateringer av IKT-systemene. Gir innspill til systemforvalter ved behov for endring.
Sårbarhetsvurdering	Sårbarhet er manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning, jf. NS 5830. Sårbarhetsvurderingen skal vise eventuelle gap mellom innførte sikringstiltak og en trussel aktørs intensjon og kapasitet (NSM)
Tingenes internett	Tingenes internett (Internet of Things (IoT) på engelsk) vil si at hverdagslige gjenstander som lyspærer, døråser, biler o.l. kobles til internett

Begrep	Beskrivelse
Tjeneste	En logisk representasjon av en repeterbar forretningsaktivitet med et gitt resultat. En tjeneste er selvstendig, kan være komponert av andre tjenester, og er en "svart boks" sett fra konsumentens side. Eksempler kan være "Sjekk kundekreditt", "Hent værddata", og "Sammenstill borerapporter". (TOGAF)
Tjenesteavtale	Avtale som beskriver og kravsetter tjenester.
Tjenesteleverandør	Aktør og part som leverer tjenester.
Trusselvurdering	Vurdering av trusler beskriver det gjeldende trusselbildet for det som ønskes beskyttet, og gir en vurdering av hvordan trusselbildet kan utvikle seg. Hovedfokuset er på reelle og potensielle trussel aktørers intensjon om og kapasitet til å ramme virksomheten (NSM).
Verdivurdering	Vurdering og kartlegging av virksomhetens verdier. Formålet med vurderingen er å identifisere hvilke verdier som er de viktigste for politiets oppdrag og leveranser. Politiet skal utføre verdivurderingen på en systematisk måte ved å vurdere hvilke konsekvenser det kan få dersom verdiene skulle rammes.
Virksomhetsområde	Logisk område virksomhetsmodellen er delt inn i. Er virksomhetsområde inneholder en samling av oppgaver som naturlig hører sammen.
Virksomhetsstrategi	En plan for hvordan virksomheten skal nå sine mål

9 Figuroversikt

Figur 1: Strategiske temaer og mål for politiet.....	5
Figur 2: Sammenheng mellom strategiske temaer og informasjon	7
Figur 3: Sikkerhetsmessige rammer for politiets IKT-funksjon	9
Figur 4: Retning for digitale løsninger i politiet.....	10
Figur 5: Forventet utvikling av opplysningsmengde og dagens evne til å behandle disse.....	11
Figur 6: Sikkerhet i hele IKT-livssyklusen.....	15
Figur 7: Sikringsnivå for de ulike verdinivåene.....	15
Figur 8: Illustrasjon av fremtidig leveransemodell	17
Figur 9: Grovinndeling av IKT-løsninger	21

10 Oversikt over vedlegg

Vedlegg	Format
1. Hensikt, mål og prinsipper for fremtidig IKT-funksjon	Presentasjon
2. Fremtidig informasjonslandskap	Presentasjon
3. Fremtidig applikasjonslandskap	Dokument
4. Sikkerhet i IKT-funksjonen i politiet	Dokument
5. Bruk av leverandørmarkedet	Presentasjon
6. Tiltak for fremtidig IKT-funksjon	Presentasjon
7. Fremtidig leveransemodell	Dokument
8. Mandat for utredning av fremtidig IKT-funksjon og leveransemodell for raskere digitalisering av politiet	Dokument