Revisjon Midt-Norge

Digital sikkerhet

Trøndelag Fylkeskommune

Prosjektplan forvaltningsrevisjon

FR1369

2025

1 FAKTA OM OPPDRAGET

FORMÅL

Formålet med forvaltningsrevisjonen er å belyse hvordan fylkeskommunen arbeider med digital sikkerhet, herunder styring, organisering, rutiner og praksis knyttet til informasjonssikkerhet. Revisjonen skal gi innsikt i hvordan arbeidet er lagt opp gjennom styringssystemer og rutiner, hvordan avvik håndteres og følges opp som del av internkontrollen, hvilken kompetanse og opplæring som finnes på området, hvordan tilgangsstyring praktiseres i informasjonssystemene, samt hvordan krav i personvernlovgivningen etterleves ved behandling av pasientdata, elevdata og personaldata.

PROBLEMSTILLINGER

1. I hvilken grad har fylkeskommunen etablert og gjennomført et forsvarlig arbeid med Digital sikkerhet?

   Delproblemstillinger:

   1. **Styringssystemer og rutiner:** Hvilke systemer, rutiner og prosesser har fylkeskommunen etablert for å sikre informasjonssikkerhet, og i hvilken grad er disse gjort kjent og tatt i bruk i organisasjonen?
   2. **Avvik og forbedringsarbeid:** Hvordan registreres, behandles og følges avvik innen informasjonssikkerhet opp, og på hvilken måte brukes avvik i forbedring av internkontrollen?
   3. **Kompetanse og opplæring:** Hvilken kompetanse har ansatte som håndterer informasjonssikkerhet, og hvilke tiltak er etablert for å sikre nødvendig opplæring og kompetanseutvikling?
   4. **Tilgangsstyring:** Hvordan praktiserer fylkeskommunen, tilgangsstyring og håndtering av tilganger i sine informasjonssystemer?
   5. **Etterlevelse av personvernregelverket i tjenesteområdene:** Hvordan arbeider fylkeskommunen med å etterleve krav i personvernlovgivningen ved behandling av pasientdata, elevdata og personaldata?

Hovedproblemstillingen vil bli besvart gjennom undersøkelse av flere avgrensede delproblemstillinger. Disse belyser ulike sider av informasjonssikkerhet, drift og utvikling i fylkeskommunen, og skal samlet bidra til å gi et helhetlig bilde av hvordan arbeidet er organisert, gjennomført og etterlevd i praksis.

TIDS- OG RESSURSBRUK

Timeforbruk: inntil 450 timer

Rapport til sekretær: 01.10.2026

OPPDRAGSANSVARLIG REVISOR

Cathrine Berg Mortensen
cathrine.mortensen@revisjonmidtnorge.no

Tlf. 97795080

2 MANDAT

I dette kapittelet redegjøres det for bestillingen.

2.1 Bestilling

Kontrollutvalget i Trøndelag fylkeskommune bestilte den 07.10.2025, sak 55/25 en forvaltningsrevisjon med tema «Informasjonssikkerhet, drift og utvikling». Kontrollutvalget viser til følgende formål med bestillingen:

- om fylkeskommunen har tilfredsstillende system og rutiner for informasjonstrygghet
- om avvik brukes aktivt i for å forbedre internkontrollen
- om organiseringen for arbeidet er hensiktsmessig
- om gjeldende lover og regler blir fulgt innenfor dette området
- hvordan fylkeskommunen praktiserer informasjonstrygghet med tanke på konfidensialitet og tilgangsstyring
- om fylkeskommunen jobber aktivt med å etterleve sentrale krav i personvernlovgivingen, herunder pasientdata, elevdata og personaldata
- hvilken kompetanse de ansatte har på området

Bestillingen er med utgangspunkt i Plan for forvaltningsrevisjon

2.2 Bakgrunnsinformasjon

En fylkeskommune behandler store mengder informasjon som del av sin tjenesteutøvelse, eksempelvis innen videregående opplæring, tannhelsetjenester, transport og regional utvikling. Opplysninger om elever, pasienter, ansatte og brukere inngår i driften av disse tjenestene, og informasjonssikkerhet[1] handler om å sørge for at slik informasjon er tilgjengelig når den trengs, er korrekt og ikke kommer på avveie.

Informasjonssikkerhet bygger på tre grunnleggende begreper: konfidensialitet, integritet og tilgjengelighet. Datatilsynet[2] beskriver informasjonssikkerhet som tiltak for å sikre at opplysninger er beskyttet mot uautorisert innsyn, utilsiktede endringer og tap av tilgang, og knytter dette eksplisitt til disse tre begrepene.

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

[2] https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/internkontroll_veil.pdf

Konfidensialitet innebærer at informasjon bare skal være tilgjengelig for personer som har rettmessig tilgang. Dette betyr at opplysninger om elever, pasienter eller ansatte ikke skal kunne leses eller brukes av uvedkommende.

Integritet innebærer at informasjon skal være korrekt, fullstendig og pålitelig, og at den ikke skal kunne endres eller slettes på en uautorisert eller utilsiktet måte. Dette gjelder både selve innholdet i opplysningene og sammenhengen de inngår i.

Tilgjengelighet innebærer at informasjon og systemer skal være tilgjengelige når de trengs. Dette betyr at brukere med rettmessig tilgang skal kunne hente fram nødvendige opplysninger også ved driftsforstyrrelser, feil eller andre uønskede hendelser.

Datatilsynet knytter disse tre begrepene direkte til krav om internkontroll, risikovurdering og forsvarlig behandling av opplysninger i offentlige virksomheter, og bruker dem som grunnlag for å forklare hva som menes med informasjonssikkerhet i praksis. De samme begrepene brukes av Nasjonal sikkerhetsmyndighet[3] som grunnleggende sikkerhetsmål for beskyttelse av informasjon og digitale systemer.

Digitalisering har blitt en grunnleggende del av fylkeskommunens arbeid. Ifølge KS[4] er digital utvikling en drivkraft for effektivisering, men den medfører også nye typer risiko, blant annet driftsavbrudd, tap av informasjon og økonomiske konsekvenser ved digitale angrep. For å håndtere dette må fylkeskommunen planlegge, organisere og følge opp informasjonssikkerhet som en integrert del av tjenesteproduksjonen. KS fremhever at krav til informasjonssikkerhet bør være innarbeidet allerede i planleggingsfasen for nye tjenester og løsninger.

Flere sentrale lover angir hvordan fylkeskommunen skal behandle og beskytte informasjon.

Forvaltningsloven § 13[5] (taushetsplikt) regulerer hvilke opplysninger som skal beskyttes. Bestemmelsen pålegger alle som utfører tjenesten for et forvaltningsorgan å hindre at uvedkommende får tilgang til personlige forhold eller næringsopplysninger de får kjennskap til gjennom arbeidet. Taushetsplikten gjelder også etter at arbeidsforholdet er avsluttet. Formålet er å sikre konfidensialitet rundt opplysninger som er særlig beskyttelsesverdige.

---

[3] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/introduksjon/

[4] https://www.ks.no/contentassets/c019638eeb1e4972bac838e34c75dc47/-19-03185-6-Kommunedirektorens-verktoykasse-for-personvern-og-informasjonssikkerhet-1418678-2-1.pdf?_t_tags=language%3Ano%2Csiteid%3Abfb9d852-9a87-4d2f-a25f-779a7a8be2ea&_t_hit.id=Ksno2018_Models_Media_GenericDocument/_550b6847-9948-42b5-bc12-47a65f8f2cf3&_t_hit.pos=47

[5] https://lovdata.no/dokument/NL/lov/1967-02-10/KAPITTEL_3#%C2%A713

Personopplysningsloven[6] som gjennomfører EUs personvernforordning (GDPR), stiller krav til hvordan virksomheter skal ivareta personopplysninger. Forordningen krever at behandlingsansvarlige og databehandlere etablerer tekniske og organisatoriske tiltak som gir et sikkerhetsnivå tilpasset risikoen. Dette omfatter både kontroll med hvem som har tilgang til opplysninger og vurderinger av risiko som kan påvirke konfidensialitet, integritet og tilgjengelighet. Selv om GDPR ikke har en egen «tilgjengelighetsartikkel», følger kravene om tilgjengelighet av flere bestemmelser. Åpenhets- og informasjonsplikten i artiklene 12, 13 og 14, samt retten til innsyn i artikkel 15, innebærer at personopplysninger og informasjon om hvordan de behandles skal være tilgjengelige for den registrerte på en klar og forståelig måte, også ved endringer i personvernserklæringer. Videre innebærer ansvarlighetsprinsippet i artikkel 5(2) at virksomheter må kunne dokumentere hvordan de ivaretar personvernet, noe som i praksis betyr at prosesser og vurderinger må være tilgjengelige for tilsynsmyndigheter.

Digitalsikkerhetsloven[7] (2025) regulerer tilbydere av samfunnsviktige og digitale tjenester. Fylkeskommunen er ikke nødvendigvis direkte omfattet av loven, men deler av sektorene fylkeskommunen berører, samt enkelte leverandører, kan være underlagt kravene.

Kommuneloven § 25 – 1 (internkontroll)[8] fastslår at fylkeskommuner skal ha internkontroll for å sikre at lover og forskrifter følges. Internkontrollen gjelder all administrativ virksomhet og skal være systematisk, risikobasert og tilpasset virksomhetens egenart, størrelse og aktiviteter. Bestemmelsen beskriver også at internkontroll er et ledelsesansvar og skal være forankret hos kommunedirektøren, i denne anledning fylkesdirektøren.

I tillegg til lovverket finnes det flere veiledere som forklarer hvordan en fylkeskommune kan arbeide praktisk med informasjonssikkerhet. KS' veiledninger beskriver hvordan digitalisering innebærer både muligheter og risiko, og at arbeidet med informasjonssikkerhet derfor må være systematisk og inngå som en integrert del av planlegging og drift. Datatilsynets veiledning[9] om internkontroll og informasjonssikkerhet forklarer at offentlige virksomheter forvalter store mengder informasjon som krever beskyttelse, og viser hvordan gode rutiner kan bidra til stabil tjenesteleveranse og forhindre tap av tillit dersom opplysninger kommer på avveie. Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet[10] gir anbefalinger om

---

[6] https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/%C2%A0

[7] https://lovdata.no/dokument/SF/forskrift/2025-06-20-1131

[8] https://lovdata.no/dokument/NL/lov/2018-06-22-83/KAPITTEL_7-4#%C2%A725-2

[9] https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/internkontroll_veil.pdf

[10] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/introduksjon/

risikovurderinger, tilgangsstyring, logging og hendelseshåndtering, og viser hvordan tekniske og organisatoriske tiltak kan struktureres for å støtte internkontrollen og oppfylle lovkravene knyttet til sikker behandling av informasjon.

Lovverket beskriver ulike sider av informasjonssikkerhet: Forvaltningsloven beskytter graderte og personlige opplysninger gjennom taushetsplikt, personopplysningsloven og GDPR regulerer behandling av personopplysninger, og digitalsikkerhetsloven omhandler krav til digitale systemer og håndtering av digitale hendelser. Kommuneloven stiller krav til internkontroll som skal sikre at lovene etterleves.

Veiledere fra KS, Datatilsynet og NSM forklarer hvordan fylkeskommunen kan omsette lovkravene til praksis gjennom rutiner, opplæring, risikostyring og tekniske tiltak. Til sammen danner dette et rammeverk for hvordan fylkeskommunen kan beskytte informasjon og sørge for tilgjengelige, stabile og trygge digitale tjenester.

Når informasjonssikkerhet berører både lovpålagte krav, styringssystemer og praktiske arbeidsprosesser på tvers av tjenesteområder, blir det et område som er nært knyttet til styringen av virksomheten som helhet. Dette gjør også temaet relevant for forvaltningsrevisjon, ettersom revisjonen undersøker om virksomheten arbeider i tråd med gjeldende regelverk, har hensiktsmessige rutiner og følger et systematisk rammeverk for kontroll og oppfølging.

2.3 Fylkeskommunen

Trøndelag fylkeskommune er en regional folkevalgt forvaltningsmyndighet, jf. kommuneloven[11]. Fylkeskommunen har ansvar for videregående opplæring, tannhelsetjenesten, kollektivtransport, fylkesveier, kultur og regional utvikling, med nærmere regulering i opplæringsloven[12], tannhelsetjenesteloven[13], yrkestransportlova[14], veglova[15] og øvrig sektorlovgivning.

Digitaliseringsstrategien for Trøndelag fylkeskommune 2022–2026 beskriver at samfunnsendringer, økte krav til informasjonssikkerhet og nye forventninger fra brukerne utfordrer fylkeskommunen til å levere tjenester med høy kvalitet på nye måter. Digitalisering pekes på som et sentralt virkemiddel for å forenkle, fornye og forbedre oppgaveløsningen, og

[11] Lov om kommuner og fylkeskommuner (kommuneloven) https://lovdata.no/dokument/LTI/lov/2018-06-22-83

[12] https://lovdata.no/dokument/NL/lov/2023-06-09-30

[13] https://lovdata.no/dokument/NL/lov/1983-06-03-54

[14] https://lovdata.no/dokument/NL/lov/2002-06-21-45

[15] https://lovdata.no/dokument/NL/lov/1963-06-21-23

som en forutsetning for å kunne tilby gode tjenester til innbyggere, næringsliv og offentlig sektor i Trøndelag[16].

Strategien fremhever at fylkeskommunen er en stor forvalter av personopplysninger, og at brukere av digitale tjenester har både rett til og forventning om sikre løsninger som ivaretar informasjonssikkerhet og personvern. Det slås fast at fylkeskommunen har plikt og ansvar til å arbeide systematisk for å sikre konfidensialitet, integritet og tilgjengelighet i all informasjonsbehandling, blant annet gjennom risikovurderinger i alle digitaliseringsprosjekter og vurdering av personvernkonsekvenser (DPIA) der det behandles personopplysninger.

Digitaliseringsstrategien peker samtidig på at fylkeskommunen har et bredt spekter av tjenester og at digitaliseringsarbeidet i dag i stor grad er fragmentert og preget av silotenkning. Manglende samhandling på tvers trekkes fram som en utfordring, og det understrekes at bedre styring, organisering og koordinering av digitaliseringsarbeidet er nødvendig for å ta ut gevinster for hele organisasjonen. Dette gjør informasjonssikkerhet, internkontroll og tydelig rollefordeling til sentrale forutsetninger for måloppnåelse på digitaliseringsområdet.

[16] https://www.trondelagfylke.no/globalassets/om-fylkeskommunen/rapporter-og-arsmeldinger/digitaliseringsstrategi-2022-2026.pdf

3 PROSJEKTDESIGN

Dette kapittelet redegjør for revisors forslag til løsning av oppdraget.

3.1 Problemstillinger

1. I hvilken grad har fylkeskommunen etablert og gjennomført et forsvarlig arbeid med Digital sikkerhet?

   Delproblemstillinger:

   1. **Styringssystemer og rutiner:** Hvilke systemer, rutiner og prosesser har fylkeskommunen etablert for å sikre informasjonssikkerhet, og i hvilken grad er disse gjort kjent og tatt i bruk i organisasjonen?
   2. **Avvik og forbedringsarbeid:** Hvordan registreres, behandles og følges avvik innen informasjonssikkerhet opp, og på hvilken måte brukes avvik i forbedring av internkontrollen?
   3. **Kompetanse og opplæring:** Hvilken kompetanse har ansatte som håndterer informasjonssikkerhet, og hvilke tiltak er etablert for å sikre nødvendig opplæring og kompetanseutvikling?
   4. **Tilgangsstyring:** Hvordan praktiserer fylkeskommunen, tilgangsstyring og håndtering av tilganger i sine informasjonssystemer?
   5. **Etterlevelse av personvernregelverket i tjenesteområdene:** Hvordan arbeider fylkeskommunen med å etterleve krav i personvernlovgivningen ved behandling av pasientdata, elevdata og personaldata?

Hovedproblemstillingen vil bli besvart gjennom undersøkelse av flere avgrensede delproblemstillinger. Disse belyser ulike sider av informasjonssikkerhet, drift og utvikling i fylkeskommunen, og skal samlet bidra til å gi et helhetlig bilde av hvordan arbeidet er organisert, gjennomført og etterlevd i praksis.

3.2 Avgrensing

Revisjonen omfatter fylkeskommunens arbeid med informasjonssikkerhet knyttet til digitale løsninger. Undersøkelsen vil ta for seg styring, organisering, rutiner, praktisk etterlevelse og kompetanse relatert til informasjonssikkerhet på tvers av relevante tjenesteområder. Revisjonen vil ikke undersøke alle sektorer i detalj, men benytte et utvalg enheter og systemområder for å belyse hvordan fylkeskommunens overordnede styringssystem fungerer i praksis.

Revisjonen avgrenses til å omfatte informasjonssikkerhet i betydningen konfidensialitet, integritet og tilgjengelighet i digitale tjenester og systemer. Tekniske sårbarhetstester,

penetrasjonstesting eller vurderinger av systemdesign inngår ikke i revisjonen. Det vil heller ikke gjennomføres vurderinger av kvaliteten på spesifikke fagsystemer utover det som er nødvendig for å besvare problemstillingene om tilgangsstyring, etterlevelse av regelverk og håndtering av personopplysninger.

Revisjonen omfatter etterlevelse av krav i sentrale lover og forskrifter, men vil ikke gi juridiske tolkninger utover det som er nødvendig for å vurdere om fylkeskommunens praksis er i samsvar med gjeldende regelverk. Revisjonen vil heller ikke ta stilling til digitaliseringsstrategiske prioriteringer, økonomiske vurderinger av IKT-investeringer eller vurderinger av enkeltprosjekters samfunnsnytte.

Undersøkelsen omfatter informasjonssikkerhet knyttet til behandling av elevdata, pasientdata og personaldata, herunder hvordan digitale systemer og tilhørende rutiner benyttes for å ivareta krav til personvern, konfidensialitet og tilgangsstyring. Revisjonen vil ikke vurdere innholdet i enkeltsaker, individuelle behandlingsforløp eller faglige vurderinger i tjenestene.

Revisjonen omfatter ikke fylkeskommunens eksterne leverandørers interne sikkerhetsarbeid utover det som følger av kontrakter, databehandleravtaler og fylkeskommunens oppfølgingsrutiner.

3.3 Aktuelle kilder til kriterier kan være

- Lov om behandlingsmåter i forvaltningssaker (forvaltningsloven)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Lov om kommuner og fylkeskommuner (kommuneloven)
- Lov om Arkiv (arkivlova)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Lov om sikkerhet (digitalsikkerhetsloven)
- KS veiledere om digitalisering, internkontroll og informasjonssikkerhet
- Datatilsynet, veileder om internkontroll og informasjonssikkerhet
- Nasjonal sikkerhetsmyndighet (NSM), Grunnprinsipper for IKT sikkerhet
- Digitaliseringsdirektoratet, veileder om informasjonsstyring i offentlig sektor
- Eventuelle interne styringsdokumenter i fylkeskommuen

3.4 Metoder for innsamling av data

For å besvare hoved- og delproblemstillingene, vil revisjonen benytte flere datakilder og metoder. Metodene er valgt for å belyse både formelle krav, etablerte styringssystemer og hvordan praksis fungerer i fylkeskommunen.

Dokumentanalyse

Revisjonen vil innhente og gjennomgå skriftlig materiale som er relevant for å belyse fylkeskommunens arbeid med informasjonssikkerhet. Dette kan omfatte overordnede styringsdokumenter, strategier, retningslinjer og beskrivelser av internkontroll, samt dokumenter som omhandler risikovurderinger, tilgangsstyring, avvikshåndtering, hendelseshåndtering og opplæring. Det kan også inngå materiale som beskriver organisering, roller, ansvarsfordeling, leverandørforhold og databehandleravtaler. I tillegg kan revisjonen gjennomgå rapporter, logger, avviksoversikter og annen dokumentasjon som viser hvordan informasjon håndteres og følges opp i ulike deler av organisasjonen. Dokumentanalysen vil gi grunnlag for å beskrive hvilke systemer, rutiner og prosesser som er etablert og hvordan de er dokumentert i fylkeskommunens materiale.

Intervju

Revisjonen vil innhente informasjon gjennom intervjuer med personer i relevante roller i fylkeskommunen. Intervjuene vil gi innsikt i hvordan arbeidet med informasjonssikkerhet er organisert, hvordan oppgaver og ansvar forstås, og hvordan rutiner og prosesser beskrives fra ulike nivåer i organisasjonen. Det kan omfatte ledere, ansatte med fagansvar innen digitalisering, informasjonssikkerhet og personvern, samt medarbeidere i tjenesteområder som håndterer personopplysninger som en del av sitt arbeid. Intervjuene vil bidra til å belyse hvordan sentrale funksjoner er lagt opp, hvordan ulike deler av organisasjonen arbeider med informasjonssikkerhet, og hvordan roller og prosesser oppfattes av de som har operative eller strategiske oppgaver på området.

Stikkprøver

Revisjonen kan gjennomføre stikkprøver i utvalgte deler av organisasjonen for å undersøke hvordan informasjon knyttet til elevdata, pasientdata og personaldata håndteres i praksis. Slike stikkprøver kan omfatte innsyn i et begrenset antall tilgangsrettigheter i systemer som behandler personopplysninger, eksempler på registrerte avvik som gjelder behandling av slike data, eller dokumentasjon som beskriver risikovurderinger, opplæring og andre relevante prosesser. Stikkprøvene vil inngå som én av flere datakilder for å belyse praksis i avgrensede deler av fylkeskommunens arbeid med informasjonssikkerhet.

Vurdering av metode

Metodevalget innebærer enkelte begrensninger som det er viktig å være oppmerksom på. Dokumentanalyse gir innsikt i formelle beskrivelser av rutiner, roller og prosesser, men slike dokumenter viser ikke nødvendigvis hvordan praksis gjennomføres i det daglige. Intervjuer

kan bidra til å utdype og forklare skriftlig materiale, men informasjonen som fremkommer vil være basert på informantenes erfaringer og perspektiver, og kan variere mellom ulike deler av organisasjonen.

Stikkprøver gir anledning til å undersøke utvalgte eksempler på praksis, men omfatter ikke alle systemer, enheter eller prosesser i fylkeskommunen. Slike utvalg gir dermed ikke et uttømmende bilde av praksis, og funn fra stikkprøver kan ikke generaliseres uten videre. Revisjonen gjennomfører heller ikke tekniske tester, risikoanalyser eller penetrasjonstester, og vurderer derfor ikke tekniske sikkerhetsnivåer utover det som fremgår av dokumentasjon og intervjuopplysninger.

Metoden gir dermed et grunnlag for å belyse sentrale sider av fylkeskommunens arbeid med informasjonssikkerhet, samtidig som datainnsamlingen ikke omfatter alle deler av virksomheten og ikke vurderer forhold som krever tekniske undersøkelser eller fullstendige gjennomganger av systemporteføljen.

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Oppdragsansvarlig revisor	Cathrine Berg-Mortensen
Prosjektmedarbeider	Hanne Marit Ulseth Bjerkan
Kvalitetssikrer	Merete Montero
Kvalitetssikrer	Anna Ølnes

4.2 Milepælsplan

Bestillingsdato	07.10.25
Prosjektplan til sekretær	01.01.26
Oppstartsmøte	Medio februar 2026
Datainnsamling ferdig	Medio august 2026
Rapport til uttalelse	Medio september 2026
Rapport til sekretær	01.10.2026

Mo i Rana/18.12.2025

Cathrine Berg-Mortensen

Oppdragsansvarlig revisor

VEDLEGG 1: UAVHENGIGHETSERKLÆRING

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

Vurdering av uavhengighet.
Revisors egenvurdering i forbindelse med forvaltningsrevisjonsprosjekt:

Prosjektnr: FR1369	Kommune: Trøndelag Fylkeskommune

Hovedreferanse:
Kommuneloven § 24-4
Forskrift om kontrollutvalg og revisjon kapittel 3
ISA 200 - Formål og generelle prinsipper for revisjon av regnskaper pkt. 4
ISA 220 - Vilkår for revisjonsoppdrag pkt. 4, 12-13
ISA 300 - Planlegging av revisjon av regnskaper pkt. 6
Standard for forvaltningsrevisjon RSK 001 pkt. 8
Standard for eierskapskontroll RSK 002 pkt. 3

Ansettelsesforhold:	Undertegnede har ikke ansettelsesforhold i andre stillinger enn Revisjon Midt-Norge SA
Medlem i styrende organer	Undertegnede er ikke medlem av styrende organ i noen virksomhet som ovenfor nevnte kommune deltar i.
Delta eller inneha funksjoner i annen virksomhet, som kan føre til interessekonflikt eller svekket tillit	Undertegnede deltar ikke i eller innehar funksjoner i annen virksomhet som kan føre til interessekonflikt eller svekket tillit til rollen som revisor.
Nærstående	Undertegnede har ikke nærstående som har tilknytning til ovenfor nevnte kommune som har betydning for uavhengighet og objektivitet.
Rådgivnings- eller andre tjenester som er egnet til å påvirke revisors habilitet	Før slike tjenester utføres foretas en vurdering av rådgivningens eller tjenestens art i forhold til revisors uavhengighet og objektivitet. Dersom vurderingen konkluderer med at utøvelse av slik tjeneste kommer i konflikt med bestemmelsen i forskriften § 18, skal revisor ikke utføre tjenesten. Hvert enkelt tilfelle må vurderes særskilt. Revisor besvarer løpende spørsmål/henvendelser som er å betrakte som veiledning og bistand og ikke revisjon. Paragrafen sier at også slike veiledninger må skje med varsomhet og på en måte som ikke binder opp revisors senere revisjons- og kontrollvurderinger. Undertegnede har ikke ytet rådgivnings- eller andre tjenester overfor ovenfor nevnte kommune som kommer i konflikt med denne bestemmelsen.
Tjenesten under kommunens egne ledelses- og kontrolloppgaver	Undertegnede har ikke ytet tjenester overfor ovenfor nevnte kommune som hører inn under kommunens egne ledelses- og kontrolloppgaver.
Opptre som fullmektig for den revisjonspliktige	Undertegnede opptrer ikke som fullmektig for ovenfor nevnte kommune.
Andre saregne forhold	Undertegnede kjenner ikke til andre saregne forhold som er egnet til å svekke tilliten til uavhengighet og objektivitet.

Sted: Mo i Rana Dato: 18.12.25
Rolle: Oppdragsansvarlig
Navn: Cathrine Berg Mortensen

Revisjon Midt-Norge SA
Brugata 2
7716 Steinkjer
post@revisjonmidtnorge.no
907 30 300
www.revisjonmidtnorge.no
Kontonummer: 4270.18.38658
Org.nr: 919 90 2310 MVA

Dokumentet er signert digitalt av:
- CATHRINE BERG-MORTENSEN, 18.12.2025

Forseglet av
Posten Norge

Revisjon Midt-Norge

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no