

Informasjonssikkerhet og personvern

Nesna kommune
Prosjektplan forvaltningsrevisjon

FR1395

2026



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 å ivareta informasjonssikkerhet og personvern, i samsvar med krav i regelverket?
2. Har kommunen tilfredsstillende organisatoriske tiltak for å ivareta informasjonssikkerhet og personvern?

TIDS- OG RESSURSBRUK

Timeforbruk: Inntil 300 timer

Rapport til sekretær: 1. april 2027

OPPDRAGSANSVARLIG REVISOR

Anne Grete Wold

anne.wold@revisjonmidtnorge.no

Tlf. 99100669

2 MANDAT

2.1 Bestilling

Kontrollutvalget i Nesna kommune har i sak 02/2026, i møte 13. april 2026, bestilt et forvaltningsrevisjonsprosjekt knyttet til temaet «Informasjonssikkerhet og personvern». Utvalget ber om at Revisjon Midt-Norge utarbeider forslag til prosjektplan.

2.2 Om informasjonssikkerhet og personvern

En forvaltningsrevisjon av informasjonssikkerhet og personvern er relevant fordi kommunene stadig blir mer digitaliserte og forvalter store mengder informasjonsverdier og sensitive personopplysninger om ansatte og innbyggere. Samtidig har risikoen for dataangrep og utilsiktede sikkerhetsbrudd økt betydelig de siste årene. Kommunene er derfor avhengige av å ha gode styringssystemer, risikovurderinger og internkontroll for å sikre konfidensialitet, integritet og tilgjengelighet i sine tjenester. Informasjonssikkerhet og personvern er regulert gjennom flere sentrale regelverk, blant annet kommuneloven, personopplysningsloven (GDPR), digitalsikkerhetsloven og eForvaltningsforskriften. Disse stiller krav til internkontroll, dokumentasjon og systematisk oppfølging av sikkerhets- og personvernarbeidet.^{1 2 3}

Videre viser erfaringer fra flere kommuner at menneskelige feil, manglende kompetanse og svikt i organisatoriske rutiner ofte utgjør en betydelig sikkerhetsrisiko. En forvaltningsrevisjon kan derfor bidra til å vurdere om kommunen har etablert hensiktsmessige roller, ansvar, rutiner og opplæringstiltak, og om ledelsen har tilstrekkelig styring og kontroll på området.

Informasjonssikkerhet handler om å beskytte informasjonsverdier mot skade eller tap. En informasjonsverdi kan være både informasjonen i seg selv og ressursene som blir brukt til å lagre, behandle eller formidle informasjonen. Eksempler på informasjonsverdier er data, fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og menneskelige ressurser (Jøsang 2021⁴). Ifølge Jøsang er det ingen tydelig avgrensning av hva som kan være informasjonsverdi. Derimot sier Jøsang at det er en klar definisjon på hvordan informasjonsverdier kan skades, nemlig gjennom brudd på *konfidensialitet*, *integritet* og *tilgjengelighet*.

¹ [NSM Risikorapport 2026](#)

² [Etablere internkontroll | Datatilsynet](#)

³ [Slik sikrer du oppfølging av personvern og informasjonssikkerhet - Hjem](#)

⁴ Jøsang, Audun (2021) Informasjonssikkerhet: teori og praksis. Universitetsforlaget.

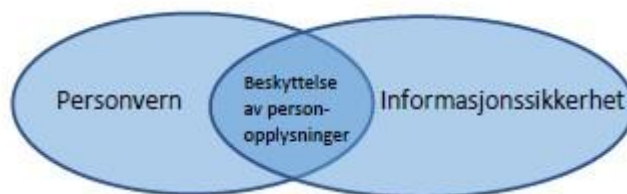
Informasjonssikkerhet omfatter derfor ivaretagelse av:

- Konfidensialiteten; å sikre at informasjonen ikke blir kjent for uvedkommende
- Integriteten; å sikre at informasjonen ikke blir endret utilsiktet av uvedkommende
- Tilgjengeligheten; å sikre at informasjonen er tilgjengelig ved behov.

Å arbeide med informasjonssikkerhet handler om hvordan en organisasjon sikrer informasjon og tjenester, og hvilke rutiner og prosesser den bruker. Da er *internkontroll*, *sikkerhetsledelse* og *risikostyring* sentrale begreper. En god sikkerhetskultur er viktig, siden angrep kan forekomme i hele virksomheten og som resultat av menneskelig svikt, og ikke bare på grunn av tekniske sårbarheter.

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger⁵. Begrepet innebærer også vern av enkeltpersoners rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv. Som innbyggere skal vi i størst mulig grad kunne bestemme over egne personopplysninger. Også innenfor dette området vil ivaretagelse av konfidensialitet og integritet stå sentralt.

Personvern og informasjonssikkerhet er to fagområder som har mye til felles, men som også er forskjellige. Det kan illustreres i figuren nedenfor:



Figur 1. Sammenhengen mellom informasjonssikkerhet og personvern⁶.

Det juridiske grunnlaget for informasjonssikkerhet og personvern i en forvaltningsrevisjon av en kommune, vil primært være basert på følgende lovgrunnlag:

- Lov om kommuner og fylkeskommuner, om internkontroll kap 25, § 25-1
- Forskrift om elektronisk kommunikasjon med og i forvaltningen § 15
- Lov om behandling av personopplysninger med personvernforordningen (GDPR)
- Lov om digital sikkerhet

⁵ [Personvern | Datatilsynet](#)

⁶ [kommunedirektorens-verktoykasse.pdf](#)

Lov om nasjonal sikkerhet (sikkerhetsloven) kan i noen grad være relevant hvis kommunen ivaretar nasjonale sikkerhetsinteresser som innehar skjermingsverdig informasjon.

Sikkerhetsloven har likevel et mer begrenset anvendelsesområde og gjelder bare for virksomheter, informasjon, objekter eller infrastruktur som er av betydning for nasjonale sikkerhetsinteresser.

I tillegg til de juridiske føringene, fungerer Nasjonal sikkerhetsmyndighet (NSM) sine **grunnprinsipper for informasjonssikkerhet** som rettesnor for virksomheters arbeid med informasjonssikkerhet. Grunnprinsippene er ikke rettslig bindende i seg selv, men de kan forstås som en operasjonalisering av de generelle sikkerhetskravene som følger av lov og forskrift samt erfaring fra det kontinuerlige trusselbildet⁷. Prinsippene fungerer derfor ofte som et anerkjent normgrunnlag for hva som kan anses som god praksis innen informasjonssikkerhet. Grunnprinsippene viser at virksomheter skal:

- Ha oversikt over enheter, programvare og tilganger (identifisere og kartlegge)
- Ivareta sikkerhet i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer (beskytte og oppdatere)
- Ha kontroll av sikkerhetstilstand og ledelsens gjennomgang (oppdage)
- Sikre håndtering, gjenoppretting og læring av hendelser (håndtering og gjenoppretting)

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 enkeltmenneske⁸. Følgende prinsipper gjelder:

1. **Lovlig, rettferdig og gjennomsiktig**; det skal være rettslig grunnlag for en planlagt behandling av personopplysninger, at behandlingen av personopplysninger skal være gjennomsiktig, og at virksomhetene har en behandlingsansvarlig som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
2. **Formålsbegrensing**; ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist.
3. **Dataminimering**; man skal begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet
4. **Riktig**; opplysningene skal være korrekte og oppdateres om nødvendig.

⁷ [NSM Risikorapport 2026](#)

⁸ [Personvernprinsippene | Datatilsynet](#)

5. **Lagringsbegrensning:** personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.
6. **Integritet og konfidensialitet:** behandlingsansvarlig må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endring av personopplysninger
7. **Ansvarlig:** 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 etterleveres til enhver tid.

Personopplysningsloven gir bestemmelser om hvordan personopplysninger skal behandles.

I eForvaltningsforskriften er internkontroll på informasjonssikkerhetsområdet regulert.

Forskriften krever at forvaltningsorganet skal ha en internkontroll på informasjonssikkerhetsområdet som bør være integrert som en del av virksomhetens helhetlige styringssystem.

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 som er tilpasset de informasjonsverdiene en virksomhet forvalter, og 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 brannmurer, overvåkingssystemer, skap, dører, rom og bygninger.

Figuren nedenfor illustrere sammenhengen i det som er beskrevet ovenfor.



Figur 2. Sammenhenger for sikkerhetsstyring.

NSM sine grunnprinsipper for IKT-sikkerhet⁹ er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene bygger på organisatoriske og teknologiske tiltak i figur 2, og er inndelt i fire kategorier gjengitt i tabellen nedenfor.

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 endringsprosesser
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

Tabell 1. Grunnprinsipper for IKT-sikkerhet. Kilde: NSM

2.3 Organisering Nesna kommune

Ifølge kommunens hjemmeside og organisasjonskart¹⁰, er Nesna kommune organisert med kommunedirektør og fire underliggende kommunalledere inkludert økonomileder.

Økonomileder har ifølge organisasjonskartet ansvar for IKT-tjenesten, i tillegg til HR, servicetorg og regnskap/lønn. Kommunen har en fagleder for IKT/sikkerhetsleder og en digitalrådgiver.

⁹ [Introduksjon - Nasjonal sikkerhetsmyndighet](#)

¹⁰ [organisasjonskart-per-19jan2026.pdf](#)

3 PROSJEKTDESIGN

3.1 Problemstillinger

Revisor har følgende forslag til problemstillinger for å besvare bestillingen:

- 1. Har kommunen etablert et styringssystem for å ivareta informasjonssikkerhet og personvern, i samsvar med krav i regelverket?**
- 2. Har kommunen tilfredsstillende organisatoriske tiltak for å ivareta informasjonssikkerhet og personvern?**

Den første problemstillingen tar utgangspunkt i kravene som gjelder for kommunens styringssystem for informasjonssikkerhet og personvern. Revisor vil undersøke om kommunen har fastsatt mål, strategier, roller og ansvar for arbeidet, og om kommunen har kartlagt sine informasjonsverdier og vurdert relevante trusler, sårbarheter og risikoer. Det vil også være aktuelt å undersøke om informasjonssikkerhet og personvern inngår i kommunens internkontroll, om kommunen følger opp identifiserte risikoer, og om den har systemer for å melde, håndtere og lære av avvik. Kommunens opplæring og informasjon til ansatte på området vil inngå.

Revisor vil videre undersøke om kommunen har oversikt over behandlingen av personopplysninger, vurderer personvernkonsekvenser der regelverket krever det, og har etablert en ordning med personvernombud.

For den andre problemstillingen vil det være aktuelt å se nærmere på om kommunen har etablert tiltak for å beskytte informasjonssystemene, gjennom å undersøke kommunens håndtering av grunnprinsippene som NSM har etablert.

Utdypingen av problemstillingene angir sentrale temaer for undersøkelsen, og er ikke uttømmende.

3.2 Avgrensing

Personopplysningsloven stiller krav til behandling av personopplysninger. Det ligger ikke i rammene for denne revisjonen å gå i dybden på alle de spesifikke kravene som omhandler behandling av personopplysninger. Oppmerksomheten vil bli rettet mot kommunens system for behandling av personopplysninger. Revisjonen vil heller 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.

Revisor vil ikke undersøke tekniske tiltak for å beskytte informasjonssystemene, som for eksempel brannmurer, overvåkingssystemer, skap, dører, rom og bygninger. Det vil heller ikke bli utført inntregningstester for å avdekke reelle sårbarheter i systemer, konfigurasjoner, tilganger eller eksponerte tjenester.

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

3.3 Kilder til kriterier

Aktuelle kilder til revisjonskriterier er:

- Lov om kommuner og fylkeskommuner kapittel 25 (kommuneloven)
- Lov om behandling av personopplysninger (personopplysningsloven), inkludert GDPR
- Lov om digital sikkerhet (digitalsikkerhetsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet
- Grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet
- ISO 27001

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 kilde for å undersøke hvordan kommunen jobber med informasjonssikkerhet. Eksempler på dokumenter er rolle- og ansvarsbeskrivelser, risikovurderinger, beredskapsplaner, politiske dokumenter som gir føringer, rutinebeskrivelser for ulike tiltak og ulike planer innenfor informasjonssikkerhet, dokumentasjon av behandling av personopplysninger med mer. Eventuelle avtaler med driftsleverandøren vil også være sentrale dokumenter 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 det er derfor relevant å se på meldte avvik på området.

Det vil bli gjennomført intervjuer med kommunens ledelse, eventuelt rådgivere som har oppgaver knyttet til teamet og utvalgte ansatte som arbeider med IKT-drift, 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 intervju personvernombudet 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.

Revisor vil underveis vurdere om det kan være behov for å gjennomføre en 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 viser at ansattes kompetanse, holdninger og bevissthet ofte er den største enkeltfaktoren for sikkerhetsrisiko.

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Oppdragsansvarlig revisor	Anne Grete Wold
Prosjektmedarbeider	Cathrine Berg Mortensen
Kvalitetssikrer	Anna Ølnes
Kvalitetssikrer	Margrete Haugum

4.2 Milepælsplan

Bestillingsdato	13. april 2026
Prosjektplan til sekretær	01. september 2026
Oppstartsmøte	Innen 30.november 2026
Datainnsamling ferdig	Innen 30. januar 2027
Rapport til uttalelse	01. mars 2027
Rapport til sekretær	30. mars 2027

Steinkjer, 1. september 2026

Anne Grete Wold

Oppdragsansvarlig revisor



Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no