LINDÅS KOMMUNE

Prosjektmandat (administrativ bestilling)

Prosjektnr	Namn	Saknr
(økonomi)	**Informasjonstryggleik i Alver kommune**	*(websak)*

Prosjektfase	**Fase 1 (Forprosjekt)**

Organisering

Oppdragsgjevar

Programansvarleg i Alver kommune

Adm. styringsgruppe:

Rådmenn i Radøy, Meland og Lindås

Prosjektgruppe:

Samansetning av medlem frå Meland, Radøy og Lindås: medlem som har informasjonstryggleik som fagansvar, samt person.

Prosjektleiar: Programansvarleg peikar ut

Arbeidsgruppe: Vert oppretta ved behov

Referansegrupper:

- IKTNH
- Systemeigarar for fagsystem og kvalitetssystem
- Tenesteeigarar

Bakgrunn og forankring

Kontrollutvalet gjennomførte hausten 2017 ei forvaltningsrevisjon av informasjonstryggleik i Lindås kommune. Rapporten konkluderer med at kommunen sitt styringssystem for informasjonstryggleik ikkje er ferdigstilt, at det ikkje har vore oppdatert på lang tid og at kommunen difor ikkje har eit styringssystem som er i samsvar med krav i regelverket. Rapporten viser også til manglar knytt til:

- Dei tilsette sin kjennskap til styringssystemet, innhaldet i dette og kva deira ansvar er knytt til informasjonstryggleik
- Risikovurderingar for fagsystem
- Internkontroll (internrevisjon)
- Databehandlaravtaler

Samtaler med informasjonstryggleiks ansvarlege i Meland kommune og Radøy kommune indikerer at dei med stor sannsyn er i same situasjon og har samanfallande behov som Lindås på området. Med tanke på kommande kommunesamanslåing er det difor naturleg at dei tre kommunane gjennomfører prosjektet i fellesskap.

I tillegg trer ny personvernforordning (GDPR) i kraft i mai 2018. Denne stiller noen ytterlegare krav til informasjonstryggleik. Til dømes stiller GDPR krav til at kommunen skal ha eit personvernombod. Desse utvida krav må verte ivaretatt av prosjektet.

Hovudmål:

Hovudmålet med prosjektet er å sikre god informasjonstryggleik i Alver kommune. Dette skal me oppnå ved å sørgje for at kommunen handsamar personopplysningar i medhald av lover og forskrifter og at kommunen gjennom dette ivaretek tilgjenge, integritet og konfidensialitet for personopplysningar.

Resultatmål og delleveransar

Prosjektet vert delt inn i 2 fasar, kor leveransar i fase 1 har høgast prioritet.

Resultatmål, fase 1:

- Kommunen har eit styringssystem for informasjonstryggleik som er i tråd med regelverket.
- Kommunen etterlever nye krav til personvern som følg av ny personvernforordning (GDPR) som trer i kraft mai 2018.
- Kommunen har eit system for ei fullstendig og ajourført oversikt over kva personopplysningar kommunen behandlar
- Kommunen har oversikt over kva risikoar den er utsett for på informasjonstryggleiksområdet

Leveransar i fase 1:

- Revidere gjeldande styringssystem for informasjonstryggleik og vidareutvikle innhaldet dette slik at det er i tråd med regelverket. Styringssystemet skal vere inndelt i ei **styrande del**, ei **gjennomførande del** og ei **kontrollerande del**.
- Kartlegge konsekvensar at ny personvernforordning og utarbeide tiltaksliste for handtering av desse konsekvensane
- Gjennomføre tiltak som sikrar etterleving av krav i ny personvernforordning
- Etablere personvernombod for Lindås, Meland og Radøy kommune
- Bestille fastsetting av nivå for akseptabel risiko (Politisk bestilling)
- Bestille gjennomføring av risikoanalyser for alle fagsystem

Resultatmål, fase 2

- Kommunane har informasjonsmateriell for dei tilsette som sikrar at dei vert i stand til å ivareta sitt ansvar på ei tilfredsstillande måte
- Kommunane har formalisert og etablert beredskapsrutinar for den generelle IKT-brukarstøtta og brukarstøtta for fagsystema. Rutinane for beredskap skal ligge i overordna beredskapsplan og lenkes til fra styringssystemet for informasjonstryggleik og i ROS-analyser.
- Kommunane har formalisere og kommunisert opningstid for- og organisering av IKT-brukarstøtta.
- Kommunane har sikra at IKTNH har etablert rutinar for rapportering på etablerte SLA'er i tenesteleveringsavtaler

Leveransar i fase 2:

- Følgje opp bestillinga på gjennomføring av risikoanalyser for fagsystem og resultat frå desse (tiltaksplanar etc.)
- Etablere årshjul for informasjonstryggleik
- Planlegge og gjennomføre opplæringstiltak som bidrar til at alle tilsette i kommunen blir kjent med innhaldet i styringssystemet, kva rolle dei har og kva som er deira ansvar knytt til informasjonstryggleik
- Planleggje og gjennomføre tiltak for tryggleiksmånaden Oktober 2018

Effektmål

- Enklare å gjennomføre internkontroll
- Gir kontroll på og oversikt over personopplysningar vi handsamer
- Gir kontinuerlig forbetring av informasjonstryggleik
- Gir dokumentert etterleving av lover og forskrifter
- Gir økt bevissthet og kompetanse om ansvar og etterleving knytt til informasjonstryggleik hos dei tilsette
- Oversikt over risikobildet for informasjonstryggleik
- Formalisert ansvarsforholdet knytt til behandling av personopplysningar
- Betre informasjonstryggleik for innbyggjarar
- Politisk og administrativ leiing får betryggande kontroll på informasjonstryggleik.

Rammer

Økonomi/finansiering	*Beløp i kr*
Vert å kome attende til.	

Avgrensingar:

Alt som ikkje er eksplisitt formulert som resultatmål er utanfor omfang av dette prosjektet

Risiko (viktigaste element identifisert ved oppstart)

Manglande **prioritet** som følgje av:

- Kommunesamanslåing
- Daglig drift

Manglande **kompetanse** på:

- Rutine for gjennomføring av ROS analyser i organisasjonen
- Vurdering av behov for ROS analyse

Manglande **kapasitet**:

- Reell disponibel tid fra prosjektressursane vert redusert pga. manglande prioritet

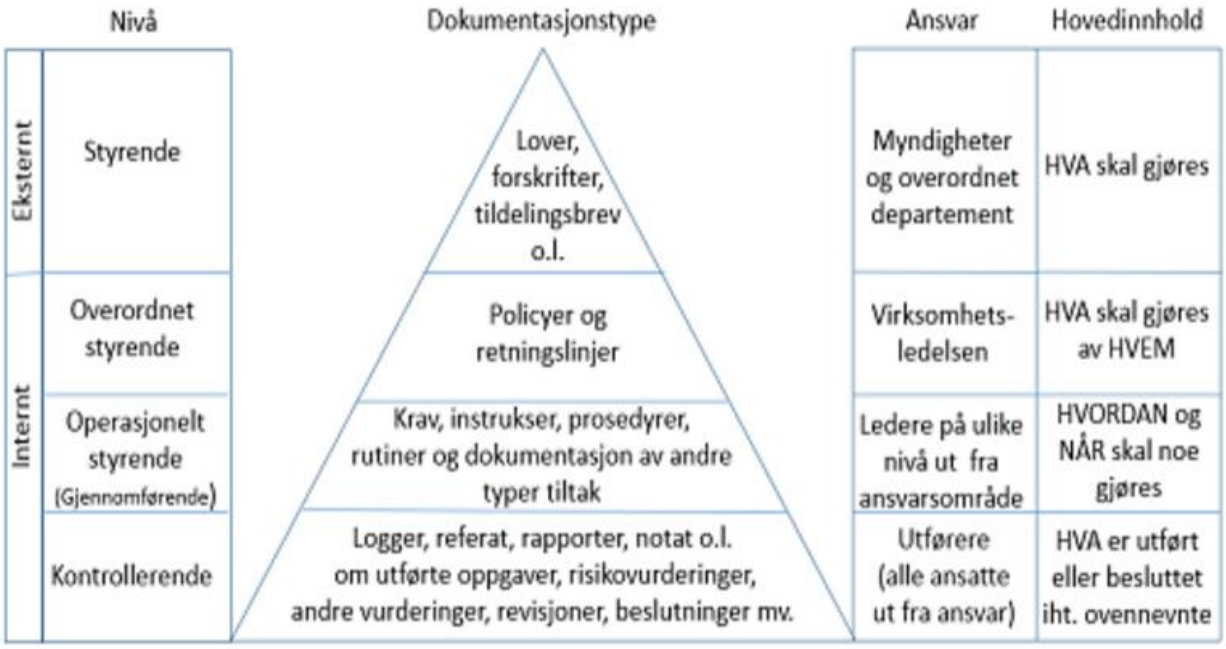
Framdrift

HMP 1: Styrande del
HMP 2: Gjennomførande del
HMP 3: Kontrollerande del
HMP 4: Revisjon
HMP 5: GDPR
HMP 6: Kompetanseutvikling

Ein tidfesta framdriftsplan vert å kome attende til.

Styringssystem og dokumentasjonskrav

Struktur for styringssystemet for informasjonstryggleik:



Lover og forskrifter i eksternt styrande del:

Direkte relevante lover og forskrifter:

- eForvaltningsforskriften § 15
- Personopplysningsloven m/forskrifter
- GDPR (ny personvernforordning – frå mai 2018)
- Helseregisterloven m/forskrifter
    - Pasientregisterforskriften
- Pasientjournalloven m/forskrifter
    - Forskrift om nasjonal kjernejournal
    - Reseptformidlerforskriften
    - Forskrift om tilgang til helseopplysningar mellom verksemder
    - Forskrift om IKT-standardar i helse- og omsorgstenesta

Andre relevante lover og forskrifter:

- Lov om helsepersonell
    - Forskrift om pasientjournal

Forskrift om internkontroll i helse- og omsorgssektoren

Krav til dokumenter i internt styrande del:

1. Overordna føringar (policy) for bruk av informasjonsteknologi
2. Sikkerheitsmål
3. Sikkerheitsstrategi
4. Nivå for akseptabel risiko
5. Sikkerheitsstrategi
6. Organisasjonskart for informasjonstryggleik
7. Oversikt over roller, aktiviteter og ansvar (ansvarsmatrise)
8. Systemoversikt og klassifisering av system (Driftshandbok)
9. IKT-sikkerheitsinstruks

Krav til dokumenter i gjennomførande del:

Krav frå Norm frå informasjonstryggleik (Norma):

- Oversikt over behandlingar av helse- og personopplysningar , samt formål og heimelgrunnlag for disse behandlingane (behandlingsoversikt)
- Oversikt over partnare, databehandlarar og leverandører
- Avtaler med partnarar, databehandlarar og leverandører
- Konfigurasjonskart over informasjonssystema og teknisk omtale av konfigurasjonen
- Prosedyre for konfigurasjonskontroll
- Omtale av løysing for å hindre øydeleggjande dataprogram
- Prosedyre for oppretting og vedlikehald av autorisasjonsregister
- Prosedyre for hendingsregistrering
- Regler for handtering av passord
- Prosedyre for sikkerheitskopiering (backup)
- Retningslinje for bruk av Norsk Helsenett (helsenettet)
- Regler for fysisk sikring av lokale og område
- Prosedyre for å hente inn informert samtykke
- Prosedyre for den registrertes innsyn i helse- og personopplysningar
- Prosedyre for ivaretaking av reservasjonsretten
- Prosedyre for å gi informasjon til den registrerte om personvernrettigheter
- Prosedyre for retting av helse- og personopplysningar
- Prosedyre for sletting av helse- og personopplysningar
- Prosedyre for bestilling, endring og sletting av brukarkontoar
- Prosedyre for handtering av utskrifter med personopplysningar (sensitive og ikkje-sensitive)
- Prosedyre for oppbevaring av dokumenter med helse- og personopplysningar
- Prosedyre for makulering av dokumenter med helse- og personopplysningar
- Prosedyre for opplæring i informasjonssikkerhet
- Prosedyrar for bruk av informasjonssystema
- Tausheitserklæring for tilsette ved tiltreding
- Prosedyre og skjema for taushets- og brukarerklæring for andre som skal ha tilgang til helse- og personopplysningar
- Prosedyre for utlevering av helse- og personopplysningar til andre
- Prosedyre for meldeplikt eller søknad om konsesjon (til Datatilsynet)

Anbefalte rutinar frå «Norma»:

- Prosedyre for forsking på helse- og personopplysningar
- Prosedyre for tilgangsstyring
- Avtale om tilgang til helseopplysningar mellom verksemder
- Prosedyre for kontroll av tilgang til helseopplysningar mellom verksemder
- Avtale om samarbeid om behandlingsretta helseregistre
- Prosedyre for utlevering av helseopplysningar til kvalitetssikring og læring
- Nødprosedyrar for manuell drift
- Prosedyre for handtering av flyttbare datalagringsmedia
- Prosedyre for bruk datanettverk
- Prosedyre for bruk av trådlaus teknologi
- Regler for sikkerhet i nettverks- og tilgangssoner
- Prosedyre for bruk av mobilt utstyr
- Krav til autentisering ved tilgang til helse- og personopplysningar via mobilt utstyr
- Prosedyrar for bruk av standard meldingar for kommunikasjon av helse- og personopplysningar
- Prosedyre for tilknyting av leverandør for fjernaksess
- Krav til IKT-leverandør ved service og vedlikehald
- Tausheitserklæring og autorisasjon for fjernaksess for intern IKT-konsulent
- Tausheitserklæring og skjema for autorisasjon av servicemedarbeidar til fjernaksess

Krav frå Datatilsynet:

- Rutinar for handtering av personopplysningar
- Rutine for vurdering av behov for risikoanalyse (ROS-analyse)
- Rutine for gjennomføring av risikovurdering (ROS-analyse)
- Sikkerheitsinstruks bruker
- Informasjonshandteringsrutine
- Sjekkliste nytilsett/tilsett slutter
- Sikkerheitsinstruks leder
- Sikkerheitsinstruks sikkerheitsansvarlig
- Driftsrutinar
- Overordna IKT beredskapsplan
- Retningsline for bruk av Internett
- Retningsline for bruk av elektronisk post
- Retningsline for utskrift og kopiering
- Retningsline for makulering av dokumenter
- Retningsline for sikkerhet og orden på eige kontor
- Retningsline for tilgangskontroll
- Retningsline for innleigd teknisk personell og handverkarar
- Retningsline for bruk av heimekontor
- Retningsline for bruk av berbar datamaskin

Andre krav til rutinar for gjennomførande del:

Dokumenter i styringssystemet skal haldas oppdatert og arkiverast frå det tidspunktet dokumentet ble erstatta med en ny gjeldande utgåve. Formålet med denne arkivering er blant anna å muliggjøre sporing og korrigering av avvik over tid.
Leiinga i verksemda skal arkivere (5 års lagring minimum fra det tidspunkt dokumentet ble tatt ut av bruk) følgjande dokumentasjon med betyding for informasjonssikkerheten:

1. Rutine for arkivering av:
    a. alle dokumenter i styringssystemet
    b. resultat frå sikkerheitsrevisjonar
    c. Resultat fra risikovurderingar
    d. Resultat fra avviksbehandling
    e. Referat fra leiinga si gjennomgang
    f. Oversikt over tildelte autorisasjonar og tilgangar til helse- og personopplysningar (autorisasjonsregister)
    g. Avtaler med partnarar, databehandlarar og leverandører til det av omsyn til helsehjelpa si karakter ikkje lenger vert antatt å bli bruk for dei
    h. Logger med betyding for sikkerheit, inkludert registrering av autorisert bruk og forsøk på uautorisert bruk av informasjonssystema
    i. Register over tilstedevering som er relevant ift kontroll mot autorisasjonsregistre og logger

Krav til dokumenter i kontrollerande del (rutinar og prosedyrar for internkontroll):

- Planer for gjennomføring av risikovurderingar
- Prosedyre for oppfølging av resultat frå desse vurderingane
- Planer for gjennomføring av sikkerheitsrevisjonar.
    - Tryggleiksrevisjon skal gjennomførast minimum årleg, men revisjonsområdet treng ikkje omfatte alle deler av informasjonstryggleiken.
- Eksempel på rullerande revisjonsplan:
- År 1 – Administrativ og organisatorisk sikkerhet (roller, rutinar, prosedyrar, kontroller)
  År 2 – Fagsystem (tryggleikskrav, risikovurdering, tilgangskontroll etc.)
  År 3 – Fysisk sikring (datarom, kontor, plassering av utstyr, låsesystem etc.)
  År 4 – Teknisk løysing (Nettverk, aksessløysingar, tryggleiksmekanismar, logiske tiltak, backup osv.)
- Prosedyre for oppfølging av resultat frå sikkerheitsrevisjonar
- Planer for leiinga si gjennomgang (minimum årleg)
- Prosedyre for leiinga si gjennomgang
- Prosedyre for oppfølging av handlingsplaner avgjort av leiinga
- Prosedyrar for avvikshandtering
- Utfylling av ny eller gjennomgang av tidligare utfylt sjekkliste for etterleving av Norma (Sjekkliste for tryggleiksrevisjon – den ligg på Normen.no, Faktaark 6b)

Endringsoversyn

Versjon	Dato	Skildring av endring	Utført av
0.1	23.05.18	Utkast til kontrollutval i Lindås	Nils-Erik Buck