Til kontrollutvalget i Bindal kommune –
Kjell Eivind Grande, leder
Gunnhild Gutvik, nestleder
Terje Moe, medlem
Jørn Petter Kveinå, medlem
Julie Tveråmo, medlem

Gjenpart går til:
Ordfører (jf. kommuneloven § 6-1)[1]
Kommunerevisjonen (jf. kommuneloven § 24-3)[1]
Kommunedirektør (til orientering – jf. kommuneloven § 13-1)[1]

Distribusjon pr. epost
Saksbehandler:
Sekretariatsleder
Tobias Langseth

INNKALLING TIL MØTE I KONTROLLUTVALGET

I samråd med utvalgets leder innkalles herved til møte som følger;

Dato: **Tirsdag 10. mars**
Tid: **kl. 12:00 – 15:00**
Sted: Rådhuset på Terråk

Til behandling:

Sak 01/2026 – Kontrollutvalgets årsrapport
Sak 02/2026 – Rapport forvaltningsrevisjon [informasjonssikkerhet og personvern]
Sak 03/2026 – Prosjektplan forvaltningsrevisjon [utenforskap og psykisk helse]
Sak 04/2026 – Aktuelle orienteringer fra administrasjonen
Sak 05/2026 – Aktuelle orienteringer fra sekretariatet
Sak 06/2026 – Eventuelt

Forfall meldes pr. telefon 909 62 145 eller epost.

Sandnessjøen 02.03.2026

Tobias Langseth (sign.)
sekretariatsleder

[1]Utdrag fra kommuneloven:

§ 6-1. Ordførerens myndighet og oppgaver

Ordføreren har møte-, tale- og forslagsrett i alle kommunale eller fylkeskommunale folkevalgte organer unntatt kommune- og fylkesråd og organer under dem. I kontrollutvalget har ordføreren likevel bare møte- og talerett. Ordføreren har bare stemmerett i organer der han eller hun er valgt medlem. Ordføreren kan la et annet medlem av kommunestyret eller fylkestinget representere seg i de organene som han eller hun ikke er medlem av.

§ 13-1. Kommunedirektør. Myndighet og oppgaver

Kommunedirektøren har møte- og talerett i alle kommunale eller fylkeskommunale folkevalgte organer, med unntak av kontrollutvalget. Kommunedirektøren kan la en av sine underordnete utøve denne retten på sine vegne.

§ 24-3. Revisors møterett, opplysningsplikt mv.

Oppdragsansvarlig revisor eller hans eller hennes stedfortreder har møte- og talerett i kontrollutvalgets møter. Revisoren har rett til å få uttalelsene sine protokollert. Møteretten gjelder likevel ikke når en sak som angår en revisors tilsettingsforhold behandles.

Til kontrollutvalget i Bindal kommune Sandnessjøen 02.03.2026

Saksbehandler:
Sekretariatsleder
Tobias Langseth

SAK 01/2026: KONTROLLUTVALGETS ÅRSRAPPORT

Innledning og bakgrunn

Kontrollutvalget skal informere kommunestyret om sitt arbeid. En årsrapport vil kunne bidra til å synliggjøre kontrollutvalgets rolle og øke kunnskapen om kontrollutvalgets oppgaver. Ut over dette er det ikke spesielle krav til innholdet i kontrollutvalgets årsrapport, og det er heller ikke formkrav.

Det er for så vidt heller ingen krav i kommunelovgivningen til årlig fremleggelse av et eget dokument, men dette er anbefalt – og i tråd med praksis hos mange av landets kontrollutvalg.

Sekretariatets vurderinger

Etter sekretariatets syn er det å anse som god tilsynsskikk at utvalget fremlegger en årlig rapport.

Sekretariatet mener at det som hovedregel er tilstrekkelig at årsrapporten dekker følgende tema:

1: Innledning og bakgrunn
2: Kontrollutvalget rolle og ansvar
3: Kontrollutvalgets sammensetning
4: Møtevirksomhet
5: Regnskapsrevisjon
6: Forvaltningsrevisjon
7: Eierskapskontroll
8: Enkeltstående kontrollsaker
9: Andre saker av betydning
10: Drift og økonomi
11: Faglig oppdatering og kompetanseutvikling
12: Oppsummering og avslutning

Oppsummering og avslutning

På bakgrunn av ovennevnte har sekretariatet utarbeidet et utkast til årsrapport, som følger vedlagt.

Årsrapportens innhold fastsettes av kontrollutvalget selv. Årsrapporten er i utgangspunktet til kommunestyrets orientering, og vil derfor normalt sett ikke være ledsaget av særskilt uttalelse eller innstilling fra kontrollutvalgets side.

Departementet konkluderer med at kommuneloven § 23-5 innebærer at kommunedirektøren skal gis anledning til å uttale seg om de sakene kontrollutvalget skal rapportere til kommunestyret etter forskrift om kontrollutvalg og revisjon §§ 3, 4 og 5. Formålet med bestemmelsen er at saken skal være mest mulig opplyst før kontrollutvalgets behandling, noe som er et alminnelig prinsipp når vedtak skal treffes. Kommunedirektøren skal gis anledning til å uttale seg til årsmelding [årsrapport] for kontrollutvalget hvis denne inneholder opplysninger om resultater av kontrollutvalgets arbeid. Spørsmålet avhenger med andre ord av årsrapportens innhold.

Sekretariatet har vurdert innholdet i utkastet til årsrapport opp mot bestemmelsens ordlyd og aktuelle tolkningsuttalelser. Kommuneloven § 23-5 kommer etter sekretariatets oppfatning til anvendelse i forbindelse med sak 01/2026, siden årsrapporten også inneholder informasjon om oppfølgingsarbeidet etter bestemmelsen i forskrift om kontrollutvalg og revisjon § 5.

På denne bakgrunn er kommunedirektøren oppfordret til å inngi uttalelse i forbindelse med utsending av møteinnkalling og saksdokumentasjon, såfremt dette er ønskelig sett fra kommunedirektørens side. Eventuell uttalelse vil i så fall bli ettersendt til kontrollutvalgets medlemmer, og tatt inn endelig årsrapport i form av eget appendiks.

Forslag til vedtak:

Utkastet til årsrapport fastsettes som fremlagt [med de endringer som ble besluttet i møtet].

Vedlegg –
1: Utkast til årsrapport 2025

1: Innledning og bakgrunn

Alle kommuner skal i henhold til kommunelovens bestemmelser ha et kontrollutvalg, som utpekes av kommunestyret. Utvalget skal etter gjeldende kommunelov ha minimum 5 medlemmer, og minst ett av dem skal velges blant kommunestyrets medlemmer. Det er gitt regler om valgbarhet – som blant annet utelukker alle ansatte i kommunen, enkelte folkevalgte og medlemmer av folkevalgte organer samt personer som har visse roller i selskap kommunen har eierinteresser i. Kommunens ordfører og revisor har møte- og talerett i kontrollutvalgets møter.

I likhet med andre folkevalgte organ, er hovedregelen at saker behandles og vedtak treffes i møter. Enhver har rett til å overvære møtene, med mindre møtet er vedtatt lukket. Kommunestyret skal sørge for at det stilles tilfredsstillende sekretariatsbistand til disposisjon. Sekretariatet skal påse at de saker som behandles av kontrollutvalget er forsvarlig utredet og at utvalgets vedtak blir iverksatt. Sekretariatet skal være uavhengig av kommunens administrasjon.

Kontrollutvalget kan hos kommunen, uten hinder av taushetsplikt, kreve enhver opplysning, redegjørelse eller ethvert dokument og foreta de undersøkelser som utvalget finner nødvendig for å gjennomføre oppgavene.

2: Kontrollutvalgets rolle og ansvar

Kontrollutvalget fører løpende kontroll med den kommunale forvaltningen på vegne av kommunestyret. Kommunestyret har det øverste ansvaret for å kontrollere kommunens virksomhet.

Kontrollutvalget skal påse at kommunens regnskaper blir revidert på en betryggende måte. Når kontrollutvalget har blitt forelagt revisjonsberetningen fra revisor, skal utvalget avgi uttalelse om årsregnskapet og årsberetningen før fastsetting av kommunestyret.

Kontrollutvalget skal videre påse at det føres kontroll med at den økonomiske forvaltningen foregår i samsvar med gjeldende bestemmelser og vedtak [etterlevelseskontroll], og at det blir gjennomført systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets vedtak [forvaltningsrevisjon]. Forvaltningsrevisjon utføres både av kommunens virksomhet og av selskaper kommunen har eierinteresser i. Kontrollutvalget skal påse at det føres kontroll med forvaltningen av kommunens interesser i selskaper mv. [eierskapskontroll]. Eierskapskontroll innebærer å kontrollere om den som utøver kommunens eierinteresser, gjør dette i samsvar med lover og forskrifter, kommunestyrets vedtak og anerkjente prinsipper for eierstyring.

Kontrollutvalget skal også påse at de vedtak som kommunestyret fatter ved behandlingen av revisjonsrapporter blir fulgt opp.

Dette utelukker selvsagt ikke at kontrollutvalget behandler enkeltstående kontrollsaker.
Siden kontrollutvalget er et organ for kontroll med den kommunale forvaltningen, er det naturlig at utvalget først og fremst betrakter enkeltsaker ut fra et systemperspektiv. Et kontrollutvalg behandler selv verken ordinære forvaltningssaker eller fatter enkeltvedtak, og er heller ikke et klageorgan. Som hovedregel prioriterer utvalget på selvstendig grunnlag hvilke forhold som er aktuelt å bruke tid og andre ressurser på. Man vil normalt sett tillegge sakenes potensial for læring og kvalitetsforbedring en del vekt, siden dette er et av hovedmålene med kontrollarbeidet.

Kontrollutvalget skal utarbeide forslag til budsjettramme for det samlede kontrollarbeidet i kommunen. Utvalget skal dessuten utarbeide innstilling til valg eller endring av revisjonsordning for kommunen, samt valg av revisor – i den grad spørsmålet er gjenstand for vurdering.

3: Kontrollutvalgets sammensetning

I 2025 har utvalget bestått av følgende representanter:

Kjell Eivind Grande, leder
Gunnhild Gutvik, nestleder
Terje Moe, medlem
Jørn Petter Kveinå, medlem
Julie Tveråmo, medlem

Det er valgt i alt 5 varamedlemmer, som innkalles i rekkefølge.

4: Møtevirksomhet

Kontrollutvalget har avholdt 4 møter i løpet av året og behandlet 20 saker.

5: Regnskapsrevisjon

Kontrollutvalget har avgitt uttalelse om kommunens årsregnskap og årsberetning for 2024. Revisors beretning var uten modifikasjoner.

Kontrollutvalget har hatt skriftlig uttalelse om resultatet av forenklet etterlevelskontroll med økonomiforvaltningen etter kommuneloven § 24-9 for regnskapsåret 2024 til behandling. Kontrollen dreide seg om etterlevelse av rutinene for oppfølging av kommunens bundne egenkapitalfond. Det ble avgitt en positiv uttalelse fra revisors side. Kontrollutvalget forutsatte likevel at kommunens administrasjon i nødvendig grad følger opp årets etterlevelseskontroll, og vurderer aktuelle forbedringstiltak. Jf. RSK 301 punkt 18.

Kontrollutvalget har fått orienteringer om revisjonsstrategi og har ellers holdt seg løpende orientert om revisjonsarbeidet gjennom regnskapsrevisors deltakelse på flere av kontrollutvalgets møter.

6: Forvaltningsrevisjon

Forvaltningsrevisjonsprosjektet «Tidlig innsats og spesialpedagogisk hjelp/spesialundervisning» ble gjennomført i 2023/24. Kontrollutvalget behandlet rapporten 25.11.2024. Kommunestyret sluttet seg 12.12.2024 til kontrollutvalgets uttalelse i tilknytning til rapporten. Kontrollutvalget fulgte opp kommunestyrets vedtak gjennom sak 11/2025 [møte 06.10.2025]. Utvalget har ingen spesielle merknader til iverksatte og planlagte tiltak.

Kontrollutvalget foretok gjennom sak 16/2024 [møte 25.11.2024] bestilling av et forvaltningsrevisjonsprosjekt knyttet til temaet «Informasjonssikkerhet og personvern». Rapport fra denne revisjonen ble levert 20.11.2025, og vil bli behandlet i løpet av 1. kvartal 2026.

Kontrollutvalget har i skrivende stund følgende prosjekter i bestilling:

- Utenforskap og psykisk helse [sak 17/2025, møte 10.11.2025]

Kontrollutvalget vil løpende rapportere resultatet av gjennomførte forvaltningsrevisjoner til kommunestyret, samt påse at de vedtak som kommunestyret fatter ved behandlingen av forvaltningsrevisjonsrapporter har blitt fulgt opp. Jf. kommuneloven § 23-2 første ledd bokstav e.

7: Eierskapskontroll

Det er ikke gjennomført eierskapskontrollprosjekter i løpet av året, grunnet ressurshensyn og avveininger knyttet til risiko og vesentlighet.

Kontrollutvalget vil løpende rapportere resultatet av gjennomført eierskapskontroll til kommunestyret, samt påse at de vedtak som kommunestyret fatter ved behandlingen av rapporter fra eierskapskontroll har blitt fulgt opp. Jf. kommuneloven § 23-2 første ledd bokstav e.

8: Enkeltstående kontrollsaker

Utvalget fått orienteringer fra kommunens administrasjon om ulike tema av relevans for kontrollutvalgets rolle i den folkevalgte delen av kommunens egenkontroll.

Skriftlige henvendelser til kontrollutvalget behandles i varierende grad som egen sak, og avsender gis som hovedregel en skriftlig tilbakemelding på henvendelsen når kontrollutvalgets arbeid med saken er avsluttet. Det er ikke mottatt slike henvendelser i løpet av året, og kontrollutvalget har heller ikke på eget initiativ fokusert på isolerte hendelser eller saker – ut over å holde seg orientert om aktuelle forhold av interesse for utvalget.

Kontrollutvalget vurderer som hovedregel selv hvilke problemstillinger som er innenfor tilsynsmandatet gitt i kommuneloven. Kontrollutvalget må dessuten uansett foreta en prioritering av så vel økonomiske som andre ressurser utvalget disponerer over.

9: Andre saker av betydning

Den som foretar revisjon skal løpende vurdere sin uavhengighet. Oppdragsansvarlig revisor skal hvert år, og ellers ved behov, avgi en skriftlig egenvurdering av sin uavhengighet til kontrollutvalget. Jf. § 19 i forskrift om kontrollutvalg og revisjon. Gjennom uavhengighetserklæringer til kontrollutvalget fra oppdragsansvarlig for hhv. regnskapsrevisjon og forvaltningsrevisjon, har revisor dokumentert skriftlig de forhold som ifølge lov og forskrift kan ha betydning for spørsmålet om uavhengighet, og som derfor skal vurderes løpende. Kontrollutvalget har lagt vekt på å legge til rette for en god dialog mellom utvalget og kommuneadministrasjonen, blant annet gjennom å invitere kommunedirektør til å delta i utvalgets møter.

10: Drift og økonomi

Når det gjelder revisjonsoppgavene, deltar kommunen i samvirkeforetaket Revisjon Midt-Norge. I følge § 6 i selskapets vedtekter fastsettes både årsbudsjett og økonomiplan av årsmøtet, etter forslag fra styret. Virksomhet organisert som samvirkeforetak er derfor i likhet med IKS indirekte underlagt folkevalgt styring i forretningsmessige forhold.

Videre deltar kommunen i et interkommunalt samarbeid om sekretariatsbistand [SE-KON]. Enheten er organisert som et kommunalt oppgavefellesskap etter reglene i kommunelovens kapittel 19. Representantskapet fastsetter i medhold av samarbeidsavtalen årsbudsjett og fordeling av kostnaden på deltakerkommunene, basert på et folketallsprinsipp. I alt 11 kommuner deltar for tiden i det interkommunale samarbeidet om sekretariattjenester.

Med henblikk på kontrollutvalgets egne kostnader, eksempelvis møtegodtgjørelse og reiseutgifter, inngår dette direkte i kommuneregnskapet. Det varierer hvordan dette løses budsjetteknisk, men kontrollutvalgets forslag til budsjettramme for det samlede kontrollarbeidet i kommunen inneholder slike kostnader – så vel som kostnadene til kjøp av revisjonstjenester og sekretariatsbistand.

Så langt kontrollutvalget kjenner til, har kostnadene samlet sett vært som forventet i 2025.

11: Faglig oppdatering og kompetanseutvikling

Utvalgets medlemmer gis innenfor budsjettrammene tilbud om deltakelse på kontrollutvalgskonferansen, som arrangeres årlig i regi av NKRF [– kontroll og revisjon i kommunene].

Sekretariatsenheten er medlem i NKRF og deltar på kurs og konferanser som arrangeres av denne yrkesfaglige interesseorganisasjonen. NKRFs årsmøte vedtok i 2018 å utvide reglene for obligatorisk etter- og videreutdanning til også å omfatte personlige medlemmer som utfører sekretariatsoppgaver for kontrollutvalg med virkning fra 2019. Tilsvarende regler har vært gjeldende siden 2001 for de personlige medlemmene som utfører lovbestemt revisjon. Formålet er å vedlikeholde og utvikle medlemmenes kompetanse, noe som gir trygghet for høy faglig kvalitet på revisjon og sekretariatsbistand som utøves av NKRFs medlemmer.

12: Oppsummering og avslutning

Kontrollutvalget legger med dette frem årsrapporten til kommunestyrets orientering. Hovedhensikten er å gi kommunestyret som oppdragsgiver et bilde av kontrollutvalgets aktivitet samt utvalgets rolle i kommunens egenkontroll.

Årsrapporten inneholder også informasjon om oppfølgingsarbeidet etter bestemmelsen i forskrift om kontrollutvalg og revisjon § 5. Kontrollutvalget anmoder derfor om at kommunestyret behandler rapporten som egen sak. I denne forbindelse er kommunedirektøren gitt anledning til å uttale seg før kontrollutvalget behandlet rapporten, jf. kommuneloven § 23-5. I den grad slik uttalelse er avgitt, er denne tatt inn i årsrapporten i form av eget appendiks.

Terråk 10.03.2026

Kontrollutvalget i
Bindal kommune

Til kontrollutvalget i Bindal kommune Sandnessjøen 02.03.2026

Saksbehandler:
Sekretariatsleder
Tobias Langseth

SAK 02/2026: RAPPORT FR [INFORMASJONSSIKKERHET & PERSONVERN]

1: Innledning og bakgrunn

Revisjon Midt-Norge har på oppdrag fra kontrollutvalget utført forvaltningsrevisjonsprosjektet «Informasjonssikkerhet og personvern» og oversendt endelig rapport datert 20. november 2025. Kommunedirektøren ble gitt anledning til å uttale seg om foreløpig rapport. Høringssvaret er gjengitt i rapportens vedlegg 2 [side 64–67]. Jf. kapittel 1.5 [side 12].

Revisjonsprosjektet har undersøkt følgende problemstillinger:

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

2: Kontrollutvalgets oppgaver og rolle

Kontrollutvalgets oppgave er i denne sammenheng å behandle forvaltningsrevisjonsrapporten, og avgi rapport til kommunestyret om at prosjektet er gjennomført samt hvilke resultat revisjonen har gitt. Jf. bestemmelsen i forskrift om kontrollutvalg og revisjon § 4:

> **§ 4. Kontrollutvalgets rapportering om forvaltningsrevisjoner og eierskapskontroller**
>
> Kontrollutvalget skal rapportere til kommunestyret eller fylkestinget om gjennomførte forvaltningsrevisjoner og eierskapskontroller og resultatet av dem.

Kontrollutvalget skal også påse at kommunestyrets vedtak i tilknytning til behandlingen av rapporter om forvaltningsrevisjon følges opp, samt rapportere til kommunestyret om hvordan kommunestyrets vedtak er fulgt opp. Jf. bestemmelsene i forskrift om kontrollutvalg og revisjon § 5.

3: Forvaltningsrevisjonsrapportens konklusjoner

Jf. rapportens avsnitt 5.1 [side 53–54].

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

På den første problemstillingen, om styringssystem for informasjonssikkerhet, konkluderer revisor med at kommunen har lagt et grunnlag for styringssystem som inneholder ledelsessystem og internkontroll for personvern, men i mindre grad informasjonssikkerhet, utover det som gjelder personvern.

Styringssystemet er i liten grad oppdatert siden brevkontrollen i 2023. Det er lagt et grunnlag for kunnskap og bevissthet i kommunen gjennom det arbeidet som ble gjennomført i 2023, og i det er gjort arbeid etter det for å få på plass et overordna styringssystem for informasjonssikkerhet og personvern.

Kommunen arbeider med å etablere et system for behandlingsprotokoller og vurdering av personvernkonsekvenser (DPIA) med bistand fra personvernombudet.

Kommunen har gjennomført kampanjer og informasjonstiltak for informasjonssikkerhet i organisasjonen. Kommunen har forbedringsmuligheter når det gjelder systematiske opplæringstiltak i informasjonssikkerhet.

Noe av informasjonen som revisor har fått, tilsier at det fortsatt er behov for å avklare hva som er kommunen sine oppgaver og hva som er Kystriket IKT sine oppgaver overfor kommunen.

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

På den andre problemstillingen, om organisatoriske og tekniske tiltak, konkluderer revisor med at Bindal kommune i stor grad har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet gjennom samarbeidet i Kystriket IKT.

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.

4: Forvaltningsrevisjonsrapportens anbefalinger

Jf. rapportens avsnitt 5.2 [side 54].

Revisor anbefaler kommunedirektøren å:

- Videreutvikle og ajourholde det overordna ledelsessystemet for informasjonssikkerhet og personvern
- Avklare ansvarsforhold mellom Bindal kommune og Kystriket IKT sitt arbeid
- Styrke opplæringen i informasjonssikkerhet
- Vurdere hvilke systemer og funksjoner som må prioriteres hvis datasystemer ikke er tilgjengelig og eventuelt må gjenopprettes

5: Sekretariatets vurderinger

Under forutsetning av at sekretariatet oppfatter rapporten riktig, konkluderer revisor i varierende grad positivt på problemstillingen knyttet til etablering av styringssystem for informasjonssikkerhet, og i stor grad positivt når det gjelder iverksetting av tilfredsstillende organisatoriske og tekniske tiltak for å ivareta hensynet til informasjonssikkerhet.

Rapporten inneholder forslag hva kommunen kan vektlegge i eget forbedringsarbeid [avsnitt 5.2].

Når det gjelder revisjonskriterier, metodevalg og datagrunnlag vises det til rapportinnholdet.

Forvaltningsrevisjonsprosjektet vil bli presentert av Revisjon Midt-Norge i møtet.

Av kommuneloven fremgår:

§ 23-5. *Rapportering til kommunestyret eller fylkestinget*
Kontrollutvalget skal rapportere resultatene av sitt arbeid til kommunestyret eller fylkestinget. I saker som skal oversendes til kommunestyret eller fylkestinget, skal kommunedirektøren gis anledning til å uttale seg før kontrollutvalget behandler saken.

Utkast til saksfremlegg har i tråd med denne bestemmelsen blitt forelagt kommunedirektøren.

Sekretariatet har vært i dialog med kommuneadministrasjonen. Tilbakemeldingen er at det ikke er behov for en særskilt [skriftlig] uttalelse til kontrollutvalgets sak.

Forslag til vedtak:

Kontrollutvalget tar forvaltningsrevisjonsrapporten «Informasjonssikkerhet og personvern» avgitt 20.11.2025 til etterretning, og oversender denne til kommunestyret i Bindal kommune for videre behandling.

I denne forbindelse uttaler kontrollutvalget følgende:

Revisjonsprosjektet har undersøkt følgende problemstillinger:

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

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

Revisor konkluderer i varierende grad positivt på problemstillingen knyttet til etablering av styringssystem for informasjonssikkerhet, og i stor grad positivt når det gjelder iverksetting av tilfredsstillende organisatoriske og tekniske tiltak for å ivareta hensynet til informasjonssikkerhet. Utvalget henviser til rapportens innhold for nærmere detaljer.

Kontrollutvalget ber kommunedirektøren merke seg rapportens anbefalinger og forbedringsforslag.

Kontrollutvalget ber videre kommunedirektøren rapportere skriftlig til kontrollutvalget hvordan a) kommunestyrets vedtak er fulgt opp og b) hvilke forbedringstiltak som er iverksatt.

Frist for kommunedirektørens rapportering til kontrollutvalget settes til 6 måneder etter dato for kommunestyrets behandling av forvaltningsrevisjonsrapporten.

Kontrollutvalgets forslag [innstilling] til kommunestyrevedtak er ut fra dette:

Kommunestyret slutter seg til kontrollutvalgets uttalelse.

Kontrollutvalget understreker imidlertid at kommunestyret, som har det øverste ansvaret for å kontrollere kommunens virksomhet, vurderer både rapporten og kontrollutvalgets uttalelse på fritt grunnlag, og at utvalgets innstilling selvsagt ikke utelukker at kommunestyret har egne merknader. Avslutningsvis bemerkes det fra kontrollutvalgets side at et av hovedformålene med kontrollarbeidet i kommunen er å bidra til læring og kvalitetsforbedring over tid. Utvalgets innfallsvinkel er derfor at eventuelle avvik først og fremst bør betraktes i et systemperspektiv.

Vedlegg –
1: Revisjonsrapport avlagt 20.11.2025

Appendiks 1 – Utdrag fra kommuneloven

Lov om kommuner og fylkeskommuner (kommuneloven) - Lovdata

§ 23-3. *Forvaltningsrevisjon*

Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak.

Kontrollutvalget skal minst én gang i valgperioden, og senest innen utgangen av året etter at kommunestyret eller fylkestinget er konstituert, utarbeide en plan som viser på hvilke områder det skal gjennomføres forvaltningsrevisjoner. Planen skal baseres på en risiko- og vesentlighetsvurdering av kommunens eller fylkeskommunens virksomhet og virksomheten i kommunens eller fylkeskommunens selskaper. Hensikten med risiko- og vesentlighetsvurderingen er å finne ut hvor det er størst behov for forvaltningsrevisjon.

Planen skal vedtas av kommunestyret og fylkestinget selv. Kommunestyret og fylkestinget kan delegere til kontrollutvalget å gjøre endringer i planen.

§ 23-5. *Rapportering til kommunestyret eller fylkestinget*

Kontrollutvalget skal rapportere resultatene av sitt arbeid til kommunestyret eller fylkestinget. I saker som skal oversendes til kommunestyret eller fylkestinget, skal kommunedirektøren gis anledning til å uttale seg før kontrollutvalget behandler saken.

RM Revisjon Midt-Norge

Informasjonssikkerhet og personvern

Bindal kommune

Forvaltningsrevisjon

2025

FR1319

FORORD

Denne forvaltningsrevisjonen er gjennomført på oppdrag fra kontrollutvalget i Bindal kommune. Forvaltningsrevisjonen er gjennomført etter NKRFs (Kontroll og revisjon i kommunene) standard, Standard for forvaltningsrevisjon (RSK 001)

Vi vil takke alle som har bidratt med informasjon i prosjektet.

Alle rapporter fra Revisjon Midt-Norge SA publiseres på www.revisjonmidtnorge.no.

Trondheim, 20.11.2025

Anna Ølnes

Oppdragsansvarlig forvaltningsrevisor

Margrete Haugum

Prosjektmedarbeider

SAMMENDRAG

Revisjon Midt-Norge har gjennomført forvaltningsrevisjonen om informasjonssikkerhet og personvern på oppdrag fra kontrollutvalget i Bindal kommune. Forvaltningsrevisjonen har undersøkt følgende problemstillinger:

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

På den første problemstillingen, om styringssystem for informasjonssikkerhet, konkluderer revisor med at kommunen har lagt et grunnlag for styringssystem som inneholder ledelsessystem og internkontroll for personvern, men i mindre grad informasjonssikkerhet utover det som gjelder personvern.

Styringssystemet er i liten grad oppdatert siden brevkontrollen i 2023. Det er lagt et grunnlag for kunnskap og bevissthet i kommunen gjennom det arbeidet som ble gjennomført i 2023, og i det arbeidet som er gjort etter det, for å få på plass et overordna styringssystem for informasjonssikkerhet og personvern.

Kommunen arbeider med å etablere et system for behandlingsprotokoller og vurdering av personvernkonsekvenser (DPIA) med bistand fra personvernombudet.

Kommunen har gjennomført kampanjer og informasjonstiltak for informasjonssikkerhet i organisasjonen. Kommunen har forbedringsmuligheter når det gjelder systematiske opplæringstiltak i informasjonssikkerhet.

Noe av informasjonen som revisor har fått, tilsier at det fortsatt er behov for å avklare hva som er kommunen sine oppgaver og hva som er Kystriket IKT sine oppgaver overfor kommunen.

På den andre problemstillingen, om organisatoriske og tekniske tiltak, konkluderer revisor med at Bindal 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.

Revisor anbefaler kommunedirektøren å:

- Videreutvikle og ajourholde det overordna ledelsessystemet for informasjonssikkerhet og personvern
- Avklare ansvarsforhold mellom Bindal kommune og Kystriket IKT sitt arbeid
- Styrke opplæringen i informasjonssikkerhet
- Vurdere hvilke systemer og funksjoner som må prioriteres hvis datasystemer ikke er tilgjengelig og eventuelt må gjenopprettes

INNHOLDSFORTEGNELSE

1 INNLEDNING

1.1 Bestilling

Kontrollutvalget i Bindal kommune bestilte i sak 16/2024 forvaltningsrevisjon med tema informasjonssikkerhet. Prosjektplanen som ble lagt fram i samme sak ble lagt til grunn for gjennomføringen av prosjektet.

Tilsvarende bestilling ble vedtatt i kontrollutvalgene i Brønnøy, Sømna og Vega kommuner, hvor tilsvarende prosjektplan ble lagt fram og vedtatt.

1.2 Problemstillinger

Problemstillingene som er belyst, er:

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?

Ansvaret for informasjonssikkerhet og personvern i Bindal kommune ligger til kommunedirektøren og de funksjonene i kommunen som kommunedirektøren har delegert ansvaret til. Bindal kommune har, sammen med Brønnøy, Vega, Sømna 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. Samarbeidet rundt Kystriket er nærmere beskrevet i kapittel 2.

Bindal kommune er også en del av Digitale Helgeland KO, som i likhet med Kystriket er et oppgavefellesskap mellom 19 kommuner, hvor Brønnøy kommune er kontorkommune. Digitale Helgeland står for digitale utviklingsprosjekt for deltakerkommunene. Personvernombudet for alle kommunene er tilknyttet Digitale Helgeland. Informasjon knyttet til Digitale Helgeland er nærmere beskrevet i kapittel 2.

Den første problemstillingen gjelder ansvaret som kommunen skal ivareta innenfor egen organisasjon, i tillegg til gjennom kommunens personvernombud, som er tilknyttet Digitale Helgeland. Den andre problemstillingen berører i hovedsak tjenester som ivaretas gjennom Kystriket IKT.

1.3 Bakgrunn

1.3.1 Informasjonssikkerhet

Informasjonssikkerhet handler om å sikre informasjon i alle former. Informasjon er noe som behandles i et samspill mellom mennesker, prosesser og teknologi. Informasjonssikkerhet handler om å sikre informasjonsbehandling som inngår i oppgaver og tjenester. Det er dreier seg om informasjonen som inngår i digitale tjenester, IKT-tjenester, tilrettelegging av utførelse av oppgaver som ivaretar god sikkerhet og å sikre tilstrekkelig kompetanse hos de som utfører oppgavene, samt å jobbe for en kultur som understøtter arbeidet med informasjonssikkerheten.[1] Informasjonssikkerhet handler om å ivareta:

- Konfidensialitet – at informasjonen ikke blir kjent for uvedkommende,
- Integritet – at informasjonen ikke blir endret utilsiktet eller av uvedkommende,
- Tilgjengelighet – at informasjonen er tilgjengelig ved behov.

Norske kommuner behandler store mengder personopplysninger om sine innbyggere og ansatte, og har ansvaret for å ivareta opplysningen på en forsvarlig måte. I tillegg har norske kommuner samfunnskritiske oppgaver og sitter på opplysninger om sin egen virksomhet, blant annet informasjon om kommunalt vann og avløp. Betydningen av å ivareta kommunens informasjonsbehov og beskyttelse er stor.

Datatilsynet gjennomførte i 2023 et tilsyn med et stort antall norske kommuner om personopplysningssikkerheten.[2] Gjennomgangen viser at mange kommuner mangler overordnede retningslinjer og praktiske rutiner/prosedyrer innenfor temaene som ble kontrollert. Blant annet skriver Datatilsynet at majoriteten av kommunene mangler tilstrekkelig overordnede retningslinjer for arbeidet med vurdering av risiko, men mange kommuner har rutiner og skjema for hvordan gjennomføre en risiko- og sårbarhetsanalyse. Resultatet viser at 60 av 94 kommuner har svært mangelfulle eller mangler en overordnet sikkerhetsstrategi. I sin presentasjon av rapporten[3] forteller Datatilsynet at mye av ansvaret for informasjonssikkerhet er lagt til de som jobber med IKT i kommunen, og ikke overordnet ledelse.

---

[1] https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-en-forutsetning-na-virksomhetens-mal/1123

[2] https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/funn-fra-tilsyn-i-kommuner-og-fylkeskommuner/

[3] Basert på revisors notater fra presentasjonen den 9. november 2023, opptak tilgjengelig på https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/seminar-om-kommunetilsyn/

Brudd på informasjonssikkerheten kan få følger for tjenestenivå, økonomi og ansatte. For kommuner kan brudd få betydning for innbyggerne. Vi har sett flere eksempler på kommuner som opplever brudd på informasjonssikkerheten, blant annet er dataangrepet mot Østre Toten i 2021 et kjent eksempel på dette. Dataangrep kan også skje for dem som leverer tjenester til kommunen.[4] Derfor er det viktig at kommuner sørger for sikre arbeidet med informasjonssikkerhet for å redusere risikoen for brudd på informasjonssikkerheten.

1.3.2 Regelverk

Det er minst tre juridiske tilnærmeringer til arbeidet med informasjonssikkerhet. Disse er:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)[5]
- Lov om behandling av personopplysninger (Personopplysningsloven)[6]
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), § 15 om internkontroll på informasjonssikkerhetsområdet.[7]

I tillegg har lov om digital sikkerhet (Digitalsikkerhetsloven)[8] tredd i kraft fra 1. oktober 2025 med tilhørende forskrift. Loven gjelder blant annet for tilbydere av samfunnsviktige tjenester innen energi, transport, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur.

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. Virksomhetsikkerhetsforskriften[9] definerer i § 3 kravet om at virksomheter som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.

Personopplysningsloven gir bestemmelser om hvordan personopplysninger skal behandles. Loven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven gjennomfører EUs personvernforordning i norsk

[4] https://www.nrk.no/innlandet/flere-kommuner-rammet-av-dataangrep-1.17484210

[5] Lov Om Nasjonal Sikkerhet (Sikkerhetsloven) (2018).

[6] Lov Om Behandling Av Personopplysninger (Personopplysningsloven), Pub. L. LOV-2018-06-15-38 (2018), https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=lov%20om%20behandling%20av%20personopplysninger.

[7] Digitaliserings- og forvaltningsdepartementet, *Forskrift Om Elektronisk Kommunikasjon Med Og i Forvaltningen (EForvaltningsforskriften)*, 2004.

[8] Lov Om Digital Sikkerhet (Digitalsikkerhetsloven) (2023).

[9] Justis- og beredskapsdepartementet, *Forskrift Om Virksomheters Arbeid Med Forebyggende Sikkerhet (Virksomhetssikkerhetsforskriften)*, 2018.

rett. Personopplysningsloven er bygget på noen grunnleggende prinsipper, og alle som behandler personopplysninger må følge disse prinsippene.

eForvaltningsforskriften har som formål å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Forskriften krever at forvaltningsorganet skal ha en internkontroll på informasjonssikkerhetsområdet og som bør være integrert som en del av virksomhetens helhetlige styringssystem. eForvaltningsforskriften krever blant annet at mål og strategier for informasjonssikkerhet er beskrevet gjennom sikkerhetsmål og sikkerhetsstrategi, som skal danne grunnlaget for internkontrollen på området.

1.3.3 Avgrensning

Personvern er i stor grad regulert av personopplysningsloven herunder personvern-forordningen, og stiller omfattende krav til behandling av personopplysninger. Revisjonen har ikke kapasitet til å gå i dybden på alle de spesifikke kravene som omhandler behandling av personopplysninger, men vil ha oppmerksomheten 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.

1.4 Metode

Forvaltningsrevisjonen er gjennomført i henhold til NKRFs standard for forvaltningsrevisjon, RSK 001. Revisor har vurdert egen uavhengighet overfor Bindal kommune, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3.

Vi har brukt flere metoder for å samle inn data til dette prosjektet.

Oppstartsmøte

Etter at kontrollutvalget vedtok prosjektplanen, ble det gjennomført oppstartmøte den 25.03.2025. Formålet med møtet var gjensidig, overordna informasjon rundt problemstillinger og revisjonskriterier. Fra kommunen deltok kommunedirektør, Fagleder IKT, arkivleder og HR-sjef. På oppstartsmøtet fikk revisor oppnevnt en kontaktperson fra kommunen i forbindelse med revisjonsprosessen. Arkivleder har vært kontaktperson, og har stått for oversendelse av ulike dokument og koordinering av intervjuavtaler.

Det ble skrevet referat fra oppstartsmøtet som er verifisert av kommunens deltakere. Informasjonen i det verifiserte referatet er brukt i rapporten.

Intervju

For å belyse den første problemstillingen har vi gjennomført intervju med:

- HR-sjef (ansvarlig for informasjonssikkerhet i kommunen),
- Arkivleder
- Fagleder IKT (driftsleder i Kystriket).

Det ble stilt spørsmål om kommunens arbeid med informasjonssikkerhet, og hva som er utarbeidet av strategier, rutiner og prosedyrer for området. Videre, ble det stilt spørsmål om hvordan de opplever at informasjonssikkerheten er i kommunen. Størstedelen av stillingen til fagleder for IT er som driftsleder i Kystriket IKT. Han ble derfor også intervjuet om organisatoriske og tekniske tiltak, som den andre problemstillingen belyser.

I tillegg til driftsleder i Kystriket (fag leder IKT i Bindal), er det flere ansatte i Brønnøy kommune og de andre kommunene som jobber for Kystriket, med oppgaver for de andre deltakerkommunene, deriblant Bindal. Dette er:

- Leder i Kystriket
- Medarbeider – systemutvikling
- Medarbeider – brukerstøtte
- Medarbeider – nettverk

Alle intervjuene er gjennomført som individuelle intervju. Det ble skrevet referat fra intervjuene som er godkjent og som inngår i rapportens datagrunnlag.

Dokumentgjennomgang

Vi har etterspurt kommunens styrende dokumenter for informasjonssikkerhet og avtaledokumenter som gjelder Kystriket IKS og Digitale Helgeland:

- Brevkontroll fra Datatilsynet - Svar på brevkontroll fra Bindal kommune
- Sikkerhetsorganisasjon og ansvar
- Internkontroll system
- ROS informasjon sikkerhet
- Samlet oversikt, sortert, protokoller
- Styrende retningslinjer for sikkerhetskopiering
- Styrende løsninger for autentiseringsløsninger og gjenoppretting av systemer
- Avtaler mellom Bindal kommune og Kystriket
- Samarbeidsavtale-kommunalt-oppgavefellesskap, Digitale Helgeland KO

- Avtale Kystriket IKT og Iteam – avtale følger vedlagt uten vedlegg. Gi beskjed om dere også ønsker vedleggene.

Vurdering av metode

Personene som ble intervjuet i Bindal kommune ble valgt på bakgrunn av at disse ble oppgitt som nøkkelpersoner med ansvar og roller knyttet til strategi og rutiner for informasjonssikkerhet og personvern i Bindal kommune. Vi kunne fått annen informasjon dersom vi intervjuet utvalgte ledere og ansatte i organisasjonen som ikke har et slikt ansvar eller rolle. Vi mener likevel at intervjuinformasjonen fra disse tre nøkkelfunksjonene, sammen med skriftlig dokumentasjon, er den som best dekker den første problemstillingen og kriterier.

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. 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.

Alt i alt er datagrunnlaget tilfredsstillende og tilstrekkelig for å svare ut problemstillingene.

1.5 Uttalelse om rapport

En foreløpig rapport ble sendt til kommunedirektøren for uttalelse den 6.11.2025. Revisjon Midt-Norge mottok uttalelse fra kommunedirektøren den 18.11.2025. Uttalelsen er vedlagt rapporten (vedlegg 2).

Uttalelsen inneholder presiseringer informasjon i datadelene, som ikke endrer på revisors vurderinger, konklusjoner og anbefalinger. Flere av presiseringene gjelder justeringer som har skjedd etter at intervjuene fant sted og referatene ble verifisert. Revisor har korrigert rapporten etter alle forslagene fra kommunedirektøren. Etter at rapporten har vært på høring, er det skrevet sammendrag. Sidetallene som det vises til i uttalelsen har derfor forskjøvet seg en side.

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**[10] 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 Bindal kommune vedtok samarbeidsavtalen i sak 92/2023, den 14.11.2023 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 2023)

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

- Bemanning av førstelinje brukerstøtte på vegne av alle deltakerkommunene

[10] 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.

- 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. I tillegg har Vevelstad en ansatt som jobber innenfor Kystriket. De som jobber for Kystriket IKT, har ulik kompetanse. (Samarbeidsavtalen 2023)

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 kommunene. (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@bindal.kommune kan logge seg på å få tilgang til Bindal 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 på å kunne skille de enkelte kommunene sine data, spesielt i forhold til personopplysninger. (Driftsavtalen 2023)

2.3 Digitale Helgeland

Digitale Helgeland er et kommunalt oppgavefellesskap med 19 kommuner[11]. Det er kommunene Alstahaug, Bindal, Brønnøy, Dønna, Grane, Hattfjelldal, Hemnes, Herøy, Leirfjord, Lurøy, Meløy, Nesna, Rana, Rødøy, Sømna, Træna, Vefsn, Vega og Vevelstad.[12]

Representantskapet er Digitale Helgeland sitt øverste organ, som velger et styre bestående av et styremedlem og et varamedlem fra hver deltakerkommune. Kommunedirektørene velges

[11] 3 nye kommuner høsten 2025 (Træna, Rødøy og Meløy).

[12] Organisering - Digitale Helgeland, lastet ned 18.10.2025/ sak 49/25, Bindal kommunestyre

som styremedlem. Brønnøy kommune er kontorkommune og medarbeiderne i Digitale Helgeland skal være ansatt i kontorkommunen. Digitale Helgeland leier kontorlokaler i den 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 viktig 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 rådgiver 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 STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET

I dette kapittelet belyser vi problemstillingen om styringssystem for informasjonssikkerhet.

3.1 Problemstilling

Problemstillingen som er belyst er:

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

3.2 Ledelsessystem for informasjonssikkerhet

I dette delkapitlet ser vi på om det er utarbeidet ledelsessystem for informasjonssikkerhet. Med ledelsessystem for informasjonssikkerhet legger vi Audun Jøsangs forklaring til grunn:

> Ledelsessystem for informasjonssikkerhet er en samling av dokumenterte samvirkende prosesser og aktiviteter for informasjonssikkerhet som organisasjonen har definert basert på anerkjente standarder, rammeverk og retningslinjer, samt egendefinerte policyer og prosedyrer. Kalles system fordi det representerer en systematisk tilnærming til informasjonssikkerhet.[13]

3.2.1 Revisjonskriterium

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

3.2.2 Data

I intervjuene med nøkkelpersoner i kommunen spurte revisor om hva de forstår med begrepet informasjonssikkerhet.

HR-sjef oppfatter at informasjonssikkerhet handler om personvern og de opplysninger som folk ønsker å holde for deg selv, i tillegg til alt det som ligger bak for at dette skal bli ivaretatt.

[13] A. Jøsang, *Cybersikkerhet - Teknologier Og Styring*, 3rd ed. (2025).

Arkivleder definerer informasjonssikkerhet som alle data kommunen forvalter, og at de håndteres på en sikker og trygg måte, internt og eksternt. Tilganger, sikker oppbevaring, taushetserklæring rundt data kommunen forvalter, er eksempler som inngår i informasjonssikkerhet, etter arkivlederens forståelse. Det gjelder alle data som ansatte i kommunen får kunnskap om, samt tekniske løsninger.

De vi intervjuet mener at det er høy bevissthet i kommunen om personvern og sikkerhet. Svakheten er at det ikke er nedfelt skriftlig i styrende dokument.

I oppstartsmøtet etterspurte revisor kommunens styringssystem for informasjonssikkerhet og personvern som angir sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisasjon, og hvor roller og ansvar framgår. Tilbakemeldingen i møtet var at gjeldende styringsdokument framgår i en oversendelse til Datatilsynet, datert 28.4.2023, i forbindelse med brevkontroll, med hjemmel i personvernforordningen artikkel 58 nr. 1. Ett av dokumentene er **Sikkerhetsstrategi for informasjonssikkerhet.** I headingen i dokumentet står det «Bindal-GDPR – 2 Prosedyrer-GDPR – 2.1 Styrende GDPR». Det angis et formål med sikkerhetsstrategien: «Sikkerhetsstrategi skal konkretisere hvordan en arbeider for å ivareta sikkerhetsmålene for organisasjonen». Det er ikke angitt sikkerhetsmål utover det i dette dokumentet.

Dokumentet inneholder beskrivelse av hvem dokumentet gjelder (alle ansatte), ansvar, og hva ansvaret går ut på:

- Behandlingsansvarlig har ansvar for å få utarbeidet en sikkerhetsstrategi i organisasjonen,
- Sikkerhetsleder har ansvar for at ledere er kjent med strategien
- Personvernombud har ansvar for å gi ledere opplæring og kunnskap om sikkerhetsstrategien
- Personvernombud har ansvar for å gi råd til ledere og ansatte om praktisk etterlevelse av sikkerhetsstrategien
- Leder har ansvar for at ansatte er kjent med sikkerhetsstrategien og hvordan denne skal etterleves i daglig arbeid
- Alle har ansvar for å melde avvik i organisasjonens internkontroll dersom sikkerhetsstrategien ikke følges.

I dokumentet beskrives aktiviteter og hvordan disse skal utøves. Noen av disse aktivitetene kommer vi tilbake til senere i dette kapitlet og i neste kapittel. Flere av aktivitetene er nå knyttet til samarbeidet i Kystriket, får vi opplyst.

Ett av dokumentene revisor har fått tilsendt, har tittelen **Sikkerhetsorganisasjon og ansvar (GDPR)**. Det har samme heading som den nevnte sikkerhetsstrategien[14]. I dokumentet går det fram at formålet er at arbeidet med informasjonssikkerhet i organisasjonen skal være av en slik karakter at sikkerhet i forhold til integritet, tilgjengelighet og konfidensialitet blir ivaretatt. Videre heter det i formålet at ledelsen har forankret dette i organisasjonen på en slik måte at nødvendig ledelsesfokus blir ivaretatt. Dokumentet beskriver funksjoner, ansvar og organisering. Ansvaret er som følger:

- Kommunedirektøren – behandlingsansvarlig
- HR-sjef – sikkerhetsansvarlig
- Sektorledere og enhetsledere – daglig ansvar
- IT-konsulent (fagleder IKT) – ansvarlig for teknisk løsning
- Personvernombud
- Arkivar/konsulent – arkivleder

For hvert av ansvarsområdene fremgår det hvilken funksjon ansvaret rapporterer til, beskrivelse av ansvarsområdet og hvilken myndighet ansvaret har.

Informantene som vi intervjuet fortalte at også dette dokumentet ble utarbeidet for brevtilsynet til Datatilsynet i 2023, og er utdatert. Etter den tid har kommunen gått inn i Kystriket, og det er ingen lokal IKT-drift lenger. Kommunen har planer om å ta i bruk KiNS'[15] styringssystem for informasjonssikkerhet og personvern. KiNS er en forening som har som formål å bidra til økt informasjonssikkerhet i kommuner og fylkeskommuner.

HR-sjef sier at rollen som sikkerhetsansvarlig ble rapportert i forbindelse med brevkontrollen til Datatilsynet, men at hun ikke har fungert i rollen. Hun sier at en utfordring i kommunen, er at det er uklare ansvarsforhold internt, når det gjelder informasjonssikkerhet og personvern, og at mye faller på hennes rolle når det ikke er adressert. Fagområdet er komplekst, og kommunen har ikke dedikerte ressurser eller kompetanse til å etterleve kravene som stilles. Det er også utfordrende å ha nok kompetanse til å ivareta så mange ulike fagfelt. Arkivleder etterlyser tydeligere ansvar og kompetanse for informasjonssikkerhet i kommunen, og mener at dette er utenfor HR-sjefenss kapasitet. Fagansvarlig for IT gir også uttrykk for at dokumentet for sikkerhetsorganisering er utdatert.

[14] «Bindal-GDPR – 2 Prosedyrer-GDPR – 2.1 Styrende GDPR»

[15] Kins.no/om-oss

I 2020 valgte kommunen å sette av 20 % av stillingsressursen til kommunens arkivleder som personvernombud. Daværende personvernombud gjennomførte en kompetansehevende studie i personvern, holdt lederforum orientert, og var sentral i arbeidet med personvern ute i hele organisasjonen.

Fra 2022 fikk kommunen felles personvernombud med flere helgelandskommuner gjennom Digitale Helgeland. Vedkommende har hatt møter i hele kommuneorganisasjonen, inklusive lederforum.

3.2.3 Revisors vurdering

Ledelsessystem for informasjonssikkerhet som angir sikkerhetsmål

Etter revisors vurdering har ikke kommunen et oppdatert styringssystem for informasjonssikkerhet og personvern

Kommunens styringssystem ble utarbeidet i forbindelse med Datatilsynets brevkontroll i 2023, og er ikke oppdatert siden. Brevkontrollen, og dokumentene som ble utarbeidet i tilknytning til den, var rettet inn mot personvern, og omfattet i liten grad informasjonssikkerhet utover det. Styringsdokumentene som ble utarbeidet i 2023 inneholder formål med informasjonssikkerhet, men ikke mer konkrete sikkerhetsmål eller sikkerhetsstrategi.

Etter revisors vurdering bærer kommunens ledelsessystem for informasjonssikkerhet preg av å være utarbeidet for en konkret anledning, og er i mindre grad et grunnleggende og løpende ledelsessystem for organisasjonen. Revisors vurdering er likevel at det er kunnskap om og bevissthet rundt den delen av informasjonssikkerhet som gjelder personvern blant kommunens ledere. Revisor vil også trekke fram at det gjøres et arbeid for å få ledelsessystem for informasjonssikkerhet og personvern på plass.

3.3 Informasjonssikkerhet i systemet for internkontroll

3.3.1 Revisjonskriterier

eForvaltningsforskriften[16] krever at det skal være etablert internkontroll på området for informasjonssikkerhet.

- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.

[16] Digitaliserings- og forvaltningsdepartementet, *Forskrift Om Elektronisk Kommunikasjon Med Og i Forvaltningen (EForvaltningsforskriften)*.

- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må ha et avvikssystem og ansatte må melde avvik.

3.3.2 Data

Regelverk, prosedyrer og rutiner i systemet for internkontroll

HR-sjef viser til at kommunen de siste to årene har vært gjennom et utviklingsprogram i prosessledelse med vekt på internkontroll. I den forbindelse er det opprettet kvalitetsgrupper i alle sektorer. Kvalitetsutvalget er overordnet disse gruppene og består av lederforum og hovedverneombud. Kvalitetsutvalget skal håndtere spørsmål om internkontroll på overordnet eller tverrfaglig nivå. Dette kan være ROS analyser, avviksrapportering og styringssystem som KiNS styringssystem.

Det digitale systemet som Bindal kommune bruker for internkontroll, er Compilo. Her ligger prosedyre for informasjonssikkerhet og personvern fordelt i gruppene «styrende», «gjennomførende», «daglige» og «kontrollerende».

Dokumentene som revisor har fått oversendt, og som er beskrevet i kapittel 3.2.2, inngår i Compilo. Revisor har også fått tilsendt et dokument som heter Internkontroll system (GDPR prosedyre). Av dokumentet fremgår det at alle som er involvert i behandling av personopplysninger skal gjøres kjent med prosedyrer og retningslinjer. I dokumentet står det at alle skal medvirke til forbedringer gjennom forbedringsforslag og avviksrapportering, alle skal få relevant opplæring og ha kunnskap ut fra sin rolle og all dokumentasjon skal være oppdatert og gjenstand for revisjon. Ledelsen skal gjennomføre systemrevisjon og årlig gjennomgang. I prosedyren fremgår det hvilket ansvar ledelse og ansatte på ulike nivå har for internkontroll for GDPR. Videre er aktivitetene beskrevet. Revisor har også fått tilsendt et dokument som heter Egenkontroll og sikkerhetsrevisjon (GDPR-prosedyre). Her fremgår det hva som er formålet med sikkerhetsrevisjon og egenkontroll, og at alle virksomheter som behandler personopplysninger er pålagt å gjennomføre sikkerhetsrevisjoner og egenkontroll. Dette skal skje minimum årlig. Det fremgår en rekke spørsmål som virksomhetene skal besvare, herunder om ansattes tilgang til system og informasjon. Dokumentet er ikke datert.

Ifølge HR-sjef jobbes det mye med Compilo og informasjonssikkerhet, og per i dag ligger Compilos GDPR-modul i systemet. Hun fortalte at Compilo har inngått et samarbeid med KiNS', og at KiNS´ styringssystem inkluderes i Compilo. Fagleder IKT viste også til Kystriket, og at mye av det som gjelder informasjonssikkerhet er løftet over i Kystriket.

ROS og informasjonssikkerhet

Revisor har fått oversendt kommunens overordnede ROS, Helhetlig risiko og sårbarhetsanalyse, 2022. I kapitlet om prioritering er oppdatering og ajourhold av overordna beredskapsplan et prioritert tiltak. Et annet prioritert tiltak er utarbeiding og etablering av plan og strategi for informasjonssikkerhet og drift av IKT-systemer i kommunen et av prioriteringene. Revisor har fått oversendt overordna beredskapsplan, sist revidert i november 2025.[17] Det er ikke beskrivelser av beredskap for informasjonssikkerhet i den planen.

Revisor har fått tilsendt et dokument kalt Risikoanalyse: Informasjon og datasikkerhet. Dokumentets versjonsdato er 12. februar 2025. I dokumentet framgår det at en gruppe bestående av IT-leder, arkivleder og HR-sjef har vært deltakere i utarbeidingen av dokumentet, sammen med personvernombudet. Dokumentet inneholder en gjennomgang av risikoobjekt og en risikoanalyse, og vurdering av betydning for konfidensialitet, integritet eller tilgjengelighet.

Revisor har også fått tilsendt et dokument kalt Risikovurderinger Personvern (GDPR-prosedyre). Dette omtaler vi under delkapitlet om personvernkonsekvenser – DPIA.

HR-sjefen viser til at kommunen har delt opp ROS i en informasjonssikkerhets-ROS og personvern-ROS, som begge er under utarbeidelse. Det har vært diskutert om dette skal løftes inn i Kystriket. HR-sjefen mener at disse analysene bør være på overordna nivå. Det er ikke utarbeidet beredskapsplan for informasjonssikkerhet. Arkivleder fortalte at det har vært gjennomført noen felles møter med Kystriket. Arkivleder sa videre, at det er noe uenighet i ledergruppa om nivået på ROS-analysene. Arkivleder hadde erfaring med å starte i det små, med avgrensede ROS-analyser.

Fagleder IKT sa at det ble laget mange ROS-analyser for de valgene kommunene tok da de etablerte en felles driftsplattform (Kystriket).

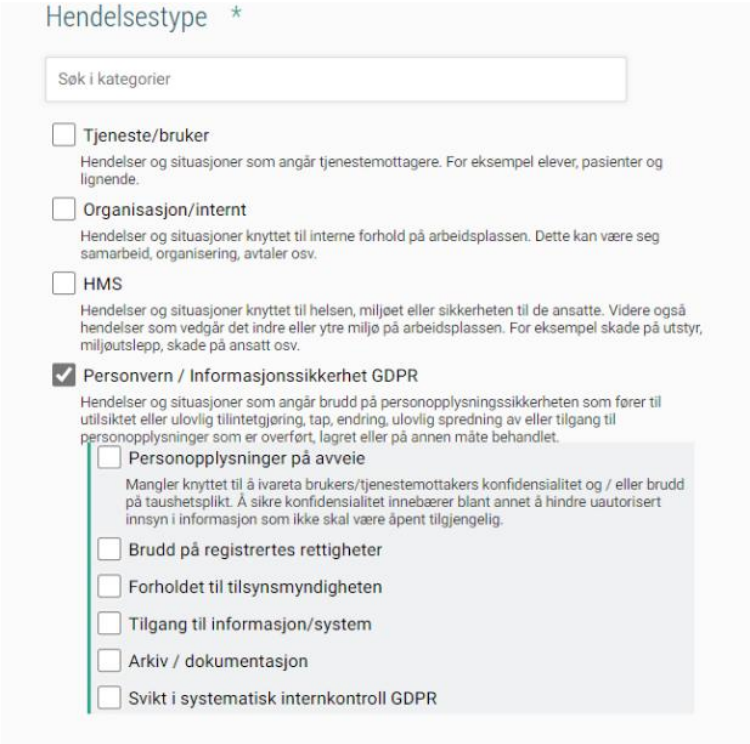
Avvik

Compilo har en avviksmodul. Generelt, forklarte arkivleder, har det vært en forbedringsprosess med avviksmelding. Ifølge arkivleder, varierer det om ansatte melder avvik, men det har blitt bedre. Arkivleder sa videre at det meldes avvik gjennom 3-4 ulike system, og at kommunen ikke er bra nok på å samle, kategorisere og analysere dem for tiltak. I tillegg har kommunen 3, kanskje 4 ulike system det meldes avvik i. Kommunen er ikke god nok til få samlet alle avvik, kategorisere og analysere dem for å treffe tiltak for å bli bedre. Fagleder for IKT viste til

[17] Bindal kommune, *Overordnet Beredskapsplan for Bindal Kommune* (2025).

Compilo, og at alt skal ligge der. I Compilo er det et eget valg for avvik på informasjonssikkerhet. Avvik som ansatte melder, blir behandlet i de enkelte avdelingene. HR-sjef viste til kvalitetsutvalget, og som blant annet skal håndtere spørsmål om internkontroll på overordna eller tverrfaglig nivå, blant annet avviksrapportering.

I svaret fra kommunen til Datatilsynet fremgår det at avviksmodulen i Compilo har egen hendelsestype på personvern/informasjonssikkerhet. Et bilde av hendelsestypen for personvern/informasjonssikkerhet er gjengitt i brevet:



Kilde: Bindal kommune

3.3.3 Revisors vurderinger

Informasjonssikkerhet i kommunens internkontrollsystem

Etter revisors vurdering inngår prosedyrer og rutiner rundt personvern i kommunens system for internkontroll, men de er ikke oppdaterte og de inneholder i mindre grad informasjonssikkerhet som gjelder andre informasjonsverdier.

Revisor vil trekke fram kvalitetsutvalget, som kan bidra til å sette dette arbeidet mer i system. Systemet for internkontroll, Compilo, inneholder rutinebeskrivelser og prosedyrer som særlig

gjelder personvern, i mindre grad informasjonssikkerhet ellers. Etter revisors vurdering kan dette bli forbedret dersom/når kommunen tar i bruk KiNS´ system.

Gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak

Etter revisors vurdering har kommunen satt i gang et arbeid med en ROS-analyse for informasjonssikkerhet og en ROS-analyse for personvern.

Intervjuinformasjonen tyder på at det er gjort et arbeid på ROS-analysene for informasjonssikkerhet og personvern. Det kan bidra til å styrke arbeidet med risikovurderinger og risikoreduserende tiltak. Det vises til Kystriket IKT, og system for internkontroll. Revisor stiller spørsmål ved om oppgaver og ansvar er helt avklart, mellom kommunen og Kystriket IKT.

Kommunen må ha et avvikssystem og ansatte må melde avvik.

Etter revisors vurdering inneholder systemet for internkontroll en avviksmodul, der informasjonssikkerhet og personvern er egen hendelse. .

Etter revisors vurdering er det generelle variasjoner i hvor og om det rapporteres på avvik, noe som også kan gjelde for avviksrapportering på informasjonssikkerhet og personvern. Kvalitetsutvalget kan bidra til at dette blir satt mer i system.

3.4 Personvern

3.4.1 Revisjonskriterier

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

3.4.2 Data

Kommunen (behandlingsansvarlig eller den behandlingsansvarliges representant) skal føre protokoll over hvilke personopplysninger de behandler. Protokollen skal inneholde minimumskravene til opplysninger.

Protokoll for behandling av personvern

I et brev fra Bindal kommune til Datatilsynet, som svar på brevkontroll, fremgår det at Bindal kommune kjøpte tjenesten personvernombud og «personvernappen» fram til 1.1.2021. Etter

det, hadde de et eget personvernombud fram til høsten 2022. Personvernappen inneholdt behandlingsprotokoller, og disse ble overført til Excel-filer i perioden etter 1.1.2021. Videre fremgår det i svaret til Datatilsynet at kommunen nå (april 2023) jobber med å få behandlingsprotokollene og DPIA[18] inn i egen GDPR[19]-modul i Compilo, med bistand fra Digitale Helgeland og felles personvernombud.

Revisor har fått tilsendt et skjema som er kalt **Samlet oversikt – Sortert – Protokoller i Bindal kommune**». Protokollen viser oversikt over behandlingsaktiviteter i Bindal kommune. I tillegg inneholder det en mer detaljert oversikt over de ulike sektorenes behandlingsaktiviteter. Skjemaet viser rubrikker for informasjon om 20 personvernrelaterte kategorier.

Ifølge intervjuinformasjon skal behandlingsprotokollene, som nå er i Excel, overføres og oppdateres i Samsvar systemforvaltning sin løsning for behandlingsprotokoller, forhåpentligvis i løpet av 2025.

Ifølge arkivleder er behandlingsprotokollene ikke oppdaterte, og det er ikke laget nye protokoller. Når kommunen går over til Samsvar systemforvaltning og personvern, kan kommunen revidere og importere protokollene den allerede har, og legge inn nye protokoller. Det er flere av de andre kommunene i Kystriket som allerede bruker Samsvar personvern på protokoller. Derfor har Bindal valgt å gå for det, slik at det er mulig å jobbe sammen med dem.

HR-sjef fortalte at det er jobbet mye med personvern i kommunen, spesielt i årene 2018 – 2019. Hun mener at arbeidet den gangen trolig har hjulpet på at kommunens ledere og ansatte har daglig oppmerksomhet på personvern og informasjonssikkerhet.

Personvernombudet bekrefter i intervju at flere kommuner i samarbeidet Digitale Helgeland bruker Samsvar.

Vurdering av personvernkonsekvenser – DPIA

Ett av spørsmålene som virksomhetene skal svare på i dokumentet Egenkontroll og sikkerhetsrevisjon er om de er kjent med prosedyren DPIA-vurdering av personvernkonsekvenser GDPR. Av dokumentasjonen revisor har fått oversendt, er det et dokument, Risikovurderinger Personvern. Dokumentet, som er udatert, inneholder beskrivelse

[18] Data Protection Impact Assessment (DPIA) – vurdering av personvernkonsekvenser. Datatilsynet.no

[19] General Data Protection Regulation (GDPR) – EUs personvernforordning (integrert i personopplysningsloven)

av ansvar og aktiviteter og hva risikovurderingen av personvernopplysninger skal inneholde. Personvernkonsekvenser eller DPIA er ikke beskrevet i dokumentet.

HR-sjefen viste til at det er laget DPIA på de gamle behandlingsprotokollene hvor det var behov, men de er utdaterte. Kommunen har fått nye systemer og det er gjort DPIA på systemer, blant annet på legekontoret. HR-sjefen sa at det er et vanskelig arbeid, for det er vanskelig å forstå hva det spørres om. Personvernombudet bistår her. HR-sjef håpet på et samarbeid gjennom Kystriket, også på dette området, sammen med personvernombudet. Det vil sannsynligvis gjøre det lettere å forstå de ulike forhold som skal vurderes i en DPIA, ifølge HR-sjefen.

Intervjuinformasjon fra arkivleder er tydeligere på at det ikke er system på DPIA. DPIA-ene finnes ute blant lederne, men de har ikke noe forhold til det, ifølge arkivleder. Det har hittil ikke vært praksis for at arkiv og IT blir involvert, men nå er det besluttet at de alltid skal være involvert når det anskaffes nye IT-system. Også arkivleder viste til Digitale Helgeland, og at DPIA er en del av prosjektene som kjøres gjennom dem. Det kjøres felles DPIA, med lokale tilpasninger.

Personvernombudet forteller i intervju at kommunene er anbefalt å etablere en systematikk for behandlingsprotokoller, risikovurderinger og DPIA.

3.4.3 Revisors vurdering

Protokoll for behandling av personvern

Etter revisors vurdering har kommunen utarbeidet et grunnlag for behandlingsprotokoller, men det er ikke oppdatert.

Skjemaet som revisor har fått tilsendt avløste en personvernapp som var i bruk fram til 2021. Kommunen har jobbet med ulike løsninger for behandlingsprotokoller, delvis gjennom Digitale Helgeland. Kommunen planlegger å gå over til Samsvar Systemforvaltning (Sikri) i løpet av 2025. Etter revisors vurdering kan det være en bedre og sikrere løsning enn det som har vært utarbeidet hittil.

Vurdering av personvernkonsekvenser – DPIA

Etter revisors vurdering har kommunen ikke et tilfredsstillende system for vurdering av personvernkonsekvenser (DPIA).

Revisor har inntrykk av at det er gjennomført DPIA-er for noen systemer, men at kommunen har utfordringer med å gjennomføre dette, og at det framstår som et vanskelig arbeid. Det er igangsatt et arbeid sammen med andre kommuner på Helgeland, der personvernombudet bistår og veileder.

3.5 Opplæring i informasjonssikkerhet og personvern

Kommunen må sørge for at ansatte får tilstrekkelig opplæring i og informasjon om informasjonssikkerhet.

3.5.1 Revisjonskriterium

- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i policy og informasjon om informasjonssikkerhet.

3.5.2 Data

KS lanserte i 2023 en kampanje om informasjonssikkerhet og personvern for ansatte i kommuner og fylkeskommuner. Kampanjen bestod av ti temaer, som ble rullet ut hver måned. Dokumentasjonen er fortsatt tilgjengelig på KS' nettsider.[20] HR-sjefen fortalte at kommunen har gjennomført KS` kampanje om informasjonssikkerhet. Det ble utarbeidet en sikkerhetsinstruks etter KiNS' mal, som ble lagt ut etter KS-kampanjen. Fagleder IKT sa at kommunen også har gjennomført interne kampanjer. For eksempel har det kommet eposter fra Kystriket IKT om ikke å trykke på lenker, eksempelvis epost eller SMS fra leder.

HR-sjef trakk fram at kommunen i lederforum har gjennomgått og tilpasset KiNS Sikkerhetsinstruks for informasjonssikkerhet (IT-regler). Ledere har sendt denne til digital signering gjennom Elements. I forkant ble det informert om dette til alle ansatte på Teams og avdelingsmøter. Nyansatte får IT-regler som en del av arbeidsavtalen som signeres. Ansatte har fått informasjon om det i forkant, og det skal tas opp i informasjonsmøter i tillegg. HR-sjef hadde ikke oversikt over om alle har signert. Nyansatte får den som en del av arbeidsavtalen.

Arkivleder og Fagleder IKT bekreftet at det er utarbeidet sikkerhetsinstruks som alle ansatte har fått tilsendt for signering.

[20] https://www.ks.no/fagomrader/digitalisering/digital-kompetanse/informasjonssikkerhet-og-personvern/veiviser-for-a-styrke-robusthet/slik-bruker-kommunen-kampanjen/

Arkivleder har hatt «elementskafé» en time annenhver fredag i halvannet år. Kommunedirektøren har vært med på alle, forteller arkivleder, og har signalisert til ansatte at det er viktig. Det har vært svært god oppslutning på disse kafeene. Arkivleder har gått gjennom alle feil som vedkommende har sett, og har i tillegg opplyst om hvordan utnytte mulighetene i systemet. Det kommer ny versjon, og det er planer om nye elementskafeer i hele Kystriket.

3.5.3 Revisors vurderinger

Etter revisors vurdering har det delvis vært opplæring av ansatte i informasjonssikkerhet og personvern.

Opplæringen har vært knyttet til KS-kampanje fra 2023, som bestod av ti temaer som ble rullet ut hver måned. Det er dessuten utarbeidet en sikkerhetsinstruks som alle ansatte skal kvittere ut. Ellers er det løpende opplæringstiltak i enkelte systemer, som Elements, men det er uklart for revisor om sikkerhet og personvern har inngått i det opplæringstiltaket.

3.6 Konklusjon

I dette kapitlet har vi belyst problemstillingen om kommunen har styringssystem for informasjonssikkerhet og personvern.

På den første problemstillingen, om styringssystem for informasjonssikkerhet, konkluderer revisor med at kommunen har lagt et grunnlag for styringssystem som inneholder ledelsessystem og internkontroll for personvern, men i mindre grad informasjonssikkerhet, utover det som gjelder personvern.

Styringssystemet er i liten grad oppdatert siden brevkontrollen i 2023. Det er lagt et grunnlag for kunnskap og bevissthet i kommunen gjennom det arbeidet som ble gjennomført i 2023, og i det arbeidet som er gjort etter det, for å få på plass et overordna styringssystem for informasjonssikkerhet og personvern.

Kommunen arbeider med å etablere et system for behandlingsprotokoller og vurdering av personvernkonsekvenser (DPIA) med bistand fra personvernombudet.

Kommunen har gjennomført kampanjer og informasjonstiltak for informasjonssikkerhet i organisasjonen. Kommunen har forbedringsmuligheter når det gjelder systematiske opplæringstiltak i informasjonssikkerhet.

Noe av informasjonen som revisor har fått, tilsier at det fortsatt er behov for å avklare hva som er kommunen sine oppgaver og hva som er Kystriket IKT sine oppgaver overfor kommunen.

4 TEKNISKE OG ORGANISATORISKE 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. Dette gjelder flere av de ansatte i Brønnøy kommune og den ansatte i Bindal kommune. Intervjudata fra Kystriket IKT er data fra intervjuer med IKT-ansatte i Brønnøy 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 i vedlegg en:

- 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 Data

Oversikt over enheter i IKT-systemet

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[21]. 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[22]. til å administrere nettbrett, mens Bindal bruker LightSpeedSystems som er et tilsvarende system som Jamf. Vega har ikke nettbrett til sine brukere. For mobiltelefoner brukes MDM (Mobile Device Management) løsningen.

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

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

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. 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.

Oversikt over programvare

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, 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 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 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.

Kystriket IKT ser hvilke applikasjoner som tas i bruk i alle kommuner, forteller en av de ansatte. 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.

Tilgangsstyring

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)[23]. 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[24]. 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[25], 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.

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

---

[23] 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.

[24] 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.

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

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[26]. 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

[26] Endret fra hver andre til hver fjerde time etter intervjutidspunktet.

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[27] 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.

4.2.3 Revisors vurdering

Oversikt over enheter i IKT-systemet

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

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

Oversikt over programvare.

Gjennom samarbeidet i Kystriket IKT har kommunen en over 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 installeres lokalt. I Kystriket IKT brukes Intune for å registrere programvare som brukes. I tillegg registreres programvare i Asset Management, som grunnlag for brukerstøtte. Ut over dette er det mulig for ansatte å bruke skybaserte applikasjoner uten noen form for godkjenning. Det henvises til at sektorlederne i kommunene må følge opp dette. Utfordringene her er hva som lagres av data i slik programvare, jfr. kapittel 3.4.

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

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 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 kommunene tatt i bruk flerfaktor der hvor det 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 i vedlegg en:

- 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 Data

Sikkerhet i anskaffelses- og utviklingsprosesser

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[28]. 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.

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

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 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.

Sikkerhet ved tjenesteutsetting

Gjennom Kystriket IKT har kommunene inngått en driftsavtale med en ekstern driftsleverandør. I utformingen av kravspesifikasjonen[29] 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

[29] Kravspesifikasjonen er et bilag til driftsavtalen.

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[30] 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)

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

[30] 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)

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

Sikker IKT-arkitektur

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».

Sentral styring med sikkerhetsoppdateringer

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[31] 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»[32], 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.

---

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

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

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.

Plan for sikkerhetskopiering og sikre at sikkerhetskopier tas

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[33].

Driftsleverandøren har ansvar for sikkerhetskopier av det som blir generert av filer, og hvis det er endringer i switcher[34] eller brannmur, forteller en av de ansatte. Type backup er avhengig av hvilket system det tas backup av, og dette er ivaretatt i driftsavtalen..

4.3.3 Revisors vurdering

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

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

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

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.

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.

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.

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

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.

Plan for sikkerhetskopiering og ta sikkerhets-kopier.

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

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 en.

- 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 Data

Plan for hva som skal overvåkes

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.

Kommunene har egentlig ikke noen rolle i overvåkningen, forteller en av medarbeiderne i Kystriket IKT. 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. Drifts-leverandør 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.

System for overvåkning av sikkerhet og analyse

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)[35]. (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[36]. 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

[35] 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)

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

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.

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 vet ikke hvor mye driftsleverandøren kan gjøre gjennom datasenteret.

4.4.3 Revisors vurdering

Plan for hva som 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.

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 en.

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

4.5.2 Data

Plan for hendelseshåndtering

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.

Kystriket IKT er en prioritert kunde hos driftsleverandøren, forteller daglig leder i Kystriket IKT. 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.

Plan for gjenoppretting

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. Ifølge fagleder IKT i Bindal kommune kan alle hendelser av en viss størrelse håndteres i henhold til beredskapsplanen i Bindal kommunen.

Håndtering av løsepengevirus kommer an på hvor omfattende det er. 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. Kystriket IKT bistår som rådgivere.

Det er sjeldent behov for gjenoppretting, forteller en av de ansatte. 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.

4.5.3 Revisors vurdering

Plan og rutiner 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. Bindal kommune har en beredskapsplan som kan håndtere alle hendelser av en viss størrelse. Utover det, håndteres hendelser innenfor driftsavtalen mellom driftsleverandøren og Kystriket IKT. Dette kan for eksempel dreie seg om

hvordan tjenesteproduksjonen skal prioriteres og opprettholdes hvis IKT-systemet ikke er tilgjengelig.

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.

4.6 Konklusjon

Problemstillingen er om Bindal kommune tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet.

Revisor konkluderer med at Bindal kommune i stor grad har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet gjennom samarbeidet i Kystriket IKT.

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 forbedringsområder innenfor informasjonssikkerhet fordi området er i stadig utvikling.

5 KONKLUSJONER OG ANBEFALINGER

I dette kapitlet oppsummerer revisor funn og vurderinger i konklusjon på de to problemstillingene som er undersøkt. På bakgrunn av vurderinger har revisor noen anbefalinger til forbedringer av arbeidet med informasjonssikkerhet og personvern i kommunen.

5.1 Konklusjoner

I denne forvaltningsrevisjonen er følgende problemstillinger belyst:

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

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

På den første problemstillingen, om styringssystem for informasjonssikkerhet, konkluderer revisor med at kommunen har lagt et grunnlag for styringssystem som inneholder ledelsessystem og internkontroll for personvern, men i mindre grad informasjonssikkerhet, utover det som gjelder personvern.

Styringssystemet er i liten grad oppdatert siden brevkontrollen i 2023. Det er lagt et grunnlag for kunnskap og bevissthet i kommunen gjennom det arbeidet som ble gjennomført i 2023, og i det er gjort arbeid etter det for å få på plass et overordna styringssystem for informasjonssikkerhet og personvern.

Kommunen arbeider med å etablere et system for behandlingsprotokoller og vurdering av personvernkonsekvenser (DPIA) med bistand fra personvernombudet.

Kommunen har gjennomført kampanjer og informasjonstiltak for informasjonssikkerhet i organisasjonen. Kommunen har forbedringsmuligheter når det gjelder systematiske opplæringstiltak i informasjonssikkerhet.

Noe av informasjonen som revisor har fått, tilsier at det fortsatt er behov for å avklare hva som er kommunen sine oppgaver og hva som er Kystriket IKT sine oppgaver overfor kommunen.

På den andre problemstillingen, om organisatoriske og tekniske tiltak, konkluderer revisor med at Bindal kommune i stor grad har tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet gjennom samarbeidet i Kystriket IKT.

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.

5.2 Anbefalinger

Revisor anbefaler kommunedirektøren å:

- Videreutvikle og ajourholde det overordna ledelsessystemet for informasjonssikkerhet og personvern
- Avklare ansvarsforhold mellom Bindal kommune og Kystriket IKT sitt arbeid
- Styrke opplæringen i informasjonssikkerhet
- Vurdere hvilke systemer og funksjoner som må prioriteres hvis datasystemer ikke er tilgjengelig og eventuelt må gjenopprettes

KILDER

Bindal kommune. *Overordnet Beredskapsplan for Bindal Kommune*. 2025.

Digitaliserings- og forvaltningsdepartementet. *Forskrift Om Elektronisk Kommunikasjon Med Og i Forvaltningen (EForvaltningsforskriften)*. 2004.

Jøsang, A. *Cybersikkerhet - Teknologier Og Styring*. 3rd ed. 2025.

Justis- og beredskapsdepartementet. *Forskrift Om Virksomheters Arbeid Med Forebyggende Sikkerhet (Virksomhetssikkerhetsforskriften)*. 2018.

Lov Om Behandling Av Personopplysninger (Personopplysningsloven), Pub. L. LOV-2018-06-15-38 (2018). https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=lov%20om%20behandling%20av%20personopplysninger.

Lov Om Digital Sikkerhet (Digitalsikkerhetsloven) (2023).

Lov Om Nasjonal Sikkerhet (Sikkerhetsloven) (2018).

Nasjonal sikkerhetsmyndighet (NSM). *Veileder i Sikkerhetsstyring*. 2020. https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-sikkerhetsstyring/om-denne-veilederen/.

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 (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften)
- Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhets-forskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet[37]
- NMSs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet

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

<u>Overordnet styringssystem og rammeverk</u>

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

[37] Nasjonal sikkerhetsmyndighet (NSM), *Veileder i Sikkerhetsstyring*, 2020, https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-sikkerhetsstyring/om-denne-veilederen/.

virksomheter som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. 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.

Sikkerhetsmål og sikkerhetsstrategi

Virksomhetsikkerhetsforskriften 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[38] 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.

Sikkerhetsorganisasjon

Jamfør sikkerhetsloven § 4-1 er det er virksomhetens leder som 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. Virksomhetsikkerhetsforskriften § 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.

Internkontroll

Internkontroll er hjemlet i kommuneloven § 25, der 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

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

- 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.

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.

Risikovurderinger

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.

Personopplysninger

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 personvernregelverket. En av pliktene Datatilsynet referer til er vurdering av personvernkonsekvenser (DPIA – Data Protection Impact Assessment) (artikkel 35 i personopplysningsloven). Artikkel 35 krever at virksomheten gjennomfører en vurdering av personvernkonsekvenser ved behandlinger som

vil medføre høy risiko for fysiske personers rettigheter og friheter. Datatilsynet[39] 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.

En av pliktene er at alle virksomheter som behandler personopplysninger, skal føre protokoll over behandlingsaktivitetene de har ansvar for (artikkel 30 i personopplysningsloven). 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.

Opplæring

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 virksomhetsikkerhetsforskriften § 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.

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

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

Hendelser

Virksomhetsforskriften § 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.

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.*»

På bakgrunn av redegjørelsen over, er følgende revisjonskriterier utledet for den første problemstillingen.

- Kommunen skal ha et styringssystem for sikkerhet som omfatter informasjons-sikkerhet, som angir
    - Sikkerhetsmål
    - Sikkerhetsstrategi
    - Sikkerhetsorganisasjon, hvor roller og ansvar framgår
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.

- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.
- 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.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

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

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

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 endringshåndtering
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

VEDLEGG 2 – UTTALELSE

Hei

Kommunedirektøren gir med dette tilbakemelding til foreløpig rapport fra forvaltningsrevisjon om informasjonssikkerhet og personvern i Bindal kommune. Dette er en samla tilbakemelding fra undertegnede, og de tre som ble intervjuet. Vi synes at rapporten gir et godt bilde av situasjonen i kommunen, og at den har en konstruktiv tilnærming til et komplisert og krevende fagfelt.

Jeg regner med at det tas en kvalitetssikring på rapporten før den blir offentlig. Vi har ikke sett på korrektur, men registrerer at det er noen tilfeller der setninger mangler ord. Se for eksempel nederst på side 6, der det står dette:

«Informasjon knyttet til Digitale Helgeland er Dette samarbeidet er nærmere beskrevet i kapittel 2.». Det er også en usammenhengende setning i andre avsnitt på side 21.

Det er nå 19 kommuner med i Digitale Helgeland. Dette kan gjerne endres på side 6 og 13.

Det må korrigeres på side 20 at vi har en beredskapsplan. Denne har kommunerevisjonen fått tilsendt.

På side 24, avsnitt 3, siste setning, er det tatt med noe om en ansatt i en annen stilling i kommunen. Selv om dette var korrekt på det tidspunkt ber jeg om at denne setningen fjernes. Dette er et internt forhold som ikke kan stå i en offentlig rapport.

Nedenfor følger noen endringer som vi mener må gjøres for at rapporten skal bli enda mer beskrivende:

Side 10
Opprinnelig tekst:
I tillegg til driftsleder i Kystriket (fag leder IKT i Bindal), er det flere ansatte i Brønnøy kommune som jobber for Kystriket, med oppgaver for de andre deltakerkommunene, deriblant Bindal.

Korrigert tekst:
I tillegg til driftsleder i Kystriket (fagleder IKT i Bindal), er det flere ansatte i Brønnøy og de andre kommunene som jobber for Kystriket, med oppgaver for de andre deltakerkommunene, deriblant Bindal.

Side 13
Opprinnelig tekst:
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.

Korrigert tekst:
Leder for Kystriket IKT forteller at Brønnøy kommune har åtte ansatte som jobber innenfor Kystriket, Bindal har en ansatt, Sømna har en ansatt, Vega har en ansatt og Vevelstad har en ansatt.

Side 17
Opprinnelig tekst:
HR-sjef sier at rollen som sikkerhetsansvarlig ble rapportert i forbindelse med brevkontrollen til Datatilsynet, men at hun ikke har fungert i rollen. Hun sier at en utfordring i kommunen, er at det er uklare ansvarsforhold internt, og at mye faller på hennes rolle når det ikke er adressert. Det kan føre til at en får mange roller i en liten kommune, og det er utfordrende å sette av tid slik at både kompetanse, strukturer og ansvarsforhold blir implementert i organisasjonen. Det er også utfordrende å ha nok kompetanse til å ivareta så mange ulike fagfelt.

Korrigert tekst:
HR-sjef sier at rollen som sikkerhetsansvarlig ble rapportert i forbindelse med brevkontrollen til Datatilsynet, men at hun ikke har fungert i rollen. Hun sier at en utfordring i kommunen er at det er uklare ansvarsforhold internt i forhold til personvern og informasjonssikkerhet. Fagområdet er komplekst, og vi har ikke dedikerte ressurser eller kompetanse til å etterleve kravene som stilles.

Side 25
Opprinnelig tekst:
HR-sjef trakk fram at kommunen har hatt oppe et internprogram om informasjonssikkerhet i lederforum, hvor også arkivleder deltok. Hver enkelt leder skal ta sikkerhetsinstruksen ut fra Elements, og sende den til digital signering til sine ansatte. Ansatte har fått informasjon om det i forkant, og det skal tas opp i informasjonsmøter i tillegg. HR-sjef hadde ikke oversikt over om alle har signert. Nyansatte får den som en del av arbeidsavtalen.

Korrigert tekst:
HR-sjef trakk fram at kommunen i lederforum har gjennomgått og tilpasset KiNS Sikkerhetsinstruks for informasjonssikkerhet (IT-regler). Ledere har sendt denne til digital signering gjennom Elements. I forkant ble det informert om dette til alle ansatte på Teams og avdelingsmøter. Nyansatte får IT-regler som en del av arbeidsavtalen som signeres.

Side 29
Opprinnelig tekst:
Brønnøy og Sømna bruker Jamf14. til å administrere nettbrett, mens Bindal bruker et annet verktøy.

Korrigert tekst:
Brønnøy og Sømna bruker Jamf14. til å administrere nettbrett, mens Bindal bruker LightSpeedSystems som er et tilsvarende system som Jamf.

Side 32
Opprinnelig tekst:
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.

Korrigert tekst:
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.

Side 33
Opprinnelig tekst:
Eksterne må logge inn annenhver time og reautentisere seg.

Korrigert tekst:
Eksterne må logge inn hver fjerde time og reautentisere seg.

Side 40
Opprinnelig tekst:
•Møter annenhver uke mellom daglig leder i Kystriket IKT og driftsansvarlig hos leverandøren. Her gjennomgår de hendelser.
•Månedlige driftsmøter med leverandøren hvor daglig leder og en av de andre i Kystriket IKT deltar.
•Møter om servicedesk en gang i måneden. Tidligere var det hver fjortende dag, men det er mindre saker nå. En i Kystriket IKT har ansvaret for å følge opp henvendelser som Kystriket IKT sender til driftsleverandøren. Det utgjør et par saker i uka.

Korrigert tekst:
•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.

Mvh
Knut Toresen
kommunedirektør
Mobil 913 25 888
E-post knut.toresen@bindal.kommune.no

All e-post er som hovedregel offentlig, og blir behandlet i tråd med offentleglova og kommunens arkivbestemmelser. Det må derfor påregnes at e-post vil komme på offentlig postliste.

PM Revisjon Midt-Norge

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no

Til kontrollutvalget i Bindal kommune Sandnessjøen 02.03.2026

Saksbehandler:
Sekretariatsleder
Tobias Langseth

SAK 03/2026: PROSJEKTPLAN FORVALTNINGSREVISJON [UTENFORSKAP]

1: Innledning og bakgrunn

Kontrollutvalget foretok gjennom sak 17/2025 [møte 10.11.2025] bestilling av et forvaltningsrevisjonsprosjekt knyttet til temaet «Utenforskap og psykisk helse». På denne bakgrunn har kommunens revisor utarbeidet prosjektplan.

Jf. RSK 001 standard for forvaltningsrevisjon punkt 4–8:

RSK 001 (nkrf.no)

Vedtakets ordlyd:

«Kontrollutvalget bestiller et forvaltningsrevisjonsprosjekt knyttet til temaet «Utenforskap og psykisk helse». Utvalget ber om at Revisjon Midt-Norge utarbeider forslag til prosjektplan på basis av de signaler som fremkom, som legges frem for kontrollutvalget i egen sak.»

2: Kontrollutvalgets oppgaver og rolle

Kontrollutvalgets oppgave er i første omgang å se til at det gjennomføres forvaltningsrevisjon av kommunens virksomhet, og av virksomheten i selskaper som kommunen har eierinteresser i. Jf. kommuneloven § 23-2 første ledd bokstav c.

3: Oppsummering og avslutning

Prosjektplanen gjennomgås og drøftes i møtet. Eventuelle kommentarer videreformidles oppdragsansvarlig revisor.

Forslag til vedtak:

Kontrollutvalget tar prosjektplanen til etterretning [med de merknader som fremkom i møtet].

Vedlegg –
1: Prosjektplan av 25.02.2026
2: Timerapportering for 2025 Revisjon Midt-Norge

Appendiks 1 – Utdrag fra kommuneloven

§ 23-2. Kontrollutvalgets ansvar og myndighet

Kontrollutvalget skal påse at
a) kommunens eller fylkeskommunens regnskaper blir revidert på en betryggende måte
b) det føres kontroll med at den økonomiske forvaltningen foregår i samsvar med gjeldende bestemmelser og vedtak
c) det utføres forvaltningsrevisjon av kommunens eller fylkeskommunens virksomhet, og av selskaper kommunen eller fylkeskommunen har eierinteresser i
d) det føres kontroll med forvaltningen av kommunens eller fylkeskommunens eierinteresser i selskaper mv. (eierskapskontroll)
e) vedtak som kommunestyret eller fylkestinget treffer ved behandlingen av revisjonsrapporter, blir fulgt opp.

Kontrollutvalgets leder har møte- og talerett i kommunestyret eller fylkestinget når utvalgets saker skal behandles. Utvalgets leder kan la ett av de andre medlemmene i utvalget utøve denne retten på sine vegne.

Kontrollutvalget kan kreve at kommunen eller fylkeskommunen legger fram enhver opplysning, redegjørelse eller dokument som utvalget finner nødvendig for å utføre sine oppgaver. Kontrollutvalget kan også foreta undersøkelser som det mener er nødvendige. Taushetsplikt er ikke til hinder for å gjennomføre kontrolltiltak etter dette leddet.

Kontrollutvalget har rett til å være til stede i lukkete møter i folkevalgte organer i kommunen eller fylkeskommunen. Kommunestyret og fylkestinget kan selv bestemme at denne retten ikke gjelder lukkete møter i kommunestyret og kommunerådet eller fylkestinget og fylkesrådet.

Departementet kan gi forskrift om kontrollutvalgets oppgaver og saksbehandling.

§ 23-3. Forvaltningsrevisjon

Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak.

Kontrollutvalget skal minst én gang i valgperioden, og senest innen utgangen av året etter at kommunestyret eller fylkestinget er konstituert, utarbeide en plan som viser på hvilke områder det skal gjennomføres forvaltningsrevisjoner. Planen skal baseres på en risiko- og vesentlighetsvurdering av kommunens eller fylkeskommunens virksomhet og virksomheten i kommunens eller fylkeskommunens selskaper. Hensikten med risiko- og vesentlighetsvurderingen er å finne ut hvor det er størst behov for forvaltningsrevisjon.

Planen skal vedtas av kommunestyret og fylkestinget selv. Kommunestyret og fylkestinget kan delegere til kontrollutvalget å gjøre endringer i planen.

RM Revisjon Midt-Norge

Utenforskap og psykisk helse

Bindal kommune

Prosjektplan forvaltningsrevisjon

FR1375

2026

1 FAKTA OM OPPDRAGET

FORMÅL

Formålet med forvaltningsrevisjonen er å undersøke hvordan Bindal kommune arbeider med å forebygge, avdekke og følge opp unge voksne som ikke er i arbeid eller utdanning. Prosjektet skal gi kunnskap om omfang og kjennetegn ved utenforskap blant unge voksne i Bindal kommune. I tillegg vil revisor vurdere kommunens planer, rutiner og strategier for å forebygge og motvirke utenforskap samt at revisor vil se på hvordan kommunen følger opp unge voksne i utenforskap.

PROBLEMSTILLINGER

- I hvilken grad står unge voksne i Bindal kommune utenfor arbeid, utdanning eller opplæring, og hvilke utfordringer har denne gruppen knyttet til psykisk helse?
- I hvilken grad har Bindal kommune planer, strategier og rutiner for å forebygge og motvirke utenforskap blant unge?
- I hvilken grad følger kommunen opp unge voksne i utenforskap i tråd med rutiner, planer og nasjonale føringer/anbefalinger?

TIDS- OG RESSURSBRUK

Timeforbruk: 300 timer

Rapport til sekretær: Tobias Langseth

OPPDRAGSANSVARLIG REVISOR

Johannes O. Nestvold

jne@rmnsa.no

Tlf. 900 123 68

1 MANDAT

1.1 Bestilling

Kontrollutvalget i Bindal kommune bestilte et forvaltningsrevisjonsprosjekt om «Utenforskap og psykisk helse». Bestillingen ble vedtatt i kontrollutvalgets møte 10.11.2025, sak 17/25. Kontrollutvalget ba Revisjon Midt-Norge utarbeide forslag til prosjektplan på bakgrunn av de signalene som fremkom i møtet, for behandling i egen sak.

1.2 Bakgrunnsinformasjon

Utenforskap blant unge er en av de mest alvorlige samfunnsutfordringene både nasjonalt og lokalt. Unge i alderen 15–29 år som står utenfor arbeid, utdanning eller opplæring over lengre tid har økt risiko for varig marginalisering, fattigdom og psykiske helseutfordringer. Ifølge SSB var 9,9 prosent av unge mellom 15 og 29 år i Norge verken i arbeid, utdanning eller opplæring i 2023.[1] Det foreligger undersøkelser som tyder på at utenforskap i ung alder og psykisk helse har en gjensidig påvirkning. En rapport fra 2025 peker på stress knyttet til skole og mobbing som faktorer som kan være mulig årsaker til økning i psykiske utfordringer for barn og unge.[2] I en rapport fra 2021 om unge som står utenfor arbeidslivet og utdanning fremgår det blant annet for personer opp til 35 år at årsaken "til uføretrygden skyldes i stor grad psykiske lidelser."[3] Ungdata-undersøkelser viser at andelen unge som rapporterer om psykiske helseplager har vært økende, men at denne trenden har snudd noe de siste fire årene.[4] Stortingsmelding "Tro på framtida – uansett bakgrunn" retter søkelys på like muligheter og legger sterk vekt på forebygging, tidlig innsats og samarbeid på tvers av sektorer og forvaltningsnivå.[5] Det er et overordnet mål å redusere utenforskap betydelig innen 2035. Opptrappingsplanen for psykisk helse 2023–2033 ligger fast som nasjonal føring for forebygging, lavterskeltilbud og sammenheng i tjenester.[6] Innen helsesektoren er det

---

[1] SSB. (2024). Tilknytning til arbeid, utdanning og velferdsordninger. Statistisk sentralbyrå. Hentet fra: Tilknytning til arbeid, utdanning og velferdsordninger – SSB

[2] FHI. (2025). Folkehelserapportens temautgave 2025: Barn og unges psykiske helse. Folkehelseinstituttet. Hentet fra:Folkehelserapportens temautgave 2025: Barn og unges psykiske helse - FHI

[3] Sluttrapport NEET 204025. Integrerings- og mangfoldsdirektoratet. Hentet fra: Microsoft Word - IM Sluttrapport NEET 204025.docx

[4] NOVA. Ungdata 2025. OsloMet / NOVA. Hentet fra: Ungdata 2025

[5]Barne- og familiedepartementet.*Tro på framtida – uansett bakgrunn (Oppvekstmeldinga)*. Meld. St. 28 (2024–2025). Regjeringen. Hentet fra: Meld. St. 28 (2024–2025)

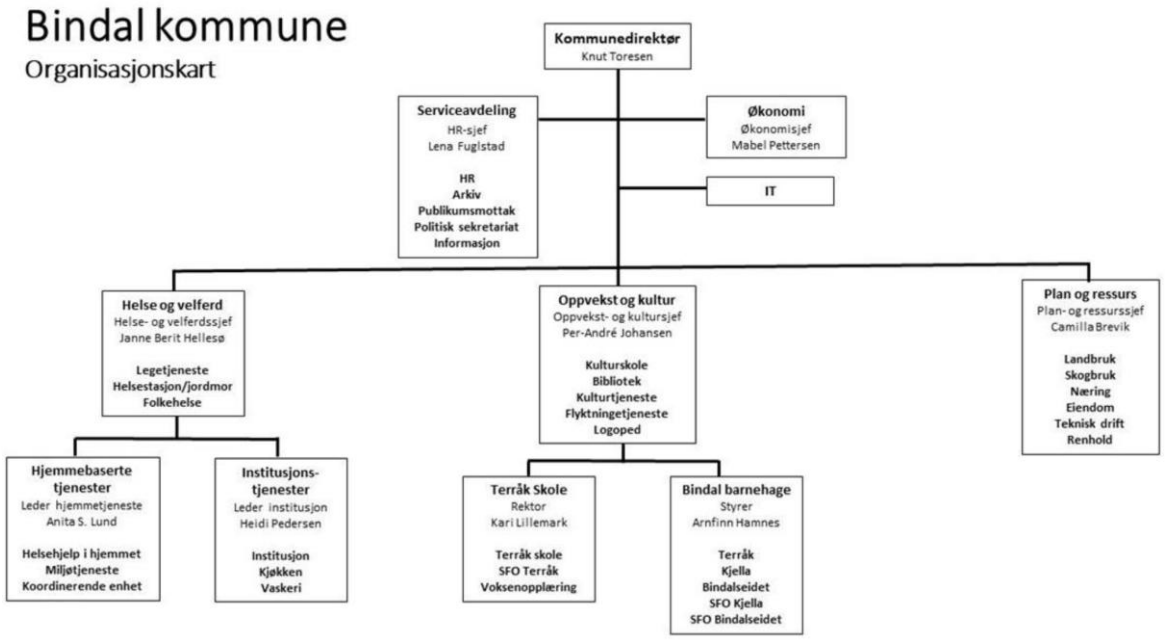
[6] Helse- og omsorgsdepartementet. *Opptrappingsplan for psykisk helse (2023-2033)*. Meld. St. 23 (2022–2023).Hentet fra: Meld. St. 23 (2022–2023)

utarbeidet pakkeforløp for barn/unge[7], for voksne[8] og TSB (rusbehandling).[9] Kommunene er pålagt å samarbeide om oppfølging av unge i risiko, bl.a. gjennom partnerskap mellom skole, NAV og helse.[10]

For mindre kommuner som Bindal kan utfordringene være særskilt store. NAV sin rapport om utenforskap i arbeidslivet fra 2024 viser at over 20 prosent av befolkningen i Bindal mellom 20 og 29 år er plassert i kategorien utenforskap.[11]

1.3 Kommunens organisering

Figur 1. Administrativ organisering i Bindal kommune



Kilde: Bindal kommune

Bindal kommune er organisert etter en sektormodell med tre hovedsektorer: oppvekst og kultur, helse og velferd samt plan og utvikling. Kommunedirektøren leder den strategiske ledergruppen, som består av HR-funksjonen, sektorlederne og økonomifunksjonen. Per

[7] Helsedirektoratet. Psykiske lidelser – barn og unge. Hentet fra: Psykiske lidelser – barn og unge - Helsedirektoratet

[8] Helsedirektoratet. Psykiske lidelser – voksne. Hentet fra: Psykiske lidelser – voksne - Helsedirektoratet

[9] Helsedirektoratet. Rusbehandling (TSB). Hentet fra: Rusbehandling (TSB) - Helsedirektoratet

[10] Bla opplæringsloven § 24, NAV-loven § 15a

[11] NAV. (2024). Utenforskap fra arbeidslivet. Hentet fra: Utenforskap fra arbeidslivet - nav.no

31.12.2022 hadde kommunen 183 ansatte, tilsvarende 155,4 årsverk, med en kjønnsfordeling på 139 kvinner og 44 menn[12].

Bindal kommune deltar i interkommunal tjeneste når det gjelder pedagogisk-Psykologisk Tjeneste (PPT), da gjennom PPT Sør-Helgeland[13]. Tilsvarende interkommunale samarbeid gjelder for barnevern hvor Brønnøy kommune er vertskommune[14], og for NAV hvor Nærøysund er vertskommune[15].

I januar 2026 ligger arbeidsledigheten i Bindal på 3,3 %, som er høyere enn nivået i Nordland (1,8 %) og landet totalt (2,3 %)[16], men likevel klart lavere enn toppunktet i årene etter konkursen i Binddalsbruket, hvor ledigheten i 2014 da var på 8,3 %[17].

I kommuneplanens samfunnsdel for Bindal kommune (2014-2024) er det i forbindelse med folkehelse vis til at forebygging av psykiske problemer og lidelser skal være et overordnet mål innenfor alt forebyggende arbeid som drives innenfor de kommunale tjenestene i forhold til barn, unge og voksne. Det er videre sagt at legetjenesten og NAV skal gi en «ekstra dytt» til de innbyggerne som har problemer med helsen og/eller økonomi. Det vil være viktig å belyse aktiviteter og trivselstiltak for ungdom framover. Dette skal bidra til å gi ungdommene og deres familier alternativer, slik at de kan få en grunnplattform til voksenlivet. I dette arbeidet bør man bygge på idretts- og kulturtiltak som bidrar til inkludering og mestring i det sosiale fellesskapet.

---

[12] Bindal kommune. *Kommunedirektør*. Hentet fra: Kommunedirektør - Hovedportal - Bindal kommune

[13] Bindal kommune. (2025). *Pedagogisk-psykologisk tjeneste (PPT)*. Hentet fra: https://www.bindal.kommune.no/tjenester/barnehage-skole-og-flyktningarbeid/pedagogisk-psykologisk-tjeneste-ppt/

[14] Bindal kommune. (2024). *Barnevern*. Hentet fra: https://www.bindal.kommune.no/tjenester/barnehage-skole-og-flyktningarbeid/bindal-barnehage/bedre-tverrfaglig-innsats-bti/barnevern/

[15] Bindal kommune. *NAV og sosiale tjenester*. Hentet fra: https://www.bindal.kommune.no/tjenester/helse-og-velferd/nav-og-sosiale-tjenester/nav-og-sosiale-tjenester.5004.aspx

[16] NAV. (2026). *Hovedtall om arbeidsmarkedet*. NAV. https://www.nav.no/no/nav-og-samfunn/statistikk/arbeidssokere-og-stillinger-statistikk/hovedtall-om-arbeidsmarkedet

[17] Kommuneplanens samfunnsdel for Bindal kommune (2014-2024). Hentet fra: 180654.DOC

2 PROSJEKTDESIGN

Dette kapittelet redegjør for revisors forslag til løsning av oppdraget.

2.1 Problemstillinger

1. I hvilken grad står unge voksne i Bindal kommune utenfor arbeid, utdanning eller opplæring, og hvilke utfordringer har denne gruppen knyttet til psykisk helse?
2. I hvilken grad har Bindal kommune planer, strategier og rutiner for å forebygge og motvirke utenforskap blant unge?
3. I hvilken grad følger kommunen opp unge voksne i utenforskap i tråd med rutiner, planer og nasjonale føringer/anbefalinger?

Den første problemstillingen er beskrivende, der kommunen ikke blir vurdert mot kriterier. Her vil revisor se nærmere på omfanget av ungt utenforskap i aldersgruppen 15–29 år i Bindal kommune. Det innebærer å kartlegge hvor mange unge i kommunen som står utenfor arbeid, skole eller opplæring, og hvordan dette har utviklet seg de siste fem-ti årene. Kartleggingen kan videre belyse hvordan utenforskapet fordeler seg på kjønn, alder og utdanningsnivå. Revisor kan se nærmere på indikatorer knyttet til psykisk helse for denne gruppen, herunder for eksempel tall fra Ungdata-undersøkelsen, statistikk over bruk av helsetjenester og medisinbruk. Det kan også undersøkes hvilke indikatorer fra grunnskole og videregående skole som kan gi innsikt i risikofaktorer for utenforskap. For å sette funnene i perspektiv, kan kommunen bli sammenlignet med kommuner fra samme KOSTRA-gruppe og landsgjennomsnittet. Det kan også være viktig å vurdere særskilte utfordringer som følger av å være en liten kommune, for eksempel begrenset tilgang på spesialiserte tjenester eller færre arenaer for arbeid og utdanning.

Den andre problemstillingen setter søkelys på om kommunen har etablert et helhetlig planverk og rutiner som understøtter arbeidet med å forebygge og motvirke utenforskap. Et sentralt spørsmål kan være i hvilken grad det finnes rutiner og planer som tydelig fordeler ansvar mellom de ulike tjenestene, herunder NAV, psykisk helse, barnevern og videregående skoler. Videre kan det være aktuelt å se på om kommunen har utarbeidet rutiner og planer som sikrer samarbeid på tvers av tjenester og forvaltningsnivå, både internt i kommunen og med eksterne aktører. Et tredje moment kan være om kommunen har rutiner og planer som bidrar til at unge i risiko for utenforskap identifiseres og fanges opp på et tidlig tidspunkt. Gjennomgangen kan dermed belyse om kommunens arbeid er tilstrekkelig planlagt, koordinert og forankret til å møte utfordringer med ungt utenforskap på en systematisk måte.

Den tredje problemstillingen handler om hvordan kommunen faktisk følger opp unge voksne som befinner seg i utenforskap, og om oppfølgingen skjer på en systematisk og helhetlig måte. Et sentralt spørsmål kan være i hvilken grad de ulike tjenestene, som NAV, psykisk helse,

barnevern og skole, gir nødvendig og koordinert oppfølging til den enkelte. Videre kan revisjonen belyse hvordan samarbeidet mellom aktører på tvers av forvaltningsnivå og sektorer fungerer i praksis. Det kan bli tematisert hvordan kommunen legger til rette for og følger opp dette samarbeidet, og om det skjer i tråd med etablerte planer og rutiner. Et tredje fokuspunkt kan være om kommunen faktisk sikrer at de rutiner og planer som skal fange opp unge i risiko, også fungerer etter hensikten i praksis. Revisjonen kan undersøke både omfanget og kvaliteten på oppfølgingen, samt i hvilken grad kommunens arbeid samsvarer med nasjonale føringer og anbefalinger på feltet.

2.2 Avgrensing

Revisjonen avgrenses til bosatte unge i Bindal kommune i alderen 15–29 år og til spørsmålet om utenforskap definert som å være utenfor arbeid, ordinær utdanning eller opplæring.

Revisjonen vurderer systemer, styring og samhandling. Det vil i liten grad være søkelys på enkeltvedtak eller data på individnivå. Slik revisor vurderer det i dag, vil vi ikke innhente informasjon direkte fra personer i målgruppen. Revisor vil vurdere behovet for dette fortløpende.

Økonomiske konsekvenser blir omtalt bare i den grad det fremstår hensiktsmessig for å svare ut ovenfor nevnte problemstillinger.

2.3 Kilder til kriterier

Grunnloven og menneskerettigheter

- Grunnloven (særlig § 92 om menneskerettighetene og § 104 om barns rettigheter)
- FNs barnekonvensjon (CRC)
- FNs konvensjon om rettighetene til personer med nedsatt funksjonsevne (CRPD)

Lover og forskrifter

- Kommuneloven
- Forvaltningsloven (saksbehandling, habilitet, utredningsplikt m.m.)
- Helse- og omsorgstjenesteloven §§ 3-1, 3-4, 4-1 og kap. 6
- Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten
- Folkehelseloven §§ 4–7 og forskrift om oversikt over folkehelsen
- Pasient- og brukerrettighetsloven
- Helsepersonelloven § 4
- Opplæringsloven (ny, i kraft 1.8.2024) og tilhørende forskrifter (bl.a. OT/oppfølging, fravær)

- Sosialtjenesteloven i NAV
- NAV-loven
- Forskrift om helsestasjons- og skolehelsetjenesten

Statlige føringer

- Meld. St. 28 (2024–2025) *Tro på framtida – uansett bakgrunn*
- Opptrappingsplan for psykisk helse 2023–2033
- Nasjonale pasientforløp for psykisk helse og rus (revidert, gjeldende fra 1.1.2025)

Bærekraftsmål

- FNs bærekraftsmål – særlig mål 3 (god helse), 4 (god utdanning), 8 (anstendig arbeid), 10 (mindre ulikhet), 11 (bærekraftige lokalsamfunn), og 17 (samarbeid for å nå målene)

2.4 Metoder

Det vil være nødvendig å innhente data på ulike måter, og primært ved å gjennomgå dokumenter og å intervjue relevante aktører.

Dokumentgjennomgang

Hovedformålet med dokumentgjennomgang vil være å avklare om kommunen har styringsgrunnlag, rutiner og samhandling som faktisk dekker risikobildet for ungt utenforskap, og om praksis følges opp. Sentrale dokumenter vi går gjennom er for eksempel overordnede styringsdokumenter: kommuneplan, handlings- og økonomiplan, temaplaner for oppvekst/folkehelse/psykisk helse, planstrategi. Videre vil revisor gå igjennom sektorvise planer og rutiner, som for eksempel NAV-avtaler (kommunal/statlig del), samarbeidsavtaler med spesialisthelsetjenesten, forebyggende plan (barnevernloven § 15-1) rutiner for tidlig identifisering, oppfølging av fravær, koordinerende enhet og ansvarsfordeling. Det vil videre være aktuelt å se på dokumentasjon knyttet til internkontroll. Gjennomgang av statistikk vil være sentralt for å belyse den første problemstillingen.

Dokumentanalyse er en sentral metode i kommunal revisjon. Metoden er spesielt nyttig for å undersøke hvordan vedtatte strategier og rutiner er fulgt opp i praksis. Den gir også mulighet til å identifisere avvik mellom mål og ambisjoner, og faktisk gjennomføring. En svakhet ved dokumentanalyse er at den primært baserer seg på allerede eksisterende materiale, som kan være utdatert, mangelfullt eller skrevet med tanke på å fremstille kommunen i et positivt lys. Metoden gir heller ikke innsikt i hvordan ansatte tolker eller praktiserer innholdet i dokumentene. Videre kan analysen bli tidkrevende hvis dokumentmengden er stor, og det kan være utfordrende å vurdere kvaliteten og troverdigheten til informasjonen. Disse svakhetene

kan imidlertid kompenseres ved å kombinere dokumentanalyse med andre metoder, som intervjuer eller observasjon, for å sikre et mer helhetlig bilde.

Intervju

Formålet med gjennomføring av intervju vil være å forstå hvordan rutiner og samarbeid fungerer i praksis, og teste dokumenterte ordninger mot faktisk gjennomføring.

Det vil være aktuelt å gjennomføre intervjuer av kommunedirektør, kommunalsjef oppvekst/helse, NAV-leder, folkehelsekoordinator, skoleledelse, skolehelsetjeneste, psykisk helse og rus, barnevern (forebyggende), koordinerende enhet, NAV veiledere.

Det vil være aktuelt å gjennomføre semistrukturerte intervjuer knyttet til tema som tidlig identifisering og oppfølging, ansvarsfordeling og samarbeidsrutiner, gjennomføring i praksis, styringsinformasjon og resultat/effekt.

Intervju er en metode som gir dypere innsikt i ansattes erfaringer, oppfatninger og praksis. Denne tilnærmingen gjør det mulig å utforske årsakssammenhenger, kontekst og nyanser som ikke fanges opp gjennom dokumentanalyse eller spørreundersøkelser. Intervjuer gir fleksibilitet til å stille oppfølgingsspørsmål og avdekke uventede temaer. Den øker også validiteten av en undersøkelse fordi det gir mulighet for å sammenligne informasjon på tvers av kilder. Metoden er derfor viktig for å sikre en helhetlig analyse og riktig vurdering av kommunens drift og forbedringsmuligheter. Intervju som metode kan ha noen svakheter. Det er tids- og ressurskrevende arbeid, og det er viktig å være bevisst at informasjon om praksis og opplevelser som gis i intervjuer er subjektive. Det kan også være utfordringer knyttet til hva som anses sosialt akseptable svar, kvaliteten på informasjon man får ut av et intervju avhenger ofte av intervjuers ferdigheter. I tillegg kan tolking av data være krevende og føre til feiltolkninger. Disse svakhetene kan imidlertid reduseres gjennom god planlegging, triangulering av data og systematisk analyse.

Bruk av generative språkmodeller (KI)

Generative språkmodeller kan brukes som støtteverktøy for informasjonsinnhenting og analyse, samt for språk- og kvalitetskontroll. Verktøyene fatter ikke konklusjoner, og alle vurderinger er fullt og helt revisors ansvar. Intervjuer kan tas opp med samtykke for å sikre korrekt gjengivelse. Opptakene blir transkribert, og lydfilene slettes når transkripsjonen er kvalitetssikret. Verktøyene kan også benyttes til å utarbeide referatutkast basert på transkripsjonen; referatet kvalitetssikres alltid av revisor og blir alltid sendt til informant for godkjenning.

2.5 Prosjektteam

Oppdragsansvarlig revisor	Johannes O. Nestvold
Prosjektmedarbeider	Anne Grete Wold
Kvalitetssikrer	Eirik G. Seim
Kvalitetssikrer	Merete M. Montero

2.6 Milepælsplan

Bestillingsdato	10.11.2025
Prosjektplan til sekretær	24.02.2026
Oppstartsmøte	10.06.2026
Datainnsamling ferdig	18.10.2026
Rapport til uttalelse	15.12.2026
Rapport til sekretær	15.01.2027

Godøy, den 25. februar 2026

Johannes O. Nestvold

Oppdragsansvarlig revisor

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no

Revisjon Midt-Norge
Bidrar til forbedring

Tor Arne Stubbe

3.2.2026

Kontrollutvalget Bindal kommune
v/Tobias Langseth, SE-KON

Rapportering til kontrollutvalget i Bindal kommune

Kontrollutvalget har ihht leveranseavtale en tilgjengelig timeressurs på 185 timer pr år til risiko- og vesentlighetsvurdering, forvaltningsrevisjon, eierskapskontroll i perioden 2024-2027. Timerammen inkluderer reiser, møter osv.

I 2025 har RMN blant annet utført følgende:

FR1275 Kvalitet i skolen
FR1319 Informasjonssikkerhet og personvern
Risiko- og vesentlighetsvurdering

Timeforbruk 2024: **203,09 timer**

Timeforbruk 2025: **193,84 timer**

Revisjon Midt-Norge har som ambisjon at kontrollutvalget skal kunne utnytte sin årlige timeressurs mest mulig fleksibelt i perioden 2024-2027. Det vil si at et eventuelt mer-/mindreforbruk av timer søkes utlignet over 4-årsperioden. Mer-/mindreforbruk overføres ikke til neste periode.

Med vennlig hilsen

Tor Arne Stubbe
Fagleder forvaltningsrevisjon

Direkte ☎ 98608070 eller ✉ tor-arne.stubbe@revisjonmidtnorge.no

Til kontrollutvalget i Bindal kommune Sandnessjøen 02.03.2026

Saksbehandler:
Sekretariatsleder
Tobias Langseth

SAK 04/2026: AKTUELLE ORIENTERINGER FRA ADMINISTRASJONEN

1: Innledning og bakgrunn

Utveksling av informasjon og synspunkter mellom administrasjonen og kontrollutvalget utgjør en blant flere viktige forutsetninger for et vellykket kontrollarbeid i kommunen. Jf. utdrag fra KDDs veileder om kontrollutvalgets rolle og oppgaver [3. utgave, kapittel 4]:

Kontrollutvalsboka - regjeringen.no

Samspel og dialog mellom kontrollutvalet og kommunedirektøren

Administrasjonen og kontrollutvalet har eit felles ansvar for å leggje til rette for ein god dialog og eit godt samspel. Både administrasjonen og kontrollutvalet har som mål å sikre god kvalitet i tenesteproduksjonen og medverke til læring og forbetring i kommunen. Begge partar har difor interesse av at samarbeidet er godt. Ein god dialog mellom kontrollutvalet og kommunedirektøren kan sikre betre prioritering og planlegging av undersøkingane kontrollutvalet gjennomfører.

> *«En forutsetning for god samhandling mellom administrasjonen, kommunerevisjonen og kontrollkomiteen er gjensidig respekt for hverandres roller. At man har en felles forståelse for at målet er en positiv utvikling for kommunen. Administrasjonen er synlig til stede på Kontrollkomiteens møter for å svare på spørsmål.» (Kontrollutvalsleiar)*

Kommunedirektøren er den viktigaste kjelda til informasjon om internkontrollen i kommunen. Kontrollutvalet bør difor invitere administrasjonen til å orientere utvalet om aktuelle problemstillingar knytte til internkontrollen. Ein bør også sende kommunedirektøren kontrollutvalet si møteinnkalling til orientering.

2: Sekretariatets vurderinger

Som et ledd i dialogen mellom administrasjon og kontrollutvalg, inviteres kommunedirektøren forholdsvis jevnlig til å gi en orientering om aktuelle temaer til kontrollutvalgets medlemmer. Kommunedirektøren avgjør selv i hvilken grad det er hensiktsmessig å involvere sektorledere og/eller fagpersonell i prosessen.

3: Oppsummering og avslutning

Kontrollutvalget har avtalt følgende orientering fra administrasjonen:

- Ikke avtalt særskilt tema [opp til adm. å vurdere hva som kan være aktuelt og av interesse]

Forslag til vedtak:

Kontrollutvalget tar orienteringen fra administrasjonen til etterretning.