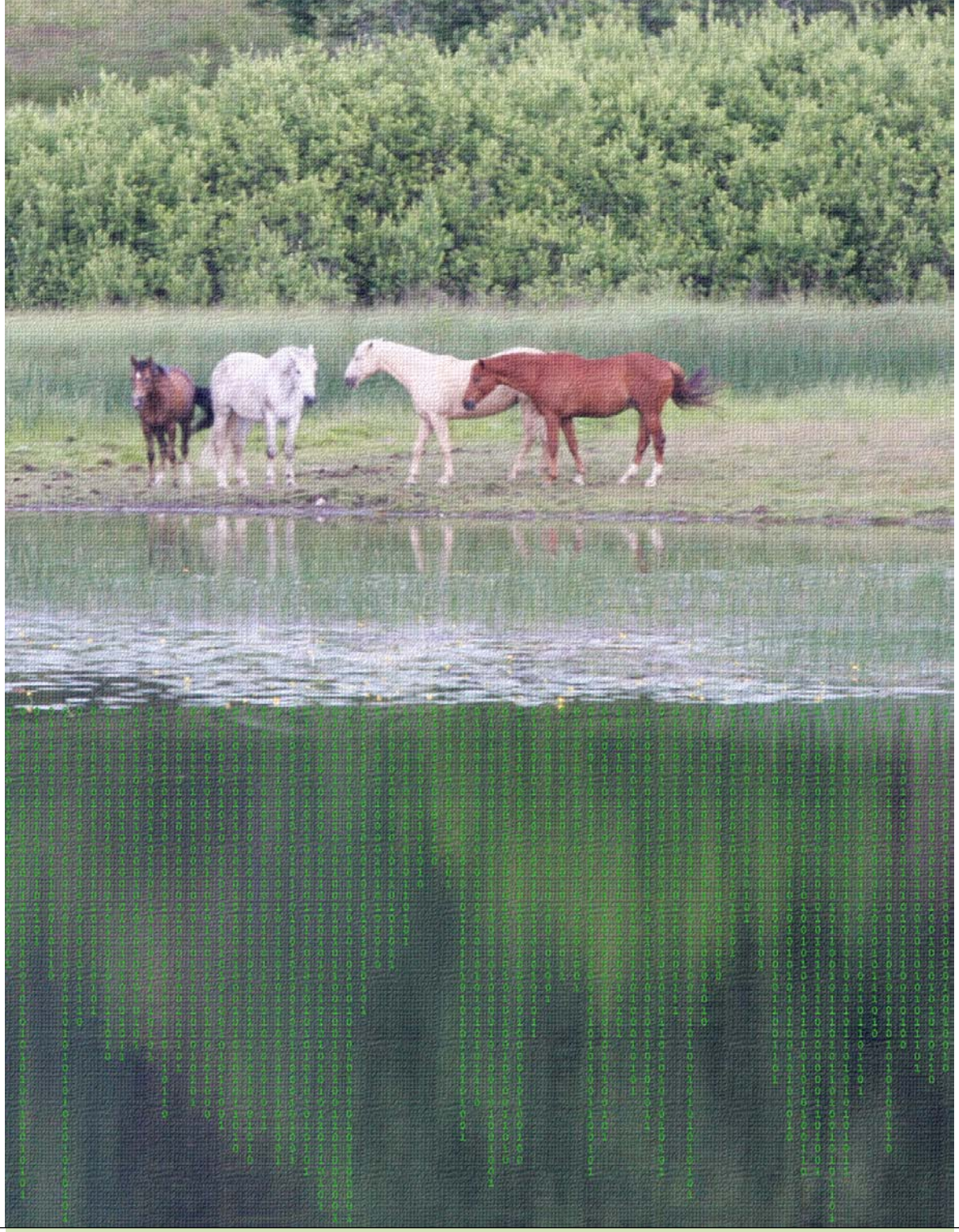

IKT-strategi 2015-2017

Statens strålevern
Norwegian Radiation Protection Authority

Forord

Strategi er en plan som beskriver hvilke virkemidler som skal benyttes for å nå et mål, mens operasjonaliseringen av strategien er taktikken – den som beskriver hvordan virkemidlene skal utføres.
Sagt på en annen måte: Den beste strategien forteller oss hva som er de riktige tingene å gjøre, mens den beste taktikken forteller oss hvordan vi best skal utføre dem.

Dette strategidokumentet omhandler hvordan bruk av IKT skal hjelpe Strålevernet til å nå sine overordnede mål. Det er derfor strukturert i forhold til disse målene og fokuserer på Strålevernets arbeidsprosesser.

I dette dokumentet vil linjeorganisasjonen derfor finne operasjonelle mål som de skal styre mot i strategiperioden.

Alle deler av strålevernets organisasjon har bidratt til dette dokumentet, enten direkte eller gjennom det grundige forarbeidet med prosesskartlegging, risikoanalyser og idédugnader.

Arbeidsgruppen har blitt ledet av Bjørn Fjeldstad, POA/IKT og har i tillegg bestått av:

Annette Andersen	ASB	Petter Arneberg	POA/IKT
Børre Knudsen	POA/IKT	Runhild Gjelsvik	OFO
Dag Robøle	POA/IKT	Scott Hiller	POA/ØKONOMI
Inger M. Nergaard	KOM	Sindre Øvergaard	ASB
Jelena Mrdakovic Popic	SBM	Synne Margrethe Egset	KOM
Lisbeth Høydahl Gundeid	POA/ØKONOMI	Terje Sætren	POA/ARKIV
Mette Nilsen	SBM	Torbjørn Gäfvert	OFO
Monica Dobbertin	SBM		

Innhold

1 Innledning

1.1 Virksomheten

Statens strålevern er et direktorat under Helse- og omsorgsdepartementet, men også med mandat og direktoratsoppgaver for Klima- og miljøverndepartementet og Utenriksdepartementet.
Statens strålevern arbeider for å redusere negative følger av stråling og utøver sitt samfunnsoppdrag bl.a. ved å føre tilsyn, forvalte regelverk, informere, gi råd og veilede, forvalte kunnskap og forske for å:

- påse riktig og forsvarlig håndtering av strålekilder
- påse riktig og forsvarlig medisinsk strålebruk
- påse forsvarlig avfallshåndtering og bidra til reduserte utslipp
- bidra til reduserte stråledoser fra radon og UV
- påse atomsikkerhet nasjonalt og bidra til atomsikkerhet internasjonalt
- sikre en forsvarlig atomberedskap med god krisehåndteringsevne

Strålevernet leder og er sekretariat for den nasjonale atomberedskapen. Strålevernet forvalter den norske normalen for stråledoseenhet.

IKT-tjenestene ved Statens strålevern skal bidra til en best mulig måloppnåelse av Strålevernets hovedmål. IKT-tjenestene er et virkemiddel i denne sammenheng og er bare til for dette.

1.2 Mål for IKT i Strålevernet

IKT-tjenestene er begrenset av interne og eksterne rammebetingelser; Dette gjelder tilgjengelige ressurser, både økonomisk og personellmessig, det gjelder samspillet og kompatibilitet med andre aktører/myndigheter – og ikke minst regelverk, som sikkerhetsloven, arkivloven, offentlighetsloven, personopplysningsloven, forvaltningsloven, geodataloven og annen særlovgivning. Videre må Statens strålevern, som en del av forvaltningen, forholde seg til den offentlige IKT-politikk – så som Strategi for IKT i offentlig sektor, regelverk for digital kommunikasjon, referansekatalogen for felles IT arkitektur, informasjonsforvaltning i offentlig sektor, digitaliseringsrundskrivet m.fl.

Dette innebærer igjen at Strålevernet skal velge IKT-løsninger som er kostnadseffektive og i tråd med direktoratets strategiske mål så vel som gitte føringer fra sentrale myndigheter, i hovedsak via Difi. Strålevernet må også sørge for å ha IKT-kompetanse og -kunnskap til å gjennomføre de faglige hovedmålene.

IKT-løsningene skal fremme kvalitet og effektivitet i arbeidet.

Målene for IKT i Strålevernet blir da:

1. **Tilgjengelighet til Strålevernets kunnskap**
   IKT-tjenestene skal legge til rette for at all kunnskap Strålevernet forvalter skal være tilgjengelig og lett gjenfinnbar helt uavhengig av hvor kunnskapen har blitt skapt og uavhengig av hvor den befinner seg. Dette gjelder for alle interessenter, interne som eksterne.
2. **Effektiv og sikker informasjonsforvaltning**
   Data skal lagres slik at det er mulig å benytte det samme datagrunnlaget til myndighets-utøvelse/tilsyn, overvåkning, beredskap og krisehåndtering, informasjonsvirksomhet og

FoU-virksomhet - uten større grad av manuelt eller annet ressurskrevende arbeid. Åpne data skal være grunnprinsippet.
Alle IKT-systemer og -tjenester skal ha en enhetlig og koordinert forvaltning gjennom hele sin livssyklus.

3. **Tilgjengelighet til ekstern informasjon**
IKT-tjenestene skal legge til rette for at elektronisk lagret informasjon fra kilder utenfor Strålevernet, slik som internasjonale tidsskrifter og web-baserte kilder og andre åpne data, er lett tilgjengelig i Strålevernets arbeidsprosesser.

4. **Enkel og sikker elektronisk samhandling med omverdenen**
IKT-tjenestene skal legge til rette for at eksterne parter skal kunne samhandle elektronisk med Strålevernet, enkelt, trygt og effektivt.

IKT strategien vil beskrive de virkemidler som skal benyttes for å sikre oppfyllelse av hvert enkelt av disse målene og vil ha følgende tre fokusområder:

- **Effektivisering**
- **eForvaltning**
- **Informasjonssikkerhet**

1.3 Fokusområder

Oppfyllelse av målene for IKT i strålevernet sikres best gjennom målrettede tiltak. Da IKT-strategien omhandler hva som skal gjøres og ikke hvordan, er det ikke naturlig at den innretter seg etter organisasjonskartet, men etter resultatene som skal oppnås. På denne måten unngås mulige begrensninger og suboptimaliseringer. Strategien blir også uavhengig av Strålevernets til enhver tid gjeldende organisering.

1.3.1 Effektivisering

Alle statlige virksomheter er pålagt å fjerne tidstyver ved å effektivisere egen drift, bidra til regelforenkling og andre forenklingstiltak i egen virksomhet og overfor innbyggere, næringsliv og offentlige virksomheter.

Kommunal og moderniseringsdepartementet har i Digitaliseringsrundskrivet blant annet pålagt alle statlige virksomheter å digitalisere sine tjenester, ta i bruk nasjonale tjenester som ID-porten, Altinn, og sikker elektronisk post, benytte felles arkitekturprinsipper, standarder og universell utforming. Videre skal offentlig informasjon gjøres tilgjengelig for videre bruk (åpne data) i samsvar med bestemmelsene i offentleglova og i henhold til NLOD lisensen.

1.3.2 eForvaltning

Difi uttaler at: *«Regjeringen har høye ambisjoner om et it-løft i hele offentlig sektor. Det skal bli mer fart og sterkere grep for økt gjennomføringskraft. Kommunikasjon på nett er nå hovedregelen når forvaltningen henvender seg til innbyggere, frivillige organisasjoner og næringslivet. Statlige virksomheter og kommuner har en viktig rolle i å etablere flere nyttige digitale tjenester som gjør hverdagen enklere for folk flest. Hensikten er å motivere enda flere til å kommunisere på nett.*

Digitalisering av offentlig forvaltning er en reform som vil berøre alle. Gjennomføring vil kreve innovasjon, endringsvilje og omstillingsevne fra både lokal og sentral forvaltning. Vi må samarbeide om å lage en robust infrastruktur med sikre og effektive tjenester. Innbyggerne og næringslivets evne og vilje

til å kommunisere digitalt er avgjørende for at reformen skal lykkes. Tjenestene må derfor utformes slik at de blir enkle å bruke for alle.

Å få gevinst ut av reformer kommer ikke av seg selv, det tar tid og ledelse er avgjørende for å lykkes.»

1.3.3 Sikkerhet, informasjonssikkerhet og personvern

Informasjonssikkerhet handler om å sikre at informasjon er tilgjengelig og at konfidensialitet og integritet er ivaretatt. Det er virksomhetens mål, dens arbeidsprosesser og regelverket som avgjør sikkerhetskravene. Flere regelverk stiller krav til sikring av informasjon. Et gjennomgående krav er at sikringen er risikobasert. Det er viktig å huske at informasjonssikkerhet også handler om å sikre tilgjengelighet. Ett av fokusområdene er å styrke informasjonssikkerheten gjennom økt bruk av styringssystem for informasjonssikkerhet.

Forskrift om sikkerhetsadministrasjon under sikkerhetsloven stiller krav til at man skal ha et slikt styringssystem for informasjonssikkerhet. Det er ingen motstridende krav i denne forskriften og ISO 27001 (internasjonal standard for informasjonssikkerhet). Gjennom et helhetlig, veldokumentert og etterlevd ISO 27001 styringssystem vil man ha tatt høyde for alle lovmessige krav og føringer. På denne måten slår man flere fluer i en smekk (kan også ta inn krav i Personopplysningsloven/-forskriften). I praksis kan man løse dette med å komplettere Statement of Applicability med regulatoriske krav.

Det er her viktig å balansere ønsket om beskyttelse og konfidensialitet opp mot offentleglovas krav om mer offentlighet, samt å huske at personvernet kun gjelder for sensitive personopplysninger. Grunnlovens § 100 gir også tydelige føringer når det gjelder åpenhet i avsnittene 3 til 5.

> *Forhaandscensur og andre forebyggende Forholdsregler kunne ikke benyttes, medmindre det er nødvendigt for at beskytte Børn og Unge imod skadelig Paavirkning fra levende Billeder. Brevcensur kan ei sættes i Værk uden i Anstalter.*
>
> *Enhver har Ret til Indsyn i Statens og Kommunernes Akter og til at følge Forhandlingerne i Retsmøder og folkevalgte Organer. Det kan i Lov fastsættes Begrænsninger i denne Ret ud fra Hensyn til Personvern og af andre tungtveiende Grunde.*
>
> *Det paaligger Statens Myndigheder at lægge Forholdene til Rette for en aaben og oplyst offentlig Samtale.*

Her pålegges myndighetene å gi allmenheten usensurert innsyn i sin virksomhet, sin saksbehandling og sine data.

2 Føringer og begrensninger

Strålevernets IKT-tjenester skal, så langt det er mulig, baseres på løsninger som ikke krever spesialtilpasning.

Dagens IKT-systemer skal bestå slik de fremstår i dag. Oppgradering, utskifting og videreutvikling av disse skal imidlertid skje på en slik måte at det muliggjør og understøtter de tiltak og virkemidler denne strategien beskriver.

Ansvaret for forvaltningen av IKT-tjenestene skal ligge der hvor behovet er og det skal ledes og samordnes av IKT-enheten. Finansiering av IKT-investeringer og -drift vil således bli mer desentralisert mens selve driften blir mer sentralisert.

Alle lover og forskrifter som kan komme til anvendelse skal etterleves, det samme skal alle offentlige pålegg, direktiv og rundskriv som berører IKT tjenestene.

3 Tiltak og virkemidler

I dette kapitlet beskrives de tiltak og virkemidler som skal implementeres innenfor planens gyldighetsperiode. De er gruppert etter fokusområde og det er angitt hvilke(t) mål de bidrar til. Rekkefølge og innbyrdes avhengigheter fremkommer i kapittel 4 på side 8 (siste side).

3.1 Effektivisering

3.1.1 Utarbeide en felles standard for Strålevernets IKT-systemer

Denne standarden[1] skal angi minimumskrav til alle nye IKT-systemer hva angår brukervennlighet og brukergrensesnitt, samt tekniske krav som sikrer at den enkelt kan brukes sammen med det vi har fra før. Også eksisterende løsninger skal søkes tilpasset til denne standarden ved oppgradering og/eller videreutvikling. [Mål 1 og 2]

3.1.2 Etablere og kommunisere IKT-relaterte roller og funksjoner

Det skal utarbeides rollebeskrivelser for alle IKT-relaterte roller og funksjoner som systemeier, superbruker, driftsansvarlig, brukerstøtte med flere (se også avsnitt 3.1.4 og 3.1.5, samt fotnote 2 og 3). [Mål 1 og 2]

3.1.3 Implementere aktiv forvaltning av alle systemer

Alle IKT-relaterte roller og funksjoner skal være besatt og tilhørende ansvar og myndighet skal være delegert. Dette omfatter også ansvar for budsjettering og disponering av tildelte budsjettmidler. [Mål 1 og 2]

3.1.4 Etablere forvaltningsregime[2] for alle Strålevernets IKT-systemer

Systemeier skal utarbeide en standardisert IT-tjenestebeskrivelse for alle fagsystemene hvor systemets tjenester til brukerne beskrives. Det skal også utarbeides en kortfattet avtale mellom systemeier og IKT-enheten som definerer tjenestenivået som leveres.

Det skal opprettes et IKT-forvaltningsforum under ledelse av sentral IKT-funksjon. Alle systemeiere skal koordinere seg med hverandre og med sentral IKT-funksjon gjennom et kvartalsvis møte i IKT-forvaltningsforum. [Mål 1 og 2]

3.1.5 Implementere superbrukere for systemer som brukes av mange

Alle fagsystemer og basis programvare som brukes av mer enn noen få brukere skal ha minst en superbruker[3]. Denne skal besitte brukerkompetanse ut over et normalnivå og ha noe ledig tid til å hjelpe

[1] Strålevernets standard for IKT-systemer finnes ikke som ett dokument i dag, så det må utarbeides og kommuniseres.

[2] Systemeier har forvaltningsansvar for sitt system. Dette innebærer budsjettering (finansiering) av systemanskaffelse, samt bestilling av drift og vedlikehold, og videreutvikling. Systemeier skal også sørge for at det finnes brukerstøtte og eventuelt superbruker(e).

[3] Superbruker er en bruker med standard tilgangsrettigheter som har en dypere kunnskap om systemet og dets bruk. Superbruker har ansvar for å sikre at systemets brukere har god kunnskap i bruk av systemet og utfører nødvendig brukerstøtte.

kolleger som står fast. Superbruker har også ansvar for at øvrige brukere innehar tilstrekkelig kompetanse og kan i den forbindelse avholde internkurs og samlinger. [Mål 1 og 2]

3.1.6 Etablere automatisk arbeidsflyt ved hjelp av IKT

Strålevernets arbeidsprosesser skal automatiseres så langt det er formålstjenlig og prosessflyten skal overvåkes. Dette skal skje med utgangspunkt i dokumenterte arbeidsprosesser, roller, instrukser og sjekklister. Formålet skal være å oppnå effektivisering og økt jobbtilfredshet, men skal også bidra til kvalitetssikring og forutsigbarhet i arbeidsprosessens leveranser. [Mål 1, 2, 3 og 4]

3.1.7 Utarbeide bruksinformasjon for de vanligste støtteprosessene

Det skal utarbeides enkle beskrivelser for hvordan å gjennomføre de vanligste administrative prosessene som reiseregninger, refusjoner, innkjøp, brukerstøtte med videre. Eventuelle koder som skal benyttes skal forklares. [Mål 2]

3.1.8 Muliggjøre innføring av elektroniske signaturer og elektroniske bilag

Der hvor våre systemer og infrastruktur ikke allerede støtter en enkel bruk av elektronisk signatur og elektroniske bilag, skal disse videreutvikles eller byttes ut slik at de ikke er til hinder for å effektivisere arbeidsprosessene. [Mål 2]

3.2 eForvaltning

3.2.1 Harmonisere dagens bruk av koder

Så godt som alle våre systemer benytter et eller flere kodeverk[4]. Noen følger nasjonale eller internasjonale standarder, andre er spesifikke for et system og atter andre har bare blitt slik de er uten særlig baktanke. Et eksempel er datoangivelser som forekommer som fritekst, med mange forskjellige skrivemåter eller som absolutt numerisk verdi. Et annet er adresser som angis som fritekst med ulik detaljeringsgrad (forkortelser, postnummer, kommune, land m.v.) eller som en absolutt geografisk referanse.

Våre systemer benytter også koder for type, art, hendelse, hjemmel, arkivnøkkel, stikkord og mye, mye mer. Alle systemer skal derfor gjennomgås og deres kodeverk dokumenteres. Deretter skal det utarbeides og implementeres en plan for hvordan disse skal harmoniseres. [Mål 1, 2, 3 og 4]

3.2.2 Web formularer erstatter dagens PDF- og manuelle skjemaer

Dagens PDF-skjemaer som er tilgjengelige på våre nettsider, enten for direkte utfylling eller for utskrift og manuell utfylling, skal erstattes av web-formularer som leverer innholdet elektronisk til de fagsystemene som skal behandle dem. Dette er en absolutt forutsetning for å automatisere våre arbeidsprosesser og for å etablere elektronisk kommunikasjon med eksterne parter. [Mål 4]

3.2.3 Kartlegging av eksterne systemer vi utveksler informasjon med

Vi mottar informasjon og data fra, og avleverer til, en mengde systemer hos eksterne samarbeidsparter. Dette kan være manuelle, papirbaserte systemer, halvautomatiske eller helautomatiske elektroniske systemer eller fullintegrerte løsninger med maskin til maskin kommunikasjon. Vi skal kartlegge og

[4] Kodeverk er en oversikt over koder med tilhørende forklaring (eksempler er postnummer som angir postkontornavn eller landskoder for bilkjennetegn eller telefonnummer).

dokumentere all denne informasjonsutvekslingen slik at vi kan forenkle og automatisere utvekslingsprosessene. [Mål 3 og 4]

3.2.4 Utarbeide lagringsstrategi for Strålevernets informasjon og data

Vi skal bare lagre informasjon (dokumenter og data) som vil kunne ha relevans og verdi på et senere tidspunkt. Da må vi være sikre på at det er lett å gjenfinne den, ikke bare i morgen, men også om 20 år. Det må derfor utarbeides en overordnet strategi som beskriver hva som skal lagres, hvor det skal lagres, i hvilket format det skal lagres, hvorledes det skal beskrives (metadata), og hvor lenge det skal lagres. [Mål 1, 2, 3 og 4]

3.2.5 Gjøre all relevant informasjon tilgjengelig i fagsystemer og prosesser

For å innføre web-basert kommunikasjon og/eller direkte informasjonsutveksling mellom systemer, er det nødvendig at alle relevante data er tilgjengelige for systemene. Det innebærer at data og informasjon som er lagret utenfor systemene må tilgjengeliggjøres for systemene enten gjennom federering (tilgang til eksterne databaser) eller ved tilpasning av systemene slik at det er mulig å importere den eksterne informasjonen for deretter å behandle den i fagsystemene.

Vi skal også sikre kvalitet og effektivitet ved å sørge for at det ikke er behov for støttedokumenter med informasjon som ikke er tilgjengelig i saksbehandlingsløsningene, fagsystemene og databasene da dette skal være tilgjengelig i disse. [Mål 1, 2, 3 og 4]

3.3 Informasjonssikkerhet

3.3.1 Utarbeide rutine for anskaffelse av IKT-systemer

Utarbeide en støtteprosess som alltid skal benyttes ved anskaffelse av IKT-systemer og –utstyr. Denne skal sikre at Strålevernets standard for IKT-systemer blir fulgt, at systemene oppfyller kravene i ISO 27 000 standarden, og at gjeldende avtaler og innkjøpsreglement blir fulgt. [Mål 1, 2 og 3]

3.3.2 Dokumentasjon av alle Strålevernets arbeidsprosesser

Dette innebærer en nøyaktig kartlegging og dokumentasjon av hva vi faktisk gjør i det daglige og hva vi er avhengig av for å få det gjort. Alle arbeidstrinn skal beskrives i forhold til hva som gjøres, hvilken rolle som utfører det, hva man trenger får å gjøre det og hva som blir resultatet. Alle beslutningspunkt skal dokumenteres og alle alternative veier gjennom prosessen beskrives. Dette er en absolutt forutsetning for å sikre at vår informasjonsforvaltning oppfyller kravene i ISO 27 000 standarden. [Mål 1, 2, 3 og 4]

3.3.3 Beskrivelse av roller og funksjoner som inngår

Alle rollene og funksjonene som nevnes i arbeidsprosessene skal beskrives i detalj, både når det gjelder hva de har ansvar for, hvilken myndighet de har og hvilken kompetanse de må inneha. Dette vil utfylle arbeidsprosessbeskrivelsene og er en forutsetning for å kunne automatisere prosessene. Det er også en forutsetning for god kvalitetsstyring og informasjonssikkerhet. [Mål 2 og 4]

3.3.4 Dokumentere behandlingsregler og sjekklister

Instrukser, behandlingsregler og sjekklister som brukes i utførelsen av arbeidstrinnene skal dokumenteres. Dersom de mangler skal de utarbeides. Forhold til lover og forskrifter skal også ivaretas her. Dette er også en forutsetning for god kvalitetsstyring og informasjonssikkerhet. Når dette arbeidet er gjort, er arbeidsprosessbeskrivelsene komplette og klare for hel eller delvis automatisering. [Mål 2 og 4]

3.3.5 Implementere automatisk lagring i fagsystemer og arbeidsprosesser

For å sikre at informasjon som lagres enkelt kan gjenfinnes er det viktig at den blir lagret korrekt og på en strukturert måte i samsvar med Strålevernets overordnede lagringsstrategi. Dette gjøres best ved å la det skje automatisk i arbeidsprosessene eller gjennom at fagsystemene håndtere det for brukeren. Dette sikrer også en god kvalitetsstyring og informasjonssikkerhet. [Mål 1, 2, 3 og 4]

3.3.6 Ta i bruk utvalgte IKT-prosesser og -funksjoner fra ITIL

ITIL[5] gir anbefalinger om hvordan IKT-prosesser og -funksjoner kan bidra til best mulig IKT-bruk, både når det gjelder effektivitet og medarbeidertilfredshet, informasjonssikkerhet og virksomhetsstyring. Dette rammeverket er svært omfattende og det er ikke hensiktsmessig å innføre det i sin helhet. For Strålevernet er det derfor hensiktsmessig å tilpasse deler av enkelte prosesser og funksjoner slik at de gir optimal støtte til organisasjonen. På den måten behøver vi ikke å finne opp hjulet selv men heller anvende beste kjente praksis. [Mål 1 og 2]

3.3.7 Implementere informasjonssikkerhet i henhold til ISO standard

Informasjonssikkerhet[6] kan ikke vektlegges for mye og det omhandler tre viktige områder innen informasjonsforvaltningen; konfidensialitet, integritet og tilgjengelighet. Vi må alltid være trygge på at vi behandler all informasjon i henhold til Sikkerhetsloven, personvernlovgivningen, Arkivloven, Forvaltningsloven, Offentleglova, geodatalovgivningen samt en mengde forskrifter og retningslinjer som omhandler vår forvaltning av informasjon. Dette oppnås best ved å implementere et forvaltningsregime for informasjon som er i henhold til ISO 27001 standarden.

En slik implementering er tidkrevende og nitid og vil derfor måtte strekke seg over flere år. Imidlertid passer den svært godt inn i arbeidet med å dokumentere og automatisere arbeidsprosessene og store synergier vil være tilstede. Det er derfor viktig å igangsette disse aktivitetene i parallell og å sørge for at det er sømløs koordinering dem imellom. [Mål 1, 2, 3 og 4]

4 Veikart

IKT-strategiens tiltak og virkemidler, deres innbyrdes avhengighet og plassering i tid fremgår av dokumentet IKT strategi 2015 – 2017 - Veikart.

Dette veikartet er ment å kunne brukes alene som et sammendrag av IKT-strategien

[5] Information Technology Infrastructure Library (ITIL) er et strukturert rammeverk for kvalitetssikring av leveranse, drift og support innen IT. ITIL går inn i organisasjonsstrukturen, og de faglige ferdigheter til en IT-organisasjon, ved å presentere et utførlig sett forvaltningsprosedyrer som en organisasjon kan benytte til å styre sine IT-operasjoner.

[6] Informasjonssikkerhet handler om å sikre konfidensialitet, integritet og tilgjengelighet på informasjon. Det er virksomhetens mål, dens arbeidsprosesser og regelverket som avgjør sikkerhetskravene. Flere regelverk stiller krav til sikring av informasjon. Et gjennomgående krav er at sikringen er risikobasert.