RM Revisjon Midt-Norge

Informasjonssikkerhet

Vega kommune

Prosjektplan forvaltningsrevisjon

FR 1322

2024

1 FAKTA OM OPPDRAGET

FORMÅL

Formålet med forvaltningsrevisjonen er å undersøke om kommunen sitt arbeid med informasjonssikkerhet og personvern er i tråd med regelverk og anerkjente standarder.

PROBLEMSTILLINGER

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

TIDS- OG RESSURSBRUK

Timeforbruk: 250 timer

Rapport til sekretær: 15.11.2025

OPPDRAGSANSVARLIG REVISOR

Hanne Marit Ulseth Bjerkan
hanne.bjerkan@revisjonmidtnorge.no

Tlf. 476 34 527

2 MANDAT

I dette kapitlet redegjøres det for bakgrunnen for utkast til prosjektplan.

2.1 Bestilling

Basert på plan for forvaltningsrevisjon har sekretær for kontrollutvalget bedt om å få tilsendt et prosjektutviklingsnotat som grunnlag for bestilling av en forvaltningsrevisjon om informasjonssikkerhet og personvern. Revisjon Midt-Norge har de siste årene gjennomført flere forvaltningsrevisjoner med dette teamet, eksempelvis i Bodø kommune på oppdrag fra Salten kommunerevisjon og i Melhus kommune. Basert på erfaringene fra gjennomførte forvaltningsrevisjonsprosjekter legger revisor i samråd med sekretær fram et forslag til prosjektplan som grunnlag for kontrollutvalgets bestilling.

Kommunene Brønnøy, Vega, Bindal, Sømna og Vevelstad har sammen dannet det kommunale oppgavefellesskapet Kystriket IKT, hvor Brønnøy kommune er kontorkommune. Kystriket IKT sitt formål er å samarbeide om IKT-tjenester for at den enkelte deltaker skal få utført sine lovpålagte oppgaver og andre offentlige oppgaver på en kostnadseffektiv og sikker måte. Kystriket IKT har ansvar for driftsplattformen som understøtter IKT-tjenestene i deltakerkommunene. Kommunene har gjort en felles anskaffelse av driftsleverandør som ekstern samarbeidspart for det kommunale oppgavefellesskapet.

Slik revisor har forstått det er forvaltningsrevisjonen aktuell for kommunene Brønnøy, Bindal, Sømna og Vega. Forvaltningsrevisjonene for dette temaet bør ses i sammenheng ettersom kommunene har et utstrakt samarbeid på området.

2.2 Informasjonssikkerhet og personvern

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

Informasjonssikkerhet omfatter:

- konfidensialitet (sikre at informasjonen ikke blir kjent for uvedkommende)
- integritet (sikre at informasjonen ikke blir endret utilsiktet av uvedkommende)

- tilgjengelighet (sikre at informasjonen er tilgjengelig ved behov).

Informasjonssikkerhet handler om hvordan en organisasjon sikrer informasjon og tjenester, og hvilke rutiner og prosesser den bruker. Sentralt her er sikkerhetsledelse og risikostyring. En god sikkerhetskultur er viktig, siden angrep kan forekomme i hele virksomheten, ikke bare på grunn av tekniske sårbarheter. I forvaltningsrevisjonen vil begrepet informasjonssikkerhet og IKT-sikkerhet (informasjons- og kommunikasjonsteknologi sikkerhet) brukes om hverandre.

Det er minst tre juridiske tilnærmeringer til sikkerhetsarbeidet. Disse er:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften), § 15 om internkontroll på informasjonssikkerhetsområdet.

Sikkerhetsloven stiller krav om at sikkerhetsstyringen skal gjennomføres planlagt og systematisk i et sikkerhetsstyringssystem, som samordnes med virksomhetens styrings-system. Personopplysningsloven gir bestemmelser om hvordan personopplysninger skal be-handles. I eForvaltningsforskriften er internkontroll på informasjonssikkerhetsområdet regulert. Forskriften krever at forvaltningsorganet skal ha en internkontroll på informasjonssikker-hetsområdet som bør være integrert som en del av virksomhetens helhetlige styringssystem.

Personopplysningsloven er bygget på noen grunnleggende personvernprinsipper, og alle som behandler personopplysninger må følge disse prinsippene. Datatilsynet skriver at prinsippene gir uttrykk for at behandling av personopplysninger skal skje på en måte som sikrer forutsigbarhet og forholdsmessighet for enkeltmenneske[1]. Tabellen nedenfor er basert på Datatilsynet sin gjennomgang av personvernprinsippene.

[1] Personvernprinsippene | Datatilsynet

Tabell 1. Personvernprinsippene

Prinsipp	Nærmere om prinsippene
Lovlig, rettferdig og gjennomsiktighet	Rettslig grunnlag for en planlagt behandling av personopplysninger. Behandlingen av personopplysninger skal være gjennomsiktig. Virksomhetene har en behandlingsansvarlig som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
Formålsbegrensing	Ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist.
Dataminimering	Begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet.
Riktighet	Korrekte opplysninger og skal oppdateres om nødvendig.
Lagringsbegrensning	Personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.
Integritet og konfidensialitet	Behandlingsansvarlig må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endring av personopplysninger.
Ansvarlighet	Punktet understreker ansvaret for å opptre i henhold til regelverket. Virksomhetene må kunne dokumentere at den har gjennomført tiltak for å etterleve personvernforordningen. Virksomheten må opptre proaktiv og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

Kilde: Datatilsynet

Norge har et eget ekspertorgan for informasjons- og objektsikkerhet, Nasjonal sikkerhets-myndighet (NSM), som er det nasjonale fagmiljøet for IKT-sikkerhet. NSM har utarbeidet en veileder i sikkerhetsstyring[2]. Veilederen beskriver sikkerhetsstyring som 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.

Utgangspunktet for sikkerhetsstyringen er risikovurderinger som omfatter informasjon om verdier, identifisering av trusler og avdekking av sårbarheter. Risikovurderingene danner grunnlaget for risikohåndteringen. Risikohåndtering omfatter etablering av sikkerhetstiltak, tilpasset de skjermingsverdige verdiene en virksomhet forvalter. Sikkerhetstiltak kan være både organisatoriske tiltak og tekniske tiltak. Organisatoriske tiltak er for eksempel roller og ansvar, kompetanse, retningslinjer, prosedyrer og rutiner. Tekniske tiltak er eksempelvis IKT-løsninger, brannmurer, skap, dører, rom og bygninger.

Figuren nedenfor illustrere sammenhengen i det som er beskrevet ovenfor.

[2] veileder-i-sikkerhetsstyring.pdf

Figur 1. Sammenhenger for sikkerhetsstyring.

NSM har også utarbeidet grunnprinsipper for IKT-sikkerhet[3] (NSM 2020) som er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene fokuserer på organisatoriske og teknologiske tiltak. Grunnprinsippene er inndelt i fire kategorier og er gjengitt i tabellen nedenfor.

Tabell 2. 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 Kontrollere dataflyt Ha kontroll på identiteter og tilganger Beskytte data i ro og i transitt Beskytte e-post og nettleser Etablere evne til gjenoppretting av data Integrere sikkerhet i prosess for endringshåndtering
3. Oppdage	**4. Håndtere og gjenopprette**
Oppdage og fjerne kjente sårbarheter og trusler Etablere sikkerhetsovervåkning Analysere data fra sikkerhetsovervåkning Gjennomføre inntrengingstester	Forberede virksomheten på håndtering av hendelser Vurdere og klassifisere hendelser Kontrollere og håndtere hendelser Evaluere og lære av hendelser

Kilde: Nasjonal sikkerhetsmyndighet 2020

[3] Introduksjon - Nasjonal sikkerhetsmyndighet

Organisering av tjenestene

Kommunene Brønnøy, Bindal, Sømna og Vega er revisjonsobjekt. Kommunene samarbeider innenfor IKT-området i det kommunale oppgavefellesskapet Kystriket IKT. Kystriket IKT er derfor sentral i revisjonen. Kommunene har inngått en avtale med en driftsleverandør innenfor IKT som har betydning for hvordan kommunene arbeider med informasjonssikkerhet og personvern.

3 PROSJEKTDESIGN

Kapittelet redegjør for revisors forslag til løsning av oppdraget.

3.1 Problemstillinger

I dette utkastet til felles prosjektplan er det utarbeidet to problemstillinger som skal besvares i prosjektet.

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

Den første problemstillingen tar utgangspunkt i hva som kreves av et styringssystem for informasjonssikkerhet. Risikovurderinger og risikohåndtering er sentralt her. Problemstillingen ser på om kommunen har vurdert hvilke informasjonsverdier kommunen har, hvilke trusler som finnes og hvor sårbar kommunen er hvis denne informasjonen ikke blir tilgjengelig eller kommer på avveie. Revisor vil se på om informasjonssikkerhet er en del av kommunens internkontrollsystem, uten at det er en revisjon av internkontrollen i kommunen. En del av problemstillingen er å se om kommunen ivaretar personopplysninger i tråd med krav i regelverket. Eksempelvis om kommunen har full oversikt over sin behandling av personopplysninger og om kommunen har etablert tiltak som sikrer at regelverket følges. Kommunen har blant annet plikt til å føre protokoller over behandlingsaktivitetene de gjennomfører.

Den andre problemstillingen handler om konkrete organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten. Rammene for problemstillingene er Nasjonal sikkerhets-myndighets grunnprinsipper for IKT-sikkerhet, jfr. tabell 2. Nedenfor er de fire prinsippene listet opp og det er gitt eksempler på hva som er relevant å undersøke på de fire områdene. Listen er ikke uttømmende. Revisor vil også vurdere å benytte ISO 27001 om ledelsessystemer for informasjonssikkerhet.

- Identifisere og kartlegge
    - Om kommunen har oversikt over enheter i IKT-systemet og programvare.
    - Om kommunen har oversikt over brukere av systemet.
- Beskytte og opprettholde
    - Om kommunen har etablert og dokumentert en sikker IKT-arkitektur.
    - Om kommunen har styring med sikkerhetsoppdateringer og en plan for sikkerhetskopieringer og om de tar sikkerhetskopier.

- Oppdage
    - Om kommunen har et system for å overvåke sikkerheten og analysere data fra overvåkningen.
    - Om kommunen gjennomfører inntrengningstester.
- Håndtere og gjenopprette
    - Om kommunen har en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon og loggføring) og en plan for gjenoppretting.

3.2 Avgrensing

Personopplysningsloven stiller 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.

På området informasjonssikkerhet finnes det mest sannsynlig gradert informasjon. Revisor vil undersøke dette så langt som mulig, men det er begrensede muligheter for å omtale hva som finnes av hensyn til sikkerheten.

3.3 Kilder til kriterier

Aktuelle kilder til revisjonskriterier er:

- Lov om kommuner og fylkeskommuner kapittel 25 (kommuneloven)
- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet
- NSMs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- ISO 27001
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet

3.3.1 Mulige revisjonskriterier

Revisjon Midt-Norge har de siste årene gjennomført flere forvaltningsrevisjoner innenfor informasjonssikkerhet og personvern. Dette gir oss et grunnlag for å bygge videre på kunnskap

fra disse revisjonene, og muligheten til å ta utgangspunkt i revisjonskriterier som vi har erfart fungerer god for å belyse problemstillingene.

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

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

Identifisere og kartlegge

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

Beskytte og opprettholde

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

Oppdage

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

Håndtere og gjenopprette

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

3.4 Metoder for innsamling av data

Revisor vil innhente dokumentasjon fra kommunen for å besvare problemstillingene. Gjennomgang av kommunale dokumenter vil være en viktig datakilde for å undersøke hvordan kommunen jobber med informasjonssikkerhet. Eksempler på dokumenter er risikovurderinger, beredskapsplaner, politiske dokumenter som gir føringer, rutinebeskrivelser for ulike tiltak og ulike planer innenfor informasjonssikkerhet, dokumentasjon av behandling av person-opplysninger med mer. Driftsavtalen med driftsleverandøren vil være et sentralt dokument for revisor. Dokumentgjennomgang er en god metode for å finne frem til opplysninger som er nødvendige og relevante for kommunal oppgaveløsning og forvaltning. Det offentlige har i enkelte tilfeller plikt til å dokumentere sitt arbeid og sin regeletterlevelse. Informasjonssikkerhet og personvern er underlagt internkontroll og er relevant å se på meldte avvik på dette området.

Det vil bli gjennomført intervjuer med kommunens ledelse og de som arbeider innenfor det kommunale oppgavefellesskapet, for å få dybdekunnskap om hvordan arbeidet med informasjonssikkerhet foregår i kommunen og for å forstå sammenhengene. Intervjuene kan gi informasjon om at det som er beskrevet i dokumentasjonen fungerer i praksis. Det kan også være aktuelt å intervjue personvernombudet i kommunen og andre ansatte i kommunen.

Forvaltningsrevisjoner på området informasjonssikkerhet og personvern vil kunne komme i berøring med informasjon om sikkerhetsmessige forhold som ikke bør offentliggjøres. Det betyr at ikke alle detaljer i slike forvaltningsrevisjoner kan legges fram i en rapport.

Revisor vil underveis vurdere å gjennomføre en kort elektronisk spørreundersøkelse til ansatte i kommunen, hvis dette lar seg gjøre på en enkel måte. Hensikten er å kartlegge bevisstheten om og opplæring i informasjonssikkerhet. Erfaringer fra tidligere revisjoner er at mange peker på at brukerne er den største sikkerhetstrusselen.

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Oppdragsansvarlig forvaltningsrevisor	Hanne Marit Ulseth Bjerkan
Prosjektmedarbeider	Anne Grete Wold
Kvalitetssikrer	Anne Ølnes
Kvalitetssikrer	Margrete Haugum

Prosjektteamet vil håndtere alle fire forvaltningsrevisjonene. Alle får oppdragsansvar for en kommune, er medarbeider for en kommune og kvalitetssikrer for to kommuner.

4.2 Milepælsplan

Bestillingsdato	
Prosjektplan til sekretær	Utkast 20.11.2024
Oppstartsmøte	Innen 01.05.2025
Datainnsamling ferdig	30.08.25
Rapport til uttalelse	15.10.25
Rapport til sekretær	15.11.25

Trondheim 20.11.2024

Hanne Marit Ulseth Bjerkan

Oppdragsansvarlig revisor

KILDER

Lov om nasjonal sikkerhet (Sikkerhetsloven)

Lov om behandling av personopplysninger (Personopplysningsloven)

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

«Veileder i sikkerhetsstyring», Nasjonal sikkerhetsmyndighet

«NSMs Grunnprinsipper for IKT-sikkerhet», Nasjonal sikkerhetsmyndighet

Datatilsynet – personvernprinsippene

Jøsang, A. (2021) Informasjonssikkerhet. Teori og praksis. Universitetsforlaget, Oslo

ISO 27001 Ledelsessystemer for informasjonssikkerhet

Kommunens hjemmeside

Revisjon

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no