RM Revisjon Midt-Norge

Informasjonssikkerhet og personvern

Sømna kommune

Forvaltningsrevisjon

FR1321

2025

FORORD

Revisjon Midt-Norge SA har gjennomført denne forvaltningsrevisjonen på oppdrag fra Sømna kommunes kontrollutvalg i perioden mai 2025 til november 2025.

Sømna kommune er deltaker i det kommunale oppgavefellesskapet Kystriket IKT, sammen med Bindal, Brønnøy, Vega og Vevelstad. Tilsvarende forvaltningsrevisjon er gjennomført i Bindal, Brønnøy og Vega i samme tidsperiode. Rapportene fra de fire forvaltningsrevisjonene har noe felles datagrunnlag fra Kystriket IKT og er derfor tilnærmet identisk på noen områder.

Vi vil takke alle som har bidratt med informasjon i prosjektet. Alle rapporter fra Revisjon Midt-Norge SA publiseres på www.revisjonmidtnorge.no.

Steinkjer / Trondheim, 17. november 2025

Anne Grete Wold
Oppdragsansvarlig revisor

Hanne Marit Ulseth Bjerkan
Prosjektmedarbeider

SAMMENDRAG

Revisjon Midt-Norge SA har gjennomført denne forvaltningsrevisjonen på oppdrag fra kontrollutvalget i Sømna kommune. Forvaltningsrevisjonen har undersøkt følgende problemstillinger:

1. Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?
2. Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

For den første problemstillingen konkluderer revisor med at Sømna kommune er godt i gang med å etablere et styringssystem for informasjonssikkerhet.

Kommunen har prioritert tid og ressurser på arbeidet, og har kommet et godt stykke på vei for å få styringssystemet på plass. Det er likevel mye som gjenstår, og det er elementer i styringssystemet som kommunen enda ikke har startet å jobbe med. Kommunen har ikke et godt nok system for risikovurderinger, og for å planlegge og gjennomføre risikoreduserende tiltak. Dette gjelder både for informasjonssikkerheten og personvernet.

For den andre problemstillingen konkluderer revisor med at Sømna kommune i stor grad har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet.

Konklusjonen bygger på at Kystriket IKT sammen med driftsleverandøren i stor grad har systemer og tiltak for å følge opp informasjonssikkerhet. Det vil alltid finnes forbedrings-områder innenfor informasjonssikkerhet fordi området er i stadig utvikling. Svakhetene som er avdekket er at beredskapsplanen for IKT ikke er oppdatert og at gjenopprettingsplanen mangler deler som kommunen har ansvar for.

Revisor ser og anerkjenner at fagområdet som er revidert er stort og komplekst, med et sammensatt regelverk. Dette krever mye av kommunen i form av kompetanse, tid- og ressursbruk og organisatoriske prosesser. Revisor konkluderer med at Sømna kommune har forstått behovet for å prioritere ressurser for å tydeliggjøre roller og ansvar og bygge kompetanse i hele organisasjonen, og at dette er arbeid det tar tid å få en bevissthet om i hele organisasjonen.

Revisor anbefaler kommunedirektøren å

- Videreutvikle styringssystemet for informasjonssikkerhet, og prioritere arbeidet med å innlemme risikovurderinger som en del av systemet.
- Gjennomføre planlagt arbeid med risikovurderinger av personvernkonsekvenser.
- Systematisere opplæringen av informasjonssikkerhet.
- Vurdere hvilke systemer og funksjoner som må prioriteres hvis datasystemer ikke er tilgjengelig og eventuelt må gjenopprettes, gjennom å utarbeide beredskapsplan for IKT.
- Bidra til å avklare ansvarsforhold mellom Sømna kommune og Kystriket IKT sitt arbeid overfor alle kommunene i Kystriket IKT.

INNHOLD

1 INNLEDNING

1.1 Bestilling

Kontrollutvalget i Sømna kommune bestilte i sak 19/2024, i møte 27.11.2024, en forvaltningsrevisjon med tema informasjonssikkerhet og personvern. Bestillingen er i henhold til plan for forvaltningsrevisjon 2024-2027.

Til grunn for bestillingen ligger også at kommunene Brønnøy, Vega, Bindal, Sømna og Vevelstad sammen har dannet det kommunale oppgavefellesskapet Kystriket IKT.

1.2 Problemstillinger

Følgende problemstillinger blir besvart i denne forvaltningsrevisjonen:

1. **Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?**

2. **Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?**

Den første problemstillingen gjelder primært ansvaret som kommunen skal ivareta innenfor egen organisasjon. Ansvaret for informasjonssikkerhet og personvern i Sømna kommune ligger til kommunedirektøren, og de funksjonene i kommunen som kommunedirektøren har delegert ansvaret til. En del av problemstillingen er å se om kommunen ivaretar personopplysninger i tråd med krav i regelverket. Personvern er i stor grad regulert av personopplysningsloven herunder personvernforordningen, og stiller omfattende krav til behandling av personopplysninger. Oppmerksomheten vil være rettet mot systemet for behandling av personopplysninger. Revisjonen vil ikke se på behandlingsgrunnlaget som ligger til grunn for behandling av hver enkelt personopplysning til hvert enkelt formål, for eksempel om det er innhentet samtykke.

Den andre problemstillingen berører i hovedsak tjenester som ivaretas gjennom Kystriket IKT. Sømna kommune har, sammen med Brønnøy, Vega, Bindal og Vevelstad dannet det kommunale oppgavefellesskapet Kystriket IKT KO, hvor Brønnøy kommune er kontorkommune. Kystriket IKT sitt formål er å samarbeide om IKT-tjenester for at den enkelte deltakerkommune skal få utført sine lovpålagte oppgaver og andre offentlige oppgaver på en kostnadseffektiv og sikker måte.

Kommunens personvernombud er tilknyttet samarbeidet Digitale Helgeland. Samarbeidet om Kystriket IKT og Digitale Helgeland er nærmere beskrevet i kapittel 2.

1.3 Om temaet

Begrepet informasjonssikkerhet er nært beslektet med begreper som digital sikkerhet, datasikkerhet, IKT-sikkerhet, IT-sikkerhet og cybersikkerhet. Ulikhetene mellom begrepene er så små at det er lite meningsfullt å skille mellom dem (Jøsang 2025).

Informasjonssikkerhet handler om å beskytte informasjonsverdier mot skade eller tap. En informasjonsverdi kan være selve informasjonen, men også ressurser for representering og behandling av informasjonen. Eksempler på informasjonsverdier er data, fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og til og med menneskelige ressurser (Jøsang 2021). Videre skriver Jøsang (2021) at det ikke er noen tydelig avgrensning av hva som kan være informasjonsverdi. Derimot er det en klar definisjon på hvordan informasjonsverdier kan skades, nemlig gjennom brudd på konfidensialitet, integritet og tilgjengelighet.

Informasjonssikkerhet omfatter:

- konfidensialitet (sikre at informasjonen ikke blir kjent for uvedkommende)
- integritet (sikre at informasjonen ikke blir endret utilsiktet av uvedkommende)
- tilgjengelighet (sikre at informasjonen er tilgjengelig ved behov).

Informasjonssikkerhet handler om hvordan en organisasjon sikrer informasjon og tjenester, og hvilke rutiner og prosesser den bruker. Sentralt her er sikkerhetsledelse og risikostyring. En god sikkerhetskultur er viktig, siden angrep kan forekomme i hele virksomheten, ikke bare på grunn av tekniske sårbarheter.

Bergsjø og Windvik (2018) bruker begrepet datasikkerhet og skriver at datasikkerhet handler ikke lengre om teknologi, men også om ledelsesoppgaver som kulturbygging, kompetanse-utvikling, verdivurdering, risikohåndtering, styring, kontroll, kriseledelse og personvern.

Personvern er dermed nært koblet til informasjonssikkerhet og personopplysninger kan ses på som en særskilt kategori informasjon som reguleres personopplysningsloven herunder personvernforordningen. Personopplysninger er opplysninger som direkte eller indirekte kan identifisere en person[1] Som eksempel på direkte opplysninger nevner datatilsynet navn, epostadresse, fødselsnummer, bilder og film hvor du kan gjenkjennes, lydopptak og

[1] Personopplysninger | Datatilsynet

biometriske data. Indirekte personopplysninger er postadresse, bilnummer, ansattnummer, brukernavn, telefon-nummer og dynamisk IP-adresse[2].

I utledningen av revisjonskriterier i vedlegg 1 blir temaet gjennomgått nærmere med utgangspunkt i lovverket og veiledere på området.

1.4 Kommunens organisering

Sømna kommune har organisert tjenestene i tre sektorer med hver sin kommunalsjef; Helse og velferd, Oppvekst og kultur og Teknisk, landbruk og næring. Kommunedirektørens administrasjon består av personal- og fellestjenester, økonomi og lønn og plan, miljø og utvikling. Disse har ansvar for støtte, veiledning og oppfølging av enhetene, samt fellesadministrative tjenester i organisasjonen. Leder for plan, miljø og utvikling har fått delegert ansvar og oppgaver for arbeidet med informasjonssikkerhet og personvern. Seniorrådgiver for informasjonssikkerhet og personvern er underlagt denne lederen.

Organisasjonskartet er tilgjengelig på kommunens hjemmeside[3].

1.5 Metode

Forvaltningsrevisjonen er gjennomført i henhold til NKRFs standard for forvaltningsrevisjon, RSK 001[4]. Revisor har vurdert egen uavhengighet overfor Sømna kommune, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3. Revisor har brukt flere metoder for å samle inn data til dette prosjektet.

Dokumentgjennomgang

Revisor har gjennomgått dokumenter som regnes som relevant for revisjonen. Sømna kommune har oversendt dokumenter knyttet til generell virksomhetsstyring og internkontroll, og dokumenter som særskilt handler om styring av informasjonssikkerhet og personvern. Dokumentene er blant annet policyer, prosedyrer, rutiner og instrukser.

Kystriket IKT er et kommunalt oppgavefellesskap, og derfor har det vært aktuelt å se på bakgrunnen og intensjonen med å opprette det kommunale oppgavefellesskapet. Slik

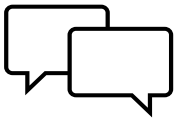
[2] Dynamisk IP-adresse er når nettstedseieren får mulighet til å identifisere brukeren bak IP-adressen ved hjelp av tilleggsinformasjon fra internettleverandøren, eller i tilfeller der nettstedeieren har mulighet til å få slik informasjon utlevert. (Kilde: Dynamiske IP-adresser | Datatilsynet)

[3] Organisasjonskart, 23.01.2025

[4] NKRF = faglig interesseorganisasjon og kompetanseorgan for kontroll og revisjon av kommunal virksomhet. RSK001

informasjon framgår av saksframlegg og vedtak i kommunestyret, hvor opprettelsen av det kommunale oppgavefellesskapet ble besluttet. Det kommunale oppgavefellesskapet Kystriket IKT har en operativ rolle i driftsavtalen med ekstern driftsleverandør. Kommunene i det kommunale oppgavefellesskapet er parter i avtalen. Driftsavtalen er en viktig kilde til data, fordi den beskriver oppgavene, spesielt tekniske tiltak for å ivareta informasjonssikkerhet, samt at den sier noe om oppgavefordelingen mellom driftsleverandøren og Kystriket IKT. Revisor har fått tilgang på de deler av driftsavtalen som er relevant i denne revisjonen. Revisor har etterspurt og fått tilsendt prosedyrer som Kystriket har.

Intervjuer



Et digitalt oppstartsmøte ble gjennomført i april 2025, med kommunedirektør, leder for plan, miljø og utvikling, seniorrådgiver for informasjonssikkerhet og personvern og IT-ansvarlig i kommunen. I juni og juli 2025 ble det gjennomført digitale intervju med følgende seks ansatte med ulike roller i og i tilknytning til kommunen:

- Leder plan, miljø og utvikling
- Seniorrådgiver informasjonssikkerhet og personvern
- Leder for personal og fellestjenester
- IT-konsulent
- Arkivleder
- Fagutviklingssykepleier pleie- og omsorg

I oktober 2025 hadde revisor et digitalt oppfølgingsintervju med seniorrådgiver for informasjonssikkerhet og personvern, blant annet for å få en demonstrasjon av systemet kommunen bruker for å føre protokoll over personopplysninger.

I mai 2025 ble det gjennomført intervju med fire representanter for Kystriket IKT. Disse intervjuene ble foretatt i rådhuset i Brønnøy kommune. Det er også gjennomført stedlige intervju med daglig leder og personvernombudet i Digitale Helgeland. Digitale Helgeland er et kommunalt oppgavefellesskap som jobber med digitalisering i kommunene i Kystriket IKT og flere andre kommuner. Digitale Helgeland har et personvernombud for alle kommunene i samarbeidet, inkludert kommunene i Kystriket IKT. Personvernombudet har en sentral rolle i arbeidet med personvern i kommunene og er derfor en viktig informant. Digitale Helgeland jobber med utvikling av digitale løsninger for kommunene, og derfor er det aktuelt å belyse hvordan de arbeider for å ivareta sikkerhet i utviklingsprosjekter.

Referater fra intervjuene er godkjent av informantene, og kun godkjente intervjudata er brukt i rapporten.

Bruk av generativ språkmodell (KI)

Revisor har brukt ChatGPT som støtte i arbeidet med å analysere dataene opp mot kriteriene. Verktøyet er primært brukt som hjelp til å systematisere datamengdene, og informasjon som kan identifisere kommunen eller enkeltpersoner er tatt bort når verktøyet blir brukt. Alle funn og vurderinger er kvalitetssikret av revisor, som fullt og helt har ansvar for innholdet.

Vurdering av metode

Revisor vurderer at metodene i forvaltningsrevisjonen er relevante for å belyse problemstillingene. En utfordring spesielt med tekniske tiltak for å ivareta informasjonssikkerheten er et stort tilfang av forkortelser og tekniske begreper, som kan påvirke begrepsvaliditeten i revisjonen. Det betyr at revisor kan ha benyttet begrep som forstås annerledes av den som blir intervjuet, og at svaret fra intervjuobjektet blir et svar på noe annet enn det det er stilt spørsmål om. Dette kan enkelt forklares som misforståelser. For å luke ut slike misforståelser i den andre problemstillingen, har leder for Kystriket IKT lest utkastet til rapport for å begrense slike feil. Det kan ikke utelukkes at kommunen har mer dokumentasjon enn det revisor har klart å framskaffe. Dette kan skyldes at revisor bruker andre begreper slik at de vi spør, ikke forstår hva vi etterspør, selv om de har de aktuelle dokumentene.

Intervjuene med de som har en funksjon i Kystriket har, sammen med skriftlige rutiner og beskrivelser, gitt informasjon om de organisatoriske og tekniske tiltakene for informasjonssikkerhet.

Oppdragsansvarlig revisor deltok ikke på intervjuene med Digitale Helgeland, da disse ble gjennomført av oppdragsansvarlig revisor for Brønnøy kommune, men har fått tilgang til referatene fra disse intervjuene i etterkant. Dette kan ha påvirket revisors vurdering og vinkling av dataene.

Vi har ikke gjort tester på egen hånd, eller leid ekstern kompetanse for å gjennomføre slike tester. Det kunne ha avdekket noen svakheter som ikke har kommet fram i intervju og skriftlig dokumentasjon. Vi har heller ikke hentet informasjon fra ansatte og ledere som daglig skal etterleve kommunens arbeid med informasjonssikkerhet og personvern, da revisjonen primært har hatt fokus på systemnivået. Vi vurderer likevel metodene gir et tilstrekkelig grunnlag for vurdering av kriterier og konklusjoner i rapporten.

1.6 Uttalelse om rapport

En foreløpig rapport ble sendt til kommunedirektøren for uttalelse 4.november 2025. Revisjon Midt-Norge SA mottok svar 12.november 2025. I tillegg ble det oversendt et dokument med noen merknader knyttet til funnene som var beskrevet. Selve uttalelsen er vedlagt rapporten (vedlegg 2).

På bakgrunn av merknadene, er det gjort noen små endringer i beskrivelser av funn. Uttalelsen fra kommunedirektøren har ikke ført til endringer i vurderinger og konklusjoner.

1.7 Begrepsforklaring

I dette kapitlet forklares noen av de mer overordnede begrepene som er brukes flere ganger i rapporten. Innenfor det datatekniske området brukes det mange forkortelser og fagbegreper som ikke er dagligdagse. De mer spesifikke begrepene forklares direkte i teksten hvor det er naturlig eller i en fotnote. Det er skilt mellom begreper innenfor informasjonssikkerhet og innenfor personvern.

1.7.1 Begreper om informasjonssikkerhet

Informasjonssikkerhet. Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet (Jøsang 2025).

Konfidensialitet. Innebærer at informasjonen ikke avsløres av uvedkommende og at kun autoriserte personer får tilgang til den (Bergsjø og Windvik 2018).

Integritet. Innebærer at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig og et resultat av autorisert og kontrollerte aktiviteter (Bergsjø og Windvik 2018).

Tilgjengelighet. Innebærer at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov (Bergsjø og Windvik 2018).

1.7.2 Begreper fra personvernforordningen

GDPR (General Data Protection Regulation). Dette er en forkortelse for **personvern-forordningen,** som er en lov som EU har vedtatt. Personvernforordningen er tatt inn i den norske lov om personopplysninger. I stedet for paragrafer henviser forordningen til artikler.

Personopplysning: enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan

identifiseres, særlig ved hjelp av en identifikator, eksempelvis et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet. (Personvernforordningen artikkel 4)

Behandling: enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, eksempelvisinnsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. (Personvernforordningen artikkel 4)

Behandlingsansvarlig: en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. (Personvernforordningen artikkel 4).

Behandlingsprotokoll: den behandlingsansvarliges representant skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Det stilles også krav til hva behandlingsprotokollen skal inneholde (Personvernforordningen artikkel 30).

Databehandler: en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige (Personvernforordningen artikkel 4).

DPIA – personvernkonsekvensvurdering: dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (Personvernforordningen artikkel 35).

2 INFORMASJONSSIKKERHET OG PERSONVERN PÅ HELGELAND

Flere kommuner på Helgeland har ulike samarbeid som berører informasjonssikkerhet og personvern. I dette kapitlet presenteres samarbeidet i de kommunale oppgavefellesskapene Kystriket IKT og Digitale Helgeland. I revisjonen henvises det til disse to organisasjonene. Kommunene i Kystriket har en felles driftsavtale for IKT og denne presenteres her.

2.1 Felles IKT-strategi

Det er utarbeidet en felles IKT-strategi for kommunene på Sør-Helgeland og omfatter Bindal, Brønnøy, Sømna, Vega og Vevelstad. Felles IKT-strategi, versjon 1.0 er for perioden 2022-2024 og en nesten identisk versjon gjelder for perioden 2024-2027. Denne strategien legger føringer for hvordan kommunene skal jobbe med drift og forvaltning av systemer og er førende for samarbeidet om IKT-tjenestene i kommunene på Sør-Helgeland.

2.2 Kystriket IKT

Kystriket IKT er et **kommunalt oppgavefellesskap**[5] med en samarbeidsavtale fra 26.11.2023. I dette kommunale oppgavefellesskapet deltar kommunene Bindal, Brønnøy, Sømna, Vega og Vevelstad med like stor andel. Kystriket IKT er ikke et eget rettssubjekt. Den enkelte kommune har ubegrenset ansvar for sin del av oppgavefellesskapets forpliktelser. Representantskapet er det øverste organet i oppgavefellesskapet, og fastsetter hvem som skal fungere som daglig leder i samråd med kontorkommunen. Brønnøy kommune er kontorkommune og oppgave-felleskapet har ingen egne ansatte. Kommunestyret i Sømna kommune vedtok samarbeidsavtalen i sak 23/108, den 14.12.2023 og i samme sak ble IKT-strategi 2024-2027 vedtatt.

Formålet med Kystriket IKT er å samarbeide om IKT-tjenester for at den enkelte deltaker skal få utført sine lovpålagte og andre offentlige oppgaver på en kostnadseffektiv og sikker måte. (Samarbeidsavtalen 2024)

Kystriket IKT har ifølge samarbeidsavtalen **ansvar for driftsplattformen** som understøtter IKT-tjenestene i deltaker-kommunene. Det innebærer blant annet:

[5] KS gjorde en vurdering for Brønnøy kommune om hvilken samarbeidsform som er mest egnet i forbindelse med innhenting av tilbud på ny driftsavtale, datert 25.10.2022.

- Bemanning av førstelinje brukerstøtte på vegne av alle deltakerkommunene
- Oppfølging av saker som meldes inn via selvbetjeningsløsningen
- Avtaleoppfølging med leverandører
- Overvåkning av tjenesteporteføljen
- Klientadministrasjon for ansattes enheter som PC og mobiltelefon.

Deltakerkommunene plikter å stille til rådighet relevant kompetanse. Menneskelige ressurser fra deltakerkommunene inngår i en samlet bemanning for IKT-samarbeidet, og skal delta i utførelsen av løpende oppgaver for samarbeidet rundt IKT-driftsavtalen. Leder for Kystriket IKT forteller at Brønnøy kommune har åtte ansatte som jobber innenfor Kystriket, Bindal har en ansatt, Sømna har en ansatt og Vega har en ansatt. De som jobber for Kystriket IKT, har ulik kompetanse. (Samarbeidsavtalen 2024)

Bindal, Brønnøy, Sømna, Vevelstad og Vega har inngått en **felles driftsavtale**. Driftsavtalen bygger på at det er opprettet en felles isolert enhet for Kystriket IKT med ulike områder for hver kommune samt et felles område for alle. kommune (Driftsavtalen 2023).

Brukerne i hver enkelt kommune benytter sitt eget domene for å logge på, og får tilgang til de ulike systemene som er tilgjengelig for den aktuelle kommunen. Det betyr at brukeren nn@somna.kommune kan logge seg på å få tilgang til Sømna kommune sine systemer. Brukeren kan også få tilgang til systemer i fellesområdet Kystriket.onmicrosoft.com samt de andre kommunene hvis det er ønskelig og mulig i forhold til blant annet personvernregelverket. Kommunespesifikke løsninger og data blir da liggende innenfor den enkelte kommune sitt område. Felles systemer i felles område må først gjennomgå en grundig analyse, med tanke å kunne skille de enkelte kommunene sine data og spesielt i forhold til personopplysninger (Driftsavtalen 2023).

2.3 Digitale Helgeland

Digitale Helgeland er et kommunalt oppgavefellesskap med 16 kommuner. Det er kommunene Alstahaug, Bindal, Brønnøy, Dønna, Grane, Hattfjelldal, Hemnes, Herøy, Leirfjord, Lurøy, Nesna, Rana, Sømna, Vefsn, Vega og Vevelstad.[6]

Representantskapet er Digitale Helgeland sitt øverste organ, som velger et styre bestående av et styremedlem og et varamedlem fra hver deltakerkommune. Kommunedirektørene velges som styremedlem. Brønnøy kommune er kontorkommune og medarbeiderne i Digitale Helgeland skal være ansatt i kontorkommunen. Digitale Helgeland leier kontorlokaler i den

[6] Organisering - Digitale Helgeland, lastet ned 18.10.2025

kommunen ansatte er lokalisert og bor. Sekretariatet består av daglig leder, to prosjektledere og personvernombudet. Sekretariatet skal ivareta følgende **funksjoner**:

- Kartlegge og identifisere muligheter for digitalisering.
- Være et teknologisk rådgivende bindeledd mellom fagområder, tjenesteproduksjon og teknologi for Helgelandskommunene.
- Bidra i utarbeidelse av behov og krav i felles digitaliseringsprosjekter for helgelandskommunene.
- Bidra med kartlegging av gevinster og utarbeidelse av gevinstrealiseringsplaner.
- Bidra med tjenestedesign og prosessforbedring i digitaliseringsprosjekter.
- Lede og/eller delta i felles digitaliseringsprosjekter.
- Være en pådriver for innføring og bruk av nasjonale felleskomponenter og fellesløsninger.
- Være en pådriver for regionalt samarbeid blant IT-miljøene i de 16 Helgelandskommunene.

Kommunene har gått sammen om å etablere et **felles personvernombud**. På nettsidene til Digitale Helgeland står det at personvern og informasjonssikkerhet er viktige i dagens digitale verden. Ved å ha et dedikert personvernombud og å samarbeide om å etablere robuste systemer og rutiner, kan de sikre at personvernet blir ivaretatt og at innbyggernes personopplysninger behandles på en trygg og pålitelig måte. Informasjonssikkerhet og personvern er et felles ansvar og krever kontinuerlig innsats og oppmerksomhet fra alle involverte parter.

Personvernombudets rolle innebærer

- Uavhengig person som er ansvarlig for å overvåke og veilede kommunene.
- Sikre at personopplysninger behandles i samsvar med gjeldende regelverk.
- Være seniorrådgiver for kommunene og gi veiledning om beste praksis.
- Gjennomføre risikovurderinger, utvikle og implementere retningslinjer og prosedyrer for å sikre personopplysninger.
- Sørge for at medarbeidere i organisasjonen kjenner til sitt ansvar innenfor personvern.
- Kontaktperson for enkeltpersoner som har spørsmål om personopplysninger.

(www.digihelgeland.no)

3 KOMMUNENS STYRINGSSYSTEM

3.1 Problemstilling

Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

For å besvare problemstillingene, har revisor utarbeidet revisjonskriterier som Sømna kommune blir målt opp mot. Revisjonskriteriene er synliggjort under hvert delkapittel. Utledningen av kriteriene finnes i vedlegg 1.

3.2 Kommunens styringssystem

3.2.1 Revisjonskriterie

Følgende kriterie er lagt til grunn:
Kommunen skal ha et ledelsessystem for informasjonssikkerhet, som angir

- *Sikkerhetsmål*
- *Sikkerhetsstrategi*
- *Sikkerhetsorganisasjon, hvor roller og ansvar framgår.*

3.2.2 Funn om ledelsessystemet

Kommunen har gitt revisor tilgang til følgende dokumenter:

Policy for informasjonssikkerhet og personvern (udatert), som beskriver målsettinger, grunnleggende prinsipper og ansvar.

Følgende mål er beskrevet, og gjelder for alt arbeid med informasjonssikkerhet og personvern:

- Kommunen skal sikre konfidensialiteten, integriteten og tilgjengeligheten i all sin informasjonsbehandling.
- Kommunen skal sikre kontinuiteten til kritiske systemer og tjenester.
- Kommunen skal sikre samsvar med gjeldende personvernlovgivning. Det innebærer å ivareta pliktene som er tillagt behandlingsansvarlig, samt å legge til rette for at de registrerte kan utøve sine rettigheter.

I dokumentet er det skrevet at disse prinsippene skal ligge til grunn for alt arbeid med informasjonssikkerhet og personvern:

- *Forankring i ledelsen.* Arbeidet skal være forankret i kommunens ledelse.

- *Helhetlig tilnærming*. Kommunen skal ha en helhetlig tilnærming til arbeidet med informasjonssikkerhet og personvern. Retningslinjer og instrukser skal samordnes slik at de fremstår som enkle og oversiktlige for ansatte. Alle ansatte skal akseptere kommunens sikkerhetsinstruks.
- *ISO-basert styringssystem.* Kommunen skal ha et styringssystem for informasjonssikkerhet og personvern som baserer seg på ISO 27001 og ISO 27701.
- *Risikostyring.* Risikovurderinger og risikohåndtering av informasjonssystemer og behandlinger skal gjennomføres i henhold til prosedyre for risikostyring.
- *Kritikalitetsvurdering*. Alle informasjonssystemer skal kritikalitetsvurderes. Krav til tilgjengelighet skal inngå som en del av kritikalitetsvurderingen.
- *Etterlevelse av lovpålagte krav.* Kommunen skal etterleve selvpålagte krav, lovkrav og regulatoriske krav.
- *Kontinuerlig forbedring.* Kommunen skal sørge for at informasjonssikkerheten og personvernet forbedres over tid, gjennom kontinuerlig forbedring av alle aktiviteter og prosesser relatert til styringssystemet.

I dokumentet er dette sagt om ansvar:

- Kommunedirektørens ledergruppe eier denne policyen.
- Roller og ansvar relatert til arbeid med informasjonssikkerhet og personvern skal være tydelig definert. Se policy for roller og ansvar for rolle- og ansvarsbeskrivelser.

Policy for roller og ansvar (udatert, men det står «04.09.24 siste utkast» i fil-tittel) som har som formål å sikre at ansvar og myndighet for roller som er relevante for informasjonssikkerheten og personvernet er tildelt og kommunisert.

I dette dokumentet beskrives sikkerhetsorganisasjonen, og følgende roller er lagt dit:

- Kommunedirektørens ledergruppe (en representant fra SLG, → leder plan, miljø og utvikling)
- Informasjonssikkerhetsansvarlig (CISO[7]) og sikkerhetsseniorrådgivere, personvernansvarlig (→ seniorrådgiver for informasjonssikkerhet innehar alle rollene)
- Sikkerhetsarkitekt (→ kommunens IT-medarbeider og Kystriket IKT)
- Opplæringsansvarlig (→ seniorrådgiver for informasjonssikkerhet i samarbeid med leder for personal og fellestjenester)
- Personvernombud (→ felles personvernombud i Digitale Helgeland)

[7] Chief Information Security Offiser

Fra høsten 2025 opplyser kommunen at også konstituert kommunedirektør/kommunalsjef oppvekst og enhetsleder pleie og omsorg tatt inn i sikkerhetsorganisasjonen.

Det er i policyen også beskrevet flere roller som er vurdert som relevant for arbeidet med informasjonssikkerhet: Informasjonssikkerhetsleder, Personvernombud, Systemeier (informasjonseier, behandlingsansvarlig), Systemforvaltere (systemansvarlig), Sikkerhetsarkitekt, Beredskapsansvarlig, Kommunedirektørens ledergruppe (SLG), Brukerstøtte, Enhetsledere og fagledere, Ledere med personalansvar, Lokal IT og Kystriket, Opplæringsansvarlig, Alle ansatte.

Det er for hver rolle listet opp hvilket ansvar og hvilke oppgaver rollen har. Seniorrådgiver informasjonssikkerhet forteller at hun for tiden har rollen som sikkerhetsansvarlig, og at kommune utprøver og vurderer fortløpende hvem som skal ha alle de forskjellige rollene som er opplistet i dokumentet roller og ansvar.

Kommunen har utarbeidet et vedlegg til Policy roller og ansvar, som beskriver rolle i organisasjonen og knytter dette til rolle og ansvar i arbeidet med informasjonssikkerhet. I vedlegget er det også beskrevet hvilken rolle som er overordnet systemeier og behandlingsansvarlig, og hvem som er systemforvaltere.

I oppstartsmøte forteller seniorrådgiver for informasjonssikkerhet og personvern at kommunen har vært medlem i KiNS[8] i flere år. De bruker verktøykasse og styringssystem som KiNS tilbyr. Det ligger maler i styringssystemet, oppdelt i styrende, gjennomførende og kontrollerende dokumenter. Disse dokumentene har kommunen integrert i kvalitetssystemet Compilo. Kommunen gjennomgår malene fortløpende i samarbeid med personvernombudet (PVO) og prioriterer hvilke maler kommunen skal bruke og tilpasse til sine.

Seniorrådgiver for informasjonssikkerhet forteller at kommunen har begynt arbeidet med de styrende dokumentene, og tar dokument for dokument og tilpasser til Sømna kommune sitt behov. Ferdige utkast presenteres i ledergruppen før de blir lagt i Compilo. Hun forteller at kommunen langt fra er i mål med arbeidet, men at de har begynt. Status på arbeidet er samlet i en **relevanserklæring**[9], der det framgår hva som er prioritert og hva som er implementert. Revisor har fått oversendt relevanserklæringen.

Seniorrådgiver forteller at sikkerhetsorganisasjonen i Sømna kommune er opprettet i september 2024 i samsvar med anbefalinger fra KiNS, og har til nå hatt tre møter. Første møte

[8] KiNS = Foreningen Kommunal Informasjonssikkerhet

[9] Relevanserklæring = en oversikt over hvilke sikkerhetstiltak (kontroller) fra ISO 27001 som er relevante for virksomheten, og hvorfor de er valgt eller eventuelt utelatt.

ble avholdt i desember 2024. På neste møte blir det sagt at relevanserklæringen skal gjennomgås på nytt. I arbeidet prioriterer de bolker av dokumenter. PVO er medlem i sikkerhetsorganisasjonen, og prioriteringene skjer i samarbeid med PVO.

3.2.3 Revisors vurdering

Kommunen er i gang med å utarbeide et styringssystem for sikkerhet som omfatter informasjonssikkerhet, som angir sikkerhetsmål, sikkerhetsstrategi og beskriver sikkerhetsorganisasjon. I systemet framgår roller og ansvar.

Sømna kommune har startet et arbeid med å etablere et styringssystem som angir mål og strategi. Revisor vurderer at kommunen har kommet godt i gang og har prioritert tid og ressurser i dette arbeidet, selv om mye arbeid fortsatt gjenstår. Sikkerhetsorganisasjonen er etablert, og roller og ansvar er definert. Praktisk oppfølging og implementering er fortsatt på et tidlig stadium, og revisor vurderer at alle dokumenter og prosesser ikke enda er godt nok implementert og gjort til kommunens egne.

3.3 Internkontroll av informasjonssikkerhet

3.3.1 Revisjonskriterier

Følgende kriterier om internkontroll er lagt til grunn:

- *Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.*
- *Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.*
- *Kommunen bør ha rutiner og prosedyrer for å redusere risiko for avvik og uønskede hendelser.*
- *Kommunen må ha et avvikssystem og ansatte må melde avvik.*
- *Kommunen bør evaluere og lære av hendelser.*

3.3.2 Funn om internkontrollen

Kommunen har gitt revisor tilgang til dokumentet «Virksomhetsstyring, ledelse, medarbeiderskap og internkontroll. Retningslinjer for ansatte i Sømna kommune. Administrativt vedtatt 19.04.23.» Generell internkontroll, risiko og vesentlighet er beskrevet i dette dokumentet. Informasjonssikkerhet og personvern er særskilt omtalt i eget kapittel, og det vises tilbake til Policy for informasjonssikkerhet og personvern, som definerer mål, rammer og føringer.

I dokumentet er det en tabell som viser kontrollaktiviteter i Sømna kommune. Blant annet er kommunedirektørens styringsdialog med kommunalsjefene beskrevet gjennom at strategisk ledergruppe går gjennom informasjonssikkerhet og personvern to ganger i året.

Kommunen har også gitt revisor tilgang til dokumentet «Prosedyre for ledelsens gjennomgang – informasjonssikkerhet og personvern». I dokumentet står det innledningsvis at ledelsen med planlagte mellomrom skal gjennomgå styringssystemet for informasjonssikkerhet og personvern, for å sikre at systemet er velegnet, tilstrekkelig og virkningsfullt. Prosedyren beskriver hvordan en slik gjennomgang skal utføres. Det første møtet i ledelsens gjennomgang er gjennomført høsten 2025. Revisor har fått tilsendt referatet, som viser elementene som er vurdert som viktige i arbeidet per nå.

Risikovurderinger

I oppstartsmøtet forteller leder for plan, miljø og utvikling, som har hovedansvar for informasjonssikkerheten, at kommunen ikke har kommet så langt med risikoanalyser. Dette blir forklart med at de har jobbet for å få på plass de overordnede styringssystemene. Seniorrådgiver for informasjonssikkerhet forteller at det ikke er gjennomført overordnede risikovurderinger knyttet til informasjonssikkerhet og personvern, men at de har planer om å arbeide med dette til høsten (2025).

Redusering av risiko er overordnet beskrevet i dokumentet «Virksomhetsstyring, ledelse medarbeiderskap og internkontroll», side 24:

> «Risiko reduseres gjennom dokumenterte kontrolltiltak, herunder nye nødvendige rutiner og prosedyrer. Kontrollaktivitetene tilpasses type risiko og formålet; er det en forebyggende kontroll, eller er det en kontroll som gjennomføres for å avdekke uønskede forhold. (…)
>
> Våre overordnede strategier for å gjennomføre kontroll er:
>
> - Sikre god informasjonsflyt om tjenestene generelt, og risiko spesielt.
> - Utnytte råd, utvalg og faste møter til å drøfte risiko og utfordringer.
> - Gjennomføre regelmessige undersøkelser blant brukere og ansatte.
> - Gjennomføre intern og ekstern opplæring av både nyansatte og andre medarbeidere.
> - Styrke bevisstheten rundt gjeldende regelverk.
> - COMPILO holdes a jour.
>
> Vi skal alltid tilstrebe å gjennomføre kontroller på laveste, egnede nivå i organisasjonen.»

Revisor har også fått oversendt følgende dokumenter:

- Reglement for elektronisk kommunikasjon – telefon og bredbånd for ansatte i Sømna kommune.
- Endringer i ovenstående retningslinjer, som inkluderer en presisering av at TikTok og Telegram ikke skal installeres på tjenesteenheter i Sømna.

Seniorrådgiver for informasjonssikkerhet sier i intervju at den største trusselen for informasjonssikkerheten i kommunen er naiviteten knyttet til hva som faktisk kan skje. Mange tenker at brudd på informasjonssikkerhet og uønskede hendelser bare skjer i store kommuner eller store virksomheter. De må få opp en forståelse av at verdensbildet har forandret seg på fem år, og at det er mer sannsynlig at slike hendelser kan skje nå. Må også forstå at kommunen er sårbar. Hun sier at man ikke kan forsikre seg mot alt, men kommunen må ha en plan dersom noe skjer og også drive forebyggende arbeid.

Kommunen har ikke utarbeidet rutiner og prosedyrer for å redusere risiko. Seniorrådgiver for informasjonssikkerhet forteller at kommunens IKT-konsulent sier at Kystriket IKT heller ikke har gjennomført ROS-analyser på området. Kommunen ønsker tettere samarbeid mellom kommunene og Kystriket, slik at man snakker samme språk om de samme temaene. KiNS-materialet blir trukket fram som en god, felles ressurs. Seniorrådgiveren sier at Kystriket IKT bør ta et tydeligere ansvar, og vurdere å utvikle felles opplegg for kommunene for blant annet kritikalitetsvurdering og ROS-analyser innenfor informasjonssikkerhet og personvern.

Avvik og uønskede hendelser

Revisor har fått oversendt kommunes rutine for å melde og behandle avvik, som gjelder for alle ansatte i Sømna kommune. Rutinen er på fem sider. Det står blant annet at ledere har lesetilgang til alle meldte avvik i egen enhet. Kommunen bruker Compilo som avvikssystem. Verneombudene har lesetilgang til HMS-avvik for eget verneområde.

Informasjonssikkerhet er ikke beskrevet som en egen avvikskategori eller hendelsestype i rutinen. Kommunen informerer revisor om at informasjonssikkerhet og personvern ikke er en hovedkategori i avvikssystemet, men ligger inne som en underkategori innenfor hovedkategoriene «organisasjon/internt» og «tjeneste/bruker». Kommunen sier at de har en gammel versjon av avvikskategoriene i Compilo, og har fått opplyst fra Compilo at avviksstrukturen skal oppdateres til en ny versjon.

Personvernombudet får ikke automatisk kopi av avvik. Avvik innen informasjonssikkerhet og personvern blir formidlet personvernet muntlig, og det blir i samarbeid med ombudet vurdert hensiktsmessige tiltak.

Leder for personal og fellestjenester opplever at avvik knyttet til informasjonssikkerhet og personvern blir meldt. Arkivtjenesten har opplevd avvik knyttet til Elements og tilgang til elevmapper i forbindelse med overganger fra barnehage til skole. Ett av avvikene handlet om at det var feil lærer som fikk tilgang til en slik mappe. På bakgrunn av dette, ble rutinene endret for å sikre oppdaterte lister knyttet til lærere som skal ha de ulike tilgangene. Oppfølgingen av avvik er lagt til de respektive enhetene og følger linja. Oppfølgingen blir ofte knyttet til gjennomgang av rutiner. Seniorrådgiver for informasjonssikkerhet blir påkoblet oppfølgingen av avvik dersom det er personopplysninger på avveie der avviket må meldes til Datatilsynet.

Seniorrådgiver for informasjonssikkerhet sier at når det gjelder å melde unormale aktiviteter og hendelser knyttet til informasjonssikkerhet og personvern, opplever hun at ansatte melder dette i linja i avvikssystemet. Ledere informerer henne, som vurderer avviket og sender melding til Datatilsynet hvis det er aktuelt. Det er meldt fire brudd i perioden 2020-2024. Disse blir imidlertid ikke lagt inn i avvikssystemet, og blir derfor ikke synlige internt. Hun sier samtidig at det sjeldent blir meldt avvik for informasjonssikkerhet og personvern i Compilo.

På sikt ønsker seniorrådgiver for informasjonssikkerhet at kommunalsjefer/enhetslederne selv melder avviket videre til Datatilsynet. Prosedyre for vurdering og melding til Datatilsynet er under utarbeidelse. Til denne prosedyren kommer på plass, ligger det en lenke i Compilo til Datatilsynet sine sider. Det er viktig at kommunen har strakstiltak og tiltak på lengre sikt, og seniorrådgiver opplever at kommunen stort sett har det.

Evaluering og læring

Ifølge seniorrådgiver for informasjonssikkerhet, blir avvik synliggjort og diskutert i Arbeidsmiljøutvalget (AMU), i strategisk ledergruppe, i enhetsledermøter og i ledelsens gjennomgang.

Det blir i intervju med leder for personal og fellestjenester sagt at ett avvik har handlet om at det var feil lærer som fikk tilgang til en elevmappe. På bakgrunn av dette, ble rutinene endret for å sikre oppdaterte lister knyttet til lærere som skal ha de ulike tilgangene.

3.3.3 Revisors vurdering

Informasjonssikkerhet inngår i kommunens internkontrollsystem, men det er fortsatt mangler i sentrale elementer i systemet.

Til grunn for revisors vurdering ligger at kommunen har etablert policyer, retningslinjer og noen kontrollaktiviteter, og ledelsen følger opp informasjonssikkerhet på overordnet nivå. Manglene

ligger særlig i manglende gjennomførte risikovurderinger, mangelfull systematisk avvikshåndtering og mangelfull dokumentasjon av gjennomførte tiltak for å redusere risiko.

Revisor legger også til grunn at det i intervjuer blir sagt at kommunen ikke har prioritert å gjennomføre risikovurderinger som grunnlag for tiltak innenfor informasjonssikkerhet. Revisor vurderer at det er viktig å komme i gang med arbeidet med risikovurderinger og læring av hendelser, da dette skal bidra til å kartlegge hvilke områder innenfor informasjonssikkerheten det er viktig å prioritere.

Sømna kommune har etablert et system for å melde og behandle avvik. Dette er blant annet dokumentert med en omfattende rutine, og et digitalt system for melding og behandling av avvik (Compilo). Det blir imidlertid i liten grad meldt avvik som handler om informasjonssikkerhet og personvern. Det er vanskelig for revisor å vurdere om dette handler om at det reelt sett oppstår lite avvik på området, eller om det er knyttet til underrapportering. Revisor legger til grunn at det finnes elementer i informasjonen som er samlet inn som tilsier at kommunen evaluerer og lærer av hendelser, men vurderer at systematikken omkring læring og evaluering kunne vært bedre.

3.4 Personopplysninger

3.4.1 Revisjonskriterier

Følgende kriterier er lagt til grunn:

- *Kommunen skal føre protokoll over hvilke personopplysninger de behandler.*
- *Kommunen må gjennomføre risikovurderinger og dokumentere vurderinger av personvernkonsekvenser.*

3.4.2 Funn om personopplysninger

Behandling av personopplysninger

I kommunens styringsdokument «Policy for roller og ansvar» står det at det er systemeier som også er behandlingsansvarlig. Systemeiers oppgaver og ansvar er ifølge dokumentet å:

- definere kravene til informasjonen som behandles i systemet, og sikre at disse kravene blir implementert.
- definere kravene til informasjonssikkerhet og personvern for selve informasjonssystemet, og sikre at disse kravene blir implementert.
- sikre at behandlingen av personopplysninger som gjennomføres i systemet skjer i samsvar med personvernregelverket.

Kommunen har oversendt et dokument som viser en oversikt over behandlingsansvarlige og systemeiere. Dette dokumentet skal fungere som et vedlegg til policy for roller og ansvar.

I oppstartsmøte blir det sagt at kommunen har behandlingsprotokoller i fagsystemet Samsvar, som blir levert av Sikri[10]. Kommunen har tatt utgangspunkt i nasjonalt protokollbibliotek, som viser en oversikt over protokoller som kommunene bør ha. Det blir sagt at kommunen gjennomgår malene fortløpende i samarbeid med personvernombudet (PVO) og prioriterer hvilke maler kommunen skal bruke og tilpasse til sine. Noen av protokollene har kommunen utarbeidet på egen hånd. I protokollene kommunen har mottatt fra leverandør, er det lagt inn forslag til løsning på omtrent halvparten av spørsmålene i hver protokoll. Disse protokollene blir gjennomgått, tilpasset Sømna kommune sitt behov og ferdigstilt.

Protokollbiblioteket inneholder totalt 210 protokoller, og kommunen sier at de har vurdert at det er behov for 176 av disse protokollene. Per i dag er 158 protokoller ferdigstilt, mens 18 er delvis ferdige.

Personvernerklæringer som gjelder innbyggere er publisert på kommunens hjemmeside, hvor de blir presentert under aktuell tjeneste. Erklæringer som gjelder ansatte, blir lagt i Compilo. I tillegg ligger det en generell personvernerklæring på kommunens hjemmeside som opplyser om innbyggerne sine rettigheter. En generell personvernerklæring for ansatte ligger i Compilo.

Revisor har i digitalt møte med seniorrådgiver for informasjonssikkerhet fått demonstrert Samsvar, og hvordan systemet er bygd opp og blir brukt. Samsvar er bygd opp etter organisasjonskartet. Det er seniorrådgiver for informasjonssikkerhet som legger inn tilgangene i Sikri og dermed har totaloversikt. Hun har gitt opplæring i flere omganger til de ansvarlige, både generelt om GDPR og forordningen, og mer praktisk rettet opplæring. Dette har vært gjort i samarbeid med enhetene, blant annet for å avklare hvem som skal ha tilgang. Enhetsleder har enhetstilgang og rettigheter til å publisere.

Seniorrådgiver for informasjonssikkerhet forteller at det i hver behandling er mellom 18 og 20 elementer som skal fylles ut. Revidering skjer fortløpende ved behov. Protokoller blir merket grønn i Samsvar når de er ferdige og godkjent, og ingen kan publiseres før de er grønne. Formålene i protokollene må være tydelige og spesifikke, og behandlingsgrunnlaget følger personvernforordningens artikkel 6 og 9. Personvernerklæringene genereres automatisk i Samsvar når behandlingsprotokollene er utarbeidet og publisert.

[1010] Sikri er et programvarehus og en leverandør av forvaltningssystemer til offentlig sektor.

Leder for personal og fellestjenester forteller at staben (fellestjenester og økonomi) møtes en gang i måneden for å se på rutiner i Compilo og behandlingsprotokoller i Samsvar.

På Sømna kommune sin nettside ligger 125 erklæringer om håndtering av personopplysninger[11]. Personvernerklæringene blir automatisk laget i Samsvar når behandlingsprotokollene er utarbeidet og publisert. Fra demonstrasjonen av programmet Samsvar, ser revisor at disse erklæringene er hentet Samsvar. Det blir i intervju sagt at personvernerklæringer som gjelder ansatte, blir gjort tilgjengelig internt i Compilo.

Funn om risikovurderinger av personvernkonsekvenser (DPIA)

I dokumentet «Policy for roller og ansvar» står det at informasjonssikkerhetsleder, sikkerhetsseniorrådgivere og personvernansvarlig (som i realiteten er en og samme person) har som oppgave å bistå i arbeidet med risikovurderinger knyttet til DPIA. PVO sin rolle er å bistå med rådgivning av risikovurderingene, og kontrollere gjennomføringen av den.

Seniorrådgiver for informasjonssikkerhet forteller i intervju at kommunen har gjennomført DPIA for noen protokoller i Samsvar, og at de skal arbeide mer med dette fra høsten 2025. Da skal de arbeide med både ROS-analyser knyttet til informasjonssikkerhet og personvern og DPIA. Kommunen har vurdert at før arbeidet med DPIA begynner, skal aktuelle ansatte ha kurs i dette for å få kompetansen som trengs for å utarbeide en DPIA.

Angående DPIA sier leder for personal og fellestjenester at hun ikke har kommet i gang med dette på hennes område. Seniorrådgiver for informasjonssikkerhet mener at de ansatte som skal gjennomføre DPIA må få en grunnopplæring i DPIA før de kan gjøre dette.

Seniorrådgiver for informasjonssikkerhet sier i intervju at personvernombudet har vært i kommunen og holdt kurs knyttet til DPIA. Kommunen bruker Samsvar til behandlingsprotokollene, der det er en ny modul for DPIA. Det er noe utfordringer med systemet knyttet til utarbeidelse av DPIA, som nå håndteres av personvernombudet. Det blir vurdert som viktig at systemet er på plass før utarbeidelsen av DPIA starter. De som skal jobbe med DPIA i kommunen skal få opplæring i dette, og målet er at alle ansatte som har en rolle i forhold til DPIA skal ha opplæring i regi av personvernombudet. Seniorrådgiver sier at hun har gjennomført opplæring ute på enhetene, men dette er ikke dokumentert.

I kommunens kompetanseplan for informasjonssikkerhet og personvern er temaet risikovurdering nevnt som tema for både ledere, sikkerhetspersonell og alle ansatte.

[11] Personvernerklæringer

Kompetanseplanen plasserer ikke ansvar for opplæring eller gir tidsangivelse for når opplæring skal skje.

3.4.3 Revisors vurdering

Kommunen fører protokoll over de fleste personopplysninger de behandler.

Sømna kommune har etablert en struktur for protokollføring, og tar utgangspunkt i nasjonalt protokollbibliotek. Roller og ansvar knyttet til behandling av personopplysninger er definert. Kommunen har tatt i bruk systemet Samsvar for føring av behandlingsprotokoller. Kommunen har vurdert hvilke protokoller de trenger, og har gjort ferdig de fleste. Kommunen har gjort personvernerklæringene tilgjengelig for innbyggerne på hjemmesiden.

Oppsummert vurderer revisor at kommunen fører protokoller og har system og ansvar på plass, men at oversikten ikke er komplett da enkelte protokoller fortsatt mangler ferdigstillelse og publisering.

Kommunen gjennomfører ikke risikovurderinger og dokumenterer ikke vurderinger av personvernkonsekvenser.

Revisor legger til grunn for sin vurdering at kommunen ikke kan dokumentere at det er gjennomført vurderinger av personvernkonsekvenser (DPIA). I intervjuer kommer det fram at kommunen skal arbeide med dette høsten 2025, og at det er vurdert at utvalgte ansatte skal få kompetanseheving knyttet til dette for arbeidet begynner. Kompetanseplanen er etter revisors vurdering uklar knyttet til dette temaet.

3.5 Opplæring

3.5.1 Revisjonskriterie

Følgende kriterie er lagt til grunn:

- *Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.*

3.5.2 Funn om opplæring

Revisor har fått oversendt kommunens kompetanseplan for informasjonssikkerhet og personvern. Slik revisor leser kompetanseplanen er den overordnet, og gir føringer for hvordan tjenestene kan utforme sine egne kompetanseplaner som dekker temaet. Kompetanseplanen beskriver hvilke temaer som bør dekkes i kompetanseplaner for ledere, for sikkerhetspersonell og personvernansvarlige og for alle ansatte. Den plasserer ikke ansvaret for opplæringer eller gir tidsangivelse for når opplæring skal skje. Seniorrådgiver for informasjonssikkerhet

informerer revisor på epost om at ansvar og tidsangivelse for opplæringen er planlagt vurdert sammen med personvernombudet i neste møte i sikkerhetsorganisasjonen.

Det er også oversendt en presentasjon som omhandler virksomhetsstyring og internkontroll, som er brukt til opplæring i utvidet ledergruppe og som gir kommunalsjefene med sine ledergrupper en bestilling på arbeidet for å følge opp internkontrollen i tjenestene.

Revisor har også fått oversendt Sikkerhetsinstruks for informasjonssikkerhet (IT-regler) for alle ansatte.

Leder for personal og fellestjenester sitter selv i sikkerhetsorganisasjonen i kommunen. Hun er opplæringsansvarlig i sikkerhetsorganisasjonen, sammen med seniorrådgiver for informasjonssikkerhet. Hun sier at de blant annet har rutiner for at nyansatte må signere sikkerhetsinstruks og taushetserklæring samtidig som arbeidsavtalen. Seniorrådgiver for informasjonssikkerhet informerer revisor om at det er enhetsleder som informerer sine ansatte om instruksen, men at kommunen planlegger seniorrådgiveren skal informere nærmere om arbeidet med informasjonssikkerhet, personvern og sikkerhetsinstruksen i personalmøter på alle enhetene før jul i 2025.

Kommunen har også en opplæringskanal for ansatte gjennom KS-læring, som er felles digital opplæring om informasjonssikkerhet for medarbeidere og ledere. Det er seks moduler som de ansatte må gjennomføre. Det er KiNS som har utviklet disse kursene. Fellestjenestene har gjennomført opplæringen, men lederen har ikke oversikt over hvor mange andre ansatte som har gjennomført modulene.

Opplæringen vil blant annet skje ved webinar i regi av KS, KS-Læring, lokale kurs i regi av personvernombudet og intern opplæring i regi av enhetsledere og seniorrådgiver for informasjonssikkerhet.

Kunstig intelligens (KI)

Leder for personal og fellestjenester forteller i intervju at kommunen i liten grad bruker kunstig intelligens (KI) og ikke har satt dette i et system. De ansatte har mulighet til å bruke Copilot. IT-medarbeider forteller at kommunen ikke har tatt KI i bruk, men at noen ansatte har tilgang til det. Han forteller også at kommunen holder på å lage en rutine for hvordan KI skal brukes. I oppfølgingsintervju og demonstrasjon av Samsvar med seniorrådgiver informasjonssikkerhet, forteller hun at kommunen er i ferd med å utvikle et system for bruk av KI i epostbehandling, og at de på grunn av dette må endre behandlingsprotokoll for innkommende epost.

3.5.3 Revisors vurdering

Kommunen sørger ikke i tilstrekkelig grad for at ansatte får opplæring i informasjonssikkerhet.

Sømna kommune er i ferd med å etablere struktur og planer som skal sikre opplæring, og kommunen tilbyr flere kanaler for opplæring, både obligatoriske kurs og tilpassede kurs for spesifikke roller. Revisor vurderer at kommunen ikke har full oversikt over gjennomført opplæring, og heller ikke kan dokumentere at alle ansatte har fått tilstrekkelig opplæring. Opplæringsplaner knyttet til temaet er i liten grad systematisert ved å plassere ansvar og tidsfrister for gjennomføring av opplæringsaktiviteter.

Revisor kan ikke se at kommunen har sørget for retningslinjer og opplæring i bruk av kunstig intelligens, selv om de ansatte har tilgang til KI-verktøy.

3.6 Konklusjon

På bakgrunn av funn og vurderinger konkluderer revisor slik på første problemstilling: **Sømna kommune er godt i gang med å etablere et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket.**

Kommunen har prioritert tid og ressurser på arbeidet, og har kommet et godt stykke på vei for å få styringssystemet på plass.

Det er likevel mye som gjenstår for at systemet blir fullverdig, og det er elementer i styringssystemet som kommunen enda ikke har startet å jobbe med. Kommunen har ikke et godt nok system for risikovurderinger, og for å planlegge og gjennomføre risikoreduserende tiltak. Dette gjelder både for informasjonssikkerheten og personvernet. Kommunen har ikke systematisert evaluering og læring av hendelser. Opplæringsplaner knyttet til temaet er også i liten grad systematisert ved å plassere ansvar og tidsfrister for gjennomføring av opplæringsaktiviteter.

4 ORGANISATORISKE OG TEKNISKE TILTAK

4.1 Problemstilling

Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Revisor har tatt utgangspunkt i Nasjonal sikkerhetsmyndighet sine grunnprinsipper for IKT-sikkerhet for å besvare problemstillingen. Grunnprinsippene er en samling med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene omhandler teknologiske og organisatoriske tiltak, og de er inndelt i fire kategorier:

- Identifisere og kartlegge
- Beskytte og opprettholde
- Oppdage
- Håndtere og gjenopprette

Spesielt tekniske tiltak og noen av de organisatoriske håndteres av Kystriket IKT. Arbeidsoppgavene i Kystriket IKT er beskrevet i kapittel 2.2. Ansatte i de fem samarbeidskommunene jobber i varierende grad for egen kommune eller mer overordnet for Kystriket IKT. Intervjudata fra Kystriket IKT er data fra intervjuer med IKT-ansatte i Brønnøy kommune og Bindal kommune.

Driftsavtalen som kommunene har med driftsleverandøren, er en sentral datakilde for tekniske og organisatoriske tiltak. Den er kort omtalt i kapittel 2.2 og 4.3.3.

Revisjonskriteriene er presentert for hvert delkapittel og revisors vurdering følger etter hvert revisjonskriterium.

4.2 Tiltak for å identifisere og kartlegge

4.2.1 Revisjonskriterier

Følgende revisjonskriterier om å identifisere og kartlegge er utledet (se også vedlegg 1):

- *Kommunen bør ha en oversikt over enheter i IKT-systemet.*
- *Kommunen bør ha en oversikt over programvare.*
- *Kommunen skal ha et system for styring av tilganger.*

4.2.2 Oversikt over enheter i IKT-systemet

Data

Nasjonal sikkerhetsmyndighet (2024) skriver at kartlegging av enheter er viktig for å få oversikt over hva som befinner seg i virksomheten. En oversikt gjør det mulig å få oversikt over sårbarheter før angriperne gjør det.

Med enheter i IKT-systemet forstås alt fra PCer, mobiltelefoner, nettbrett, skrivere, servere, lagringsmedium, skjermer og ulike enheter som er koblet til virksomhetens IKT-system, populært kalt IoT (internet of things – tingenes internett). Et eksempel på det siste er låsesystem for dører.

Driftsavtalen omtaler klienthåndtering, som er administrasjon og sikring av sluttbrukerenheter, eksempelvis PCer, mobiltelefoner og nettbrett. Klienthåndteringen er i hovedsak basert på tjenester som er inkludert i Microsoft 365. Innfasing av nye klienter gjøres med Windows autopilot i kombinasjon med Intune[12]. Dette er en prosess som i stor grad er standardisert og automatisert.

I driftsfasen håndteres klienter med

- MDM - Mobile Device Management (programvare for oppsett, administrasjon og sikring av mobilene enheter (PC, mobiltelefoner og nettbrett)
- MAM - Mobile Application Management (programvare for styring og sikring av applikasjoner på mobile enheter)

Løsninger basert på Intune sørger for å holde klienter oppdatert, sikret og kontrollert i forhold til definert regelsett (policyer).

Kystriket IKT bruker Intune for å ha oversikt over alle PC-er og status på dem, forteller en ansatt i Kystriket IKT. Brønnøy og Sømna bruker Jamf[13]. til å administrere nettbrett, mens Bindal bruker et annet verktøy. Vega har ikke nettbrett til sine brukere. For mobiltelefoner brukes MDM (Mobile Device Management) løsningen.

En av medarbeiderne i Kystriket IKT forteller at vedkommende har vært med å bygge opp regler for enheter som skal kobles til nettverket, blant annet at ingen enkeltperson skal ha ansvaret for alle enheter. Maskiner som ikke er registrert i Intune kommer ikke inn i nettverket.

En av de ansatte i Kystriket IKT har ansvar for oppgradering av utstyret i nettverket, mens det er driftsleverandøren som har ansvar for oppdateringer av software for alt av nettverksutstyr.

---

[12] Intune – en skybasert løsning for endepunktsadministrasjon. (Microsoft Intune-funksjoner | Microsoft Sikkerhet)

[13] Jamf er et system for å administrere mobile enheter.

Driftsleverandør har ansvar for alt av konfigurasjon. Kystriket IKT gir driftsleverandøren beskjed om hvilket behov det har, forteller en av de ansatte.

Når ansatte slutter er ansvaret for å få inn alt utstyret delegert til leder, sier en av de ansatte i Kystriket IKT. Hvis utstyr er borte fanges det opp. Brukertilgangen blir stengt når ansatte slutter, og det er lite en tidligere ansatt kan gjøre mot kommunens system, men det er mer verdien i selve utstyret. En av de andre i Kystriket IKT forteller at leder får informasjon om at tilgangen skal stenges 21 dager før den ansatte slutter, og den ansatte skal da levere inn PC og annet utstyr til sin leder.

I driftsavtalen framgår det at utfasingen av enheter håndteres gjennom driftsleverandørens gjenbruksordning - Grønn IT i praksis. Driftsleverandøren garanterer for sikker sletting av innholdet i PCer. På driftsleverandørens hjemmeside står det at sikker sletting betyr at de garanterer for at alt innhold og data fra tidligere er fjernet fra maskinen, og at de bruker en sertifisert løsning til arbeidet.

Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha en oversikt over enheter i IKT-systemet.

Gjennom samarbeidet i Kystriket IKT har Sømna kommune oversikt over enhetene i IKT-systemet.

Revisor vurderer at Kystriket IKT har en god oversikt over plattformen og enhetene der, sammen med driftsleverandøren.

4.2.3 Oversikt over programvare

Data

Nasjonal sikkerhetsmyndighet (2024) skriver at kartlegging av programvare er viktig for å få oversikt over hva som befinner seg i virksomheten, både det som er installert av IT-avdelingen og uautorisert programvare. Det gjør det mulig å få oversikt over sårbarheter før angriperne gjør det.

Programvare omfatter firmware[14], operativsystemer og applikasjoner. Driftsavtalen legger opp til å bruke Intune for å sikre at kun godkjent programvare blir installert. Løsninger basert på Intune sørger for å holde klienter oppdatert, sikret og kontrollert i forhold til definert regelsett. Her sikres også at godkjente applikasjoner blir installert/avinstallert automatisk basert på

[14] Firmware kan enkelt beskrives som programvare for at maskinvare skal fungere.

kommunenes ønsker og standarder. Gjennom driftsleverandøren har Kystriket IKT Microsoft Enterprise og samme type Microsoft lisens, men ulike entrepriseversjoner..

Det framgår av flere intervjuer at Intune benyttes for å ha oversikt over programvare, og nesten all programvare styres i Intune. Ansatte kan ikke laste ned og installere programvare selv. Det er kun administratorbruker til PC som får installere apper, og den rettigheten er det få som har. Kystriket IKT har oversikt over rettighetene i Microsoft Azure, noe som er viktig å ha oversikt over. Det meste av programvare er skyløsninger og det er bare en håndfull applikasjoner[15] som er installert hos noen få ansatte. Når det gjelder skyløsninger som er tilgjengelig på nett, uten at applikasjonen lastes ned, kan ansatte bruke disse.

En av de ansatte forteller at Kystriket IKT ser hvilke applikasjoner som tas i bruk i alle kommuner. Det fortelles at en kommune i Kystriket IKT har strammet inn hvilke applikasjoner som brukes, og noen er blokkert. Kystriket IKT kan ikke styre alle nettsider, og medarbeideren tror ikke det er et stort problem at det brukes annen programvare. Den ansatte henviser til at sektorlederne har ansvar for oppfølging og behandlinger av data som skjer i applikasjonene.

I et av intervjuene fortelles det at de har en oversikt over applikasjoner i Asset Management. Asset Management er en modul i Pureservice, som er Kystriket IKT sin løsning for servicedesk for brukerne. Kystriket IKT er avhengig av at kommunene selv registrerer sine applikasjoner her. Kystriket IKT har i varierende grad systemdokumentasjon for applikasjonene og mye avhenger av driftsleverandørene som har satt opp systemene. Kystriket IKT kan se koblingen mellom programvare, brukere og utstyr. Dette er viktig for å finne feil som meldes inn til servicedesken.

Underveis i arbeidet med å få kommunens systemer over på en felles plattform, har Kystriket IKT hatt en oversikt over applikasjoner i et regneark, men dette er ikke et godkjent format ettersom det må oppdateres manuelt. Driftsleverandøren har oversikt over programvare som driftsleverandøren har ansvar for, forteller en av de ansatte. Vedkommende er involvert i arbeidet med å få bedre oversikt over programvare.

Daglig leder i Digitale Helgeland forteller at det er behov for å følge kommunene tettere ved implementering av nye løsninger og sikre at gamle avtaler avsluttes i tide. Kommunene har ulik størrelse og modenhet, noe som må tas i betraktning når de vurderer innsats og oppfølging.

[15] Revisor antar at dette er fagapplikasjoner som få bruker og som ikke finnes som skybaserte løsninger.

Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha en oversikt over programvare.

Gjennom samarbeidet i Kystriket IKT har kommunen en oversikt programvare som brukes.

Revisor finner at kommunen har oversikt over programvare som må installeres for å fungere. Mer og mer programvare er skybasert, og kan brukes uten å bli installert lokalt. I Kystriket IKT brukes Intune for å registrere programvare som brukes. I tillegg blir programvare registrert i Asset Management, som grunnlag for brukerstøtte. Ut over dette er det mulig for ansatte å bruke skybaserte applikasjoner uten noen form for godkjenning. Kystriket IKT viser til at sektorlederne i kommunene må følge opp dette. Utfordringene her er hva som lagres av data i slik programvare, jfr. kapittel 3.4.

4.2.4 Tilgangsstyring

Data

Nasjonal sikkerhetsmyndighet (2024) skriver at kartlegging av brukere og tilganger er viktig for kartlegging av sikkerhet og for at angripere har begrensede muligheter hvis de først får tilgang til en konto.

I driftsavtalen går det fram at det er en streng kontroll med tilgangen til systemer og data. Først må brukerne defineres med relevante og bestemte roller og tillatelser, eksempelvis gjennom AD (Active Directory)[16]. Deretter blir brukerne satt opp etter mer detaljerte beskrivelser.

I driftsavtalen beskrives en løsning med identitets- og tilgangsstyring (IDM – Identity Management) basert på en løsning i Microsoft. Denne løsningen kan lese data fra regnskaps-programmet og legge inn og ta ut brukere i AD og Azure AD[17]. Basen med brukere finnes da i regnskapsprogrammet.

I intervjuene med ansatte i Kystriket IKT fortelles det om den tekniske løsningen med tilgangsstyring. Kystriket IKT har tatt i bruk eAdm[18], som synkroniseres videre til Azure og AD. AD er primærkatalogen for interne tjenester og alle brukere har konto her. Azure er neste nivå og interne fagsystemer krever at bruker er registrert både i AD og Azure.

---

[16] AD - Active Directory er en lokal tjeneste I et driftsmiljø, som brukes til å autentisere og autorisere brukere og enheter i et nettverk, forteller leder i Kystriket IKT.

[17] Azure AD – har skiftet navn til **Entra ID** – er en skybasert identitetstjeneste som autentiserer brukere for Microsoft 365, Azure og andre skyapplikasjoner, forteller daglig leder i Kystriket IKT.

[18] eAdm – Enterprise Identity and Access Management. Et system for å automatisere identitets- og tilgangsstyring. (eADM Integrasjoner | Identum)

Det er en avveining mellom kostnader og nytte om alle fagsystemer integreres med AD. Fagsystemer må være integrert mot AD for å kunne styres derfra. Ofte tilbyr leverandørene dette, men det er mer et spørsmål om kostnaden med å få det integrert. Compilo er eksempel på et system som er lønnsomt å få integrert med AD. En av de ansatte forteller at noen applikasjoner ikke kan kobles via AD. Da må brukerne informeres om at enhver ansatt skal ha egen bruker og at det ikke benyttes fellesbrukere.

Fra høsten 2024 er tilgangssystemet integrert med lønnssystemet. eAdm er rollebasert, automatisert og knyttet til ansettelse. På klientnivå (eksempelvis PC) styrer det hvilke applikasjoner og nett ansatte har tilgang til, gjennom tilgangen de har fått i rollen sin. En av de ansatte forteller at systemet skal håndtere skifte av stilling internt så fremt leder melder inn endring til personal. Personal gjør endringer i stilling i sitt system og deretter registreres det i Agresso. Da synkroniseres det videre til eAdm som sørger for riktige tilganger.

Alle fagsystemer krever at det er en bruker som er koblet til nettverket for at de kan logge seg inn. Når en ansatt skal ha tilgang, må Kystriket IKT først åpne opp for fagsystemet til brukeren (snarvei), mens systemadministrator i kommunen må lage tilgang i systemet til brukeren. Noen fagsystemer har både provisjonering og autentisering av brukerkontoer via Entra. Det betyr at brukerkontoene opprettes, endres og slettes automatisk, og at innlogging skjer med Entra som identitetsleverandør. eAdm kan sende en melding til systemadministrator om å lage en tilgang. Kystriket IKT gjør løsningen tilgjengelig og systemadministrator har rettighet til å gi tilgang.

I et av intervjuene kommer det fram at det tidligere har vært utfordringer med tilgangsstyringen. Ledere sier ifra når ansatte skal begynne, men ikke når de slutter. Det har ført til utfordringer med å deaktivere kontorer, og kommunene har betalt for lisenser som ikke brukes. Flere ansatte forteller at når en ansatt nå er ute av rollen, mister vedkommende tilgangen. Med eAdm er det mindre behov for å gjennomgå og fjerne tilganger, og Kystriket IKT forutsetter at lederne melder fra når noen slutter. Dette håndteres gjennom lønns- og personalprogrammet, og det er laget rutiner for dette. Kystriket IKT opplever stadig færre tilfeller av at ansatte får feil tilgang. Kystriket IKT gjennomgår tilganger som ikke er automatisert, men det er ikke fast eller regelmessig. Det er også gjennomganger av lisenser, men dette er ikke fullt ut automatisert. Leder for Kystriket IKT forteller at lisenser i Microsoft er knyttet til rollestyring og Kystriket IKT har detaljstyring på disse lisensene på grunn av kostnaden med dem.

En av de ansatte forteller at det er knyttet risiko til at det er mange systemadministratorer som skal følge opp tilganger. Selv om tilgangsstyringen har blitt mer automatisert, er det ingen garanti for at alt er i orden. Derfor må tilgangene gjennomgås. Kystriket IKT begynner å få rutiner på det, og skal høsten 2025 vurdere anskaffelse av et system til hjelp i revisjon av

tilganger. En revisjon må gjøres årlig og enkelte systemer bør gjennomgås oftere. I gjennomgangen må det sees på brukere og hvilke roller de har.

For ansatte som er tilknyttet Kystriket IKT er også tilgangen rollestyrt, og alle har ikke de samme tilgangene. Administratorer og systemansvarlige har utvida rettigheter. Det er to-tre superbrukere per program. Superbrukere arbeider mer med support inn i selve programmene.

Driftsleverandøren har omkring ti tilganger og alle har personlige brukere. Driftsleverandøren har tilgang til servere og kan også ha tilgang til databaser. Drifts-leverandøren har tilgang til driften av programmene, men kan ikke bruke selve programmene.

Det kan åpnes tilganger for andre eksterne ved behov, og da settes det en tidsbegrensning på tilgangen. Eksterne må logge inn hver fjerde time og reautentisere seg. Det er en helt annen kontroll i dag enn for noen år siden, forteller daglig leder i Kystriket IKT.

Flerfaktor brukes hvor det er mulig, fortelles det i intervjuene. Det er noen systemer som ikke støtter flerfaktor, og da kan det være slik at programmet kun kan brukes på kommunal PC på kontoret. Tilgangen til systemet er bare åpen for pålogging i Norden. Ved annet behov må tilgang bestilles særskilt, og med avgrensa område og periode.

Det fortelles i intervju med medarbeidere i Kystriket IKT at det er en felles passordpolicy med visse krav og multifaktor i tillegg. Kystriket IKT har fulgt nye krav fra Helse- og KommuneCert[19] om langt passord i stedet for jevnlige bytter av passord. Endring av passord må gjøres med bank-ID. Dette er en løsning som Kystriket IKT har utviklet sammen med driftsleverandøren og bygger på prinsippet om en person – en bruker.

Elevene i skolen har ikke hatt flerfaktorautentisering, sier en av de ansatte i Kystriket IKT. Tradisjonell flerfaktor er avhengig av smarttelefon, og dette er noe ikke alle elevene har. Kystriket IKT ser derfor på alternative løsninger for ekstra sikkerhet ved innlogging for elever.

Revisors vurdering

Revisjonskriteriet sier at kommunen skal ha et system for styring av tilganger.

Gjennom samarbeidet i Kystriket IKT har kommunen et system for styring av tilganger.

Revisor finnet at tilgangsstyringen er automatisert gjennom rolletildeling og koblet til lønns- og personalsystemet. Det er fortsatt programmer som ikke støttes av en slik løsning og krever jevnlige gjennomganger for å rydde i tilganger. Kystriket IKT er i ferd med å få på plass rutiner

[19] Helse- og KommuneCert er et cybersikkerhetssenter for både helse- og kommunesektoren i Norge. (Helse- og KommuneCERT - Norsk helsenett)

for slike gjennomganger, noe revisor mener er viktig både i forhold til informasjonssikkerhet og for ikke å betale for lisenser som ikke brukes.

Kystriket IKT har også en bevisst holdning til eksterne brukeres tilgang til plattform og systemer, gjennom at tilgangen er behovsprøvd og det legges inn tidsbegrensning.

Gjennom Kystriket IKT har kommunen tatt i bruk flerfaktor der dette er mulig, og følger nye krav til bruk av passord.

4.3 Tiltak for å beskytte og opprettholde

4.3.1 Revisjonskriterier

Følgende revisjonskriterier om å beskytte og opprettholde er utledet (se også vedlegg 1):

- *Kommunen bør ivareta sikkerhet i anskaffelses- og utviklingsprosesser.*
- *Kommunen bør ta ansvar for sikkerheten ved tjenesteutsetting.*
- *Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.*
- *Kommunen bør ha sentral styring med sikkerhetsoppdateringer.*
- *Kommunen må ha en plan for sikkerhetskopiering og ta sikkerhetskopier.*

4.3.2 Sikkerhet i anskaffelses- og utviklingsprosesser

Data

Nasjonal sikkerhetsmyndighet (2024) skriver at målet med prinsippet om å ivareta sikkerhet i anskaffelses- og utviklingsprosesser er at sikkerhet er en integrert del av prosessene for anskaffelse og utvikling. For virksomheten handler dette om å minimere risiko for at nye IKT-produkter og IKT-tjenester fører til sårbarheter i konfigurasjon og arkitektur av IKT-systemet.

De kommunale oppgavefellesskapene Kystriket IKT og Digitale Helgeland har en rolle i arbeidet med anskaffelses- og utviklingsprosesser. Begge oppgavefellesskapene er nærmere omtalt i kapittel 2.

I strategien for Kystriket IKT beskrives en utvikling i retning av et tettere integrert samarbeid, først med felles teknisk drift av noen fagsystemer, og videre til fullstendig felles programvare-plattform, fagsystemer, virksomhetsportal og utnyttelse av felles IKT-faglig kompetanse. Denne utviklingen krever også at arbeidsprosesser synkroniseres på tvers av kommunene. (Kystriket IKT, udatert) Flere og flere anskaffelser for kommunene skjer i fellesskap i Kystriket IKT, forteller en av de ansatte.

Utviklingsarbeidet i kommunene skjer gjennom Digitale Helgeland[20]. Digitale Helgeland har et mandat om å styrke digitaliseringen i regionen. Daglig leder i Digitale Helgeland forteller at informasjonssikkerhet anses som en grunnleggende forutsetning i alt utviklingsarbeid. I den nye strategien til Digitale Helgeland er dette tydelig forankret, og selv om det er et felles anliggende ligger det endelige ansvaret hos kommunene. Et av prinsippene for prioritering av prosjekter og løsning av oppgaver er innebygd personvern og informasjonssikkerhet.

I strategien til Digitale Helgeland står det at i de tilfellene kommunene skal skifte sine systemer, bør det gjøres med tanke på at flest mulig kommuner deltar i utskiftingen. I strategien står det også at de vil øke kompetansen rundt offentlige anskaffelser og herunder utarbeide en egen anskaffelsesstrategi som vil være et godt verktøy for å kunne sette langsiktige mål for anskaffelsene som skjer i regi av Digitale Helgeland. Det kommunale oppgavefellesskapet ønsker å jobbe for at kommunene går sammen om anskaffelser som omhandler teknologi og digitale løsninger, slik at de ikke risikerer å anskaffe flere ulike systemer til samme formål. Felles skyplattform er også et av innsatsområdene i strategien. (Digitale Helgeland, udatert)

Digitale Helgeland jobber med ulike prosjekter, spesielt innenfor e-helse. Eksempel på prosjekter er felles anskaffelse av pasientjournalsystem, velferdsteknologisk plattform, digital hjemmeoppfølging, Altinn-baserte fellestjenester, utvikling av automatiske løsninger for dokumenthåndtering og arkiv samt bruk av kunstig intelligens innenfor postmottak. I noen av utviklingsprosjektene deltar Kystriket IKT. I de tilfellene hvor det utvikles skjema i Altinn er Kystriket IKT trygge på at sikkerheten ivaretas, forteller en av de ansatte. Kystriket IKT deltar i utviklingsprosjektet om digitalt arkiv og her får Kystriket IKT en aktiv rolle når løsningen skal tas i bruk som en Altinn-løsning.

En av medarbeiderne i Kystriket IKT forteller at målet er at system og programmer skal være mest mulig like i kommunene. Det tar tid, men inntrykket er at alle kommunene etterlever dette. Så langt er det ikke byttet ut så mange fagapplikasjoner, men lederne i kommunene får gradvis en forståelse for at Kystriket IKT skal konsulteres før anskaffelsen gjøres. På noen fagområder i kommunene er det etablert fagnettverk på tvers av kommunene i Kystriket IKT. Ansatte i kommunene oppfordres til å melde seg inn i fagnettverkene for å sjekke om kommunene har de samme behovene for digitale hjelpemidler.

Kystriket IKT forholder seg til anskaffelseslovverket og anskaffelser skjer i hovedsak gjennom Kystriket IKT, forteller daglig leder. Det kan være noen unntak, eksempelvis skjermer og skrivere på perifere lokasjoner. Anskaffelse av fagapplikasjoner går gjennom Kystriket IKT og

[20] Digitale Helgeland er et kommunalt oppgavefellesskap som omfatter hele Helgeland og det vurderes forløpende utvidelser.

det gjennomføres risikovurdering av personvernkonsekvenser (DPIA) og databehandleravtaler skal være på plass. En av de ansatte opplever at Kystriket IKT involveres i slike anskaffelser i tide. En annen mener at Kystriket IKT ikke kan involveres tidlig nok, men at det har blitt veldig mye bedre. Når det skal gjøres en anskaffelse må de tenke hele kommunen eller alle kommunene i Kystriket IKT. Kommunene må også tenkte alternativt på om data kan hentes fra andre steder og unngå silotenking.

En av de ansatte forteller at hovedjobben for Kystriket IKT først har vært å få på plass en felles driftsplattform for kommunene, slik at kommunene etter hvert kan ha lik programvare. I dette arbeidet fungerer Kystriket IKT mer som en veileder og kan påvirke litt, men det er tjenestene i de ulike kommunene som må samarbeide om å få lik programvare. Dette er et ønske både fra kommunedirektørene og politikerne, mener den ansatte. At det er felles systemer i kommunene, gir driftsmessige fordeler og de kan hjelpe hverandre på tvers av kommunene. Det er enklere å følge opp ett system som ivaretar samme behov, enn flere.

Revisors vurdering

Revisjonskriteriet sier at kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.

Revisor vurderer at kommunen gjennom samarbeidet i Kystriket IKT og Digitale Helgeland i stor grad ivaretar sikkerheten i anskaffelses- og utviklingsprosesser.

For at Kystriket IKT skal ha muligheten til å ivareta sikkerheten i anskaffelses- og utviklingsprosesser er det viktig at de involveres i starten, slik at det ikke velges løsninger hvor det er utfordrende å ivareta en tilfredsstillende sikkerhet. Revisor finner at Kystriket IKT i stor grad involveres tidlig nok i prosessene. Tanken med at kommunene i Kystriket IKT benytter de samme systemer og applikasjoner gjør det enklere for Kystriket IKT å drifte løsningene. I tillegg er det slik at jo flere systemer og applikasjoner som benyttes, jo større er potensialet for at det finnes sårbarheter som kan utnyttes. En utfordring kan være gratis skybaserte applikasjoner som ikke må gjennomgå en anskaffelsesprosess før de tas i bruk.

Digitale Helgeland jobber med digitale utviklingsprosjekter for flere kommuner enn de som inngår i Kystriket IKT. Digitale Helgeland er opptatt av informasjonssikkerhet og Kystriket IKT involveres i noen av utviklingsprosjektene. Det betyr at det finnes gode rammer for at sikkerheten ivaretas i utviklingsarbeidet.

4.3.3 Sikkerhet ved tjenesteutsetting

Data

Gjennom Kystriket IKT har kommunene inngått en driftsavtale med en ekstern driftsleverandør. I utformingen av kravspesifikasjonen[21] til driftsavtalen hadde kommunene bistand fra en ekstern konsulent, forteller daglig leder i Kystriket IKT. Alle som er tilknyttet Kystriket IKT i dag har vært involvert i den gjeldende driftsavtalen, og flere av de ansatte jobbet under den forrige driftsavtalen.

Avtalens varighet er tre år og fornyes automatisk for ett år. Et av tildelingskriteriene i kravspesifikasjonen er at det spesielt skal legges vekt på løsningens arkitektur, skyløsning, sikkerhet og robusthet, som en del av kvalitet på tjenesten. På generelt grunnlag er sikkerhet alltid en del av kravspesifikasjonen i anskaffelser, ikke minst i anskaffelsen av driftsavtalen, forteller daglig leder i Kystriket IKT.

Driftsleverandøren benytter selv et ITIL-basert[22] kvalitetssystem og benytter underleverandører med ISO27001/27002/27017-sertifisering. Leverandøren har en sikkerhetshåndbok basert på maler utarbeidet av Norsk Senter for informasjonssikring (NorSIS), med tilhørende sikkerhets-instrukser rettet mot ansatte, leder, sikkerhetsansvarlig og eksterne brukere. Leverandørens styringssystem for informasjonssikkerhet omfatter risikoanalyse og -håndtering, personvern-konsekvensvurderinger (DPIA) og prosesser og rutiner for hendelseshåndtering.

Ifølge driftsavtalen skal leverandøren iverksette forholdsmessige tiltak for å ivareta krav til informasjonssikkerhet i forbindelse med gjennomføring av tjenesten. Dette er nærmere presisert som forholdsmessige tiltak for å ivareta konfidensialitet av kundens data, sikre at data ikke kommer på avveie, tiltak mot utilsiktet endring og sletting av data, samt tiltak mot angrep av virus og annen skadevoldende programvare. Leverandøren plikter å holde kundens data adskilt fra andre, gjennom nødvendige tekniske tiltak, for å redusere faren for skade på data og innsyn i data. Dette omfatter også begrenset tilgang for ansatte hos leverandøren og andre som ikke har behov for informasjonen. Leverandøren skal påse at leverandører av tredjepartsleveranser foretar nødvendig sikring av kundens data.

Leverandøren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av personopplysninger. Leverandøren skal dokumentere at informasjons-systemet og sikkerhetstiltakene er tilfredsstillende. (Driftsavtalen 2023)

[21] Kravspesifikasjonen er et bilag til driftsavtalen.

[22] ITIL er en forkortelse for Informasjon Teknologi Infrastruktur Bibliotek. Det er et rammeverk for administrering og forbedring av support og tjenesteleveranser. (What Is IT Infrastructure Library (ITIL)? | IBM)

Driftsavtalen regulerer også leverandørens bruk av underleverandører. Det omfatter at kunden må gi tillatelse hvis personopplysninger overlates til andre for lagring, bearbeidelse og sletting. Leverandøren skal også sørge for at eventuelle underleverandører påtar seg tilsvarende forpliktelser som i avtalens punkt 6.2. Avtalens punkt 6.2 handler om kundens plikter om tilrettelegging.

Personopplysninger skal ikke overføres til land utenom EØS-området uten at det er dokumentert at overføringsgrunnlaget er oppfylt. Det er en plikt til å inngå databehandleravtale hvis oppdraget omfatter behandling av personopplysninger. (Driftsavtalen 2023) Hvis leverandøren skal behandle personopplysninger, skal leverandøren beskrive hvordan tilfredsstillende behandling av personopplysninger skal oppnås og gjennomføres, eksempelvis krav til innebygget personvern. Det bør vurderes å gjøre en personvernkonsekvensvurdering (DPIA) for driftsplattformen, noe som leverandøren kan bistå med. (Vedlegg til driftsavtalen, 2023)

Driftsavtalen har bestemmelser om at nye versjoner av programvaren som benyttes for å levere driftstjenesten følger leverandørens alminnelige oppgraderingsløp.

Leverandøren skal månedlig rapportere om driftstjenesten, herunder faktisk oppnådd tjenestenivå, uønskede hendelser og problemer. Det er egne krav til måling av tjenestenivået. Det holdes driftsmøter med driftsleverandøren og Kystriket IKT på Teams månedlig. Leverandøren er ansvarlig for å rapportere månedlig på tjenestenivå, avvik i tjenestenivå og refusjoner (basert på nedetider) som er oppnådd for de ulike tjenestene. Rapportmalen inneholder også et punkt om hendelser og avvik, samt forslag til endringer i infrastruktur. Daglig leder i Kystriket IKT bekrefter at det er regelmessige møter hver andre uke og daglig leder har i tillegg møter med driftsansvarlig hos leverandøren.

Det er opprettet en driftshåndbok mellom Kystriket IKT og driftsleverandøren. Den ivaretar bestemmelsene i driftsavtalen om en samhandlingsplan og en driftsspesifikasjon. Samhandlingsplanen omfatter rutiner og prosedyrer for endringshåndtering og prosedyrer for å håndtere uønskede hendelser. Driftsspesifikasjonen er en beskrivelse av driftstjenesten som leveres.

Daglig leder opplever at driftsavtalen er god og fungerer godt, men det alltid kan dukke opp noe. En av de andre i Kystriket IKT som var involvert i anskaffelsen forteller at de har fått det som var intensjonen og leverandøren har levert. De møter også forståelse hos leverandøren for endringer som de ønsker underveis.

Kystriket IKT hadde mer behov for bistand fra driftsleverandøren i startfasen, men det vil bli mindre behov for det når Kystriket IKT blir kjent med leveransen, forteller daglig leder.

Grenseflaten mellom driftsleverandør og Kystriket IKT er tydelig. En av de andre i Kystriket IKT utdyper at det har vært behov for å presisere grenseflatene mellom Kystriket IKT og leverandøren. Kystriket IKT er en kunde som har sagt at de skal gjøre mye selv og leverandøren har måttet tenke annerledes. Kystriket IKT ønsket en plattform hvor de selv kunne administrere rettighetsstyring og ha god innsikt i det som skjer. Eksempelvis ved utrulling av programvare er driftsleverandøren støttepersoner. Ved anskaffelse av nye systemer er driftsleverandøren med. Nytt nettverk må Kystriket IKT ta gjennom leverandøren, men Kystriket IKT er utførere. Denne arbeidsfordelingen var ny og annerledes for leverandøren.

I intervjuene fortelles det om ulike møter mellom Kystriket IKT og driftsleverandøren:

- Månedlige driftsmøter med leverandøren hvor daglig leder og driftsleder i Kystriket IKT deltar sammen med SAM (Service Account Manager), KAM (Key Account Manager) og TAM (Technical Account Manager) fra leverandøren.
- Møter om servicedesk en gang i måneden mellom SAM (Service Account Manager) hos leverandør, Incident manager (Kystriket IKT) og driftsleder (Kystriket IKT). Tidligere var det hver fjortende dag, men det er mindre saker nå. Incident manager har ansvaret for å følge opp henvendelser som Kystriket IKT sender til driftsleverandøren. Det utgjør et par saker i uka.
- Månedlige CAB (Change Advisory Board) møter. Formålet med et CAB-møte: Vurdere og godkjenne foreslåtte endringer i IT-miljøet før de implementeres. Sikre at endringer ikke skaper uønskede konsekvenser for drift, sikkerhet eller tjenester. Prioritere endringer basert på risiko, kostnad og forretningsverdi. Deltagere: SAM, TAM, driftsleder og andre aktuelle personer hos begge parter avhengig av innmeldte saker.

En av de ansatte forteller at Kystriket IKT i all hovedsak får innsyn på områder som de har bruk for i drifta. Kystriket IKT får det som er etablert, men systemet er fortsatt under oppbygging og alle loggsystemer er ikke satt i drift.

Ifølge driftsavtalen har kunden rett til å foreta revisjon og verifikasjon av at leverandøren overholder avtalte forpliktelser for driftstjenesten.

Revisors vurdering

Revisjonskriteriet sier at kommunen bør ta ansvar for sikkerheten ved tjenesteutsetting.

Revisor vurderer at kommunen gjennom avtalen med felles driftsleverandør tar ansvar for sikkerheten ved tjenesteutsetting.

Revisor finner at kommunene har signert driftsavtalen og at ansatte knyttet til Kystriket IKT har vært involvert i utformingen av driftsavtalen. Utfordringen for kommunene kan være å forstå

ansvaret som hviler på driftsleverandøren og ansvaret som ligger til den enkelte kommune. Når det gjelder ansvaret som ligger til den enkelte kommunen vil mye håndteres av ansatte tilknyttet Kystriket IKT. Her kan det oppstå en gråsone mellom det Kystriket IKT håndterer på vegne av alle kommunene i samarbeidet, og det som den enkelte kommune har ansvar for.

4.3.4 Sikker IKT-arkitektur

Data

I kravspesifikasjonen er det satt krav til at leverandøren skal levere dokumentasjon som beskriver kundens systemoppsett og konfigurasjon, samt at løsningen genererer oppdatert dokumentasjon (Driftsavtalen 2023). I driftsavtalen går det fram at grundig teknisk design av arkitekturen og plan for tilhørende konfigurasjonsstyring er et viktig fundament for å sikre optimal kvalitet i etablerings- og driftsfasen.

Ifølge driftsavtalen skal leverandøren sørge for detaljert dokumentasjon av oppdragsgivers systemer og løsninger. Dette skjer i den månedlige rapporteringen fra driftsleverandøren til Kystriket IKT, hvor et av de faste punktene på agendaen er gjeldende konfigurasjon (Driftsavtalen 2023).

Driftsleverandøren har overtatt driften av nettverket, det brukes kjent utstyr og sikkerhetstiltakene i nettverket er i henhold til driftsavtalen. Kystriket IKT har også stilt strengere krav enn opprinnelig til noen av sikkerhetstiltakene. Driftsleverandøren har ansvar for sikker IKT-arkitektur, forteller en medarbeiderne i Kystriket IKT.

Kystriket IKT har en egen IKT-arkitekt. Nettverksansvarlig i Kystriket IKT har en skisse over nettverket og nettverksutstyr. Kystriket IKT har ansvar for den fysiske delen og brannmurene, mens driftsleverandøren har ansvar for oppdatering av brannmurer, sier en av medarbeiderne i Kystriket IKT.

Kystriket IKT har skisse over det fysiske nettet med nettverksutstyr og adresser, fortelles det i intervju med Kystriket IKT. Dette omfatter både fast tilkoblet utstyr og trådløst utstyr. Det er en digital oversikt som to ansatte i Kystriket IKT bruker aktivt og andre har tilgang.

De som er nettverksansvarlige har egnede verktøy og nødvendige visualiseringer som benyttes. Det sies at det er vanskelig å få en felles forståelse i Kystriket IKT av hvordan nettverkene ser ut, og det er varierende grad av kompetanse hos medarbeiderne i Kystriket IKT. Driftsleverandøren har sin dokumentasjon, og for dem kan være vanskelig å forstå hva en kommune er, og hva Kystriket IKT holder på med.

Kommunene har fortsatt litt ulike løsninger i IKT-arkitekturen og Kystriket IKT jobber for at de skal ha like løsninger, men møter noe motstand. Fra Kystriket IKT sin side handler det om

sikkerhet og forenkling. Graden av IT-kompetanse er veldig forskjellig innenfor og mellom kommunene.

Kystriket IKT sitt nettverk er oppdelt i ulike soner, fortelles det i intervjuene. Sikker sone ligger i driftsleverandørens datasenter. Dokumenter kan ikke flyttes ut eller kopieres fra sikker sone. Sensitiv personinformasjon blir i sikker sone. Sikker sone er sikret mot både utilsiktet og tilsiktet feil (datainnbrudd). Det er tilgang til sikker sone kun ved tjenstlig behov. Nettverket er oppdelt slik at det ikke er tilgang mellom elevnett og ansattnett. Mobiltelefoner bruker i hovedsak gjestenett. Kommunene har samme type brannmur, «firewall as a service».

Revisors vurdering

Revisjonskriteriet sier at kommunen bør etablere og dokumentere en sikker IKT-arkitektur.

Revisor vurderer at kommunen har avtalt med driftsleverandøren at den skal sørge for en sikker IKT-arkitektur

Driftsavtalen regulerer at driftsleverandøren skal levere dokumentasjon på systemoppsett og konfigurasjon. Driftsleverandøren skal sørge for dokumentasjon av kundens systemer og løsninger, og at systemet genererer denne dokumentasjonen når det skjer endringer. Ansatte i Kystriket IKT forstår det slik at driftsleverandøren har ansvaret for at det er en sikker IKT-arkitektur.

4.3.5 Sentral styring med sikkerhetsoppdateringer

Data

Kravspesifikasjonen setter krav til at driftstjenesten tilbyr en modell for administrering av applikasjonstjenester som inkluderer installasjon, oppdateringer slik som patching og sikkerhetsfikser, samt sanering. Slik kan leverandøren ha et totalansvar for applikasjons-tjenestenes avtalte kvalitet. (Driftsavtalen 2023) Leverandøren svarer ut at oppdateringer (patching) av operativsystem og annen systemprogramvare på leverandørens tjenester utføres etter anbefalinger fra programvare- og systemleverandørene. Dette gjelder både sikkerhetsoppdateringer og feilretting. Slike oppdateringer utføres automatisk og så snart de er tilgjengelige. Oppgraderinger er overgang til ny hovedversjon og gjøres i dialog med kunden og leverandøren av programvare eller system. (Driftsavtalen 2023) Ifølge driftsavtalen skal sikkerhetsoppgraderinger for programvare som benyttes til levering av driftstjenesten alltid driftsettes uten unødig opphold.

Serverparken eies av driftsleverandøren og de er avtalemessig forpliktet til å oppgradere disse fortløpende. Applikasjoner oppdateres av fagsystemleverandører og med bistand fra

driftsleverandøren der det er nødvendig. De ulike SaaS-løsningene[23] og fagsystem-leverandørene håndterer sikkerhetsoppgraderinger og det skjer løpende i drift. Ved gjennomgang av systemene kan Kystriket IKT se hva som må forbedres ved systemene. Det er systemeier som etterspør oppgradering av programvare og Kystriket IKT koordinerer selve oppgraderingen med alle parter.

Kystriket IKT styrer sikkerhetsoppdateringer i applikasjoner og mange skjer automatisk, men med varsel. Flere forteller om «patchtuesday»[24], som er en gang i måneden. Da går det ut et varsel om oppdateringer to dager før patchen kjøres. Brukerne får en frist til å restarte PC og etter denne fristen kommer de ikke inn på programmet før maskinen er oppdatert. Daglig leder i Kystriket IKT forteller at det ikke er noen tvungen oppdatering av PC-er, som betyr at oppdateringen kan utsettes i inntil sju dager. Ette den tid tvinges brukeren til å oppdatere.

Kystriket IKT kan vurdere om oppdateringer i serversystemet til driftsleverandøren trengs eller ikke fordi det koster en del, forteller daglig leder i Kystriket IKT. En av de andre ansatte forteller at Kystriket IKT har policy på at de ikke skal gjøre oppdateringer først, men at kritiske oppgraderinger blir prioritert. Oppgraderinger rulles vanligvis ut etter to uker. Kystriket IKT avventer for å sjekke at oppgraderingen ikke inneholder store feil. Kystriket IKT har en gang opplevd å miste innebygd funksjonalitet i operativsystemet i forbindelse med en oppgradering.

Kystriket IKT har ansvar for faste oppdateringer på noen fagapplikasjoner. Det inngår i årshjulet. En del av fagapplikasjonene på helse har egne oppdateringsrutiner.

Daglig leder i Kystriket IKT er klar over at kommunen har noen enheter som kan utgjøre en risiko fordi de sjelden er i bruk. Det finnes noen enheter hvor medarbeidere fra Kystriket IKT må oppdatere den enkelte enhet ved fysisk tilstedeværelse, men snart vil de kunne iverksette oppdateringer fra kontoret for alle enheter.

Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha sentral styring med sikkerhetsoppdateringer.

Revisor vurderer at kommunen gjennom Kystriket IKT i stor grad har sentral styring med sikkerhetsoppdateringer.

Revisor finner at begrepene sikkerhetsoppdatering (reparasjon) og sikkerhetsoppgradering (ny versjon) benyttes om hverandre, noe som kan være forvirrende for de som ikke kjenner til

[23] SaaS står for software as a service. Det betyr skybasert levering av programvare.

[24] Patchtuesday – er en betegnelse på at enkelte tirsdager kjøres det oppgraderinger fra flere leverandører av programvare.

arbeidet veldig godt. Driftsavtalen beskriver en arbeidsdeling mellom driftsleverandøren og Kystriket IKT på grunnleggende systemer. Mange leverandører av skybaserte fagapplikasjoner sørger for oppdateringer. Utfordringen kan være fagapplikasjoner hvor ansvaret for oppdateringer er lagt til systemeiere ute i kommunen. Det finnes et årshjul for oppdatering av fagapplikasjoner som ikke oppdateres automatisk. Årshjulet gjør det mulig for Kystriket IKT å følge opp at det gjøres sikkerhetsoppdateringer. Kritiske oppdateringer blir i all hovedsak varslet av leverandørene.

4.3.6 Plan for sikkerhetskopiering og sikre at sikkerhetskopier tas

Data

Ifølge kravspesifikasjonen bør leverandøren ha rutiner for regelmessig å sikre kvalitet på sikkerhetskopiering. Driftsleverandøren redegjør i driftsavtalen for hvilke rutiner for sikkerhetskopiering som tilbys, både type sikkerhetskopiering og tidsintervall for uttak og oppbevaring. Det framgår av driftsavtalen at alle sikkerhetskopierte data er lagret i henhold til oppdragsgivers krav om uforanderlig sikkerhetskopi (immutable backup) (Driftsavtalen 2023).

I intervjuene med Kystriket IKT fortelles det at driftsleverandøren har ansvaret for sikkerhetskopiering. Kystriket IKT er ikke tjent med å ha lokale sikkerhetskopier. Det er to servere i systemet til Kystriket IKT som snart vil bli tatt ut av drift. Av hensyn til personopplysninger er det viktigst for Kystriket IKT at sikkerhetskopiene ligger der det er avtalt i driftsavtalen. Kommunene har databehandleravtaler med alle leverandører, som forplikter leverandørene til sikker lagring i GDPR-vennlig område[25].

Driftsleverandøren har ansvar for sikkerhetskopier av det som blir generert av filer, og hvis det er endringer i switcher[26] eller brannmur, forteller en av de ansatte. Type backup er avhengig av hvilket system det tas backup av, og dette er ivaretatt i driftsavtalen.

Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

Revisor vurderer at kommunen gjennom driftsavtalen har en plan for sikkerhetskopiering, og at driftsavtalen pålegger driftsleverandøren å ta sikkerhetskopier.

[25] GDPR-regelverket har bestemmelser om hvor data kan lagres.

[26] Switch også kalt nettverksveksler er en nettverkskomponent som styrer datatrafikk mellom ulike noder i et nettverk. (Svitsj – Wikipedia)

Revisor har sett en detaljert beskrivelse av form og hyppighet på sikkerhetskopieringen. Det er ikke redegjort nærmere for innholdet ettersom slik informasjon ikke bør offentliggjøres av sikkerhetshensyn.

4.4 Tiltak for å oppdage

4.4.1 Revisjonskriterier

Tiltak for å oppdage handler om å overvåke IKT-systemet slik at trusler kan oppdages tidligst mulig og helst før det skjer noen skade. Følgende revisjonskriterier om å oppdage er utledet i vedlegg 1:

- *Kommunen bør fastsette hvilke deler av IKT-systemet som skal overvåkes.*
- *Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.*

4.4.2 Plan for hva som skal overvåkes

Data

Kravspesifikasjonen stiller krav om en overvåkningsløsning som overvåker kundens komponenter som driftes på plattformen og som driftes lokalt. I leverandørens tilsvar på disse punktene handler dette om overvåkning av eksempelvis tilgjengelighet og kapasitet. Denne delen av avtalen sier ikke noe om sikkerhet. Kravspesifikasjonen stiller også krav om at overvåkningsløsningen bør støtte rolle- og tilgangsstyringen og være en del av kundens vakttjeneste. Det bør også tilbys en form for selvbetjening hvor kunden kan konfigurere egne dashboard med valgte datapunkter. (Driftsavtalen 2023)

Overvåkningsverktøyet inneholder et dashboard som Kystriket IKT har tilgang til, slik at de løpende kan følge med. Det settes også opp varsling av hendelser og mulige kommende hendelser via epost eller tekstmelding i henhold til avtalen.

Driftsleverandøren benytter verktøy som logger all aktivitet på Kystriket IKT sine løsninger. Det gjør at driftsleverandøren hele tiden har kontroll på hvem som har fått tilgang til hva og på hvilket tidspunkt. (Driftsavtalen 2023)

I intervjuer med ansatte i Kystriket IKT bekreftes det at det er en plan for overvåkning. Driftsleverandøren har to parallelle løsninger. Den ene er driftsleverandørens datasenter og den andre er Azure-miljøet. I planen er det slik at kritiske systemer, eksempelvis innenfor helse, har lavere terskel for aksjon enn andre deler av systemet. Planen for overvåkning endres jevnlig. Sist ble den endret på grunn av en applikasjon som ikke har vært på listen og som oppførte seg litt rart.

Kystriket IKT har bestemt hvilke deler av systemet de skal ha overvåkning på. Drifts-leverandøren får ofte et varsel før Kystriket IKT ser det. Hendelser tas opp på driftsmøter. Kystriket IKT får hendelsesrapporter fra driftsleverandøren, eksempelvis endringer i driftsleverandørens datasenter som gjør at noe feiler.

En av medarbeiderne i Kystriket IKT forteller at kommunene egentlig ikke har noen rolle i overvåkningen. Dette er en tjeneste kommunene betaler for, men Kystriket IKT ønsker tilgang for å ha bedre kjennskap til de ulike lokasjonene og dermed forstå varslene bedre. Driftsleverandør har et mer helhetlig. overordnet perspektiv på IKT-systemet. Begge parter har tilgang til overvåkningen. Kystriket IKT følger med og observerer av egen interesse og har tilgang til å logge inn og se. Driftsleverandøren har ansvaret for å følge med.

Ideelt skulle Kystriket IKT hatt en liste med advarsler eller alarmer før brukerne tar kontakt, sier en av medarbeiderne i Kystriket IKT. Det er viktig å avdekke ting før telefonene ringer, og da er de avhengig av overvåkningsutstyr som Kystriket IKT per nå ikke har. Drifts-leverandørens overvåkningssystem dekker bare en liten del av behovet som medarbeiderne i Kystriket IKT har.

Revisors vurdering

Revisjonskriteriet sier at kommunen bør fastsette hvilke deler av IKT-systemet som skal overvåkes.

Revisor vurderer at kommunene gjennom driftsavtalen har fastsatt hvilke deler av IKT-systemet som skal overvåkes.

Det finnes en plan for overvåkning som dekker overvåkning av driftsleverandøren sin tjenesteleveranse, eksempelvis oppetid i systemet. Revisor har forstått det slik at denne planen endres underveis etter behov. Gjennom overvåkningen varsles det også hendelser i IKT-systemet.

4.4.3 System for overvåkning av sikkerhet og analyse

Data

Innsamling og analyse av sikkerhetsrelevant data kan bidra til å oppdage sikkerhetshendelser tidlig, vurdere skadeomfang og hendelsens karakter og forstå hendelsesforløpet. (NSM 2020)

Leverandøren har et overvåkningsverktøy, og enkelte ansatte i Kystriket IKT har tilgang til et dashboard der de kan følge med på status. Varsling av hendelser skjer via e-post og SMS.

Leverandøren har mekanismer for å oppdage og forhindre distribuerte tjenestenektangrep (DDoS)[27]. (Driftsavtalen 2023)

En av de ansatte i Kystriket IKT forteller at de skiller på hendelser og forespørsler. Hendelse er et avbrudd hvor noen ikke får gjort det de skal. En forespørsel er noen som trenger noe eller mangler noe, og omtales som brukerstøtte.

I driftsavtalen er det en opsjon på en skybasert sikkerhetsløsning for å identifisere, oppdage og undersøke trusler, kompromitterende identiteter og ondsinnede aktivitet rettet mot kommunene. Daglig leder i Kystriket IKT forteller at høsten 2025 er det tatt i bruk en løsning som strammer inn mulighetene for angrep og gir et svært høyt sikkerhetsnivå på klientsiden. I den samme løsningen er det muligheter for å gjennomføre målrettede kurs og simulerings-øvelser for ansatte.

Driftsleverandøren skal i forkant av driftsmøtene rapportere på utførte driftstjenester, herunder oversikt over alle registrerte hendelser fordelt på sakstyper. Det skal også være en oversikt over eventuelle avviksrapporter fra kritiske hendelser og feilsituasjoner, med beskrivelse av årsak, konsekvens og tiltak. (Driftsavtalen 2023)

I overvåkningen ser Kystriket IKT det meste av hvor og når innlogginger blir gjort. Det gjør det lettere å forstå hvorfor Kystriket IKT får henvendelser fra brukerne.

En av medarbeiderne i Kystriket IKT kunne ønsket seg tilgang til overvåkningen for å ha oversikt som grunnlag for arbeidet med feilsøking og oppretting. I den forbindelse er det behov for å overvåke det som skjer i nettverket, eksempelvis trafikk over portene[28]. Det er liveoppdateringer på switcher, men Kystriket IKT har ikke tilgang til disse. Kystriket IKT får informasjon om brudd på switcher, og finner raskt ut hva som skjer likevel. Porter er viktig og kritisk, men den ansatte er usikker på om trafikken der loggføres.

Kunstig intelligens brukes i analyser fra overvåkningen, forteller en av de ansatte i Kystriket IKT. Funn i overvåkningen diskuteres på driftsmøtene med driftsleverandøren, for eksempel problemer knyttet til nedetid. Kystriket IKT får oversikt over driftsproblemer og nedetid. Et eksempel på driftsproblemer er en applikasjon som Kystriket IKT sliter med å holde i drift.

---

[27] DDoS – Distributed Denial of Service som på norsk beskrives som distribuert tjenestenektangrep. DDoS innebærer at et nettsted blir bombardert med så mye trafikk at legitime brukere ikke når fram. (Jøsang 2025)

[28] Porter er et adressepunkt i en logisk forbindelse mellom to programmer som kommuniserer. (Port (datakommunikasjon) – Wikipedia)

Kystriket IKT har prøvd å stanse reelle angrep, etter varsel fra brukere. Da sendte de informasjon til brukerne underveis. Brukerne er både største trussel og største hjelper i forhold til hendelser.

Kystriket IKT får varsling fra HelseCert, og får ukentlig oversikt over angrep de har oppdaget. Helse- og KommuneCert har jevnlig kjørt test på nettsidene til kommunene og funnene rapporteres til kommunen. De sender epost med informasjon og det arrangeres webinarer. I Kystriket IKT er det en felles epostadresse som får hendelsesvarsel og meldingen videresendes til tre ansatte.

Kystriket IKT gjør ikke inntregningstester på systemet selv, og en av de ansatte forteller at han ikke vet hvor mye driftsleverandøren kan gjøre gjennom datasenteret.

Revisors vurdering

Revisjonskriteriet sier at kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.

Revisor vurderer at kommunen gjennom driftsleverandøren har et system for å overvåke sikkerheten og analysere data fra overvåkningen.

Revisor finner at det finnes et system for overvåkning av sikkerheten, men at dette ikke er eksplisitt uttrykt i driftsavtalen. Noen av denne overvåkningen skjer i henhold til plan for overvåkning, men det er uklart om det er spesifikke overvåkningstiltak rettet mot trusler og faren for hendelser. Revisor tolker at overvåkning av IKT-systemet spenner fra at systemet skal ha oppetid til å overvåke trusler eller faren for uønskede hendelser. Det er positivt at Kystriket IKT er knyttet til Helse- og KommuneCert og får varsel og annen informasjon fra dem.

4.5 Tiltak for å håndtere og gjenopprette

4.5.1 Revisjonskriterier

Følgende revisjonskriterier om å håndtere og gjenopprette er utledet i vedlegg 1:

- *Kommunen skal ha rutiner for hendelseshåndtering og det bør foreligge en plan for hendelseshåndtering.*
- *Kommunen skal ha en plan for gjenoppretting.*

4.5.2 Plan for hendelseshåndtering

Data

Kravspesifikasjonen krever at leverandøren har en beredskapsplan for å oppfylle sine forpliktelser til kommunen hvis uforutsette hendelser inntreffer og den normale virksomheten

blir berørt og vanlige arbeidsprosesser slutter å fungere. Det skilles mellom kritiske, alvorlige og mindre alvorlige hendelser. Avhengig av type hendelse er det satt ulike krav til responstid, krav om tilbakemelding, påbegynt hendelseshåndtering, retting av feil, mål om løsningstid og servertilgjengelighet. Kravene er også avhengig av om hendelsen skjer hos leverandøren eller hos Kystriket IKT. Det er også bestemmelser om krav til eskalering hvis hendelsen ikke løses innenfor målet om løsningstid. Det er også tidsfrister for varsling og hvordan varslingen skal foregå. Leverandøren skal månedlig rapportere på avvik som kritiske hendelser og feilsituasjoner med beskrivelse av årsak, konsekvens og tiltak (Driftsavtalen 2023).

Det framgår av driftsavtalen at leverandøren skal ha beredskaps- og katastrofeplaner for driftstjenesten. Leverandøren skal gjennomføre nødvendige beredskaps- og katastrofeøvelser minst en gang per år. Videre skal leverandøren bidra i gjennomføringen av kundens egne beredskaps- og katastrofeøvelser på IKT inntil en gang per år. (Driftsavtalen 2023)

Driftsleverandøren har beredskap for Kystriket IKT, forteller daglig leder i Kystriket IKT. Prosedyren for de ansatte i kommunene er å ringe Kystriket IKT sin supporttelefon hvis de oppdager uregelmessigheter. Noen av medarbeiderne i Kystriket IKT inngår i en vaktordning fordelt på fire vakter i løpet av ordinær arbeidsdag. Andre ansatte er ikke med i den faste rulleringen, men kan ha bakvakt. Oppstår en hendelse, starter Kystriket IKT en feilsøking for å finne ut hva som ikke fungerer og om det kan skyldes et angrep, forteller en av de ansatte. Vedkommende sin prioritet er å håndtere det som skjer på nettverket, men han har ikke oversikt over hele planen for hendelseshåndtering.

Dersom hendelsen oppstår utenfor arbeidstid, vil henvendelsen automatisk omdirigeres til driftsleverandørens supportorganisasjon som følger opp videre og eventuelt eskalerer. Ved alvorlige hendelser, som for eksempel datainnbrudd, vil også relevante myndigheter varsles, herunder politiet. Driftsleverandøren har 24/7-vakt og har en plan på hvem som kalles ut. I leverandørens 24/7-vakt inngår oppfølging av apper og tjenester som Kystriket IKT har definert som kritisk. Andre ikke-kritiske hendelser får den som melder beskjed om å melde som sak til servicedesken dagen etter. Ved tvil skal de kontakte daglig leder i Kystriket IKT. Drifts-leverandøren kan stenge ned deler av nettverket ved behov.

Kystriket IKT har en plan for håndtering av hendelser med hva, hvordan, hvem og lignende, forteller en av de ansatte i Kystriket IKT. Ved større hendelser skal det settes ned en arbeidsgruppe. Driftsleverandør er en selvsagt deltaker i arbeidsgruppa, og oftest er det deres ansvar. Driftsleverandør har også mulighet for å stenge ned systemene, og låse alle ut.

I intervju med seniorrådgiver for informasjonssikkerhet i Sømna kommune, blir det sagt at strategisk ledergruppe og kriseledelse har snakket om hva som skjer dersom de kommer på

jobb og ikke noen systemer fungerer. Dette vil komme frem i dokumentet kritikalitetsvurdering, som er et dokument som ble prioritert utarbeidet av sikkerhetsorganisasjonen i møte den 24.04.25. Hun sier at det er ledergruppen som sammen med Kystriket må samarbeide når ting ikke fungerer, og definere hva som skal prioriteres. Avklaringene er ikke gjort enda, men en kritikalitetsvurdering vil gjøre at det kommer på plass. Hun mener at en slik vurdering også bør gjøres i samarbeid med de andre kommunene i Kystriket, og krever involvering av mange.

Leder for personal og fellestjenester kan ikke svare på hva som skjer dersom hun kommer på jobb og ingen systemer fungerer. Hun sier at kommunedirektøren sannsynligvis vil kalle inn kriseledelsen, og kommunen har beredskapssystemet RAYVN som blant inneholder tiltakskort ved hendelser som strømbrudd og nettverksbrudd. Hun er ikke kjent med hvordan tjenestene er forberedt på at systemene er borte, da dette ansvaret ligger til kommunalsjefene. Når det gjelder unormale aktiviteter, har Kystriket sendt eposter til ansatte med informasjon om å melde ifra og advarsel om ulike eposter som har utilsiktede hendelser som formål.

IT-medarbeideren i Sømna forteller at det er rutiner i Kystriket IKT for hva de gjør dersom de kommer på jobb og ikke systemene fungerer eller «alt har gått i svart», da det er en hendelseshåndteringsplan i Kystriket IKT. Helse er definert som tjenester som får hjelp først, men han er usikker på om dette er definert skriftlig i planen for hendelseshåndtering. Han varsler først Kystriket ved en hendelse før det eventuelt meldes videre til Iteam. Han kjenner til at kommunen har hatt hendelser, men han har ikke vært involvert.

I intervju med daglig leder i Kystriket IKT kommer det fram at han ikke kjenner til hvilke beredskapsplaner de andre kommunene har. Han forteller at de er en prioritert kunde hos driftsleverandøren hvis en hendelse oppstår. I driftsavtalen står det at hvis det oppstår hendelser eller situasjoner som krever oppmerksom-het fra driftsleverandøren, vil Kystriket IKT være prioritert kunde i leverandørens systemer og få hjelp av kompetent personell svært raskt. Daglig leder forteller at driftsleverandøren ikke har mange kommuner i sin kundeportefølje, bare noen få små. Fem kommuner på én avtale gjør Kystriket IKT til en attraktiv kunde. En av de ansatte kjenner til at driftsleverandøren har en katastrofeplan som de har fått presentert, men kjenner ikke alle detaljene. Det framgår av driftsavtalen at driftsleverandøren skal ha beredskaps- og katastrofeplaner for driftstjenesten.

Vurdering

Revisjonskriteriet sier at kommunen skal ha rutiner for hendelseshåndtering og det bør foreligge en plan for hendelseshåndtering.

Revisor vurderer at kommunen har en praksis for håndtering av hendelser og deler av et planverk for håndtering av hendelser.

Vurderingen bygger på at driftsavtalen beskriver håndtering av hendelser. Driftsavtalen vil ivareta forhold som berører IKT-systemet.

Seniorrådgiver for informasjonssikkerhet i Sømna tilbakemelder på spørsmål fra revisor i epost, at kommunen har en beredskapsplan, men ikke en beredskapsplan for IKT. Hun forteller at de har tatt utgangspunkt i relevanserklæringen når vi utarbeider nye dokumenter. Når det gjelder beredskapsplan for IKT og kritikalitetsvurdering IKT har hun foreslått internt i Sømna kommune at dette er noe kommunene som er tilsluttet Kystriket bør vurdere å samarbeide om. Dette er så vidt hun vet ikke enda tatt opp i samarbeidsmøter kommunene har med Kystriket IKT.

4.5.3 Plan for gjenoppretting

Data

Driftsavtalen (2023) beskriver muligheten for gjenoppretting etter kritiske hendelser (disaster recovery), gjennom å flytte kommunenes løsninger over på et av leverandørens andre datasenter. Leverandøren har alternative systemer og infrastruktur for å opprettholde tilgjengelighet til tjenestene selv om det oppstår feil eller angrep. Hvis det oppstår hendelser som krever oppmerksomhet fra leverandøren, vil kommunene være en prioritert kunde, jfr. kapittel 4.5.2.

Driftsavtalen har bestemmelser om rekonstruksjon av data. Ved tap eller ødeleggelse av data skal leverandøren uten ugrunnet opphold gjenopprette disse og om nødvendig rekonstruere data. Leverandørens ansvar for kostnader er begrenset til å gjenopprette data fra siste sikkerhetskopi.

En av de ansatte forteller at driftsleverandøren har en plan for gjenoppretting for de systemene de har ansvar for. Kystriket IKT har noen planer for hva som skal prioriteres i gjenoppretting, går det fram av et intervju. Det handler om å identifisere bugs og å prioritere liv og helse. Den ansatte som har erfaring fra alvorlig hendelse i tidligere jobb, forteller at alt ble stengt ned og gjenopprettingen skjedde steg for steg. En av de andre ansatte forteller at en gjenopprettings-plan er avhengig av nivået på hendelsen. Kystriket IKT kan gjenopprette uten å være på nett.

Kystriket IKT er involvert gjennom hendelsesansvarlig. Noen av medarbeiderne i Kystriket IKT er samlet i en pool og kan bli involvert hvis det er noe som skal gjenopprettes i en annen kommune. Kommunene er ansvarlig for hva som skal gjenopprettes, men daglig leder i Kystriket IKT er usikker på om kommunene er så bevisste på det.

En av de ansatte i Kystriket IKT forteller at det sjeldent er behov for gjenoppretting. Under migreringen måtte det gjenopprettes noe data, som måtte overføres på nytt. Daglig leder i

Kystriket IKT forteller at de har gjort gjenoppretting med hell mange ganger. De gangene de ikke lykkes skyldes det vanligvis at brukerne har lagret data lokalt på enhetene, i strid med rutinene.

En av de ansatte i Kystriket IKT forteller at de har en god løsning for gjenoppretting av sikkerhetskopier, som de har brukt flere ganger, og da har de byttet hardware og gjenopprettet. En av de andre mener at driftsleverandøren har testet gjenoppretting. Ifølge driftsavtalen skal det kjøres en gjenopprettingstest en gang i året, men vedkommende er usikker på om dette er gjort, ettersom systemet ikke har vært oppe så lenge.

Revisors vurdering

Revisjonskriteriet sier at kommunen skal ha en plan for gjenoppretting.

Revisor vurderer at kommunen delvis har deler av en plan for gjenoppretting.

Driftsleverandøren har en plan for gjenoppretting etter en kritisk hendelse. Ansatte i Kystriket IKT er i liten grad kjent med planen og hva den inneholder. Det vil derfor være uklart om planen fanger opp ulike deler av en gjenoppretting, eksempelvis hva som skal prioriteres og hvem som skal prioritere. Dette er det kommunene som har ansvar for. En plan for gjenoppretting må omfatte kommunenes prioriteringer og driftsleverandørens oppgaver. Planen for gjenoppretting må omfatte både kommunens prioriteringer og de tiltakene som driftsleverandøren har ansvar for. Planen bør også si noe om utfordringer med å finne sikkerhetskopier som ikke er infiserte hvis det har skjedd et angrep samt noe om tidsperspektivet på gjenopprettingen. Sømna kommune kan ikke vise til en slik plan.

4.6 Konklusjon

På bakgrunn av funn og vurderinger konkluderer revisor slik på andre problemstilling: **Sømna kommune har i stor grad tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet.**

Konklusjonen for problemstilling 2 bygger på at Kystriket IKT sammen med driftsleverandøren i stor grad har systemer og tiltak for å følge opp informasjonssikkerhet. Det vil alltid finnes forbedringsområder innenfor informasjonssikkerhet, fordi området er i stadig utvikling. Svakhetene som er avdekket er at beredskapsplanen for IKT ikke er på plass, og at gjenopprettingsplanen mangler for deler som kommunen har ansvar for.

5 KONKLUSJONER OG ANBEFALINGER

5.1 Konklusjoner

På bakgrunn av funn og vurderinger konkluderer revisor slik på problemstillingene:

1. **Sømna kommune er godt i gang med å etablere et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket.**

På bakgrunn av data som er samlet inn og de vurderingene som er gjort på de utvalgte kriteriene, konkluderer revisor for problemstilling 1 med at Sømna kommune er godt i gang med å etablere et styringssystem for informasjonssikkerhet. Kommunen har prioritert tid og ressurser på arbeidet, og har kommet et godt stykke på vei for å få styringssystemet på plass.

Det er likevel mye som gjenstår. Det er elementer i styringssystemet som kommunen enda ikke har startet å jobbe med. Kommunen har ikke et godt nok system for risikovurderinger, og for å planlegge og gjennomføre risikoreduserende tiltak. Dette gjelder både for informasjonssikkerheten og personvernet. Kommunen har ikke systematisert evaluering og læring av hendelser. Opplæringsplaner knyttet til temaet er også i liten grad systematisert ved å plassere ansvar og tidsfrister for gjennomføring av opplæringsaktiviteter.

2. **Sømna kommune har i stor grad tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet.**

Konklusjonen for problemstilling 2 bygger på at Kystriket IKT sammen med driftsleverandøren i stor grad har systemer og tiltak for å følge opp informasjonssikkerhet. Det vil alltid finnes forbedringsområder innenfor informasjonssikkerhet, fordi området er i stadig utvikling. Svakhetene som er avdekket er at beredskapsplanen for IKT ikke er på plass, og at gjenopprettingsplanen mangler for deler som kommunen har ansvar for.

Revisor ser og anerkjenner at fagområdet som er revidert er stort og komplekst, med et sammensatt regelverk. Dette krever mye av kommunen i form av kompetanse, tid- og ressursbruk og organisatoriske prosesser. Revisor konkluderer med at Sømna kommune har forstått behovet for å prioritere ressurser for å tydeliggjøre roller og ansvar og bygge kompetanse i hele organisasjonen, og at dette er arbeid det tar tid å få en bevissthet om i hele organisasjonen.

5.2 Anbefalinger

Revisor anbefaler kommunedirektøren å

- Videreutvikle styringssystemet for informasjonssikkerhet, og prioritere arbeidet med å innlemme risikovurderinger som en del av systemet.
- Gjennomføre planlagt arbeid med risikovurderinger av personvernkonsekvenser.
- Systematisere opplæringen av informasjonssikkerhet.
- Vurdere hvilke systemer og funksjoner som må prioriteres hvis datasystemer ikke er tilgjengelig og eventuelt må gjenopprettes, gjennom å utarbeide beredskapsplan for IKT.
- Bidra til å avklare ansvarsforhold mellom Sømna kommune og Kystriket IKT sitt arbeid overfor alle kommunene i Kystriket IKT.

KILDER

Lov og forskrift

Lov om nasjonal sikkerhet (Sikkerhetsloven) LOV-2018-06-01-24. Justis- og beredskapsdepartementet

Lov om behandling av personopplysninger (Personopplysningsloven) LOV-2018-06-15-38. Justis- og beredskapsdepartementet

Lov om kommuner og fylkeskommuner (Kommuneloven) LOV-2018-06-22-83. Kommunal- og distriktsdepartementet

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) FOR-2004-06-25-988. Digitaliserings- og forvaltningsdepartementet

Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetssikkerhets-forskriften) FOR-2018-12-20-2053. Justis- og beredskapsdepartementet

Forskrift om kontrollutvalg og revisjon. FOR-2019-06-17-904. Kommunal- og distriktsdepartementet

Litteratur

Bergsjø, H. og Windvik, R. (2018). Datasikkerhet for ledere – hvordan beskytte din virksomhet. Universitetsforlaget

Datatilsynet (lastet ned 18.03.2024) www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Digitale Helgeland, udatert. Digitaliseringsstrategi 2020-2023

Felles IKT-strategi for kommunene på Sør-Helgeland, udatert. Felles IKT-strategi for kommunene på Sør-Helgeland, Bindal, Brønnøy, Sømna, Vega og Vevelstad 2024-2027 versjon 1.1. Jøsang, A. (2025) Cybersikkerhet – teknologier og styring. 3. utg. Universitetsforlaget

Nasjonal sikkerhetsmyndighet (NSM) (2020) NSMs grunnprinsipper for IKT-sikkerhet. Versjon 2.0. Nasjonal Sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM), udatert. Grunnprinsipper for sikkerhetsstyring. Versjon 1. Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM), udatert. Veileder i sikkerhetsstyring. Versjon 1.

VEDLEGG 1 – UTLEDNING AV REVISJONSKRITERIER

Ifølge forskrift om kontrollutvalg og revisjon (§ 15) skal det etableres revisjonskriterier for gjennomføring av forvaltningsrevisjon. Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal vurderes i forhold til. Disse kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. Slike autoritative kilder kan være lov, forskrift, forarbeider, rettspraksis, politiske vedtak (mål og føringer), administrative retningslinjer, samt statlige føringer og praksis. I denne forvaltningsrevisjonen har vi benyttet oss av følgende kilder til revisjonskriterier:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger, herunder personvernforordningen (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften)
- Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhetsforskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet
- NSMs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet

Nasjonal sikkerhetsmyndighet (NSM) utgir veiledere for sikkerhetsloven og digitalsikkerhetsloven. Veilederne fastsetter NSMs forståelse og tolkning av lover og forskrifter. Datatilsynet har laget en oversikt over plikter etter personvernregelverket og gir veiledning knyttet til hvordan lover og regler skal forstås.

Lov om digital sikkerhet ble vedtatt i 2023, men trådte ikke i kraft før 01.10.2025. Denne loven er derfor ikke en del av utledning av kriterier i denne revisjonen. Samme dato som loven trådte i kraft ble det publisert en ny veileder til loven fra Nasjonal sikkerhetsmyndighet. Denne er heller ikke benyttet i arbeidet med revisjonen. For kommunen vil det være sentralt å sette seg inn i nytt regelverk og vurdere hvilke konsekvenser dette har for kommunens virksomhet. Loven gjelder for tilbydere av samfunnsviktige tjenester innenfor blant annet sektorene helse og vannforsyning, og vil således berøre kommunene.

Problemstilling 1: Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

Ledelsessystem for informasjonssikkerhet

Sikkerhetsloven stiller generelle krav til forebyggende sikkerhetsarbeid i kapittel 4. Sikkerhetsstyring er hjemlet i § 4-1; forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Virksomhetssikkerhetsforskriften definerer i § 3 kravet om at virksomheter som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. På engelsk brukes betegnelsen Information Security Management System (ISMS) og kan oversettes til norsk som informasjonssikkerhetssystem eller ledelsessystem for informasjons-sikkerhet (Jøsang 2025). Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.

Nasjonal sikkerhetsmyndighets veileder i sikkerhetsstyring skriver at sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Skjermingsverdige verdier er definert i sikkerhetslovens § 6-1 første ledd: *Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.*

Nasjonal sikkerhetsmyndighets grunnprinsipper for sikkerhetsstyring (NSM 2020) er overordnet for hele virksomheten og disse utfylles av grunnprinsipper for fysisk sikkerhet, IKT-sikkerhet og personellsikkerhet.

Ifølge veilederen i sikkerhetsstyring omfatter sikkerhetsstyring alle aktiviteter som har betydning for det forebyggende sikkerhetsarbeidet. Sikkerhetsstyring skal gjennomføres planlagt og systematisk i form av et sikkerhetsstyringssystem som omfatter planlegging, etablering, gjennomføring og forbedring av det forebyggende sikkerhetsarbeidet. Utformingen av styringssystemet for sikkerhet skal omfatte følgende prinsipper:

- Risikostyring
- Sikkerhetsledelse
- Sikkerhetsorganisering
- Sikkerhetstiltak og prosedyrer
- Forhold til andre virksomheter
- Sikkerhetsoppfølging
- Sikkerhetsdokumentasjon

Datatilsynet anbefaler i sin veileder om virksomhetens plikter at det benyttes anerkjente standarder, rammeverk og veiledere som beskriver styringssystem for informasjonssikkerhet. ISO 27001 er en anerkjent standard som på norsk har betegnelsen ledelsessystemer for informasjonssikkerhet[29].

Virksomhetssikkerhetsforskriften fastsetter krav om sikkerhetsmål i § 5. Virksomheten skal fastsette hvordan kravene til et forsvarlig sikkerhetsnivå skal oppfylles og kriterier for å evaluere om kravene er oppfylt.

eForvaltningsforskriftens § 15 omhandler internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan. Første ledd krever at mål og strategier for informasjonssikkerhet er beskrevet (sikkerhetsmål og sikkerhetsstrategi). Dette skal danne grunnlaget for forvaltningsorganets internkontroll på området for informasjonssikkerhet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. Kravene i personvernforordningen vil være aktuelle å innarbeide i en slik sikkerhetsstrategi.

Datatilsynet[30] skriver at sikkerhetsstrategien skal omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette gjelder blant annet fordeling og avklaring av arbeidsoppgaver mellom ledelse og driftspersonell, men også beslutning om eventuelt å ta i bruk eksterne leverandører i sikkerhetsarbeidet. Videre skal sikkerhetsstrategien gjøre rede for organisatoriske og tekniske strategiske valg. Strategien beskriver hvilke virkemidler virksomheten velger å bruke for å nå målene.

Det kommer frem av sikkerhetsloven § 4-1 at virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet. I forskriften om virksomhetens sikkerhet stilles det i § 4 krav om styringsdokument. Leder av virksomheten skal fastsette et styringsdokument som beskriver hvilke deler av sikkerhetsloven som gjelder for virksomheten, roller og ansvar i virksomhetens forebyggende sikkerhetsarbeid og prinsipper for virksomhetens sikkerhetsarbeid. Styringsdokumentet skal gjøres kjent og tilgjengelig for blant annet alle ansatte. Virksomhetssikkerhetsforskriften § 6 definerer videre krav til roller og ansvar for det forebyggende sikkerhetsarbeidet. Det er leder sitt ansvar å fordele roller og ansvar, og at disse gjøres kjent i virksomheten.

På bakgrunn av denne redegjørelsen er følgende revisjonskriterie for ledelsessystem utledet:

[29] Ledelsessystemer for informasjonssikkerhet – ISO/IEC 27001

[30] www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Kommunen skal ha et ledelsessystem for informasjonssikkerhet, som angir ○ Sikkerhetsmål ○ Sikkerhetsstrategi ○ Sikkerhetsorganisasjon, hvor roller og ansvar framgår

Internkontroll av informasjonssikkerhet

Andre ledd i § 15 i eForvaltningsforskriften krever at det skal være etablert internkontroll på området for informasjonssikkerhet. Internkontrollen skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være integrert som en del av virksomhetens helhetlige styringssystem. Tredje ledd i § 15 krever at omfang og innretning på internkontroll skal være tilpasset risiko.

I fjerde ledd bokstavene a til h, § 15, gis det eksempler på hvilke forhold sikkerhetsstrategien og internkontrollen bør adressere, herunder prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Internkontroll er hjemlet i kommuneloven kapittel 25, hvor det i § 25-1 det står at internkontrollen skal være systematisk og tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Kommunedirektøren er ansvarlig for internkontrollen og skal:

- utarbeide en beskrivelse av virksomhetens **hovedoppgaver, mål og organisering**
- ha nødvendige **rutiner og prosedyrer**
- avdekke og følge opp **avvik og risiko for avvik**
- **dokumentere internkontrollen** i den formen og det omfanget som er nødvendig
- **evaluere** og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Sikkerhetsloven § 4-2 krever at virksomheten regelmessig skal gjennomføre vurdering av risiko. Vurderingen danner grunnlaget for iverksetting av forebyggende sikkerhetstiltak. Videre skal virksomheten, som en del av vurderingen av risiko, kartlegge hvilke virksomheter den er avhengig av for å fungere som den skal. Vurderingen skal gjennomgås jevnlig og om nødvendig revideres. Kravet om vurdering av risiko er videre utdypet i virksomhetssikkerhetsforskriften § 12. Forskriften skriver i andre ledd at behovet for å gjennomføre en ny helhetlig vurdering av risikoen skal vurderes årlig.

NSM sine grunnprinsipper for sikkerhetsstyring (versjon 1) sier at etter en uønsket hendelse bør det forebyggende sikkerhetsarbeidet i virksomheten evalueres. Virksomheten må forsikre

seg om at tiltakene som er etablert fungerer etter hensikten og vurdere om hendelsen ble håndtert tilfredsstillende. NSM skriver at dette er viktig fordi:

«*Når en hendelse er ferdig håndtert og akseptabelt sikkerhetsnivå gjenopprettet, er det viktig at virksomheten hurtig identifiserer og lærer fra det inntrufne og sørger for at konklusjoner blir gjennomgått og tatt tak i. Dersom dette ikke gjøres vil kunnskap og erfaring forsvinne, og man kan gjøre de samme feilene om igjen neste gang en uønsket hendelse oppstår. Det kan være at det oppdages nye sårbarheter, eller behov for nye eller forbedrede sikringstiltak som kan forhindre at fremtidige situasjoner oppstår.*»

Følgende revisjonskriterier for internkontroll er utledet:

- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen bør ha rutiner og prosedyrer for å redusere risiko for avvik og uønskede hendelser.
- Kommunen må ha et avvikssystem og ansatte må melde avvik.
- Kommunen bør evaluere og lære av hendelser.

Personopplysninger

En av pliktene i personvernforordningen er at alle virksomheter som behandler personopplysninger, skal føre protokoll over behandlingsaktivitetene de har ansvar for (artikkel 30 i personvernforordningen). Protokollen skal inneholde formålet med behandlingen, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Dersom det er aktuelt, skal eventuelle databehandlere stå oppført i protokollen.

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven gjennomfører EUs personvernforordning i norsk rett. Personopplysningsloven er bygget på noen grunnleggende prinsipper, og alle som behandler personopplysninger må følge disse prinsippene.

Datatilsynet har laget informasjon om pliktene en virksomhet har etter personvernregel-verket. En av pliktene Datatilsynet referer til er vurdering av personvernkonsekvenser (DPIA – Data Protection Impact Assessment) (artikkel 35 i personvernforordningen). Artikkel 35 krever at virksomheten gjennomfører en vurdering av personvernkonsekvenser ved

behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter. Datatilsynet[31] skriver følgende om DPIA:

«*En vurdering av personvernkonsekvenser er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak*.»

DPIA skal som minimum inneholde:

- En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.
- En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.
- En vurdering av risikoene for de registrertes rettigheter og friheter
- De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes.

Følgende revisjonskriterier om personopplysninger er utledet:

• Kommunen skal føre protokoll over hvilke personopplysninger de behandler. • Kommunen skal gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA).

<u>Opplæring</u>

Sikkerhetsloven definerer i § 4-1 at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. Kravet om ressurser og kompetanse er videre utdypet i virksomhetssikkerhetsforskriften § 7. Forskriften krever blant annet at de ansatte som får tilgang til skjermingsverdige verdier, får tilstrekkelig kompetanse om sikkerhet og kartlegge at personene kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser.

Veilederen fra NSM skriver at riktig kompetanse oppnås og opprettholdes gjennom planmessig opplæring, kvalifisering og kompetansevedlikehold.

Datatilsynet skriver at målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt. Brukerne

[31] www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

må være gitt muligheten til å etterleve dette i sitt daglige arbeid gjennom tilpasset opplæring ut fra behovet. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.

På bakgrunn av redegjørelsen over er følgende revisjonskriterium for opplæring utledet:

- Kommunen bør sørge for at ansatte får tilstrekkelig opplæring i informasjons-sikkerhet.

Problemstilling 2: Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Sikkerhetsloven § 4-3 sier at virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet. Virksomhetssikkerhetsforskriften § 14 sier at grunnsikringstiltak skal bidra til et forsvarlig sikkerhetsnivå i virksomheter i en normaltilstand. grunnsikringstiltakene kan være

a) fysiske, elektroniske, menneskelige eller organisatoriske barrierer

b) systemer som skal oppdage og varsle om aktiviteter eller hendelser

c) systemer og rutiner for å avklare aktiviteter og hendelser og bakgrunnen for dem

d) oppfølging av uønskede aktiviteter og uønskede hendelser

Nasjonal sikkerhetsmyndighet har utgitt en veileder om grunnprinsipper for IKT-sikkerhet for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk.

NSMs grunnprinsipper for IKT-sikkerhet er en samling med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Samlingen er basert på NSMs erfaringer og tilbakemeldinger fra en rekke offentlige og private virksomheter. Selv om NSM anbefaler alle virksomheter å følge prinsippene betyr ikke det at virksomheten oppfyller sikkerhetsloven ved å følge dem.[32]

Grunnprinsippene fokuserer på teknologiske og organisatoriske tiltak, og hovedfokuset er på tilsiktende handlinger.

Grunnprinsippene for IKT-sikkerhet er delt inn i fire kategorier og er gjengitt i tabellen under.

[32] Hva er NSMs grunnprinsipper for IKT-sikkerhet? - Nasjonal sikkerhetsmyndighet

Tabell 1. Grunnprinsipper for IKT-sikkerhet.

1. Identifisere og kartlegge	**2. Beskytte og opprettholde**
Kartlegge styringsstrukturer, leveranser og understøttende systemer Kartlegge enheter og programvare Kartlegge brukere og behov for tilgang	Ivareta sikkerhet i anskaffelses- og utviklingsprosesser Etablere en sikker IKT-arkitektur Ivareta en sikker konfigurasjon Beskytte virksomhetens nettverk Kontroller dataflyt Ha kontroll på identiteter og tilganger Beskytt data i ro og i transitt Beskytt e-post og nettleser Etabler evne til gjenoppretting av data Integrer sikkerhet i prosess for endrings-håndtering
3. Oppdage	**4. Håndtere og gjenopprette**
Oppdage og fjerne kjente sårbarheter og trusler Etablere sikkerhetsovervåkning Analysere data fra sikkerhetsovervåkning Gjennomfør inntrengingstester	Forberede virksomheten på håndtering av hendelser Vurdere og klassifisere hendelser Kontrollere og håndtere hendelser Evaluere og lære av hendelser

Kilde: Nasjonal sikkerhetsmyndighet 2020

Identifisere og kartlegge

Virksomhetssikkerhetsforskriften § 14 første ledd punkt a sier at grunnsikringstiltak kan være fysiske, elektroniske, menneskelige eller organisatoriske barrierer.

NSM skriver at kartlegging av enheter og programvare er viktig for å få oversikt over hva som befinner seg i kommunen. Det er viktig at kommunen selv får oversikt over enheter, programvare og deres sårbarheter før angripere gjør det.

Videre skriver NSM at risikobildet må vurderes knyttet opp til valget mellom sikkerhet og behovet for leveranser til kommunen. Det kan hende at kommunen må godta enheter med lavere sikkerhetsnivå enn ønsket, og det er derfor viktig at kommunen er bevisst på strategier som velges og vurderer de funksjonelle behovene opp mot risiko. Anbefalt tiltak fra NSM er å kartlegge enheter og programvare.

Det er også viktig at kommunen har oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i en kommune. En angriper har ofte som mål å øke tilgangen ved et angrep på informasjonssystemet. Mange brukere kan ha tilganger og rettigheter til systemer og tjenester de egentlig ikke har behov for. Derfor bør tilganger og rettigheter begrenses slik at skaden fra en potensiell angriper eller utro ansatt reduseres. Derfor bør kommunen kartlegge brukere og behov for tilgang.

Utledede revisjonskriterier:

- Kommunen bør ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.
- Kommunen bør ha et system for styring av tilganger.

Beskytte og opprettholde

NSM har et prinsipp som sier at sikkerheten i anskaffelse- og utviklingsprosesser må ivaretas. Målet med prinsippet er å minimere risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter.

Et av prinsippene under denne kategorien er å etablere en sikker IKT-arkitektur. Et IKT-system består av mange sikkerhetsfunksjoner og ulike IKT-produkter fra ulike produsenter som skal fungere godt og sikkert sammen. Manglende kompatibilitet kan øke sårbarheten på en måte som angriperne kan utnytte. Videre skriver NSM at drift- og sikkerhetskonfigurasjon bør skje sentralt og likt per type enhet, hvis ikke øker risikoen for dobbeltarbeid, menneskelige feil og flere sårbarheter. IKT-systemet bør videre deles opp i forskjellige deler avhengig av tillitsnivå for å begrense risiko.

Under prinsippet om å ivareta en sikker konfigurasjon, anbefaler NSM å etablere et sentralt styrt regime for sikkerhetsoppdatering. I dette ligger det blant annet at kommunen bør installere sikkerhetsoppdatering så fort som mulig. Videre bør kommunen ha en prioriteringsliste for oppdateringer og etablere en rutine med klare ansvarsforhold for hvor ofte oppdateringer skal utføres og hvem som er ansvarlig dersom en oppdatering ikke kan gjennomføres eller må utsettes.

NSM skriver at et av prinsippene er å etablere en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap. Et av de anbefalte tiltakene er å lage en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.

Utledede revisjonskriterier:

- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.
- Kommunen bør ta ansvar for sikkerheten ved tjenesteutsetting.
- Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer.
- Kommunen bør ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

Oppdage

Virksomhetssikkerhetsforskriften 14 første ledd punkt b angir at grunnsikringstiltak kan være systemer som skal oppdage og varsle om aktiviteter eller hendelser.

NSM har et prinsipp som omhandler etablering av sikkerhetsovervåkning for å overvåke og samle inn relevante data for å oppdage sikkerhetshendelser og legge et grunnlag for å analysere data. Dette for at kommunen kan oppdage sikkerhetshendelser tidlig som mulig for å minimere skadeomfang eller forhindre hendelser. Det er viktig at kommunen har tilgang på tilstrekkelig data siden det kan være avgjørende for at kommunen skal gjenopprette normaltilstand og hindre gjentagelse av en hendelse. NSM anbefaler derfor at kommunen etablerer sikkerhetsovervåkning.

Videre anbefaler NSM at kommunen analyserer data fra sikkerhetsovervåkningen. Gjennom analyse av sikkerhetsrelevante data kan kommunen oppdage aktiviteter som påvirker informasjonssystemer, data og tjenester. NSM skriver at systematisert prosessering, gjennom sammenstilling og analyse av innhentet data vil bidra til å øke sannsynligheten for å avdekke hendelser.

Et prinsipp til under kategorien oppdage, er at kommunen bør gjennomføre inntrengnings-tester. Kommunen bør jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Angripere utnytter ofte svakheter i virksomhetens rutiner.

Utledede revisjonskriterier:

- Kommunen bør fastsette hvilke deler av IKT-systemet som skal overvåkes.
- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.

Håndtere og gjenopprette

Virksomhetssikkerhetsforskriften § 8 sier at ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet skal en virksomhet gjennomføre umiddelbare tiltak for å redusere skadeomfanget og gjenopprette et forsvarlig sikkerhetsnivå. Virksomheten skal vurdere konsekvensene av den sikkerhetstruende virksomheten eller avviket. Virksomhetssikkerhetsforskriften § 14 sjette ledd sier at virksomheten skal ha en plan for å gjenopprette forsvarlig sikkerhetsnivå.

For å forberede kommunen på håndtering av hendelser anbefaler NSM at kommunen etablerer et planverk for hendelseshåndtering. Uten en plan og en prosess for hendelseshåndtering vil det være vanskelig for kommunen å begrense skaden og gjenopprette normal tilstand.

Ved en hendelse er det viktig at kommunen håndtere hendelsen korrekt og med riktige ressurser slik at spredning og konsekvenser minimeres og normaltilstand opprettholdes eller gjenopprettes effektivt. For å få til dette er det viktig at kommunen har en plan for gjenoppretting som iverksettes i løpet av eller i etterkant av hendelsen.

Utledede revisjonskriterier:

- Kommunen skal ha rutiner for hendelseshåndtering og det bør foreligge en plan for hendelses håndtering.
- Kommunen skal ha en plan for gjenoppretting.

Identifisere og kartlegge

NSM skriver at kartlegging av enheter og programvare er viktig for å få oversikt over hva som befinner seg i kommunen. Det er viktig at kommunen selv får oversikt over enheter, programvare og deres sårbarheter før angripere gjør det.

Videre skriver NSM at risikobildet må vurderes knyttet opp til valget mellom sikkerhet og behovet for leveranser til kommunen. Det kan hende at kommunen må godta enheter med lavere sikkerhetsnivå enn ønsket, og det er derfor viktig at kommunen er bevisst på strategier som velges og vurderer de funksjonelle behovene opp mot risiko. Anbefalt tiltak fra NSM er å kartlegge enheter og programvare.

Det er også viktig at kommunen har oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i en kommune. En angriper har ofte som mål å øke tilgangen ved et

angrep på informasjonssystemet. Mange brukere kan ha tilganger og rettigheter til systemer og tjenester de egentlig ikke har behov for. Derfor bør tilganger og rettigheter begrenses slik at skaden fra en potensiell angriper eller utro ansatt reduseres. Derfor bør kommunen kartlegge brukere og behov for tilgang.

Utledede revisjonskriterier:

- Kommunen må ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.
- Kommunen må ha et system for styring av tilganger.

Beskytte og opprette

NSM har et prinsipp som sier at sikkerheten i anskaffelse- og utviklingsprosesser må ivaretas. Målet med prinsippet er å minimere risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter.

Et av prinsippene under denne kategorien er å etablere en sikker IKT-arkitektur. Et IKT-system består av mange sikkerhetsfunksjoner og ulike IKT-produkter fra ulike produsenter som skal fungere godt og sikkert sammen. Manglende kompatibilitet kan øke sårbarheten på en måte som angriperne kan utnytte. Videre skriver NSM at drift- og sikkerhetskonfigurasjon bør skje sentralt og likt per type enhet, hvis ikke øker risikoen for dobbeltarbeid, menneskelige feil og flere sårbarheter. IKT-systemet bør videre deles opp i forskjellige deler avhengig av tillitsnivå for å begrense risiko.

Under prinsippet om å ivareta en sikker konfigurasjon, anbefaler NSM å etablere et sentralt styrt regime for sikkerhetsoppdatering. I dette ligger det blant annet at kommunen bør installere sikkerhetsoppdatering så fort som mulig. Videre bør kommunen ha en prioriteringsliste for oppdateringer og etablere en rutine med klare ansvarsforhold for hvor ofte oppdateringer skal utføres og hvem som er ansvarlig dersom en oppdatering ikke kan gjennomføres eller må utsettes.

NSM skriver at et av prinsippene er å etablere en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap. Et av de anbefalte tiltakene er å lage en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.

Utledede revisjonskriterier:

- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.
- Kommunen bør ta ansvar for sikkerheten ved tjenesteutsetting.
- Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer.
- Kommunen må ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

Oppdage

NSM har et prinsipp som omhandler etablering av sikkerhetsovervåkning for å overvåke og samle inn relevante data for å oppdage sikkerhetshendelser og legge et grunnlag for å analysere data. Dette for at kommunen kan oppdage sikkerhetshendelser tidlig som mulig for å minimere skadeomfang eller forhindre hendelser. Det er viktig at kommunen har tilgang på tilstrekkelig data siden det kan være avgjørende for at kommunen skal gjenopprette normaltilstand og hindre gjentagelse av en hendelse. NSM anbefaler derfor at kommunen etablerer sikkerhetsovervåkning.

Videre anbefaler NSM at kommunen analyserer data fra sikkerhetsovervåkningen. Gjennom analyse av sikkerhetsrelevante data kan kommunen oppdage aktiviteter som påvirker informasjonssystemer, data og tjenester. NSM skriver at systematisert prosessering, gjennom sammenstilling og analyse av innhentet data vil bidra til å øke sannsynligheten for å avdekke hendelser.

Et prinsipp til under kategorien oppdage, er at kommunen bør gjennomføre inntrengnings-tester. Kommunen bør jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Angripere utnytter ofte svakheter i virksomhetens rutiner.

Utledet revisjonskriterier:

- Kommunen bør fastsette hvilke deler av IKT-systemet som skal overvåkes.
- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen

Håndtere og gjenopprette

For å forberede kommunen på håndtering av hendelser anbefaler NSM at kommunen etablerer et planverk for hendelseshåndtering. Uten en plan og en prosess for hendelseshåndtering vil det være vanskelig for kommunen å begrense skaden og gjenopprette normal tilstand.

Ved en hendelse er det viktig at kommunen håndtere hendelsen korrekt og med riktige ressurser slik at spredning og konsekvenser minimeres og normaltilstand opprettholdes eller gjenopprettes effektivt. For å få til dette er det viktig at kommunen har en plan for gjenoppretting som iverksettes i løpet av eller i etterkant av hendelsen.

Utledede revisjonskriterier:

- Kommunen bør ha en plan for hendelseshåndtering.
- Kommunen må ha en plan for gjenoppretting.

VEDLEGG 2 – UTTALELSE

Sømna kommune

kommunedirektør

Uttalelse fra kommunedirektøren – forvaltningsrevisjon «Informasjonssikkerhet og personvern – Sømna kommune»

Innledning

Det vises til høringsutkastet *FR1321 Informasjonssikkerhet og personvern – Sømna kommune*, datert november 2025, utarbeidet av Revisjon Midt-Norge SA på oppdrag fra kontrollutvalget.

Kommunedirektøren takker for et nyttig revisjonsarbeid som belyser både styrker og forbedringsområder i kommunens arbeid med informasjonssikkerhet og personvern. Rapporten bidrar til å synliggjøre et komplekst fagområde og gir kommunen et grunnlag for videre utvikling av styringssystemer, internkontroll og kompetanse. Sømna kommune er godt i gang med å etablere et helhetlig styringssystem, men erkjenner at det fortsatt gjenstår arbeid med risikovurderinger, opplæring og implementering av rutiner. Rapporten samsvarer i hovedsak med kommunens egen situasjonsforståelse.

Overordnet vurdering

Sømna kommune kjenner seg i stor grad igjen i revisjonens vurderinger. Det er gjort et betydelig arbeid de to siste årene for å bygge opp struktur, rolleavklaringer og rutiner, og kommunen har nå et godt fundament for videre forbedringsarbeid.

Revisjonen påpeker likevel mangler knyttet til risikovurderinger og opplæring. Disse punktene er reelle og vil få prioritet fremover. Kommunedirektøren er tilfreds med at rapporten også anerkjenner den positive utviklingen og de tiltakene som allerede er igangsatt, særlig etableringen av sikkerhetsorganisasjonen, bruk av Compilo og Samsvar, og implementeringen av ISO-baserte prinsipper i styringssystemet og innføring av sikkerhetsinstruks for alle ansatte.

Kommentarer til hovedfunn

1. Styringssystem for informasjonssikkerhet

Kommunen har etablert et styringssystem basert på ISO 27001 og 27701. Sikkerhetsorganisasjonen er opprettet, roller og ansvar er definert, og det foreligger overordnede policyer og rutiner. Arbeidet med å tilpasse og ferdigstille dokumentasjonen i Compilo fortsetter, og kommunedirektøren vil sikre at systemet er fullt implementert og operativt innen utgangen av 2026.

2. Internkontroll og risikovurderinger

Revisjonen peker på behovet for systematiske risikovurderinger og dokumenterte tiltak. Dette er et viktig forbedringsområde. Kommunen planlegger å gjennomføre helhetlige ROS-analyser og risikovurderinger innen informasjonssikkerhet og personvern i første halvår 2026, i samarbeid med Kystriket IKT.

3. Avvikshåndtering

Kommunen har stort sett en systematisk avvikshåndtering. Avvikshåndtering er tema i kommunens styringsdokument og vi har utarbeidet rutiner for å melde og behandle avvik. Avvik og tiltak tas opp i interne møter på enhetene og i strategisk ledergruppe. I tillegg gjennomgås avvik i ledelsens gjennomgang og i AMU. Tiltak som gjøres etter avvik kan være innføring av nye rutiner, endring av rutiner og innskjerping av rutiner. I meldinger til Datatilsynet blir det informert om tiltak både på kort

Sømna kommune

kommunedirektør

og lang sikt. Meldinger til Datatilsynet har ikke blitt lagt inn i vårt avvikssystem. Rutinene for dette vil nå bli endret.

4. Behandling av personopplysninger

Kommunen har etablert et strukturert system for behandlingsprotokoller i *Samsvar* og har utarbeidet de fleste nødvendige protokoller og personvernerklæringer. De resterende skal ferdigstilles i løpet av 2025. Arbeidet med personvernkonsekvensvurderinger (DPIA) er planlagt igangsatt når ny modul i Samsvar er på plass. Opplæring i DPIA vil bli gjennomført i samarbeid med personvernombudet.

5. Opplæring og kompetanse

Arbeidet i en kommune er komplekst, og det er mange tema som skal på plass også når det gjelder opplæring. Vi må tilpasse oss den daglige drift og annen opplæring som også må gjennomføres. Kommunen har en egen opplæringsplan for informasjonssikkerhet og personvern. Denne vil bli konkretisert i forhold til ansvar og tidsfrister.

6. Samarbeid med Kystriket IKT og Digitale Helgeland

Kommunen deler revisjonens vurdering av at samarbeid er avgjørende for en helhetlig sikkerhetsforvaltning. Kommunedirektøren vil arbeide for tydeligere ansvarsdeling og bedre koordinering mellom partene, herunder felles risikovurderinger, felles opplæring og erfaringsutveksling der dette er mulig.

Oppfølging og videre arbeid

Kommunedirektøren vil fortsette videreutviklingen av kommunens arbeid med informasjonssikkerhet og personvern.

Det vil spesielt bli lagt vekt på:

- Ferdigstillelse og implementering av styringssystemet ihht relevanserklæring i KINS styringssystem.
- Opplæring i ROS og DPIA
- Regelmessige risikovurderinger og dokumenterte tiltak
- Styrket opplæring og bevisstgjøring blant ansatte
- Videreutvikling av samarbeidet med Kystriket IKT

Sømna 12.11.25

Cathrine Theting
Fung. kommunedirektør

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no