

Informasjonssikkerhet og personvern

Overhalla kommune
Prosjektplan forvaltningsrevisjon

2025

FR1364



1 FAKTA OM OPPDRAGET

FORMÅL

Formålet med forvaltningsrevisjonen er å gi svar på kontrollutvalgets bestilling, om kommunen sitt arbeid med informasjonssikkerhet og personvern er i tråd med regelverk og anerkjente standarder.

PROBLEMSTILLINGER

- 1) Har Overhalla kommune etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstillende krav i regelverket (systematisk rammeverk)?
- 2) Har Overhalla kommune etablert tilfredsstillende avtaler med og oppfølging av Namsos kommune (vertskommunen), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

TIDS- OG RESSURSBRUK

Timeforbruk: inntil 300 timer

Rapport til sekretær: 15.05.2026

OPPDRAGSANSVARLIG REVISOR

Anna Ølnes
aol@rmnsa.no
Tlf. 906 33 713

2 MANDAT

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

2.1 Bestilling

Kontrollutvalget i Overhalla kommune bestilte følgende den 18.09.2025 i sak 25/25:

- 1) Kontrollutvalget bestiller forvaltningsrevisjon av informasjonssikkerhet og digitalisering.
- 2) Det gis følgende innspill til prosjektplanen:
 - Ledelsens styringssystem for informasjonssikkerhet og personvern, grensesnittet mot Namsos og avklaring av ansvaret mellom de to kommunene.
 - Tekniske og organisatoriske tiltak
- 3) Revisjonen bes utarbeide prosjektplan til kontrollutvalgets møte den 11.11.25.

Bestillingen er en følge av at temaet er prioritert i gjeldende plan for forvaltningsrevisjon, behandlet i sak 89/24¹. Kontrollutvalget har fått en orientering fra administrasjonen om informasjonssikkerhet i sak 01/25, hvor det ble pekt på en del utfordringer, som blant annet behov for økte ressurser, personvern og vertskommunesamarbeid. Det ble bestilt et notat fra revisjonen med aktuelle tilnærminger for en revisjon innen informasjonssikkerhet, jf. sak 16/25. Revisjonen la fram et notat i sak 25/25. Som det fremgår ovenfor ble det bestilt forvaltningsrevisjon med søkelys på blant annet grensesnittet mot Namsos kommune som vertskommune.

2.2 Informasjonssikkerhet og personvern

Informasjonssikkerhet handler om å verne alle typer informasjon. Eksempler på informasjonsverdier er data, fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og til og med menneskelige ressurser (Jøsang 2025).² Ulike typer informasjon vil ha forskjellig beskyttelsesbehov. Videre skriver Jøsang 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/eller tilgjengelighet.

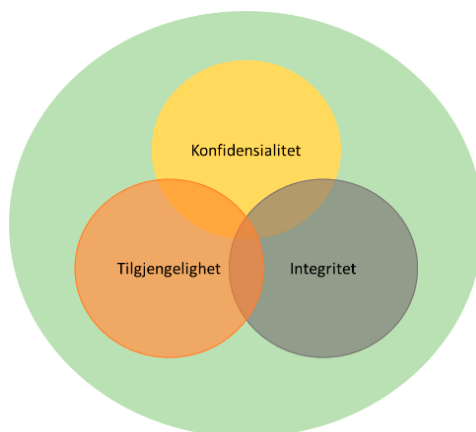
¹ Plan for forvaltningsrevisjon og eierskapskontroll 2025 - 2028

² A. Jøsang, *Cybersikkerhet - Teknologier Og Styring*, 3rd ed. (2025).

Beskyttelsesbehovet kan deles opp i tre:

- **Konfidensialitet:** informasjon er beskyttet mot uautorisert innsyn
- **Integritet:** informasjonen er riktig, komplett og til å stole på
- **Tilgjengelighet:** informasjonen er tilgjengelig når det er behov for den.³

Dette kan illustreres i figuren nedenfor.



Figur: KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet: Konfidensialitet, integritet og tilgjengelighet

Informasjonsverdi

KS beskriver begrepet informasjonsverdi på følgende måte:

All informasjonen kommunen eier og behandler har en verdi. Verdien varierer ut fra typen informasjon og hvilken type virksomhet informasjonen tilhører. Informasjon i denne sammenheng er alt fra kunnskap, personopplysninger, forretningshemmeligheter, beregningsmodeller, informasjon om hvordan saksbehandlingen skal gjennomføres, IKT-systemer hvor informasjon blir behandlet, teknisk infrastruktur mv. Det å kjenne sine verdier er viktig i informasjonssikkerhetssammenheng, ettersom det avgjør hvordan den skal beskyttes. Beskyttelsesgraden vurderes ut ifra hvor viktig informasjonen er, og hvordan behovet for konfidensialitet, tilgjengelighet og integritet skal bli ivaretatt.⁴

³ KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

⁴ KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Personvern

Personopplysningsloven, som innlemmer personvernforordningen (GDPR), regulerer behandlingen av personopplysninger, jf. § 1 i personopplysningsloven. Personopplysninger er enhver opplysning som kan knyttes til en identifisert eller identifiserbar person, jf. personvernforordningen artikkel 4 nr. 1. Personvernet skal verne om personopplysninger (formålsbestemmelsen i artikkel 1) og er knyttet til blant annet den enkeltes rett til privatliv. (Se blant annet Den europeiske menneskerettskonvensjonen, EMK artikkel 8 og grunnloven § 102) Et viktig element i personvernet er at den enkelte skal ha kontroll over og i størst mulig grad kunne bestemme over egne personopplysninger. Dette fremgår blant annet innledningsvis til personvernforordningen i punkt 1 og 7. Personopplysningsloven skal regulere og sikre at innsamlingen og bruken av personopplysninger i minst mulig grad går ut over vårt personvern og våre rettigheter. Personvernforordningen er utformet for å beskytte personopplysninger. Forordningen stiller krav til personvernet som kommunen må etterleve, blant annet innbyggernes rett til innsyn i egne personopplysninger og til å kreve retting av opplysninger, jf. artikkel 15-17 i personvernforordningen. Det er tre sentrale prinsipper for behandlingen av personvernopplysninger, og disse er lovlighet, rettferdighet og åpenhet. (jf. personvernforordningen § 5). Det er flere prinsipper enn disse. Datatilsynet har en oversikt⁵

Sikkerhetsloven

Sikkerhetsloven gjelder nasjonale sikkerhetsinteresser, men kommuner kan også ha en viktig rolle i dette. Sikkerhetsloven skal beskytte nasjonal suverenitet, territoriell integritet og demokratiske styreformers og andre nasjonale sikkerhetsinteresser mot sikkerhetstruende virksomhet. Dette kan for eksempel handle om tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Sikkerhetsloven stiller krav om at sikkerhetsstyringen skal gjennomføres planlagt og systematisk i et sikkerhetsstyringssystem, som samordnes med virksomhetens styringssystem. For kommunene gjelder det for det som handler om nasjonal sikkerhet.

Internkontroll

Internkontroll følger av kommuneloven kapittel 25. I tillegg er internkontroll regulert av eForvaltningsforskriften på informasjonssikkerhetsområdet. Forskriften har hjemmel i forvaltningsloven § 15 a om elektronisk kommunikasjon. Forskriften krever at

⁵ <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/>

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

Grunnprinsipper for IKT-sikkerhet

Norge har en egen tilsyns- og fagmyndighet for informasjons- og objektsikkerhet, Nasjonal sikkerhetsmyndighet (NSM), som er det nasjonale fagmiljøet for IKT-sikkerhet. NSM har også utarbeidet grunnprinsipper for IKT-sikkerhet⁶ (NSM 2020) som er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene bygger på ISO 27002⁷, og setter søkelys 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	Forberede virksomheten på håndtering av hendelser Vurdere og klassifisere hendelser

⁶ Nasjonal sikkerhetsmyndighet, 2020, Veileder i sikkerhetsstyring, versjon 1

⁷<https://standard.no/fagomrader/it-sikkerhet-og-personvern/informasjonssikkerhetstiltak--ns-en-isoiec-27002/#:~:text=NS%2DEN%20ISO/IEC%2027002%20inneholder%20organisatoriske%2C%20personellrelaterte%2C,har%20et%20klart%20definert%20omfang.>

Analysere data fra sikkerhetsovervåkning	Kontrollere og håndtere hendelser
Gjennomføre inntrengingstester	Evaluere og lære av hendelser

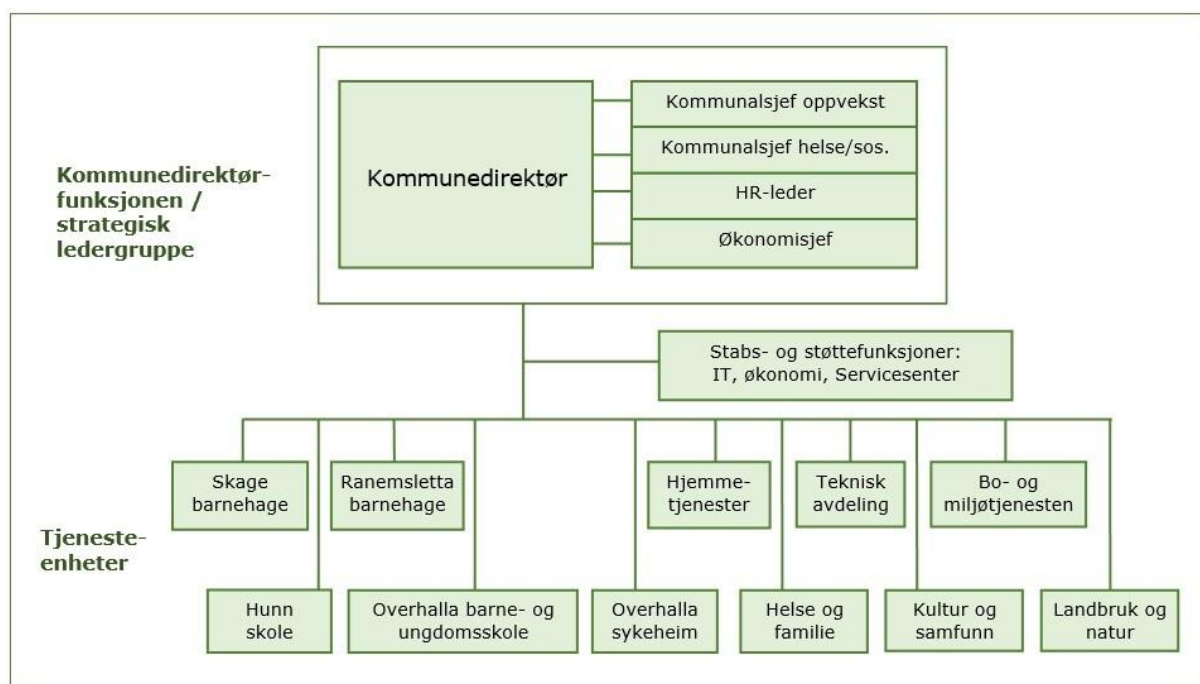
Lov om digital sikkerhet (digitalsikkerhetsloven)

Loven ble vedtatt den 20.12.2023 og trådte i kraft den 01.10.2025. Loven skal bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverks- og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester. Loven skal også legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser.

Helhetlig tilnærming til regelverket

Personopplysningsloven, sikkerhetsloven og eForvaltningsforskriften er sektorovergrepene lover og forskrifter som regulerer personvern og informasjonssikkerhet, og som gjelder for kommunal sektor. I tillegg til sektorovergrepene lovgivning, finnes det også sektorspesifikk lovgivning som regulerer personvern og informasjonssikkerhet spesifikt. Dette gjelder for eksempel særlig helselovgivningen. De relevante lovene og forskriften som er omtalt over er risikobasert og er i noen grad overlappende når det gjelder personvern og informasjonssikkerhet.

2.3 Kommunens organisering



Kilde: Kommunens hjemmeside, 04.11.2025

Kommunedirektøren i Overhalla er ansvarlig for all informasjonssikkerhet og personvern i kommunen. Overhalla kommune samarbeider med blant annet Namsos kommune IKT-tjenester, hvor Namsos kommune er vertskommune etter kommunelovens bestemmelser i kapittel 20. Namsos kommune utfører tjenester innen IKT for Overhalla kommune.

Vertskommuneavtalen ble inngått i mai 2019. Vertskommunen har ifølge avtalen ansvar for organisering av felles infrastruktur, IKT-oppgaver og programvare. Det ble gjennomført forvaltningsrevisjon om informasjonssikkerhet og personvern i Namsos kommune i 2022.⁸

Her er et utdrag fra rapporten:

IT kommer sent inn i anskaffelse av programvare, noe som kan gjøre det vanskelig å ivareta sikkerheten og lage et effektivt driftsmiljø.

Noen av de ansatte har god oversikt over enheter og strukturen på IKT-systemet, men det finnes ikke noe konfigurasjonskart. [.....] Namsos kommune har system for å overvåke, oppdage og fjerne sårbarheter. Kommunen har gjennomført en sikkerhetstest.

IT-avdelingen har en plan for håndtering av sikkerhetshendelser og gjenoppretting. Det finnes en beredskapsplan på IT, men det er uklart om beredskapsplanen har en rolle i andre deler av organisasjonen.

Det som kommer fram her vil være aktuelt for hvordan Namsos kommune utfører tjenestene i Overhalla kommune også. Det foreligger ikke sak i kontrollutvalget om hvordan rapporten er fulgt opp.

⁸ https://revisjonmidtnorge.no/prosjekter_rapporter/informasjonssikkerhet-i-namsos-kommune/

3 PROSJEKTDESIGN

Dette kapittelet redegjør for revisors forslag til løsning av oppdraget.

3.1 Problemstillinger

På bakgrunn av kontrollutvalgets bestilling foreslår revisor disse problemstillingene:

- 1) Har Overhalla kommune etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstillende krav i regelverket (systematisk rammeverk)?
- 2) Har Overhalla kommune etablert tilfredsstillende avtaler med og oppfølging av Namsos kommune (verts-kommune), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

Revisor tar forbehold om redigering og endring av ordlyden i problemstillingene, uten at innholdet blir endret.

3.2 Avgrensing

Kontrollutvalget bestiller en forvaltningsrevisjon av informasjonssikkerhet og digitalisering. Revisor anbefaler at forvaltningsrevisjonen avgrenses til informasjonssikkerhet og personvern, og holder digitalisering som gjelder de andre strategiske målene i digitaliseringsstrategien utenfor. 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. Kilder til kriterier

3.3 Metoder

3.3.1 Innsamling og analyse 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 personopplysninger med mer. Eventuell driftsavtale 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 være aktuelt å gjennomføre intervjuer med kommunens ledelse og nøkkelpersoner for informasjonssikkerhet og personvern. Hvorvidt det vil bli gjennomført intervju med ansatte i vertskommunen, Namsos, er avhengig av hvilket alternativ for problemstillinger som velges og om kommunen stiller ansattressurser til disposisjon. Intervju gir utfyllende informasjon 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 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 ansatte den største sikkerhetstrusselen.

3.3.2 Utledning av kriterier – kilder

Aktuelle kilder til revisjonskriterier er:

- Lov om kommuner og fylkeskommuner (kommuneloven), kapittel 20 (vertskommunesamarbeid) og 25 (kommunedirektørens internkontroll).
- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger med personvernforordningen (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet
- NSMs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- ISO 27001
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet
- KS' veileder i internkontroll (Orden i eget hus)

- KS´ veileder for interkommunalt IKT-samarbeid
- Andre veileder som f.eks. gjelder informasjonssikkerhet og personvern og internkontroll i kommuner

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Oppdragsansvarlig revisor	Anna Ølnes
Prosjektmedarbeider	Grethe Gilstad
Kvalitetssikrer	Cathrine Berg-Mortensen
Kvalitetssikrer	Hanne Marit Ulseth Bjerkan

4.2 Milepælsplan

Bestillingsdato	17.09.2025
Prosjektplan til sekretær	28.11.2025
Oppstartsmøte	Ca. 05.01.2026
Datainnsamling ferdig	Ca. 20.04.2026
Rapport til uttalelse	Ca. 25.04.2026
Rapport til sekretær	15.05.2026

Trondheim, 24.11.2025

Anna Ølnes

Oppdragsansvarlig revisor

KILDER

(slett hvis denne ikke brukes. Kilder til revisjonskriterier listes opp i kapittel 3.3. med nok informasjon til å finne de – trenger ikke å listes opp her).

VEDLEGG 1: UAVHENGIGHETSERKLÆRING

(signer uavhengighetserklæring og lim inn her/legg ved prosjektplanen)

Riv Revisjon

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no