FORVALTNINGSREVISJON

Informasjonssikkerhet

Troms fylkeskommune

Sladdet versjon, jf. offentleglova § 24

KOMREV NORD

Rapport 2026

Forord

På grunnlag av bestilling fra kontrollutvalget i Troms fylkeskommune har KomRev NORD gjennomført forvaltningsrevisjon rettet mot informasjonssikkerhet. Kontrollutvalgets plikt til å påse at forvaltningsrevisjon gjennomføres, følger av lov om kommuner og fylkeskommuner § 23-2 bokstav c. Ifølge kommuneloven § 23-3 innebærer forvaltningsrevisjon å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak.

Krav til revisors uavhengighet følger av kommuneloven § 24-4 og av forskrift om kontrollutvalg og revisjon §§ 16, 17, 18 og 19. Før igangsetting av forvaltningsrevisjonen har revisjonen vurdert egen uavhengighet overfor Troms fylkeskommune. Vi kjenner ikke til forhold som er egnet til å svekke tilliten til vår uavhengighet og objektivitet.

Vi takker Troms fylkeskommune for samarbeidet i forbindelse med forvaltningsrevisjonen.

Tromsø, Alta, 22.04.2026

Margrete Mjølhus Kleiven
Oppdragsansvarlig forvaltningsrevisor

Ranveig Olaussen
Prosjektleder, forvaltningsrevisor

SAMMENDRAG

Denne forvaltningsrevisjonen omhandler informasjonssikkerhet. Ledelsen, ansatte og eksterne brukere trenger kontinuerlig og effektiv tilgang til relevant informasjon og relevante IKT-systemer og digitale tjenester. Med dagens bruk av IKT er styring og kontroll med informasjonssikkerhet kritisk for de fleste aktiviteter i en virksomhet.

Etter vedtak i kontrollutvalget har vi undersøkt to problemstillinger:

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

Styringssystem og internkontroll
Et styringssystem inneholder ulike aktiviteter, blant annet planlegging, risikovurdering, risikohåndtering, måling og evaluering. Det er flere regelsett som oppstiller krav til fylkeskommunens behandling og sikring av informasjon; sikkerhetsloven, digitalsikkerhetsloven, personopplysningloven, digitalsikkerhetsforskriften og eForvaltningsforskriften. Kommuneloven § 25-1 angir fylkeskommunens internkontrollansvar, og er også gjeldende på området. I tillegg er anerkjente standarder, herunder IEC/ISO 27001 og NSM sine grunnprinsipper styrende. Fylkeskommunedirektøren er ansvarlig for internkontrollen. Internkontrollen skal sikre at regelverk og Troms fylkeskommunes egne mål etterleves.

Troms fylkeskommune har siden oppdelingen med Finnmark fylkeskommune og endring i styringsform, arbeidet med styringssystem for informasjonssikkerhet og personvern. Arbeidet er organisert som et prosjekt, og det er forankret i øverste ledelse. Prosjektet «*Helhetlig styring av informasjonssikkerhet og personvern*» skal bidra til å tydeliggjøre ansvarsfordelingen i organisasjonen med kjente linjer fra øverst og nedover i organisasjonen, og unngå etablering av rammeverk på siden av, eller på tvers av andre rammeverk som omfatter kvalitet og styring. Fylkeskommunen har i prosjektet, gjennomgått, oppdatert og utarbeidet styringsdokumenter som omhandler informasjonssikkerhet og personvern.

Styrende dokumenter for informasjonssikkerhet og personvern er stort sett ferdig utarbeidet, og skal implementeres i organisasjonen i løpet av 2026. Vi har ikke ved vår gjennomgang av utarbeidede styringsdokumenter funnet at innholdet bryter med kravene i lovverk eller anerkjente standarder.

Av *Policy for informasjonssikkerhet og personvern* framgår overordnet sikkerhetsmål, forpliktelse til å stille relevante sikkerhetskrav, samt overordnede føringer og grunnleggende prinsipper. Fylkeskommunen har gjennomført ROS-analyse, og det er gjennomført virksomhets-ROS ved IT-avdelingen.

Rutiner, retningslinjer og prosedyrer legges inn i kvalitetssystemet *Datakvalitet*, etter hvert som de utarbeides og godkjennes. Troms fylkeskommune har systematisert informasjon i form av en kvalitetshåndbok. Kvalitetshåndboken er opplyst å være tilgjengelig for alle ansatte via fylkeskommunens intranett.

Troms fylkeskommune har rutiner og etablerte prosesser for å håndtere avvik, men funn i undersøkelsen viser at det er noe svakhet knyttet til avviksoppfølgingen. Revisor har, som følge av at de fleste styringsdokumentene på undersøkelsestidspunktet ikke er implementert i organisasjonen, lite grunnlag for å uttale oss om effektiviteten av disse. Fylkeskommunen opplyser å se viktigheten av å ha styringsdokumenter som til enhver tid gjenspeiler virkeligheten, og tilstreber at dokumentene oppdateres ved behov.

Protokoll over behandlingsaktiviteter, behandling og lagring av personopplysninger
Undersøkelsen viser at Troms fylkeskommune ikke har behandlingsprotokoll som tilfredsstiller krav i personvernforordningen. Mangler knyttet seg blant annet til at det ikke er en fullstendig oversikt over hvilke personopplysninger som er registrert i systemene og hvilke formål disse har. Det er igangsatt et arbeid, og fylkeskommunen angir at behandlingsprotokoll som er i tråd med krav i GDPR, vil være på plass i 2026.

Ved gjennomføringen av forvaltningsrevisjonen hadde ikke fylkeskommunen full oversikt over hvor det er gjennomført personvernkonsekvensvurdering (DPIA). Vi fikk opplyst at dette vil bli en del av oppfølgingen av protokoll når behandlingene systematiseres. Vi har fått forklart at det er vanskelig å gjennomføre DPIA før arbeidet med behandlingsprotokoll er ferdigstilt.

Utarbeidet *Prosedyre for vurdering av personvernkonsekvenser (DPIA*) beskriver hvordan Troms fylkeskommunens vurdering av personvernkonsekvenser skal gjennomføres. Revisor har fått opplyst at det sannsynligvis er etterslep med gjennomføringen av DPIA på flere områder i Troms fylkeskommune.

Sikkerhetsbevissthet blant ansatte er et viktig sikkerhetstiltak. Som et fast opplæringstiltak arrangeres sikkerhetsmåneden, hvor ulike tema innenfor sikkerhet presenteres for ansatte. Revisor er kjent med at det er vanskelig å få god deltakelse blant alle ansatte. Deltakelsen ved Nanokurs med tema innenfor IT-sikkerhet har vært varierende. Vi ser positivt på at det for informasjonssikkerhet og personvern planlegges for en systematisering av opplæring, og utarbeidelse av en kompetanseplan.

Tiltak for å ivareta informasjonssikkerhet
Gjennomført virksomhets-ROS ved IT-avdelingen avdekket noen sårbarheter, og det er iverksatt flere tiltak. Noen tiltak jobbes det ennå med. Blant annet pågår det for tiden et arbeid med å utarbeide en felles oversikt over alle IT-systemene i Troms fylkeskommune. Dette fordi manglende oversikt blant annet gir utfordringer med tanke på kontroller som IT-avdelingen gjennomfører. Vi har fått opplyst at risikoen knytter seg til leverandørene, ved at en ikke klarer å underlegge disse tjenestene den strukturen som bygges opp i styringssystemet for å ivareta en forsvarlig IT-sikkerhet i systemene. Det meste av prosessen ved tilgangsstyringen er automatisert, og multifaktorautentisering er etablert som grunnleggende identitetssikring.

Redundans på flere av IT-systemene skal sikre uavbrutt drift på viktige IT-systemer, og ivaretar sammen med beredskapsplaner eventuelt bortfall av IT-systemer. Det er utarbeidede varslingslister som skal benyttes ved alvorlige sikkerhetshendelser.

Undersøkelsen viser at nivå på sikkerhetsovervåking er vurdert. Det er også gjennomført sårbarhetskartlegging og inntrengningstest. Fra KommuneCERT har fylkeskommunen fått tilbakemelding om at sikkerhetsnivået i organisasjonen i dag er godt. Vi har fått presisert fra IT-avdelingen at dette gjelder de nye IT-løsningene. Det er ikke planlagt å gjennomføre testing av sikkerhetsnivået i de gamle systemene som skal fases ut.

Konklusjoner
Revisors konklusjon på problemstilling 1 er at Troms fylkeskommune ikke fullt ut har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket.

Revisors konklusjon på problemstilling 2 er at Troms fylkeskommune i all hovedsak har truffet tilfredsstillende tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet.

Anbefalinger
Gjennom prosjektet *Helhetlig styring for informasjonssikkerhet og personvern* skal Troms fylkeskommune få på plass et styringssystem på området. Arbeidet med styringssystemet pågår. Vi anser det ikke som hensiktsmessig å gi særskilte anbefalinger knyttet til styringssystemets innhold da fylkeskommunen selv har laget en plan for videre arbeid. Det er beskrevet utfordring med deltakelse i opplæringstiltakene som gjennomføres. *Vi anbefaler derfor fylkeskommunen å vurdere å etablere pålagte opplæringstiltak for å øke sikkerhetskulturen i organisasjonen*.

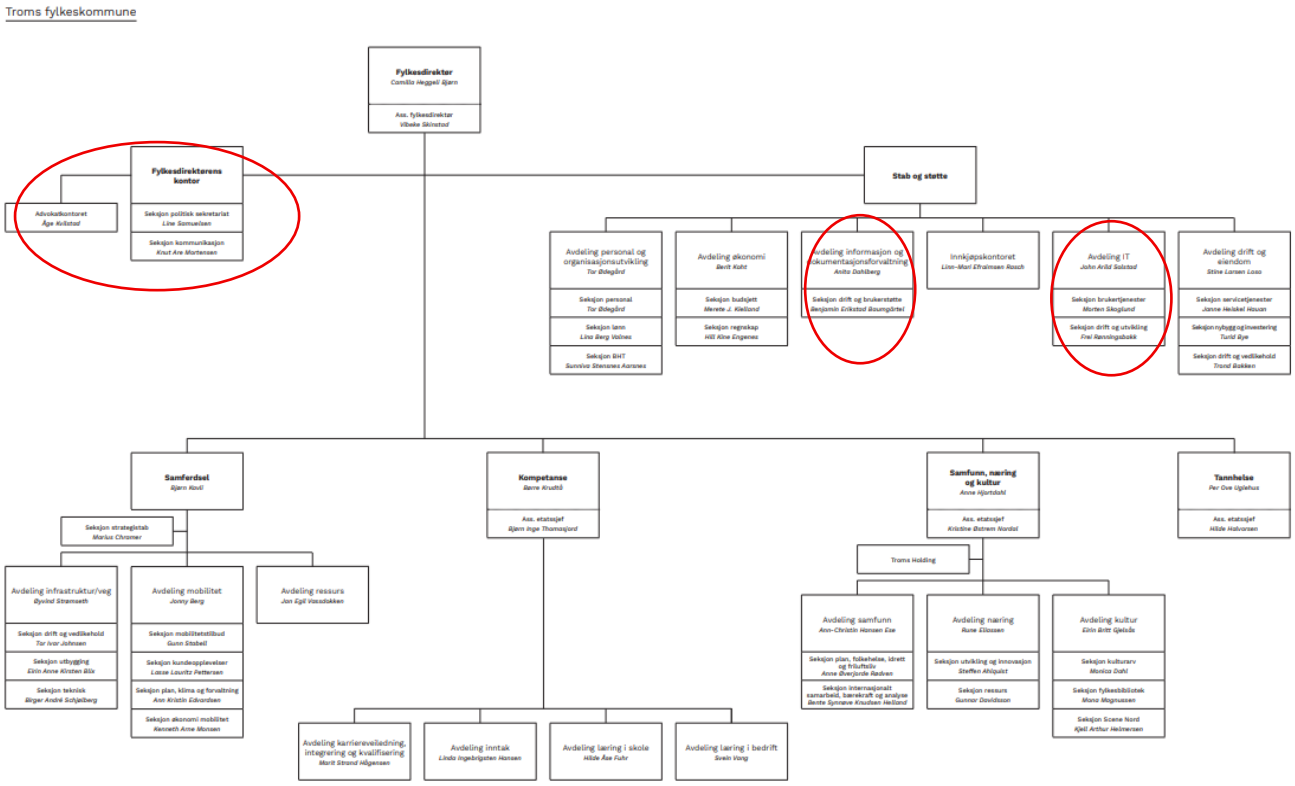
Vår undersøkelse har avdekket at sentrale bestemmelser i personvernlovgivningen ikke ivaretas, og at fylkeskommunen derfor bør treffe tiltak for å lukke disse avvikene. *Vi anbefaler derfor Troms fylkeskommune å ferdigstille arbeidet med behandlingsprotokoll, og gjennomføre personvernkonsekvensvurderinger (DPIA) i hele organisasjonen.*

Innhold

1 BAKGRUNN OG BESTILLING

Kontrollutvalget i Troms fylkeskommune vedtok 13.06.2025 i sak 27/2025, å bestille en forvaltningsrevisjon med tema datasikkerhet. Kontrollutvalget ønsket undersøkt om fylkeskommunen har etablert styringssystem for informasjonssikkerhet i henhold til regelverket. Videre om det er truffet tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet

Utklippet under er hentet fra Troms fylkeskommunes hjemmeside. Fagleder sikkerhet er forvaltningsansvarlig for personvern og informasjonssikkerhet, og stillingen er organisasjonsmessig plassert ved fylkeskommunedirektørens kontor. Avdeling INFODOK ledes av avdelingsleder. Avdelingen forvalter styringssystemet for informasjonssikkerhet og personvern, og har blant annet særskilt fagansvar for personvern, herunder rådgiving innenfor behandling av informasjon, dokumentasjon og arkiv knyttet til personvernet. IT-sikkerhetsleder har ansvar for IKT-sikkerheten, og er en del av IT-avdelingens lederteam. Avdeling INFODOK og IT-avdelingen er avdelinger under *Stab og støtte*. Personvernombudet innehar fra mars 2026 100 % stilling, og stillingen er organisasjonsmessig plassert ved fylkeskommunedirektørens kontor.



2 PROBLEMSTILLINGER OG REVISJONSKRITERIER

2.1 Problemstillinger

For denne forvaltningsrevisjonen gjelder, som følge av vedtak i kontrollutvalget, følgende problemstillinger:

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

Troms fylkeskommunes ansvar og oppgaver gjør at det behandles store mengder data og informasjon. Informasjonen behandles av mange ansatte i ulike virksomheter i fylkeskommunen og i mange ulike systemer. Herunder vil noen opplysninger om innbyggere, ulike selskaper, andre kommuner og fylkeskommuner, samt om egne ansatte og politikere, være personsensitivt og taushetsbelagt.

For å ivareta krav til informasjonssikkerhet og personvern tenker vi ofte på bruken av tekniske sikkerhetstiltak slik som kryptering, tilgangsstyring, passordstyrke eller utvikling av sikre IKT-systemer. Tekniske sikkerhetstiltak er viktig, men god informasjonssikkerhet og godt personvern er også avhengig av andre typer sikkerhetstiltak som gode arbeidsrutiner og sikkerhetsbevissthet hos de ansatte.[1]

Problemstilling 1 og 2 går på noen områder over i hverandre. Problemstilling 1 gjelder i all hovedsak innholdet i styringssystemet, herunder formaliserte internkontrollrutiner-, reglementer og prosedyrer. Problemstilling 2 retter fokus mer mot det arbeidet som utføres i Troms fylkeskommune for å ivareta sikkerheten i IKT-systemene, og ved bruken av disse systemene.

2.2 Revisjonskriterier

2.2.1 Kilder for utledning av revisjonskriterier

Revisjonskriterier er krav, normer og/eller standarder som fylkeskommunens praksis på det reviderte området skal vurderes opp mot. Revisjonskriterier utledes fra autoritative eller anerkjente kilder innenfor det aktuelle området. Det finnes flere regelverk som stiller krav til internkontroll/systemer og rutiner knyttet til informasjonssikkerhet, og det er derfor flere relevante kilder for å utlede kriterier og kunne svare på problemstillingene, herunder:

- Lov av 22. juni 2018 om kommuner og fylkeskommuner (kommuneloven)
- Lov av 1. juni 2018 om nasjonal sikkerhet (sikkerhetsloven)
- Lov av 15. juni 2018 om behandling av personopplysninger (personopplysningsloven)
- Forskrift av 25. juni 2004 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet. Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus
- Datatilsynet; En veiledning om internkontroll og informasjonssikkerhet
- Nasjonalt rammeverk for håndtering av digitale angrep og cyberhendelser
- ISO/IEC 27001
- NSMs grunnprinsipper for IKT-sikkerhet

[1] KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

2.2.2 Utledning av revisjonskriterier

Kommuneloven § 25-1 pålegger fylkeskommunen å ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Internkontrollen skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold. De samlede kravene i bestemmelsen utgjør et minstekrav til hvordan internkontrollen skal være.[2]

Av bestemmelsens tredje ledd følger det at kommunedirektøren – ved internkontroll etter denne paragrafen skal:

a. utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
b. ha nødvendige rutiner og prosedyrer
c. avdekke og følge opp avvik og risiko for avvik
d. dokumentere internkontrollen i den formen og det omfang som er nødvendig
e. evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll

På området informasjonssikkerhet og personvern er det et omfattende regelverk, og forpliktelser til å ha system og rutiner følger av ulike lover, forskrifter og rammeverk. Ved utarbeidelse av internkontroll vil det være behov for å se til ulike krav som stilles for å oppfylle forpliktelsene. Noe av regelverket gjelder særskilt for enkelte områder i fylkeskommunen. Revisor innretter undersøkelsen mot det overordnede kravet som stilles til å ha internkontroll. Under denne kommer vi inn på kravene som gjelder for fylkeskommunen etter særskilte lover og forskrifter som omhandler informasjonssikkerhet.

Det følger av KS sin veileder, *Orden i eget hus. Kommunedirektørens internkontroll* at kravene som følger av kommuneloven § 25-1, må forstås som minstekrav. KS argumenterer videre for tre forutsetninger for god internkontroll:

- Internkontrollen må være basert på et bevisst forhold til *risiko*; altså må risikovurderinger ikke bare være en løpende aktivitet i - men også være *grunnlag for innretning av* - internkontrollen
- Internkontrollen må være formalisert; den bør innebære en organisering med ulike roller og ansvar, dokumentasjon, rutiner og prosedyrer samt rapportering og aggregering[3]
- Internkontrollen bør ta form av kontrollaktiviteter i daglig og faglig virksomhet, gjennom stikkprøver og planlagte kontrollhandlinger, og gjennom avvikshåndtering

Kommuneloven § 25-1 tredje ledd bokstav c angir at kommunedirektøren ved internkontroll skal *avdekke* og følge opp avvik og *risiko for avvik*.

Fylkeskommunedirektøren er ansvarlig for internkontrollen, og må påse at internkontrollen er systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Et overordnet utgangspunkt etter kommuneloven § 25-1, er at det er opp til fylkeskommunen (fylkeskommunedirektøren) å avgjøre hva av internkontroll som er nødvendig å *dokumentere*. Som KS påpeker, må imidlertid dette relative kravet også ses i sammenheng med bokstav b og e i bestemmelsen; som angir at det skal finnes *nødvendige rutiner og prosedyrer,* og at slike skal evalueres, og ved behov, forbedres.

[2] Prop. L. (2017-2018) s. 411

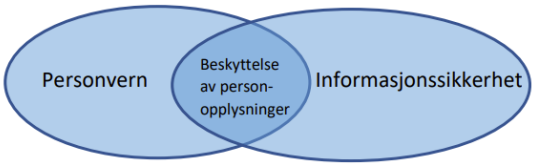
[3] 6 Aggregering innebærer å slå sammen eller kombinere data på ett nivå (for eksempel data som angår individer eller definerte grupper) og bruke disse til analyser på et mer overordnet nivå (som f.eks. angår hele kommuneorganisasjonen over tid.)

Det følger av KS sin veileder at internkontrollen bør integreres og tilpasses det styringssystemet som fylkeskommunen bruker. Det er ikke nødvendig å etablere et særskilt internkontrollsystem, men å sikre at den styringsmodellen og det systematiske arbeidet som gjøres også gir trygghet for at det er tilstrekkelig intern kontroll.

Personopplysningsloven, sikkerhetsloven og eForvaltningsforskriften er sektorovergripende lover og forskrifter som regulerer personvern og informasjonssikkerhet, og som gjelder for kommunal sektor. Det finnes også sektorspesifikk lovgivning som regulerer personvern og informasjonssikkerhet spesifikt, eksempelvis helselovgivningen. Fylkeskommunedirektøren har det øverste ansvaret for at kravene i personopplysningloven, sikkerhetsloven og eForvaltningsforskriften etterleves i Troms fylkeskommune. Selv om kravet til internkontroll framgår av ulike regelverk, kan alt inngå i ett og samme styringssystem.

Personvern og informasjonssikkerhet er to fagområder som har mye til felles, men også noen forskjeller. Fagene overlapper hverandre når det gjelder beskyttelse av personopplysninger. Det er viktig å være oppmerksom på at informasjonssikkerhet er mer enn personopplysninger, på samme måte som personvern er mer enn informasjonssikkerhet.

Forholdet mellom fagområdene kan forklares av figuren nedenfor.[4]



Revisor finner det derfor ikke naturlig å skille helt mellom informasjonssikkerhet og personvern. Fylkeskommunen – spesielt tannhelse og videregående skoler – behandler i stor utstrekning personopplysninger om innbyggere. Av den grunn vil undersøkelsen, der det synes nødvendig for å svare ut problemstillingene, omfatte personopplysninger (med internkontrollforpliktelser).

Ifølge Datatilsynet dreier informasjonssikkerhet seg om å håndtere *risiko* relatert til virksomhetens *informasjonsverdier* og *behandling av personopplysninger*. Personopplysninger kommer i mange former. De kan trykkes eller skrives på papir, lagres elektronisk, overføres via post eller elektronisk media, eller formidles muntlig. Uansett hvordan informasjonen formidles og lagres skal den alltid beskyttes på en tilfredsstillende måte. Videre går det fram at informasjonssikkerhet omfatter:

- Konfidensialitet – at informasjonen ikke blir kjent for uvedkommende
- Integritet – at informasjonen ikke blir endret utilsiktet eller av uvedkommende
- Tilgjengelighet – at informasjonen er tilgjengelig for autoriserte ved behov
- Robusthet – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser

[4] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet, Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus.

Sikkerhetslovens krav om sikkerhetsstyring gjelder uavhengig av om fylkeskommunen har skjermingsverdige verdier[5]. Troms fylkeskommune må sikre at forebyggende sikkerhetsarbeid inngår som en del av fylkeskommunens styringssystem, noe som innebærer å:

- Gjennomføre risikovurderinger og iverksette tiltak for å sikre et forsvarlig sikkerhetsnivå
- Sikre tilstrekkelig kompetanse og ressurser for å kunne gjennomføre forebyggende sikkerhetsarbeid
- Vurdere om fylkeskommunen har skjermingsverdige verdier som faller inn under loven
    - Eventuelt iverksette tiltak for å sikre disse verdiene

Formålet med eForvaltningsforskriften er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Forskriften gjelder kommunal sektor, og § 15 stiller krav til internkontroll på informasjonssikkerhetsområdet. Herunder at forvaltningsorganet som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Videre at sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. Ifølge Datatilsynet omfatter sikkerhetsmålene ledelsens beslutninger om hva IKT skal brukes til i virksomheten, samt benyttes for å nå virksomhetens øvrige mål. Konkrete sikkerhetsmål vil slik utgjøre en del av virksomhetens beskrivelse av sin totale målsetning. Sikkerhetsmålene bør i størst mulig grad være målbare, men dette er ikke alltid enkelt. Uansett skal sikkerhetsmålene være retningsgivende for strategien.

Digitaliseringsdirektoratet (Digdir)[6] er en norsk statlig etat som har som oppgave å bidra til digitalisering av offentlig sektor. Ifølge Digdir er virksomhetsledelsen avhengig av tilstrekkelig styring på informasjonssikkerhetsområdet, for å lede virksomheten på en god måte. Dette oppnås gjennom etablering og oppfølging av et systematisk arbeid med styring av informasjonssikkerheten i hele virksomheten. Både ledelsen, ansatte og eksterne brukere trenger kontinuerlig og effektiv tilgang til relevant informasjon og relevante IKT-systemer og digitale tjenester. Med dagens bruk av IKT er styring og kontroll med informasjonssikkerhet kritisk for de fleste aktiviteter i en virksomhet.

For å få tilstrekkelig styring og kontroll må ledelsen og virksomheten ellers arbeide systematisk og effektivt med informasjonssikkerhet etter anerkjente prinsipper for internkontroll og styringssystem for informasjonssikkerhet. Styring og kontroll på informasjonssikkerhetsområdet handler om systematiske styringsaktiviteter. Disse skal sørge for at relevante risikoer blir vurdert, at nødvendige og hensiktsmessige sikkerhetstiltak blir etablert, og at det systematisk blir kontrollert og fulgt opp at tiltakene og styringsaktivitetene faktisk fungerer som forutsatt. En viktig forutsetning for å lykkes med en velfungerende internkontroll knyttet til informasjonssikkerhet og personvern, er at virksomheten har kapasitet til, og kunnskap på området.

KS veileder viser til at tekniske sikkerhetstiltak er viktige, men god informasjonssikkerhet og godt personvern er også avhengig av andre typer sikkerhetstiltak som gode arbeidsrutiner og sikkerhetsbevisste ansatte.

[5] Objekter og infrastruktur er skjermingsverdige etter sikkerhetsloven dersom de kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse.

[6] Hvorfor styring av informasjonssikkerhet? | Digdir

Når internkontroll er etablert og forankret, bør den gjøres kjent og etterleves blant ansatte i virksomheten.

Figuren over er hentet fra https://www.digdir.no

Personopplysningsloven består av nasjonale regler og EUs personvernforordning (også kalt GDPR-General Data Protectian Regulation). Personvernforordningen er et sett regler som gjelder for alle EU/EØS-land. Sammen med særlovgivning om personvern på enkelte områder, utgjør dette personvernregelverket. Personvernforordningen stiller krav til internkontroll i form av egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen. Tiltakene skal gjennomgås, og oppdateres ved behov.

Det følger av EUs personvernforordning artikkel 32 at behandlingsansvarlige og databehandlere skal «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen».

Personvernforordningen er laget for å styrke personvernet til enkeltpersoner i EU/EØS-området. For å opprettholde et godt personvern kreves det at informasjonssikkerheten ivaretas, og at man gjør fornuftige vurderinger om hvilke personopplysninger man trenger å behandle og over hvilket tidsrom, samt å kunne kommunisere godt og åpent til innbyggerne. Personvernforordningen stiller krav til personvernet som fylkeskommunen må etterleve. Alle virksomheter som ønsker å behandle personopplysninger er underlagt personopplysningsloven. Personvernforordningen skiller mellom begrepene *behandlingsansvarlig* og *databehandler*. Fylkeskommunedirektøren er som øverste administrative leder i Troms fylkeskommune behandlingsansvarlig. Behandlingsansvarlige bestemmer over personopplysningene, og databehandleren opptrer på vegne av den behandlingsansvarlige. Det stilles ulike krav til behandlingsansvarlige og databehandlere. Behandlingsansvarlige har det overordnede ansvaret for å behandle personopplysninger i tråd med regelverket. Databehandleren skal kun behandle personopplysninger på vegne av den behandlingsansvarlige. Personvernforordningen artikkel 28 angir databehandlerens plikter.

Alle virksomheter som behandler personopplysninger, skal føre protokoll over behandlingsaktivitetene de har ansvar for. En behandlingsprotokoll er et dokument som

beskriver hvordan en virksomhet behandler personopplysninger. Det er et viktig verktøy for å sikre at personvernreglene, som GDPR[7], følges. Protokollen skal inneholde informasjon om hvilke personopplysninger som behandles, hvorfor de behandles, hvem som har tilgang til dem og hvilke sikkerhetstiltak som er iverksatt. En behandlingsprotokoll er dokumentasjon av personopplysninger om egne ansatte, kunder, leverandører, innbyggere og andre som fylkeskommunen behandler personopplysninger om. Fylkeskommunen behandler og skal ikke oppbevare personopplysninger uten behandlingsgrunnlag. Dette gir nyttig grunnlag for risikovurderinger og identifisering av tiltak.

Det er ikke noen formkrav til hvordan protokollen skal føres, eller hva slags verktøy som skal benyttes. Datatilsynet har utarbeidet to maler i excel, for henholdsvis behandlingsansvarlig og databehandler, men oversikten kan også føres som et tekstbehandlingsdokument, eller via andre verktøy. Fylkeskommunen må likevel påse at krav til obligatorisk innhold blir med i en samlet skriftlig og elektronisk tilgjengelig oversikt. Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale. Avtalen skal sikre at personopplysninger blir behandlet i samsvar med regelverket, og setter en klar ramme for hvordan databehandleren kan behandle opplysninger.

Datatilsynet viser til at det i *personvernregelverket* understrekes at arbeidet med informasjonssikkerhet er en kontinuerlig prosess. Det stilles blant annet krav til å sikre vedvarende robusthet i tillegg til konfidensialitet, integritet og tilgjengelighet. Det betyr blant annet at virksomheten har plikt til å ta hensyn til den tekniske utviklingen, altså hvilken teknologi som er tilgjengelig på markedet til enhver tid. Den teknologien som var akseptabel for å sikre virksomhetens behandlinger i fjor, er ikke nødvendigvis akseptabel i år.

Flere standarder kan benyttes for å sikre en systematisk tilnærming til arbeidet med informasjonssikkerhet. Digitaliserings- og forvaltningsdepartementet anbefaler at styringen av informasjonssikkerhet baserer seg på den gjeldende versjonen av den internasjonale standarden NS-ISO/IEC 27001. ISO/IEC 27001 beskriver retningslinjer og prosesser som hjelper virksomheter med å beskytte informasjon. Standarden stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av styringssystemet for informasjonssikkerhet.

Av ISO/IEC 27001 følger at sikkerhetstiltak gjennomføres basert på en risikovurdering og er tilpasset virksomhetens nivå. Standarden beskriver retningslinjer og prosesser som hjelper virksomheter med å beskytte informasjonen sin på en systematisk og effektiv måte. Videre stiller standarden krav til gjennomføring av risikovurderinger, etablering av roller og ansvar for informasjonssikkerhet, definering og implementering av sikkerhetstiltak, sikring av tilgangsstyring og beskyttelse av informasjon, utvikling av prosedyrer for håndtering av sikkerhetshendelser, samt gjennomføring av regelmessige revisjoner og evalueringer.

NSM anbefaler at virksomheten bør kartlegge de nåværende fysiske sikkerhetstiltakene og identifisere hva som må til for å redusere risikoen til akseptabelt nivå. Ved å identifisere områder og funksjoner som er sårbare og har risiko, vil virksomheten kunne planlegge spesifikke fysiske tiltak som vil redusere risiko forbundet med dette. Sikkerhetstiltakene bør utformes på en slik måte at de oppnår balansert sikring og at tiltakene virker uavhengig av hverandre. Virksomheten må selv velge strategi og utforming av tiltak for å effektivt kunne forebygge, detektere, forsinke og håndtere sikkerhetstruende virksomhet, og begrense skader

[7] General Data Protection Regulation, personvernforordningen, omhandler virksomheters behandling av personopplysninger og gjelder for all behandling av personopplysninger

på sine verdier. Tiltakene bør settes sammen slik at virksomheten oppnår helhetlig og balansert sikring. For å oppnå helhetlig sikring er man avhengig av at de fysiske, elektroniske, menneskelige og organisatoriske tiltakene fungerer sammen og understøtter hverandre. Virksomheten bør derfor gjennomføre øvelser for å kontrollere at tiltakene fungerer som de skal, og at de fungerer sammen. Etter en hendelse bør virksomheten kartlegge hendelsesforløp og evaluere om egne sikkerhetstiltak fungerte etter hensikten. Hendelser bør evalueres slik at virksomheten og de involverte skal kunne ta lærdom av hendelsen og med dette forbedre sikkerheten.

Felles for regelsettene over er at innretningen for internkontrollen må tilpasses organisasjonen og baseres på risikoforholdene.

På bakgrunn av ovenstående utleder vi som revisjonskriterier for **problemstilling 1** at Troms fylkeskommune v/fylkeskommunedirektør må for å ivareta kravene i regelverkene i arbeidet med informasjonssikkerhet og personvern:

- Utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
- Ha nødvendige rutiner og prosedyrer
- 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

Fylkeskommunedirektøren må som behandlingsansvarlig sørge for at:

- det føres protokoll over behandlingsaktiviteter
- all behandling av personopplysninger sikres

Vi utleder videre som kriterium at:
Troms fylkeskommune bør sørge for at ansatte gis tilstrekkelig opplæring i personvern og informasjonssikkerhet

For **problemstilling 2** utleder vi som revisjonskriterier at Troms fylkeskommune bør etablere sikringstiltak, herunder tekniske og organisatoriske tiltak ved å:

- kartlegge alle enheter og programvare som er i bruk
- gjennomføre risiko- og sårbarhetsanalyse av kritiske IKT-systemer, og sørge for at disse oppdateres ved vesentlige endringer
- ha kontroll på alle identiteter og tilganger
- gjennomføre jevnlig sårbarhetskartlegging, inntrengingstester, og vurdere nivå av sikkerhetsovervåking
- ha prosesser som sikrer at avvik som avdekkes gjennom iverksatte tiltak håndteres
- ha rutiner og prosesser som sikrer evaluering av effektiviteten til styringssystemet for informasjonssikkerhet

3 METODE, DATAMATERIALE OG AVGRENSING

3.1 Metode og datamateriale

Forvaltningsrevisjonen er gjennomført i henhold til gjeldende standard for forvaltningsrevisjon[8]. Revisor sendte brev om oppstart av forvaltningsrevisjonen til fylkeskommunedirektøren, og ba i den forbindelse om å få oppnevnt en kontaktperson i fylkeskommunen som vi kunne forholde oss til i prosjektgjennomføringen. Fagleder sikkerhet ved fylkeskommunedirektørens kontor ble oppnevnt som kontaktperson, og deltok i oppstartsmøtet sammen med IT-sikkerhetsleder ved IT-avdelingen og avdelingsleder ved informasjons- og dokumentsenter (INFODOK). I oppstartsmøtet 16.10.2025 informerte vi om forvaltningsrevisjonen, og startet innledende informasjonsinnhenting.

Fra fylkeskommunen ble det opplyst at det for tiden pågår arbeid i Troms fylkeskommune med internkontrollen på områdene for informasjonssikkerhet og personvern. Vi ble i oppstartsmøtet gitt en presentasjon av igangsatt prosjekt «*Helhetlig styring av informasjonssikkerhet og personvern»,* og presentasjonen ble i etterkant av møtet tilsendt oss. Presentasjonen omfattet prosjektorganisasjon, innhold, varighet og kostnader. Bakgrunnen for prosjektet opplyses å være behovet for overordnet styring etter opprettelsen av Troms fylkeskommune, herunder helhetlig ledelse og felles rammeverk, etterlevelse av lovverk og endret behov for beredskap som følge av endringer i måten digitale angrep gjennomføres på. Tidligere ble angrepene rettet mot organisasjonene, mens angrepene i dag rettes mot organisasjoner, den enkelte ansatte i organisasjonene og leverandører som organisasjonene benytter. Det er gjennomført overordnet ROS-analyse i Troms fylkeskommune. For tiden pågår arbeidet i fylkeskommunen med internkontrollen knyttet til IT-sikkerhet, informasjonssikkerhet og personvern. Som følge av at mange av de utarbeidede/endrede rutiner og prosedyrer skal implementeres i organisasjonen i 2026, omfatter undersøkelsen ikke etterlevelse av rutiner i ulike deler av organisasjonen.

Våre beskrivelser bygger på både skriftlige og muntlige data. Vi har fått tilsendt og gjennomgått dokumenter i form av retningslinjer, rutiner og prosedyrer. Videre har vi gjennomført intervjuer med ansatte som vi anser å være sentrale i arbeidet med styringssystem og internkontroll innen IT-sikkerhet, informasjonssikkerhet og personvern.

3.2 Gyldighet og pålitelighet

Med gyldige data menes at dataene som samles inn i undersøkelsen, skal utgjøre et relevant og tilstrekkelig grunnlag for å vurdere den reviderte virksomheten opp imot revisjonskriteriene og konkludere på problemstillingene. Revisor vurderer at det datamaterialet som er presentert som «revisors funn» i rapporten, oppfyller dette gyldighetskravet. Muntlig informasjon er innhentet fra ansatte i Troms fylkeskommune som medvirker til utarbeidelse og implementering av rutiner og prosedyrer, og som har et oppfølgingsansvar av at rutiner og prosedyrer følges. Vi har fått svar på de spørsmål vi har stilt, og fått oversendt den dokumentasjon vi har bedt om. Informantene har under intervjuer henvist til hendelser, som har bidratt til å belyse praksis og sikre validitet i funnene. Vi har ikke indikasjoner på at det finnes informasjon som er relevant for denne forvaltningsrevisjonen og som vi ikke er gitt tilgang til. Vi er fortalt at det er gjennomført en inntrengningstest, men revisor har ikke gjennomført sikkerhetsrevisjoner eller andre tekniske undersøkelser av systemenes faktiske robusthet. Våre vurderinger baseres på dokumenter som beskriver rutiner, prosesser og policyer, samt redegjørelser fra informanter i Troms fylkeskommune.

[8] *RSK 001 Standard for forvaltningsrevisjon* fastsatt av NKRFs styre 12.08.2020 og gjort gjeldende som god kommunal revisjonsskikk for forvaltningsrevisjoner med oppstartsbrev sendt etter 30.09.2020

Med pålitelige data menes at dataene skal være mest mulig nøyaktige. Revisor har vurdert eventuelle feilkilder i det innsamlede datamaterialet. Vi har ikke funnet motsetninger mellom skriftlige og muntlige data som framkommer i rapportens datagrunnlag. I tillegg har vi fremlagt datamaterialet for fylkeskommunen. Revisor har innarbeidet korrigeringer og supplerende opplysninger fra fylkeskommunen i rapporten.

Påliteligheten og gyldigheten i det presenterte datamaterialet er også på et overordnet nivå sikret gjennom KomRev NORDs interne kvalitetssikringssystem.

4 STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET

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

Revisjonskriterier

Troms fylkeskommune v/fylkeskommunedirektør må for arbeidet med personvern og informasjonssikkerhet:

- Utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
- Ha nødvendige rutiner og prosedyrer
- Avdekke og følge opp avvik og risiko for avvik
- Dokumentere internkontrollen i den formen og omfanget som er nødvendig
- Evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll

Fylkeskommunedirektøren må som behandlingsansvarlig sørge for at:

- det føres protokoll over behandlingsaktiviteter
- all behandling av personopplysninger sikres

Troms fylkeskommune bør sørge for at ansatte gis tilstrekkelig opplæring i personvern og informasjonssikkerhet

4.1 Styringssystem og internkontroll

Kommuneloven § 25-1 krever at fylkeskommunen skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Fylkeskommunedirektøren er ansvarlig for internkontrollen. Internkontrollen skal sikre at regelverk og fylkeskommunens egne mål etterleves. Konkrete krav til internkontroll følger som tidligere nevnt av ulikt regelverk, mens kommunelovens internkontrollbestemmelse er den generelle gjeldende for all virksomhet i fylkeskommunen.

Etter kommuneloven § 25-1 er hensikten med internkontrollen å sikre at lover og forskrifter følges. Bokstav b) krever at fylkeskommunedirektøren ved internkontroll skal ha nødvendige rutiner og prosedyrer. Risikovurderinger sier noe om hva som er nødvendige rutiner og prosedyrer. Kontrollaktiviteter skal bidra til at definerte internkontrollaktiviteter gjennomføres og fungerer som forutsatt, og bidra til videreutvikling av internkontrollen.

Fylkeskommunedirektøren er - som en del av internkontrollen – pålagt å utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering. Etter kommuneloven § 25-1 bokstav d) skal internkontrollen dokumenteres i den formen som er nødvendig å dokumentere. Det er opp til fylkeskommunedirektøren å avgjøre hva som er nødvendig å dokumentere, men KS angir at det er opplagt at kravet gjelder både rutiner og prosedyrer, risikoanalyser, iverksatte tiltak og avvikshåndtering m.m.[9]

I fylkeskommunens årsmelding for 2024[10] står at det er etablert en policy inkludert roller og ansvar for informasjonssikkerhet og personvern som skal danne grunnlag for iverksettelse av

[9] KS, Veileder Orden i eget hus, Kommunedirektørens internkontroll, side 45-46
[10] Fylkestinget 17.06.2025, sak 22/25

styringssystem på samme områder. Videre at det er lagt vekt på å etablere internkontroll for informasjonssikkerhet og personvern som et ledd i øvrig kontrollarbeid, og at arbeidet vil fortsette i 2025.

Kommuneloven § 25-2 pålegger fylkeskommunedirektøren om årlig å rapportere til fylkestinget om internkontroll og statlige tilsyn. I fylkeskommunedirektørens rapportering 07.10.2025 (sak 45/25) til fylkestinget om internkontroll og statlige tilsyn, gis en oppsummering for perioden 2023-2025. Her framgår at målsetningen i perioden har vært på etablering og bruk av felles kvalitetssystem som skal være grunnlag for internkontrollarbeidet i organisasjonen. I 2024 startet et omfattende arbeid med å få oversikt på fagområdene personvern og informasjonssikkerhet. Dette er fagområder som er gjennomgående i organisasjonen, og krever at fylkeskommunen har et godt system for internkontroll for å lykkes. Gjennomgangen viste at internkontrollarbeidet fortsatt i liten grad er risikobasert, og vil ha hovedfokus i det videre arbeidet.

4.1.1 Kvalitetspolicy og overordnede målsetninger for arbeidet med internkontroll og kvalitet

Det er fastsatt kvalitetspolicy og overordnede målsetninger for arbeidet med internkontroll og kvalitet for perioden 2023-2025:
1. Etablere et felles kvalitetssystem for hele Troms fylkeskommune
2. Samle og tilgjengeliggjøre styringsdokumentene og sørge for god dokumentstyring
3. Avvik: Organisasjonen skal aktivt melde avvik og lære av feil
4. Sikre og kontinuerlig forbedre vesentlige arbeidsprosesser

Når det gjelder langsiktige mål for perioden 2026-2028, skriver fylkeskommunedirektøren at det vil være behov for en mer helhetlig tilnærming til arbeidet med virksomhetsstyring og internkontroll. Dette på bakgrunn av de regulatoriske krav som settes til virksomhetene, og økt behov for digitalisering og effektivisering. Sammenhengen mellom arbeidsprosesser, digital infrastruktur og dataflyt vurderes av fylkeskommunedirektøren som essensielt for å lykkes med en helhetlig styring framover. I første omgang vurderer fylkeskommunedirektøren at følgende områder bør prioriteres:

- *Prosessbeskrivelser og risikovurderinger:* Tegne opp kritiske arbeidsprosesser og risikovurdere disse, inkludert hvilke faser som utløser behov for kontrolltiltak. Dette arbeidet vil samtidig bidra til å identifisere behandlingen av personopplysninger, hvor data er lagret og dataflyt inn og ut av organisasjonen.

- *Overordnet risikovurdering og tiltaksplan:* Dataene fra prosessgjennomgangene vil gi grunnlag for en overordnet risikovurdering for Troms fylkeskommune. Dette vil gi bedre grunnlag for en helhetlig prioritering av internkontrollarbeidet inn mot de områdene hvor det foreligger høyest risiko. Det bør utformes konkret tiltaksplan i etterkant av risikovurderingen.

Videre bør det settes tidsperspektiv på målsettingen i tråd med de ressurser som stilles tilgjengelig. I saksframlegget foreslås følgende tidsplan:

1. 2025 (høst): Utforme prosjektbeskrivelse og forankre i organisasjonen. Kartlegge ressurser og bestemme metodikk. Klargjøre grunnlagsdokumenter og planlegge opplæring.

2. 2026-2027: Gjennomføre opplæring av aktuelle ledere og av superbrukere, eventuelt med bistand fra ekstern aktør og/eller annen fylkeskommune (erfaringsutveksling). Utførelse av prosesskartlegging og risikovurdering.
3. 2027-2028: Overordnet risikovurdering og tiltaksplan. Iverksette tiltak. Evaluere. Gevinstrealisering.

Fylkeskommunedirektøren skriver at den langsiktige målsetningen er å ha en samlet oversikt over og kontroll på virksomhetenes arbeidsprosesser for bedre å kunne styre i tråd med fylkeskommunens målsetninger og regulatoriske/kvalitetsmessige krav, herunder håndtere risiko. Denne målsetningen vil det ta flere år å nå, men innretningen arbeidet og tiltakene bør gjenspeile dette langsiktige målet.

For å sette kvalitetsarbeidet jevnlig på dagsorden og forankre i ledelsen, gjennomføres *Ledelsens gjennomgang* årlig i ledergruppene. I 2024 ble Ledelsens gjennomgang utført i alle etatene og stab- og støtteavdelingene – til sammen 12 gjennomganger. Hver ledergruppe skal i henhold til kvalitetspolicyen iverksette minimum to tiltak på bakgrunn av gjennomgangen. Tiltaksarbeidet skal rapporteres til porteføljestyret.

Fylkeskommunedirektøren skriver at i tillegg til de langsiktige målene, viser statusgjennomgang et fortsatt behov for å sikre at avvik registreres og følges opp i alle etater. Det bør også etableres en rutine for internrevisjon på utvalgte områder, for eksempel i form av stikkprøver.

4.1.2 Sikkerhetsmål og sikkerhetsstrategi

Av eForvaltningsforskriften § 15 følger at et forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).

Dokumentet *Policy for informasjonssikkerhet og personvern*, gjelder all informasjonsbehandling og behandling av personopplysninger som skjer internt i Troms fylkeskommune, som Troms fylkeskommune har ansvaret for eksternt, samt alle som behandler slik informasjon på vegne av Troms fylkeskommune. Herunder all behandling, lagring og kommunikasjon av informasjon, både muntlig, på papir og digitalt. All bruk av IKT-systemer er inkludert. I dokumentet angis sikkerhetsmål, overordnede føringer og grunnleggende prinsipper, samt strategi for informasjonssikkerhet og personvern.

Formålet med policyen er å understøtte fylkeskommunens oppgaver og tjenester slik at mål kan nås og visjon kan realiseres i tråd med overordnede visjoner og strategier. Videre at en informasjonsbehandling som er målorientert, effektiv, lovlig og til å stole på, er avgjørende for at fylkeskommunen skal lykkes. Tilstrekkelig og balansert informasjonssikkerhet er en kritisk faktor for å understøtte dette, slik at personopplysningene beskyttes.

Under sikkerhetsmål står det at Troms fylkeskommune sin behandling av informasjon skal være i samsvar med regulatoriske, interne og avtalerettslige krav til informasjonssikkerhet. Personopplysninger og annen beskyttelsesverdig informasjon skal sikres på en betryggende måte gjennom fysiske, tekniske og organisatoriske tiltak. Herunder skal konfidensialitet, integritet, tilgjengelighet og robusthet ivaretas. Strategi for informasjonssikkerhet og personvern omtales, herunder at arbeidet med informasjonssikkerhet og personvern skal:

- være forankret i linjen og utføres systematisk
- gjennomføres for å nå målene for informasjonssikkerhet og personvern

- være risikobasert og følge anerkjente standarder
- følge prinsippene for læring og kontinuerlig forbedring

Det innebærer at:

- oversikt informasjon og personopplysninger er oppdatert og dokumentert
- risikovurderinger gjennomføres systematisk, periodisk og ved vesentlige endringer i oppgaver eller omgivelser
- tiltak for å redusere risiko er basert på risikovurderinger og ledelsens føringer for risikohåndtering og akseptabel risiko
- hendelser som ut fra risiko kan påvirke sikkerhetsmålene negativt, meldes og følges på en systematisk måte
- ledelsen systematisk styrer og følger opp informasjonssikkerhets- og personvernarbeidet
- ledelsen systematisk følger opp måloppnåelse, etterlevelse, kompetanse og kultur

For å lykkes med dette skal alle ansatte:

- ha et bevisst forhold til virksomhetens sikkerhetsmål og målenes viktighet
- vite hvilke typer av informasjon og personopplysninger de behandler, og hvilke krav som stilles til deres egen informasjonsbehandling og bruk av IKT-systemer
- etterleve krav, retningslinjer, prosedyrer, rutiner mv. som gjelder for dem og det arbeidet de utfører

På spørsmål om sikkerhetsmålene er kommunisert ut i organisasjonen får vi opplyst at disse nok ikke er kjent blant alle ansatte i Troms fylkeskommune. I overgangen til en sentralisert styringsmodell, er det vektlagt at informasjon skal være enhetlig og nå ut i hele organisasjonen samtidig. Utfordringen er ikke å videreutvikle og lage et godt styringssystem, men å sikre implementering og etterlevelse i alle etater og avdelinger.

Policy for informasjonssikkerhet og personvern, angir under punkt 3 sikkerhetsmål knyttet til konfidensialitet, integritet, tilgjengelighet og robusthet. I policyen legges det til grunn at styringssystemet skal bygge på ISO-standarden som også inkluderer NSM sine grunnprinsipper. Kravene i ISO-standarden opplyses å vurderes om de er nødvendige fortløpende gjennom en SOA (samsvarserklæring) for å oppnå fylkeskommunens sikkerhetsmål.

Revisor har spurt hvordan fylkeskommunen i praksis gjennomgår disse kravene, og eventuelt dokumenterer dette arbeidet. Vi har fått fortalt at det jobbes med sikkerhetsmålene, og et godt rammeverk omkring dette, blant annet gjennom tydelige ansvarslinjer. Referansegruppen (fagressursgruppen) og styringsgruppen deltar i arbeidet.

Arbeidet som gjennomføres dokumenteres i *Datakvalitet*, og omfatter blant annet:

- Hvem som har ansvar for systemene
- Hvem som har ansvar for databehandleravtaler
- Hvem som har ansvar for tilgangsstyring
- Logging av systemer som håndterer personopplysninger
- Innføring av stillingskategorien *kritisk stilling.* Ansatte innen denne stillingskategorien har tilgang til kritiske systemer, og må dermed oppfylle særskilte vilkår, og være seg bevisst det ansvaret som er tillagt denne type stilling

Vi har fra fylkeskommunen fått opplyst at digitaliseringsstrategien er videreført fra Troms og Finnmark fylkeskommune til Troms fylkeskommune, og at det er et mål å få på plass en egen digitaliseringsstrategi for Troms fylkeskommune i løpet av 2026.

I dokumentet *Roller og ansvar – Informasjonssikkerhet og personvern* står at IT-sikkerhetsleder har ansvar for IKT-sikkerheten herunder å utvikle en helhetlig informasjonssikkerhetsstrategi. IT-sikkerhetsleder har stilt spørsmål ved om det her er en skrivefeil i dokumentet, og om det skal stå ansvar for IT-sikkerhetsstrategi, og har tatt dette opp med avdelingsleder INFODOK. Vi har fått opplyst at dokumentet skal revideres.

4.1.3 System for virksomhetsstyring

Porteføljestyring er etablert som system for virksomhetsstyring i Troms fylkeskommune, herunder styring av prosjekter på tvers av organisasjonen. Porteføljestyring skal inkludere sikring av god internkontroll i prosjektene ved hjelp av standardisering og rapportering.

Revisor har fått tilsendt *Veileder for porteføljestyring i Troms fylkeskommune*. Vi har fått opplyst at porteføljestyring som modell er under utvikling og vil etter hvert evalueres basert på erfaringer så langt. Porteføljestyret er et rådgivende organ for administrativ ledelse, og det avvikles møter ca. en gang i måneden. Porteføljestyret oppdateres jevnlig på status og saker vedrørende sikkerhet, herunder informasjonssikkerhet og personvern. Dette for å sikre at bredt omfang av ledelse er kjent med de retningslinjene som gjøres gjeldende i organisasjonen.

Porteføljestyrets sammensetning:

- Porteføljeeier - fylkeskommunedirektøren
- Porteføljesekretariat - fagleder virksomhetsstyring (vakant for øyeblikket, ny medarbeider tiltrer i mars)
- Etatssjefer – samferdsel, kompetanse, tannhelse, samfunn, næring og kultur, assisterende fylkeskommunedirektør
- Avdelingsledere stab/støtte – økonomi, personal, innkjøp, drift og eiendom, INFODOK og IT
- Fagleder for sikkerhet- og beredskap
- Kommunikasjonssjef

4.1.4 ROS-analyse

I Troms fylkeskommunes økonomiplan 2026-2029 blir gjennomført ROS-analyse omtalt på følgende måte:

> «*Sikkerhet og beredskap er et fagfelt som er i stor vekst. Troms fylkeskommune har gjennomført ROS-analyse for virksomheten 2024/2025. Sluttrapporten peker på behov for å styrke kapasiteten på sikkerhet og beredskap i organisasjonen, og den er tydelig på at organisasjonen mangler kapasitet til koordinering og systematisk arbeid. Rapporten foreslår en lang rekke med tiltak knyttet til analyse og planverk, fysisk og elektronisk sikring, organisatoriske tiltak, beredskap, opplæring og øvelse. Fylkeskommunedirektøren ser behov for å utrede omfanget og kostnadene med tiltakene. Det varsles samtidig behov for ytterligere ressurser i økonomiplanperioden for å iverksette tiltak knyttet til sikkerhet og beredskap*».

Fylkestinget har bevilget midler i årene framover for å følge opp virksomhets-ROS, og arbeidet med sikkerhet og beredskap. Overfor revisor gis det i intervju uttrykk for viktigheten av at fylkestinget er godt orientert om arbeidet og derfor bør få grundig informasjon om hva

bevilgningene brukes til. Den globale situasjonen påvirker fylkeskommunens arbeid innenfor sikkerhet og beredskap. Av den grunn må det planlegges for tiltak med tanke på datasikkerheten og informasjonssikkerheten i organisasjonen. Trusselbildet opplyses å ikke være unikt for Troms fylkeskommune. Troms fylkeskommune gjør ikke egne vurderinger av det sikkerhetspolitiske trusselbildet, og baserer sine vurderinger på de vurderinger Nasjonale sikkerhetsmyndigheter, PST og E-tjenesten gjør. Dette kan være både offentlige og graderte vurderinger, og anbefalinger følges. Som eksempel nevnes at dersom en applikasjon ikke anbefales brukt i offentlig sektor, vil Troms fylkeskommune effektuere dette.

Revisor har fått opplyst at Ledelsens gjennomgang i 2025 omfattet en orientering for fylkestinget, hvor det i desember 2025 i lukket fylkestingsmøte ble informert om tilstanden på sikkerhets- og beredskapsarbeidet i Troms fylkeskommune. Det ble i møtet gitt en presentasjon om ROS-analysen som peker på ulike risikofaktorer, herunder hvordan organisasjonen er eksponert for IT-trusler, og hvilke IT-sikkerhetstiltak som er etablert i organisasjonen. Det ble også orientert om informasjonssikkerhet og personverntilstanden i organisasjonen.

Revisor spurte om det ved gjennomført ROS-analyse ble avdekket risikoer knyttet til informasjonssikkerhet og personvern, og fikk bekreftet at det ble avdekket risikoer også innenfor disse områdene. Disse er unntatt offentlighet, og revisor har derfor ikke kartlagt dette noe nærmere for å beskrive i rapporten.

I 2026 jobbes det med å få ROS-analysen implementert i enhetene, og gjennomføre virksomhets-ROS i alle enheter. Vi er fortalt at det i første omgang planlegges å sjekke om beredskapsplaner er etablert i de ulike virksomhetene, og om det er gjennomført ROS-analyser særskilt for virksomhetene. Herunder forståelsen av hva virksomhets-ROS innebærer for den enkelte enhet. Virksomhets-ROS har flere scenarioer med forslag til tiltak, og det vil være variasjoner ved den enkelte enhet. Hvis en skole ligger i ras/skredutsatt område, må det planlegges tiltak for ekstra beredskap. Det gjennomføres øvelser, og et scenario som ble gjennomført i 2024 gjaldt IT-sikkerhetsbrudd. Deltakere her var rektorer ved de videregående skolene. Tilbakemeldingene fra deltakerne i gjennomførte øvelser har vært gode. I ettertid har det kommet henvendelser fra etater om at de ønsker mer informasjon om sikkerhet og beredskap.

4.1.5 Risikovurderinger

Fra INFODOK har vi fått opplyst at risikovurderingen for informasjonssystemene skal implementeres i egen modul, som knytter systemforvaltningen i det som kalles for *Samsvar* i dag. Systemoversikt, risikovurdering, personvernkonsekvenser og behandlingsprotokoll skal ligge i samme modul. I dag gjør systemeier risikovurderinger ved hjelp av excel-ark for informasjonssystemer, og noen bruker *Datakvalitet* til vurderinger. Det er ikke p.t. en helhetlig oversikt eller oppfølging, da det er systemeier som selv følger opp at det gjennomføres risikovurderinger av systemene.

Det er gjennomført virksomhets-ROS ved IT-avdelingen. Malene for risikovurderingene som er gjort opplyses å ligge i kvalitetssystemet. Virksomhets-ROS viste to risikoer; tap av kontroll av sensitive opplysninger og vellykkede cyberangrep. Dette er hendelser som IT-avdelingen ser får størst konsekvens om de inntreffer. Det IT-avdelingen kan gjøre er å påvirke sannsynligheten for at hendelsene inntreffer. Noen tiltak er allerede iverksatt, og andre tiltak jobbes det med. Det er også noen risikoer som en har valgt å akseptere.

Revisor er gjort kjent med at risikovurderingene gjennomført ved IT-avdelingen, er lastet opp i et eget risikoregister. Risikoregisteret er svært omfattende og inneholder mye informasjon. Det er av fylkeskommunen gjort en vurdering om at distribusjon ut i organisasjonen ikke er hensiktsmessig. Informasjonen fra risikoregisteret som skal inngå i dokumentasjonsgrunnlag i organisasjonen blir omarbeidet til powerpointpresentasjoner.

Vi er informert om at IT-sikkerhetsleder i januar 2026 ga en orientering til porteføljestyret om gjennomførte risikovurderinger, samt hvilke tiltak som er nødvendig å iverksette. Herunder hva det ikke p.t. er rammevilkår for å gjennomføre, eller at iverksettelse av tiltak ligger utenfor IT-avdelingens myndighetsområde.

4.1.6 Styringssystem

Et helhetlig styringssystem ivaretar ofte ulike funksjoner, og risikoredusering gjennom styrket internkontroll er en av dem. Måloppnåelse og resultater, krise- og beredskapshåndtering og systematisk utviklings- og forbedringsarbeid er også viktige funksjoner i internkontrollarbeidet. Manglende styringsstrukturer og prosesser for risikovurdering kan føre til at ledelsen ikke får tilstrekkelig informasjon til å prioritere og styre virksomhetens sikkerhetsarbeid.

Revisor er fortalt at selv om mye var på plass etter at Troms fylkeskommune 01.01.2024 ble etablert som egen organisasjon, var styringen fragmentert. Blant annet som følge av tidligere styringsform. Fylkeskommunedirektør ble etter endringen av styringsform øverste administrative leder, og er ansvarlig for interkontrollen etter kommuneloven § 25-1 første ledd. Det var nødvendig å få en helhetlig oversikt over hvilke dokumenter som skulle inngå som styringsdokumenter i arbeidet med å ha «orden i eget hus». Prosjektet *Helhetlig styring av informasjonssikkerhet og personvern* startet som følge av behovet for overordnet styring, etterslep på etterlevelse av lovverk, systemer og rutiner, samt endringer i rammeverket. Prosjektet er delt opp i flere leveranser av ulik størrelse og karakter, som krever ulik tilnærming. Troms fylkeskommune gjør fortløpende vurderinger av hva som skal ligge i styringssystemet. For å holde perspektivene i prosjektarbeidet har fylkeskommunen gjort et valg om å dele den IT-tekniske sikkerheten og informasjonssikkerheten, og det pågår p.t. arbeid med internkontrollen på disse områdene.

Ett av målene for prosjektet *Helhetlig styring av informasjonssikkerhet og personvern* er at det skal bidra til kjente linjer fra øverst og nedover i organisasjonen, og unngå etablering av rammeverk på siden av, eller på tvers av andre rammeverk som omfatter kvalitet og styring. Vi er fortalt at det i arbeidet med prosjektet dukker opp nye behov underveis, og det må fortløpende vurderes hva som haster mest. Som eksempel nevnes oppslag i media om kamerabruk i Tromsø kommune, som medførte at Troms fylkeskommune måtte prioritere forholdet til personvernkonsekvenser ved å se på egen praksis for kamerabruk. Erfaringen er at det nå meldes flere avvik enn tidligere, og hvor en del gjelder personvern, herunder offentliggjøring av sensitive opplysninger og sensitive opplysninger sendt feil person. Avvikssaker påvirker også prosjektarbeidet, spesielt med hensyn til utarbeidelse av styringsdokumenter.

Revisor har spurt hvilke regelsett Troms fylkeskommune selv anser som gjeldende for fylkeskommunen når det kommer til informasjonssikkerhet og personvern. Vi er fortalt at fylkeskommunen legger ulike regelverk til grunn for arbeidet med styringssystemet, herunder blant annet sikkerhetsloven, personopplysningsloven og GDPR.

Digitalsikkerhetsloven stiller krav til styringssystem og krav til innholdet i et styringssystem. Vi fikk fortalt at det pågår arbeid med å få avklart hvordan fylkeskommunen er berørt av

digitalsikkerhetsloven med tilhørende forskrift, eventuelt hvilket etater etc. Videre at digitalsikkerhetslovens krav til sikkerhetsmessig styringsstruktur hensyntas, og at tiltak iverksettes ute i alle etater og enheter i organisasjonen. Det jobbes med å finne en løsning slik at bestemmelsene i loven ivaretas på en effektiv måte, uten å bygge opp mange parallelle strukturer. Mye av rammeverket for sikkerhet og beredskap er utformet for organisasjoner som i utgangspunktet har lettere for å definere hva som er kritiske verdier.

Sikkerhetslovens krav om sikkerhetsstyring gjelder uavhengig av om fylkeskommunen har skjermingsverdige verdier[11]. Troms fylkeskommune må derfor sikre at forebyggende sikkerhetsarbeid inngår som en del av fylkeskommunens styringssystem. Fylkeskommunen benytter noen få IT-systemer som er levert på nasjonal beskyttet plattform[12]. Troms fylkeskommune er kun bruker, og har ikke forvaltningsansvar for disse systemene.

Troms fylkeskommune opplyser å ha gjort en vurdering med tanke på skjermingsverdige verdier som faller inn under sikkerhetsloven, og kommet til at gradert kommunikasjon er vurdert som verdi som krever sikkerhetsmessige tiltak. Øvrig verdivurdering av informasjon gjøres i prosjektet.

4.1.7 Styringssystemets innhold

Gjennom prosjektet *Helhetlig styring av informasjonssikkerhet og personvern* har Troms fylkeskommune igangsatt et arbeid med gjennomgang av styringssystemet. Prosjektet er delt opp i flere leveranser:

- Felles rammeverk, policyer og prosesser
- Revidering av roller og ansvar
- Oversikt over informasjonsverdier i rammeverket
- Implementering av ROS og DPIA
- Internkontroll
- Oversikt over behandlinger (protokoll)
- Avvikshåndtering og kontinuerlig forbedring
- Bevisstgjøring og sikkerhetskultur, ledelsesverktøy og opplæring

Leveransene er opplyst å være av ulik størrelse og karakter, og krever ulik tilnærming. Gjennom prosjektet gjøres det fortløpende vurderinger av hva som skal ligge i styringssystemet. Status per desember 2025 er at det jobbes på tvers i alle delprosjektene. Det leies inn bistand for noen leveranser, noen leveranser er stort sett ferdigstilt, og noen er planlagt gjennomført i 2026. Enkelte deler av prosjektet krever at andre deler er ferdigstilt før disse kan gjennomføres. Det er siden oppstart av prosjektet produsert mange styringsdokumenter i form av rutiner, prosedyrer og reglementer. Prosjektets leveranser skal implementeres i organisasjonen i 2026, og Troms fylkeskommune vil innhente bistand til deler av dette. Første del er planlagt lyst ut i januar 2026.

Styringssystemet opplyses å være et felles verktøy for Troms fylkeskommunes kvalitetsarbeid, og *Datakvalitet* benyttes som kvalitetssystem. Alt ligger ikke p.t. i kvalitetssystemet, men vil bli lagt inn etter hvert som dokumenter (rutiner, prosedyrer, retningslinjer) utarbeides og

[11] Objekter og infrastruktur er skjermingsverdige etter sikkerhetsloven dersom de kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse.

[12] Fra 1. januar 2025 ble Forsvarsdepartementets IKT-enhet etablert som en egen etat, med navnet Statens graderte plattformtjenester. Etaten skal levere graderte kommunikasjonsløsninger til offentlige og private virksomheter som er underlagt sikkerhetsloven.

godkjennes. Det har vært diskutert hvordan informasjon skal nå godt ut, og Troms fylkeskommune har fått bistand for å få systematisert informasjon i form av en kvalitetshåndbok. Kvalitetshåndboken er opplyst å være tilgjengelig for alle ansatte via fylkeskommunens intranett.

Troms fylkeskommune opplyser at standarden ISO/IEC 27001 legges til grunn for arbeidet med informasjonssikkerhet. Standarden benyttes i den utstrekning som av fylkeskommunen vurderes som relevant.

Vi har fått oversendt følgende dokumenter som omhandler informasjonssikkerhet og personvern, og som opplyses å inngå i fylkeskommunens kvalitetssystem:

- Policy for informasjonssikkerhet og personvern
- Roller og ansvar – Informasjonssikkerhet og personvern
- IKT-reglement for bruk av IKT-ressurser
- Melding av avvik på informasjonssikkerhet og personvern
- Veileder for bruk av KI – generativ kunstig intelligens
- Retningslinje for innsyn i ansattes e-post, områder i virksomhetens datanettverk og annet elektronisk utstyr
- Prosedyre for innsyn i ansattes e-post, områder i virksomhetens datanettverk og annet elektronisk utstyr
- Rutine for behandling og lagring av personopplysninger
- Prosedyre for vurdering av personvernkonsekvenser (DPIA)

4.1.8 Roller og ansvar

Informasjonssikkerhet og personvern som egne fagområder krever ressurser med definerte roller og ansvar. Det bør minimum være én dedikert ressurs for informasjonssikkerhet og personvern.[13]

Fylkeskommunedirektøren har det overordnede ansvaret for informasjonssikkerhet og personvern, og er dermed behandlingsansvarlig. Forvaltningsansvaret for personvern er delegert til fagleder sikkerhet, mens etatsjef har det daglige og operative ansvaret. Informasjonssikkerhet inngår i det overordnede sikkerhetsarbeidet, og ansvaret er delegert til fagleder sikkerhet.

Virksomhetsstyringen i Troms fylkeskommune bygger på helhetlig ledelsesprinsipp, som betyr at hver leder har ansvar innenfor sitt område. Ansvaret inkluderer internkontroll innen informasjonssikkerhet og personvern, herunder å utarbeide og gjennomføre sikkerhetstiltak innenfor sine ansvarsområder. All behandling av personopplysninger skal være lovlig, rettferdig og gjøres på en åpen måte. Enhver personopplysning skal ha et formål, og fylkeskommunen skal ikke behandle og lagre flere opplysninger enn det som er nødvendig.

Vi er fortalt at roller og ansvarsfordelingen er blitt tydeligere gjennom prosjektarbeidet, men det må gå seg litt til hvordan organiseringen av arbeidet skal gjennomføres. Noe som begrunnes med at et ikke er en egen enhet eller stab som jobber med dette. IT-avdelingen er generelt førstelinja for spørsmål/saker som gjelder IT-systemene. En erfaren ansatt fordeler innkomne saker etter tilgjengelige fagressurser i avdelingen.

[13] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Systemeier har overordnet ansvar for systemet, herunder sørge for drift, vedlikehold og informasjonssikkerhet. Systemeieransvaret skal være plassert i en virksomhet/avdeling. Leder/avdelingsleder utpeker systemansvarlig(e) som skal ha det operative ansvaret for oppfølgingen av systemet. Deler av det daglige operative behandlingsansvaret for informasjonssikkerheten i det enkelte IKT-system er delegert fra *systemeier* til s*ystemansvarlig*. Systemansvarlig har ansvar for å:

- Utarbeide dokumentasjon for bruk av IKT-systemet og gjennomføre risikovurderinger, inkludert alle behandlinger av personopplysninger
- Sørge for at avvik blir rapportert, behandlet og fulgt opp
- Oppnevne systemadministratorer og/eller superbrukere ved behov
- Sørge for at systemoversikten er oppdatert

Revisor ser at det i dokumentet *Roller og ansvar - Informasjonssikkerhet og personvern* opplyses at rollebeskrivelse for systemeier, systemansvarlige og systemadministrator ikke er utarbeidet. Det fremgår av dokumentet at stillingsbeskrivelse for systemansvarlig vgs er utarbeidet. Vi har fått opplyst at en helhetlig beskrivelse av disse rollene, vil bli utarbeidet i 2026.

Etatslederne er operativt behandlingsansvarlige, og er systemeiere for sine systemer. *Etatsjef* har det daglige operative ansvaret for personvern. Dette innebærer ansvar for at behandling av at informasjon inkludert personopplysninger i etaten, er i tråd med Troms fylkeskommune sin Policy for informasjonssikkerhet og personvern. Etatsjef kan delegere det operative ansvaret (arbeidsoppgaver) for informasjonssikkerheten i tjenestelinjen eller til systemeier. Dette skal være dokumentert.

Lengere ned i organisasjonen er systemadministrator/systemforvalter på de enkelte systemene. Vi er fortalt at det på nivåene under er mer utydelig, ikke når det gjelder systemansvar, men med hensyn til kunnskap om styringssystemet. Dette forklares med at man ennå ikke har fått ut tilstrekkelig informasjon i organisasjonen. Prosjektet er godt forankret gjennom porteføljestyret og ledere, men foreløpig er det liten oversikt over hvordan ledere har iverksatt dette i egen organisasjon. Etableringen av et helhetlig styringssystem er nytt for mange, og en vil se resultatet av arbeidet når implementeringen skjer i 2026.

Avdeling IT har ansvar for datasikkerhet, og avdeling informasjon og dokumentasjonsforvaltning (INFODOK) har ansvar for informasjonssikkerhet, herunder at personvernlovgivningen følges. Skillet mellom IT-teknisk sikkerhet og informasjonssikkerhet er opplyst å være gjort for at ikke arbeidet med informasjonssikkerhet og GDPR skal bli veldig teknisk. På noen områder jobber INFODOK tett med IT-avdelingen, og på andre områder med ansatte som jobber med kvalitet generelt for å samkjøre. Tanken er at Troms fylkeskommune skal ha helhetlig styring og helhetlig internkontroll, og styringssystemet skal være en del av det øvrige rammeverket for Troms fylkeskommune.

Dokumentet *Roller og ansvar - Informasjonssikkerhet og personvern* beskriver roller og ansvar for implementering og vedlikehold av informasjonssikkerheten og personvernet i Troms fylkeskommune. Vi er fortalt at dette dokumentet tidlig var på plass, og at dokumentet senere er oppdatert. Dette som følge av at det i prosjektet gjennomføres kartlegging av aktiviteter, noe som igjen fører til at roller og ansvar endres. Det er fra fylkeskommunen fokus på at roller og ansvar skal gjenspeile virkeligheten, og at det skal være tydelig hvem som har ansvar for hva.

Dokumentet er opplyst å gjelde alle ansatte, innleide konsulenter og leverandører som har tilgang til eller behandler fylkeskommunens informasjon, enten digitalt eller i fysisk form. Formålet er oppgitt å være: «*å sikre at ansvar og myndighet for roller som er relevante for informasjonssikkerheten og personvernet er tildelt og kommunisert*». Dokumentet inneholder detaljerte beskrivelser av definerte roller og tilhørende ansvar for informasjonssikkerhet og personvern. Vi gir i det følgende en kort beskrivelse av roller med tilhørende ansvar.

Fagleder sikkerhet er forvaltningsansvarlig for personvern og informasjonssikkerhet, og skal sørge for en hensiktsmessig og velfungerende sikkerhetsorganisasjon.

Avdelingsleder informasjons- og dokumentasjonsforvaltning (INFODOK) er fagressurs for personvern og ansvarlig for informasjonssikkerhet, jf. eget reglement. Ansvaret utøves i samarbeid med fagressursgruppen og IT-sikkerhetsleder. Fagressursen rapporterer til fagleder sikkerhet.

IT-sikkerhetsleder har ansvar for IKT-sikkerheten i Troms fylkeskommune, og er en del av IT-avdelingens lederteam. Ansvaret utøves i samarbeid med fagansvarlig for informasjonssikkerhet og personvern. IT-sikkerhetsleder rapporterer til fagleder sikkerhet.

Tverrfaglig team for forebyggende sikkerhet består av representanter fra hver etat med flere, og skal blant annet:

- Bistå sikkerhets- og beredskapsleder i koordinering og saksforberedelse til fylkeskommunedirektøren og porteføljestyret, blant annet saker om
  - overordnede styringsdokumenter om informasjonssikkerhet
  - anskaffelse eller større oppgradering av eksisterende IKT-systemer på bakgrunn av faglig vurdering fra informasjonssikkerhetsteamet
  - digitaliseringsprosjekter av større omfang

Fagressursgruppe-Informasjonssikkerhet og personvern er et rådgivende organ innen informasjonssikkerhet og personvern, og utgjør fagressurs for hele Troms fylkeskommune. Fagressursgruppen skal blant annet:

- Bistå fagansvarlig informasjonssikkerhet og personvern
- Etablere og vedlikeholde fylkeskommunens overordnede internkontrollsystem for informasjonssikkerhet som en del av fylkeskommunens kvalitetssystem
- Holde organisasjonen faglig oppdatert innen informasjonssikkerhet, herunder gi nødvendig råd og være pådriver i fylkeskommunens arbeid med fagområdet
- Avgi faglig vurdering før vedtak om innkjøp og anskaffelse av informasjonssystemer som behandler informasjon og personopplysninger eller større oppgradering av eksisterende systemer, herunder databehandleravtale
- Avgi faglig uttalelse og/eller delta i prosjekter (f.eks. referansegruppe) om større digitaliseringsprosjekter som behandler informasjon og personopplysninger, inkludert styringsdokumenter som omhandler digitalisering (digitaliseringsstrategier)

Ansattes ansvar framgår. Med ansatt menes fast og midlertidig ansatt, samt innleid personell (for eksempel konsulent eller håndverker), praktikanter, lærlinger og andre som utfører arbeid på vegne av Troms fylkeskommune. Den ansatte har ansvar for å:

- Forstå betydningen av sikker behandling av informasjon i forbindelse med eget arbeid
- Være kjent med og følge gjeldende aktuelle lovverk, instrukser og rutiner innen informasjonssikkerhet og personvern

- Rapportere avvik innen informasjonssikkerhet og personvern, herunder forbedringsforslag
- Gjennomføre obligatorisk opplæring innen informasjonssikkerhet og personvern

Personvernforordningen skiller mellom begrepene *behandlingsansvarlig* og *databehandler*. Det stilles ulike krav til behandlingsansvarlige og databehandlere. Fylkeskommunedirektøren er som behandlingsansvarlig ansvarlig for at prinsippene følges, også når behandlinger utføres av leverandør (databehandler).

Revisor er opplyst at det har vært en organisasjonsmessig utfordring knyttet at til alle vurderinger av personvernkonsekvenser dokumenteres og lagres i sak- og arkivsystemet. Det er igangsatt et eget prosjekt. Fagleder sikkerhet opplever at dette har blitt fulgt opp, og forbedret, men det er noen indikasjoner på at det fortsatt må følges opp. Det er synliggjort gjennom ansvarslinjen at det skal være en DPIA og en databehandleravtale. Vi er informert om at etatsjefene har ansvar for databehandleravtaler i egen etat, mens fylkeskommunedirektøren har ansvar for behandlinger som gjelder hele fylkeskommunen. Formålet er å sikre at det øverste ledelsesnivået i organisasjonen har kontroll på databehandleravtale og behandlingsprotokoll.

Personvernombudets oppgave står beskrevet i personvernforordningen artikkel 39. Personvernombudet er en uavhengig rolle som skal prioritere oppgavene sine ut fra hvor det vurderer at risikoen for personvernet kan være størst. Kjernen i oppgavene er å støtte den behandlingsansvarlige i å oppfylle pliktene etter regelverket.

Ifølge Digdir skal virksomheten ivareta krav til informasjonssikkerhet og personopplysningsvern i anskaffelser. Revisor har fått opplyst at retningslinjer for leverandørstyring var på plass før årsskiftet (2025), og rutiner for databehandlere, opptak av møter, retningslinjer for tilgangsstyring og logging planlagt ferdigstilt i løpet av 2025. Arbeidet med informasjonsverdier er igangsatt, og det jobbes parallelt siden mye henger sammen.

Prosjektet *Helhetlig styring av informasjonssikkerhet og personvern* opplyses å være godt kjent blant administrativ ledelse. Fylkeskommunedirektøren har delegert ansvar ned i organisasjonen for å få linjen i styringssystemet på plass i fagområdene. Når det gjelder personvern er kun det operative behandlingsansvaret delegert. Det har i prosjektet vært høy produktivitet, noe som ved implementering av rutiner og retningslinjer utløser behov for veiledning og oppfølging. Prosjektet har til nå håndtert denne oppgaven. Det må defineres i sluttrapporten hvordan oppgaven skal ivaretas når prosjektet avsluttes. Opprinnelig var det tenkt at sluttrapporten for prosjektet skulle synliggjøre behovet i organisasjonen for fagområdet, men det blir for sent, fordi implementering utløser umiddelbare behov. I oktober 2025 ble dette lagt til som et risikomoment i styringsdokumentet for prosjektet. Det meldes flere avvik, det skal utarbeides databehandleravtaler, gjennomføres personvernkonsekvenser og andre vurderinger, noe som medfører at det må være noen som veileder og bistår. Rutiner og veiledning distribueres via intranettet, men dette oppleves å ikke være tilstrekkelig. Mye er relativt nytt for mange, og det er nødvendig å ha noen som kan ivareta ansattes behov, herunder saksbehandleres og systemeieres behov. Stillingen som personvernombud var tidligere en 30 % stilling. Behovet for personvern er synliggjort gjennom prosjektet, og personvernombud er nå tilsatt i 100 % stilling.

4.1.9 Avvik og avviksoppfølging

Avvik og avviksoppfølging gir grunnlag for erfaring og læring, og fylkeskommunen bør ha etablert rutiner for å håndtere avvik og rette eventuelle feil. Avvik, eller brudd, knyttet til personopplysningssikkerhet skal meldes til Datatilsynet innen 72 timer, med mindre avviket sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.

Vi har fått opplyst at det er etablert egne kategorier i avvikssystemet, herunder på GDPR, informasjonssikkerhet, samt avvik etter sikkerhetsloven. Avvik registreres og følges opp. Videre meldes det nå flere avvik til Datatilsynet, noe fylkeskommunen mener synliggjør bedre bevissthet om avviksmeldinger i organisasjonen. Vi har fått opplyst at det lages helhetlige avviksrapporteringer.

Delprosjektet med internkontroll omfatter oppfølging av rapporterte avvik. Fylkeskommunen ønsker å lære av dette, og arbeidet med internkontroll og avviksbehandling skal tilpasses informasjonssikkerhet og personvernområdet. I dag følges samme rutiner som ellers i fylkeskommunen, men en ser økt behov for dette fagområdet, noe som medfører ekstra beskrivelser av prosedyrer og oppfølging. Avvik opplyses å rapporteres gjennom fylkeskommunens kvalitetssystem. Ansatte er blitt flinkere til å melde avvik, men oppfølgingen opplyses å være noe mangelfull.

I arbeidet med internkontroll og avviksarbeid, planlegges det for å gjøre flere tilpasninger til informasjonssikkerhet og personvern. Det planlegges for å bruke *Datakvalitet* for å undersøke hvor mange avvik som er meldt, og hvilke typer avvik som meldes. Dette for å kartlegge hvordan kulturen i organisasjonen er for å melde avvik.

På spørsmål fra revisor om hvilke typer avvik som avdekkes, opplyses det at en del gjelder personvern. Som eksempler nevnes, offentliggjøring av sensitive opplysninger og sensitive opplysninger sendt feil person. Det opplyses å ha vært noe sårbarhet i enkelte fagsystem. Flere av avvikene har gitt fylkeskommunen en indikasjon på hvordan dette skal håndteres. Som eksempel nevnes skoleskyss-saken, som omhandlet en svikt i fagsystemet for behandling av søknader om skoleskyss. Fra IT-avdelingen ble det først sjekket ut om fylkeskommunen var bruker av denne løsningen. Videre hva slags informasjon fylkeskommunens løsning behandler. Her var det ikke en helhetlig oversikt, men det ble etter hvert avklart at systemet inneholdt informasjon om elever som har søkt skoleskyss. KommuneCERT ble kontaktet for bistand for å håndtere sårbarheten. KommuneCERT konstaterte at personopplysninger ikke hadde tilfalt uvedkommende, og personopplysninger hadde ikke kommet på avveie. Leverandøren av systemet ble anmodet om å ivareta sikkerheten i systemet på en bedre måte. Dette eksempelet opplyses å kunne illustrere utfordringen ved at Troms fylkeskommune ikke har god nok kjennskap til leverandøren og de sikkerhetsløsningene leverandøren har i systemet for å ivareta informasjonssikkerheten.

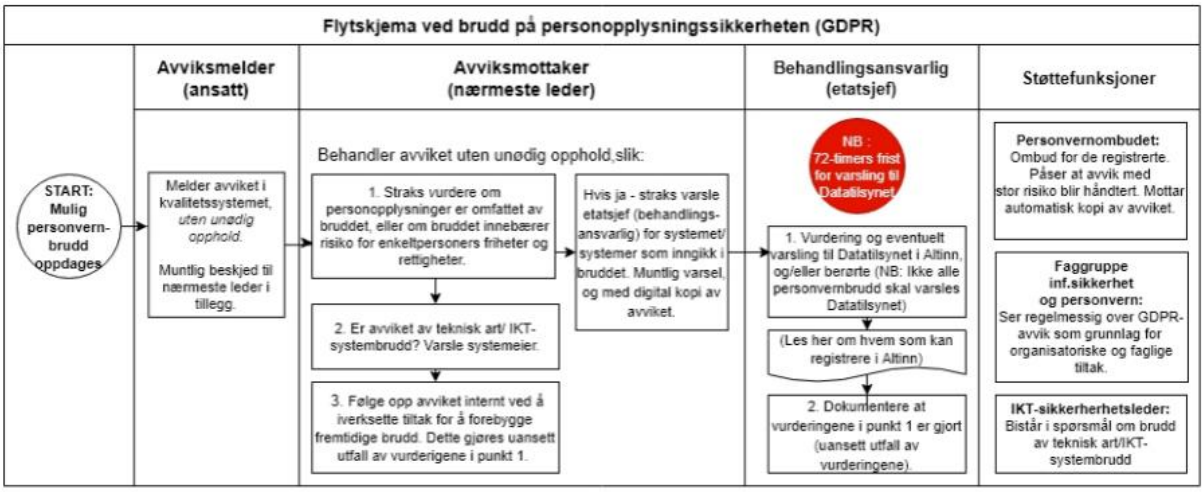
Vi får fortalt at fylkeskommunen i håndteringen av saken opplevde at det fungerte bra og at dette tyder på at strukturen som er bygget opp for å ivareta sikkerheten i systemet fra fylkeskommunen fungerer, blant annet på bakgrunn av at varslingssystemet virket. Relevante personer ble trukket inn, og det var klare roller og ansvarsfordeling i håndtering av denne saken, herunder kommunikasjon med Datatilsynet.

Videre er det meldt ett avvik på sikkerhetsloven. Dette avviket knyttet seg til at noen hadde kommet seg inn i et fylkeskommunalt bygg uten adgangskort. Det jobbes med å øke bevisstheten hos alle ansatte om at dette kan skje, og at alle bør være oppmerksomme på slike

hendelser. Vi får fortalt at det har vært en stor utvikling i organisasjonen når det gjelder bevisstheten omkring sikkerhetstiltak og hva som kan utgjøre en risiko. Ved opptelling av valget ble alle ansatte, som et sikkerhetstiltak, bedt om å gå med synlig identifikasjon, med tanke på at det ikke skulle være uvedkommende i bygget. Skilting gis som et annet eksempel på at det kan lede uvedkommende nært kritiske soner. Det må alltid gjøres en vurdering med tanke på sikkerheten, og adgangskontroll er et tiltak som gir personer begrenset tilgang til enkelte soner. I dag oppleves ikke uautorisert tilgang til fylkeskommunale bygg som et stort problem.

Vi får opplyst at det ikke er mange avvik som rapporteres når det gjelder IT-sikkerhet. Henvendelser til IT-avdelingen gjelder stort sett saker knyttet til driftsmessige forhold. Når det gjelder sårbarhetshendelsen (skoleskyss) før jul, ble det meldt avvik.

I dokumentet *Melding om avvik på informasjonssikkerhet og personvern* opplyses at et brudd på personopplysningssikkerheten (avvik) i personvernforordningen er definert som utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet. Videre at et sikkerhetsbrudd kan være både angrep utenfra, og brudd på sikkerhetsprinsippene som skjer internt i virksomheten, for eksempel på grunn av menneskelig svikt som feilsendt e-post. Melding om avvik skal meldes elektronisk i kvalitetssystemet *uten unødig opphold*, av den som oppdager avviket. Utklippet under er hentet fra dokumentet.



I dokumentet gis eksempler på situasjoner som ved informasjonsbehandling gjør det nødvendig å iverksette avviksbehandling:

- Ved utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering
- Når medarbeidere benytter informasjonssystemet uten autorisasjon
- Når medarbeidere benytter informasjonssystemet uten den opplæring som er forutsatt
- Ved feil utstyr eller program som kan ha innvirkning på informasjonssikkerheten eller driften av informasjonssystemet
- Ved behandling av personopplysninger i strid med lover, forskrifter eller interne bestemmelser

4.1.10 Evaluering

Troms fylkeskommune har – etter oppdelingen av fylkeskommunene – jobbet med forbedring av styringssystemet. Arbeidet pågår, og det foreligger derfor ikke evalueringer av et allerede

eksisterende og ferdig implementert styringssystem, herunder internkontroll knyttet til informasjonssikkerhet. Som nevnt planlegges det for at implementering av rutiner og prosedyrer i hele organisasjonen skal skje i 2026. Vi er opplyst om at noen av rutinene allerede er evaluert, fordi rutinene må stemme overens med naturlig autoritetsflyt i organisasjonen for at de skal kunne etterleves. Slike justeringer gjennomføres fortløpende. Først når rutinene er i bruk vil en kunne se om noe er uklart, eller vanskelig gjennomførbart. Det er tatt noen grep når det gjelder rapportering, og særlig kritisk er 72-timers fristen som Datatilsynet krever ved personvernbrudd. Ansatte ved avdeling INFODOK opplyses her å ha god kompetanse, og kan veilede ut i organisasjonen ved behov.

De tre første månedene av 2027 er planlagt brukt til evaluering av prosjektet *Helhetlig styring av informasjonssikkerhet og personvern.* Det skal utarbeides en sluttrapport hvor prosjektet og implementeringen av prosjektet skal evalueres. Resultatet av prosjektet skal fremgå, og det skal synliggjøres hvorvidt Troms fylkeskommune har oppnådd de gevinstene som ble satt som mål for prosjektet.

4.1.11 Effektuering av arbeidet med internkontroll

Revisor er gjennom intervjuer informert om at det er utarbeidet plan for gjennomføringen av internkontrollarbeidet. Det planlegges for å «rulle dette ut» i organisasjonen ved gjennomgang med ledelsen i hver enkelt etat. Det har vært diskutert om den samme gjennomgangen skal gjøres ved kontorstedene, tannklinikker v/overtannleger i regioner, videregående skoler etc., men dette er det ikke tatt stilling til ennå.

På spørsmål fra revisor om bruken av kvalitetssystemet i dag, fikk vi opplyst at det legges vekt på å få en god «onboarding-prosess». Det planlegges for at alle ansatte i fylkeskommunen må gjennomgå en video-opplæring i sikkerhet og beredskap. Hvordan dette skal gjennomføres er ikke avklart. KS har en kurs-plattform, *KS Kunnskap*, som sannsynligvis tas i bruk i onboarding-prosessen for å utarbeide kurs for ansatte. Kursene, som skal være obligatoriske for alle ansatte, vil vise systematikken i kvalitetssystemet, og hvem de kan spørre dersom det er behov for mer informasjon. Det er p.t. ikke avklart hvordan den tekniske løsningen for dokumentasjon av gjennomførte kurs skal gjøres, men den enkelte ansatte må kunne dokumentere å ha gjort seg kjent med og forstår IT-regelverket.

4.2 Personvern og behandling av personopplysninger

Personvernforordningen stiller krav til tilstrekkelig informasjonssikkerhet ved innføring av egnede og tekniske og organisatoriske tiltak. Behandling av personopplysninger skal skje på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltmennesket. Fylkeskommunedirektøren må som behandlingsansvarlig sørge for å etablere nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

Den enkelte enhet har sin kompetansedel på sitt område innenfor informasjonssikkerhet og personvern. Revisor har fått opplyst at prosesskartlegging på sikt vil være en del av risikovurderingen knyttet til personvern, dokumentasjon og arkiv, forvaltningskrav etc. Det gjennomføres ikke systematisk opplæring, men for den tekniske delen kjøres kampanjer. Tekniske og organisatoriske tiltak redegjøres nærmere for i kapittel 5.

4.2.1 Protokoll over behandlingsaktiviteter

Revisor har fått opplyst at Troms fylkeskommune i dag har en type *systembasert* behandlingsprotokoll, som nok ikke tilfredsstiller kravene i GDPR. Den tidligere

systemoversikten opplyses å være mangelfull, herunder var det ikke for alle systemer definert formål og hvilke typer personopplysninger som behandles.

Vi får fortalt at det er gjennomført workshop med etatene, hvor KPMG er innleid for å bistå Troms fylkeskommune i arbeidet med å snu behandlingsoversikten til en *funksjonsbasert* behandlingsoversikt. Fylkeskommunen opplyser å ha funksjonsoversikter, og god oversikt gjennom prosessene med å utarbeide funksjonsoversiktene, samt bevarings- og kassasjonsplan. Arbeidet planlegges ferdigstilt i februar 2026, slik at fylkeskommunen da får på plass en behandlingsprotokoll som tilfredsstiller krav i GDPR.

4.2.2 Behandling og lagring av personopplysninger

Revisor har fått opplyst at fylkeskommunen per desember 2025 ikke har full oversikt over hvor det er gjennomført personvernkonsekvensvurdering (DPIA). Dette vil bli en del av oppfølgingen av protokoll når behandlingene systematiseres. Vi har fått forklart at det er vanskelig å gjennomføre DPIA ut fra en systembasert protokoll. Når funksjonsbasert protokoll kommer på plass vil det bli lettere å se hvor det er behov for DPIA, og hvor det er gjennomført.

Revisor er fortalt at dette var et område hvor fylkeskommunen raskt fikk ut veiledere på intranett. Blant annet som følge av tidligere nevnte sak knyttet til kameraovervåking. Videre er det gjort en del på områder hvor det er avdekket mangler, og hvor saker er meldt inn til Datatilsynet. Revisor har i intervju fått bekrefter at det sannsynligvis er etterslep med gjennomføringen av DPIA på flere områder i Troms fylkeskommune.

Prosedyre for vurdering av personvernkonsekvenser (DPIA) beskriver hvordan Troms fylkeskommunens vurdering av personvernkonsekvenser skal gjennomføres. Vurdering gjennomføres når en behandling vurderes å resultere i høy risiko for de registrertes rettigheter og friheter. Vurderingen av personvernkonsekvenser skal gjøres før behandlingen av personopplysninger starter opp. Det kan også være endringer i pågående behandlingsaktiviteter som krever ny eller oppdatert vurdering. Basert på vurderingene og anbefalingene, samt personvernombudets og de registrertes uttalelse, skal den behandlingsansvarlige foreta en beslutning om videre behandling.

Alle vurderinger av personvernkonsekvenser skal dokumenteres og lagres i sak- og arkivsystemet. Informasjon om gjennomført DPIA skal inkluderes i behandlingsprotokollen. Illustrasjonen under er hentet fra nevnte dokument, *Prosedyre for vurdering av personvernkonsekvenser*.

Maler for *Forhåndsvurdering – innledende DPIA* og *Vurdering av personvernkonsekvenser (DPIA)*, samt *Forklaring til malene for DPIA* er en del av prosedyredokumentet.

Prosedyren opplyses å gjelde for all vurdering av personvernkonsekvenser (DPIA). Prosedyren opplyses å ikke gjelde for risikostyring av informasjonssikkerhet og personopplysningssikkerhet.

Rutine for behandling og lagring av personopplysninger gjelder for alle ansatte i Troms fylkeskommune som skal behandle eller behandler personopplysninger. Rutinen skal gjennomføres hver gang en ny personopplysning behandles, og rutinen må jevnlig ses hen til for å sørge for at behandlingen ivaretar lovkravene. Med behandling menes alle handlinger som foretas med personopplysninger, både automatisert og ikke automatisert, herunder innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. Det henstilles i rutinen til at den som skal behandle og lagre personopplysninger må sette seg inn i kravene og prinsippene i personvernforordningen artikkel 5.

Av utarbeidet *Veileder for bruk av KI – generativ kunstig* intelligens, fremgår at bruk av generativ KI fungerer som en chatbot[14], og kan være et nyttig verktøy som gir god hjelp i oppgaveløsning, eksempelvis lage oppsummerende tekst, utkast til dokumenter, sammenligninger og analyser. Troms fylkeskommune bruker *Microsoft Copilot*, som av Troms fylkeskommune regnes som en mer sikker versjon enn andre åpne verktøy.

Av veilederen går fram tre regler for bruk av generativ kunstig intelligens:

1. Bruk Microsoft Copilot
2. Still flere spørsmål og vær nøyaktig
3. Sjekk kilder og kvalitet - vær kritisk til svarene du får

Under punkt 1. Bruk Microsoft Copilot, står det: *"Legg aldri inn personopplysninger om deg selv eller andre, eller andre opplysninger som ikke kan og skal distribueres på internett!».*

4.2.3 Opplæring

Troms fylkeskommune har utarbeidet rutiner og prosedyrer som ligger til grunn for at ansatte i arbeidet skal kunne ivareta informasjonssikkerhet og personvern.

Opplæring innenfor IT-sikkerhet gis til ansatte gjennom tilgjengelige kanaler, og årlig sikkerhetsmåned arrangeres i oktober. Sikkerhetsmåneden er et fast opplæringstiltak, hvor det presenteres ulike tema innenfor sikkerhet for ansatte i fylkeskommunen. I tillegg utarbeider IT-avdelingen Nanokurs[15] med tema innenfor IT-sikkerhet, som sendes alle ansatte på epost. Det arrangeres seminarer og presentasjoner, samt at intranettet brukes for å nå ut til ansatte med informasjon.

I årsberetning for 2024 nevnes at IT-avdelingen publiserer instrukser og veiledning ved behov, og gir sikkerhetsopplæring gjennom Nanolæringskurs. Videre står det at «*årets kurs IT-Sikkerhet 2024, hadde en deltakelse på 26 % som er for lavt*».

Noen av fylkeskommunens enheter har ikke så stor portefølje av personopplysninger, og har av den grunn ikke blitt prioritert når det gjelder kompetanseheving innen personvern og informasjonssikkerhet. Etatene har tidligere hatt ansvaret, og små enheter har hatt noe ulikt

[14] Samtalerobot
[15] Korte og intensive kurs

behov for å inneha denne kompetansen. Som eksempel får vi nevnt fagskolen som har hatt god kontroll som følge av at de er avhengige av godkjenning, og jobber systematisk etter ISO-standard. Andre mindre enheter er i større grad er avhengig av hjelp for å opprettholde tilfredsstillende nivå innen personvern og informasjonssikkerhet. INFODOK og IT-avdelingen bidrar ved behov. Det gis overfor revisor uttrykk for at når det gjelder det tekniske med systemer og systemforvaltning har det vært greit, størst mangel har vært knyttet til det organisatoriske.
I 2025 var digital sikkerhet tema for sikkerhetsmåneden, og det ble publisert fire opplæringsvideoer som omhandlet:

- Den globale situasjonen
- Ansattes rolle i sikkerhetsarbeid
- IT-sikkerhet, og informasjon om internkontrollprosjektet
- Egen beredskap

På spørsmål fra revisor om deltakelse i 2025, fikk vi opplyst at det ble registrert ca. 100 deltakere per presentasjon/sekvens, noe som av fylkeskommunen anses som lavt med tanke på at fylkeskommunen har rundt 2 500 ansatte. Videre at dette viser noe av den kulturelle utfordringen når det gjelder IT-sikkerhet; det er vanskelig å få god deltakelse blant alle ansatte. Opptak av presentasjoner fra sikkerhetsmåneden er gjort tilgjengelig for alle ansatte, men det er ikke statistikk på hvor mange som ser opptakene. Når det gjelder Nanokurs har fylkeskommunen sett litt på den etatsvise deltakelsen, men det er vanskelig å se noen trender. Gjennomføringsgraden opplyses å være størst i stab og støtte og i næringsetaten, noe som sannsynligvis skyldes fysisk nærhet for ansatte lokalisert på fylkesbygget. Tannhelse og kompetanse har lav deltakelse, noe som fra fylkeskommunen forklares med at de er opptatt med tjenesteproduksjon.

Det er gjort tiltak for å nå bedre ut til ansatte, blant annet er det opprettet distribusjonsgrupper som når alle ansatte på epost. Tidligere ble invitasjoner sendt ut via intranett og Teams-kanaler, men det nevnes at det blant ansatte nok ikke i stor grad er kultur for å lete etter informasjon på intranettet.

Revisor har fått opplyst at det er behov for å innhente kompetanse når det gjelder systematisering av opplæring og opplæringsmateriell basert på en kompetanseplan som prosjektet skal utarbeide. Mange produserte retningslinjer og rutiner i prosjektet *Helhetlig styring av informasjonssikkerhet og personvern*, opplyses å gi utfordringer med hensyn til god implementering i organisasjonen. Det er besluttet at det skal gjennomføres obligatorisk opplæring som må systematiseres og tilrettelegges. Det har hittil blitt holdt noen fysiske og digitale presentasjoner knyttet til personvern og informasjonssikkerhet, i tilknytning til etableringen av et helhetlig styringssystem. Imidlertid har det ikke vært tilstrekkelige ressurser til å gjennomføre opplæring, webinarer eller informasjonskampanjer som et gjennomgående arbeid.

4.3 Revisors vurderinger

Styringssystem og internkontroll
Gjennom prosjektet *Helhetlig styring av informasjonssikkerhet og personvern* blir styringssystemet gjennomgått. Gjennomgangen av styringssystemet innebærer en oppdatering og utarbeidelse av styringsdokumenter som av fylkeskommunen anses som nødvendig for å ivareta internkontrollen innen informasjonssikkerhet og personvern. Vi har ikke ved vår gjennomgang av utarbeidede styringsdokumenter funnet at innholdet bryter med kravene i lovverk eller anerkjente standarder.

Troms fylkeskommune har – etter oppdelingen av fylkeskommunene – jobbet med forbedring av styringssystemet. Det er ikke eksplisitte krav til styringssystemets innhold, men det tilligger fylkeskommunedirektøren å vurdere hva som skal inngå. Internkontrollen som omhandler informasjonssikkerhet, bør være en integrert del av fylkeskommunens helhetlige styringssystem.

eForvaltningsforskriften § 15 angir at forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten. Mål og strategier skal danne grunnlaget for fylkeskommunens internkontroll på informasjonssikkerhetsområdet. Videre legger forskriften føringer om at internkontrollen på området skal baseres på anerkjente standarder for styringssystem for informasjonssikkerhet. Digdir anbefaler at IEC/ISO 27001, som er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et styringssystem, legges til grunn for arbeidet.

Revisor vurderer at Troms fylkeskommune v/fylkeskommunedirektør for arbeidet med personvern og informasjonssikkerhet har utarbeidet en beskrivelse av virksomhetens hovedoppgaver, mål og organisering. Fylkeskommunen har utarbeidet skriftlige rutiner hvor det fremkommer hvem i organisasjonen som har hvilket ansvar og oppgaver knyttet til informasjonssikkerhet og personvern. Når det gjelder mål, har vi i vurderingen også vektlagt at fylkeskommunen har sikkerhetsmål, som er en forpliktelse etter eForvaltningsforskriften § 15.

Sikkerhetsmål omfatter ledelsens beslutninger om hva IKT skal brukes til i virksomheten. Ifølge eForvaltningsforskriften § 15 skal det også foreligge sikkerhetsstrategi. Sikkerhetsmålene skal være retningsgivende for strategien, og bør i størst mulig grad være målbare. Retningen for arbeidet med strategi for informasjonssikkerhet er angitt i *Policy for informasjonssikkerhet og personvern*, men slik vi forstår det er det ikke utarbeidet et eget strategidokument.

Troms fylkeskommunes styringssystem for informasjonssikkerhet og personvern bygger på *ISO/IEC 27001 – Ledelsessystem for informasjonssikkerhet*. Standarden stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av styringssystemet for informasjonssikkerhet. Fylkeskommunen opplyser å bruke anbefalingene i standarden i den utstrekning som vurderes som relevant. Videre legges NSM sine grunnprinsipper til grunn for tekniske og organisatoriske tiltak for å ivareta sikkerheten.

Vår vurdering er at Troms fylkeskommune i all hovedsak har sørget for å dokumentere internkontrollen i den formen og omfanget som av fylkeskommunedirektøren vurderes som nødvendig. Flere rutiner og retningslinjer for arbeidet med informasjonssikkerhet og personvern, herunder IT-teknisk sikkerhet, er gjennomført, og mye av innholdet i kvalitetssystemet opplyses å være på plass. Revisor er gjort kjent med at det fortsatt gjenstår å utarbeide noen styringsdokumenter, og at disse legges inn i kvalitetssystemet så snart de er utarbeidet og godkjent. På bakgrunn av gjennomgått dokumentasjon og informasjon gitt revisor, sannsynliggjøres det at det foretas en gjennomgang og kontinuerlig oppdatering av styringssystemets innhold, og også en vurdering av omfanget av nødvendige rutiner og prosedyrer slik regelverket krever.

Innretningen og omfanget av gjennomgåtte styringsdokumenter i form av policy og rutiner og retningslinjer, synes å være egnet til å sikre etterlevelse av regelverket for IT-sikkerhet, informasjonssikkerhet og personvern. Innretningen for internkontrollen må tilpasses

organisasjonen og baseres på risikoforholdene. Risikovurderinger er gjennomført, både gjennom overordnet ROS-analyse, og virksomhets-ROS ved IT-avdelingen. Det planlegges for at virksomhets-ROS skal gjennomføres ved alle enheter i 2026. Virksomhetsledere er ansvarlig for å gjennomføringen, og for å utarbeide nødvendige rutiner og prosedyrer. Undersøkelsen viser at Troms fylkeskommune har gjort en intern vurdering av sikkerhetsnivået, og også har innhentet ekstern bistand i arbeidet. Vi har i undersøkelsen fått bekreftet at det er avdekket noen svakheter, både organisatoriske og tekniske, men disse gjengis ikke i vår rapport av sikkerhetshensyn.

Med bakgrunn i funn i undersøkelsen anser revisor at øverste administrative ledelse synes å være godt orientert om arbeidet med styringssystemet og internkontrollen, men at øvrige ansatte i varierende grad er gjort kjent med arbeidet. Slik vi ser det vil implementeringen av rutiner og retningslinjer i organisasjonen nødvendigvis involvere alle ansatte.

Vår vurdering er at kommunedirektøren i stor grad oppfyller kriteriet om å avdekke og følge opp avvik og risiko for avvik. Funn i undersøkelsen synliggjør noe svakhet knyttet til arbeidet med oppfølging av meldte avvik. Vi har fått opplyst at avvik som gjelder IT-sikkerhet, informasjonssikkerhet og personvern registreres i kvalitetssystemet, og følges opp etter samme rutiner som ellers i Troms fylkeskommune. Det er etablert egne kategorier i avvikssystemet, herunder på GDPR, informasjonssikkerhet og avvik etter sikkerhetsloven. Igangsatt delprosjekt skal ivareta behovet for mer tilpasset avviksbehandling på informasjonssikkerhet og personvernområdet.

Troms fylkeskommune har gjennomført en øvelse knyttet til IT-sikkerhetsbrudd. Øvelser er viktige for å kontrollere at internkontrollen fungerer som planlagt. Hendelsen knyttet til svikt i fagsystem, viser at Troms fylkeskommune har prosedyrer som iverksettes ved hendelser. For fylkeskommunen synliggjorde hendelsen utfordringen ved å ikke ha god nok kjennskap til leverandøren og de sikkerhetsløsninger leverandøren har for å ivareta informasjonssikkerheten.

Revisor vurderer at fylkeskommunedirektøren for arbeidet med personvern og informasjonssikkerhet synes å ha vurdert omfanget av nødvendige rutiner og prosedyrer, men arbeidet med å få alle dokumenter utarbeidet og implementert er ikke ferdigstilt. Vår vurdering er at fylkeskommunedirektøren evaluerer og vurderer behovet for å forbedre skriftlige prosedyrer og andre tiltak for internkontroll. Vi begrunner dette med at vi har fått opplyst at skriftlige rutiner og prosedyrer tilpasses og endres dersom det ved implementering avdekkes behov for revidering. Vi er også forelagt skriftlig dokumentasjon på dette i form av revidert dokument *Roller og ansvar - Informasjonssikkerhet og personvern*. Vi vil likevel påpeke at mange av de utarbeidede rutiner og prosedyrer ikke er implementert i organisasjonen, slik at det kan knyttes svakhet til effektiviteten av disse. Implementering av rutiner og retningslinjer er planlagt gjennomført i 2026.

Personvern og behandling av personopplysninger
Revisor finner at fylkeskommunen har utarbeidet rutiner for behandling og lagring av personopplysninger. Videre er det utarbeidet prosedyre for vurdering av personvernkonsekvenser.

Personvernforordningen krever at behandlingsansvarlig fører protokoll over behandlingsaktiviteter. Revisor vurder at fylkeskommunedirektøren som behandlingsansvarlig ikke oppfyller kravet om at det føres protokoll over behandlingsaktiviteter. Vi har merket oss

at det i Troms fylkeskommune pågår et arbeid med å få på plass en behandlingsprotokoll som tilfredsstiller krav i GDPR.

Vår vurdering er at fylkeskommunedirektøren som behandlingsansvarlig har planlagt for, og gjennom rutiner og retningslinjer som skal ivareta behandlingen av personopplysninger har iverksatt tiltak for å ivareta kravet om at all behandling av personopplysninger sikres. Gjennom prosjektet *Helhetlig styring av informasjonssikkerhet og personvern* pågår et omfattende arbeid, hvor også tiltak for sikring av behandling av personopplysninger inngår. Implementering av rutiner kan, slik vi ser det, bidra til å gjøre disse kjent blant ansatte, og gi et grunnlag for gode arbeidsrutiner.

Opplæring
Sikkerhetsbevissthet blant ansatte er et viktig sikkerhetstiltak. Undersøkelsen viser at det utformes kurs for ansatte med sikte på å forbedre sikkerhetskulturen i organisasjonen. Målingene som gjøres i etterkant av gjennomføring og publisering av kurs viser lave tall for deltakelse. Lav deltakelse kan, slik revisor ser det, skyldes flere forhold; lavt engasjement, utilstrekkelig informasjon og tilrettelegging, eller at kursene ikke oppleves som relevante. Lav gjennomføringsgrad kan innebære risiko for manglende etterlevelse av fylkeskommunens sikkerhetskrav, noe som på sikt kan medføre økt risiko for alvorlige konsekvenser som følge av dataangrep.

Vi er gjennom undersøkelsen oppmerksomme på at Troms fylkeskommune er i en prosess med å ferdigstille styringssystemet for informasjonssikkerhet og personvern. Selv om kvalitetshåndboken er tilgjengeliggjort for ansatte via intranett, viser funn i undersøkelsen at ikke alle ansatte kjent med innholdet. Revisor ser positivt på at det planlegges for en systematisering av opplæring, og utarbeidelse av en kompetanseplan.

4.4 Revisors konklusjon

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

Revisor konkluderer med at Troms fylkeskommune ikke fullt ut har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket.

Det pågår arbeid med et helhetlig styringssystem for informasjonssikkerhet og personvern. Vi baserer vår konklusjon på at styringssystemet ikke er ferdig utviklet. Troms fylkeskommune har utarbeidet overordnede styringsdokumenter. Utarbeidede rutiner og prosedyrer som skal ivareta internkontrollen er ikke implementert i organisasjonen, og effektiviteten av disse kan følgelig ikke vurderes. Videre oppfyller ikke fylkeskommunedirektøren som behandlingsansvarlig kravet om at det føres protokoll over behandlingsaktiviteter. Funn i undersøkelsen viser at det sannsynligvis er etterslep med gjennomføring av personvernkonsekvensvurdering på flere områder i Troms fylkeskommune.

Revisor er informert om at det mens forvaltningsrevisjonen gjennomføres vil rutiner og prosedyrer implementeres i organisasjonen, og det er igangsatt arbeid med å få på plass en behandlingsprotokoll som ivaretar kravene i GDPR.

5 TILTAK FOR Å IVARETA INFORMASJONSSIKKERHET

Har Troms fylkeskommune truffet tilfredsstillende tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet?

Revisjonskriterier

Troms fylkeskommune bør etablere sikringstiltak, herunder tekniske og organisatoriske tiltak ved å:

- Kartlegge alle enheter og programvare som er i bruk
- Gjennomføre risiko- og sårbarhetsanalyse av kritiske IKT-systemer, og sørge for at disse oppdateres ved vesentlige endringer
- Ha kontroll på alle identiteter og tilganger
- Gjennomføre jevnlig sårbarhetskartlegging, inntrengingstester, og vurdere nivå av sikkerhetsovervåking
- ha prosesser som sikrer at avvik som avdekkes gjennom iverksatte tiltak håndteres
- ha rutiner og prosesser som sikrer evaluering av effektiviteten til styringssystemet for informasjonssikkerhet

I Troms fylkeskommunes årsmelding 2024 står det under virksomhet IT, at året har vært hektisk for IT-avdelingen med oppdeling av Troms og Finnmark som det største enkeltprosjektet. Det er håndtert mange nye løsninger og tilpasninger. Utfasing av gamle systemer har vært en viktig oppgave, både på grunn av økonomi, men også for å øke IKT-sikkerheten i fylkeskommunens systemer. Brannmurer er etablert på flere lokasjoner, med økt sikkerhet i organisasjonen. Nettverkssystemer er oppgradert, og det er etablert trådløse nettverk som foretrukket løsning for nettverkstrafikk internt i Troms fylkeskommune.

Revisor har fått opplyst at da IT-sikkerhetsleder begynte i stillingen for halvannet år siden, manglet det litt retning for arbeidet med IT-sikkerhet. Dette er det jobbet med, ikke bare for å ivareta IT-sikkerheten sentralt i administrasjonen, men i hele organisasjonen. Utfordringer i etterkant av endret styringsmodell, var noe av bakgrunnen for arbeidet med å sørge for en tydeliggjøring av ansvarslinjene, slik at beslutninger kan tas på riktig nivå.

Sikkerhetsmål for informasjonssikkerhet er standardisert, herunder kravene til konfidensialitet, integritet, tilgjengelighet og robusthet. I tillegg skal NSM sine grunnprinsipper og anbefalinger følges. Alt skal ikke etterleves, men det tas utgangspunkt i det som vurderes som nødvendig og relevant for Troms fylkeskommune. Vurderingene, som opplyses å være skriftliggjort, er gjort med utgangspunkt i NSMs grunnprinsipper. NSM angir at organisasjonen selv må gjøre en vurdering av hva som er relevant, og fylkeskommunen gjør kost-nytte vurderinger. Det er gjennomført en kvalitativ vurdering av hvilke krav som er relevante for fylkeskommunen, med hensyn til iverksetting av tiltak for å sikre etterlevelse.

I Troms fylkeskommunes årsmelding for 2024 står under IT (måloppnåelse) at god kvalitet i brukertjenesten er viktig for at organisasjonen skal få løst sine oppgaver. Videre at det har kommet inn 7564 saker til brukertjenesten, og av disse er 7214 løst før årsskiftet. Førstelinje løser mange av disse sakene, noe som vil si at *Brukertjeneste* i snitt håndterer 30 saker pr. dag, og mange av sakene er til dels svært komplekse. Mål/fokusområder og status framgår også av årsmeldingen, herunder mål/fokusområde *Økt søkelys på digitale sikkerhetstiltak.* Status her er

at mange tiltak er gjennomført, blant annet tilsatt IT-sikkerhetsleder, og at det er etablert 24/7/365 overvåking av deler av IT-skymiljø, noe som skal utvides i 2026.

5.1.1 Kartlegging av enheter og programvare

Vi har fått fortalt at etater og avdelinger selv har anskaffet en del IT-tjenester (software og service), hvor applikasjoner er installert på PC´er. Videre at det i per i dag ikke finnes felles oversikt over alle IT-systemene i Troms fylkeskommune, men det jobbes med å etablere dette. Dette gjør at IT-avdelingen, som har ansvaret for datasikkerheten, ikke har hatt god nok oversikt og kontroll over enheter og programvare for de løsningene som forvaltes av andre etater og avdelinger. Risikoen, som IT-sikkerhetsleder opplyser å ha påpekt overfor porteføljestyret, knytter seg til leverandørene, ved at en ikke klarer å underlegge disse tjenestene den strukturen som bygges opp i styringssystemet for å ivareta en forsvarlig IT-sikkerhet i systemene. Manglende oversikt opplyses også å gi utfordringer med tanke på å gjennomføre kontroller. Oppdateringer av versjoner i systemene blir gjort av den som anskaffer systemet. Utfordringen er at IT-forvaltningen er fragmentert. Det jobbes med å få oversikten i *Samsvar*, men den helhetlige oversikten er fortsatt mangelfull.

Vi får fortalt at det er etablert rutine for gjennomgang av teknisk dokumentasjon ved nye versjoner. IT-avdelingen har eget dokumentasjonssystem hvor IT-løsninger dokumenteres, og et sakssystem, hvor endringer legges inn, og vurderes enten av faggruppen eller ledergruppen.

5.1.2 Oversikt over IT-systemer og IT-tjenester

Utfordringene med helhetlig styring innenfor digital sikkerhet er at det er flere ulike IT-miljøer i organisasjonen, noe revisor har fått opplyst representerer noen styringsmessige utfordringer. Dette fordi IT-avdelingen som sitter med ansvaret ikke har helhetlig oversikt over alle IT-systemer som er i bruk i organisasjonen. Troms fylkeskommune bruker *Samsvar*[16]*,* og er i gang med å utarbeide en helhetlig oversikt over IT-systemer og IT-tjenester, samt hvem som har ansvar for disse. Alle som behandler personopplysninger skal utarbeide en oversikt over hvilke systemer de bruker som behandler personopplysninger, og hva som gjøres for å ivareta integriteten i systemene.

Fylkeskommunen bruker sky-tjenester på administrative applikasjoner, Microsoft 365. Dette er stabile tjenester og stabile plattformer. Dersom disse tjenestene er utilgjengelige skyldes det gjerne større nasjonale hendelser, fiberbrudd og lignende som fylkeskommunen ikke rår over.

5.1.3 Tilgangsstyring

Når det gjelder retningslinjer for tilgangsstyring, har vi fra INFODOK fått opplyst at noe av den sentrale rollefordelingen tilligger IT-avdelingen, men at flere ansatte ute i organisasjonen tildeler roller i ulike fagsystemer. Det legges føringer for at den enkelte systemeier skal ha rutiner for rolletildeling i sitt system; herunder et forvaltningssystem hvor også roller er beskrevet, og prosedyrer skal være dokumentert. Når retningslinjer for tilgangsstyring implementeres i 2026 vil det bli behov for å tilrettelegge for at informasjon når ut til ansatte.

5.1.4 Tekniske og organisatoriske tiltak

For tekniske og organisatoriske tiltak for digital sikkerhet legger fylkeskommunen NSM sine grunnprinsipper til grunn. Grunnprinsippene som følges er en blanding av tekniske og organisatoriske tiltak, og rangeres etter prioritet; 1, 2 og 3. [redacted]

[16] Skybasert kvalitets- og internkontrollsystem

[redacted] Det rapporteres ikke på øvrige tiltak. I arbeidet hentes det inspirasjon fra andre rammeverk, eksempelvis ISO.

[redacted]

Når det gjelder organisatoriske tiltak for ivaretakelse av informasjonssikkerheten får vi fortalt at inntrykket er at de enkelte etatene har hatt god kontroll på enkelte prosesser og prosedyrer på egne områder gjennom sine informasjonssystemer. Dette gjelder særlig samferdsel, tannhelse og skole og opplæring. Når det gjelder IT-sikkerhet, er det ikke planlagt for å tilføre flere ressurser i organisasjonen, men legge vekt på å sikre at alle er underlagt samme styringssystem.

Ved utforming av tiltak forsøker IT-sikkerhetsleder å se helheten for at tiltakene skal få størst mulig effekt, både når det gjelder tekniske og organisatoriske tiltak. Videre at det menneskelige aspektet må vektlegges. Alle ansatte må få tilstrekkelig informasjon og opplæring for å være godt rustet til å håndtere trusselbildet fylkeskommunen står ovenfor, noe som ble presentert i en av sekvensene i sikkerhetsmåneden 2025. Hvordan organisasjonen er bygd opp og styres påvirker sikkerhetsbildet. Det jobbes i 2026 med implementering av faste rapporteringer, og det å få faggruppene til å fungere godt.

Revisor er kjent med at det er utarbeidet en tiltaksplan for IT-sikkerhet. IT-avdelingen følger opp tiltaksplanen gjennom ukentlige ledermøter, hvor IT-sikkerhetsleder deltar. Utfordringen angis å være at de samme ressursene som jobber med implementering av mer langsiktige IT-sikkerhetstiltak, er de samme ressursene som til daglig har ansvar for IT- systemene. Noen tiltak ligger utenfor IT-avdelingens myndighetsområde. Opprettholdelse av daglig drift må prioriteres, og det tar derfor tid å nå målene om å iverksette planlagte sikkerhetstiltak. Manglende implementering medfører risiko. Basert på dagens trusselbilde ser det ikke ut til at risikoen med utsatt implementering blir mindre, men tvert imot øker. IT-avdelingens kapasitet, kompetanse og gjennomføringsevne er avgjørende for å ivareta den digitale sikkerheten. Porteføljestyret er av IT-sikkerhetsleder orientert om at implementering av sikkerhetstiltak tar tid.

Dokumentet *IKT-reglement for bruk av IKT-ressurser* beskriver retningslinjer for bruk av IT-ressurser i Troms fylkeskommune. Formålet med reglementet er å sikre at IT-ressursene brukes på en sikker, effektiv og ansvarlig måte. I dokumentet angis at alle brukere må lese og godkjenne reglementet før de får tilgang til organisasjonens IT-ressurser. Reglementet er opplyst å gjelde alle ansatte, konsulenter, elever og andre som har tilgang til Troms fylkeskommunes IT-ressurser. IT-ressurser omfatter blant annet datamaskiner, nettverk, programvare og annen IT-infrastruktur. Revisor har fått opplyst at IT-avdelingen har faste møter med etatene for å koordinere, samt sikre effektiv drift.

5.1.5 Identiteter og tilganger

Det meste av prosessen for tilgangsstyring er automatisert. [redacted]

[redacted]

[redacted]

Gjennomgang av dokumentet *IKT-reglement for bruk av IKT-ressurser* er, sammen med signering av taushetserklæring, oppgitt å være en del av ansettelsesprosessen i Troms fylkeskommune. Reglementet beskriver retningslinjene for bruk av IT-ressurser i fylkeskommunen, og formålet er å sikre at IT-ressursene brukes på en sikker, effektiv og ansvarlig måte.

5.1.6 Sårbarhetskartlegging, inntrengingstester og sikkerhetsovervåking

Revisor er gjort kjent med at det gjennomføres testing, [redacted] Hurtigtestene er automatiske inntrengingstester som går gjennom systemer og leter etter sårbarheter og svakheter, eksempelvis sensitive personopplysninger. Det er avdekket tilfeller hvor personopplysninger som skulle ha vært slettet, ikke har vært slettet. Ansvarlige for disse opplysningene kontaktes og sletting av personopplysninger ivaretas. Det gjennomføres også tester med tanke på om personopplysninger kan være på avveie. Hittil er det ikke avdekket noen slike tilfeller, men det har vært tilfeller hvor det er avdekket at personopplysninger har vært for dårlig sikret. [redacted]
Etter dette lå det igjen informasjon som ikke skulle være der, noe som innebar at opplysninger ikke var godt nok slettet.

KommuneCERT kan bistå med å forebygge, oppdage og håndtere cyberhendelser.[18] [redacted] I 2025 har fylkeskommunen to ganger forespurt kommuneCERT om å gjennomføre inntrengingstester, men kommuneCERT har ikke hatt kapasitet til å gjennomføre testene.

Troms fylkeskommune anskaffet våren 2025 en leverandør for å gjennomføre sikkerhetsovervåking, herunder overvåking av enheter, systemer, nettverk og innhente logger. Leverandøren det er inngått avtale med er godkjent av nasjonale sikkerhetsmyndigheter. Informasjon som hentes ut går inn i en sentral pool, og leverandøren gjennomfører analyser og gir fylkeskommunen tilbakemeldinger. [redacted] Jo tidligere hendelser oppdages, dess mindre blir konsekvensen. Så langt har fylkeskommunen klart å stoppe angrepene. Men trenden er negativ, ved at det er en økning i antall hendelser. Angrep i det digitale rom er normalt, og ikke spesielt for Troms fylkeskommune. Det er ikke mulig å motvirke angrep helt. Derfor er det viktig å kunne oppdage og respondere raskt på sikkerhetshendelser. Revisor har

[17] [redacted]

[18] Om Helse- og KommuneCERT - Norsk helsenett

fått beskrivelse av beredskapen ved IT-avdelingen knyttet til tilgjengelighet dersom hendelser skjer utenfor arbeidstid.

Vi er fortalt at IT-hendelser isolert sett kan indikere at IT-sikkerheten har sviktet, og at uvedkommende har fått tilgang til informasjon eller systemer de ikke skal ha tilgang til. Alvorlighetsgraden av et IT-sikkerhetsbrudd vil imidlertid variere, blant annet avhengig av hvor godt organisasjonen arbeider med informasjonssikkerhet.

[redacted]

IT-avdelingen gjennomfører intern testing for å verifisere og/eller avkrefte tankene fylkeskommunen selv har om eget sikkerhetsnivå. Det er innført målinger på forskjellige styringsparametere (KPI), hvor det tas utgangspunkt i eksisterende data. Dette gjør det mulig å se trender, utviklingen og sårbarheter. Som eksempel nevnes passord på avveie og sikkerhetshendelser. Effekten av sikkerhetsarbeidet følges opp, og også om arbeidet som utføres har den ønskede effekten. Sikkerhetsarbeidet påvirkes av endringen i trusselbildet.

5.1.7 Evaluering og rapportering

Resultatet av intern testing og målinger rapporteres i IT-ledergruppen. Ut over dette rapporteres det til porteføljestyret ved behov, men minst en til to ganger i året.

5.2 Revisors vurderinger

Revisor vurderer at Troms fylkeskommune har etablert sikringstiltak, herunder tekniske og organisatoriske tiltak, men at det knytter seg noe svakhet til noen av sikringstiltakene.

Revisor vurderer revisjonskriteriet om å kartlegge alle enheter og programvare som er i bruk som til dels oppfylt. Undersøkelsen viser at det ikke per i dag er en felles oversikt over alle IT-systemer som er i bruk i organisasjonen. Vi ser her at det kan hefte noe risiko ved at IT-avdelingen, som har ansvaret for IT-sikkerheten, ikke har en felles oversikt over alle systemer som benyttes i Troms fylkeskommune.

Revisor vurderer revisjonskriteriet om å gjennomføre ROS-analyse av kritiske IKT-systemer, og sørge for at disse oppdateres ved vesentlige endringer som ikke fullt ut oppfylt. Det er gjennomført virksomhets-ROS-analyse ved IT-avdelingen, og avdelingen har gjennom ROS-analysen grunnlag for å planlegge spesifikke tiltak som vil redusere risiko. Manglende oversikt over alle systemer, kan medføre at mindre viktige deler av IKT-systemene er godt sikret, mens andre kritiske deler kan være eksponert og sårbare for angrep. Vi er gjennom undersøkelsen gjort kjent med at det som i dag vurderes som kritiske IKT-systemer oppdateres ved vesentlige endringer, og at fylkeskommunen har igangsatt et arbeid med å få på plass en felles oversikt over IT-systemer.

Det er utarbeidet en tiltaksplan for IT-sikkerhet, som følges opp gjennom ledermøter. Revisor er gjennom undersøkelsen gjort kjent med at opprettholdelse av daglig drift må prioriteres, og at det derfor kan ta tid å nå målene om å iverksette planlagte sikkerhetstiltak. Helhetlig sikring avhenger av at de fysiske, elektroniske, menneskelige og organisatoriske tiltakene fungere sammen og understøtter hverandre.

Vår vurdering er at Troms fylkeskommune i all hovedsak oppfyller revisjonskriteriet om å jevnlig gjennomføre sårbarhetskartlegging, inntrengingstester og vurdere nivå av sikkerhetsovervåking. I tillegg til at fylkeskommunen får bistand fra ekstern leverandør, gjennomføres det intern testing. Det er innført målinger på ulike styringsparametere, som gjør det mulig å se trender, utvikling og sårbarheter. Vår vurdering av revisjonskriteriet som ikke fullt ut oppfylt bygger vi på informasjon om at kommuneCERT er kontaktet for å gjennomføre inntrengningstest, men ikke har hatt kapasitet til å gjennomføre dette. Slik revisor ser det har fylkeskommunen gjennom henvendelsen til kommuneCERT synliggjort et behov for slik testing, uten at dette er gjennomført.

Vi vurderer at Troms fylkeskommune har system for å sikre kontroll på alle identiteter og tilganger. Revisor finner at det er etablert retningslinjer for personellsikkerhet, og vi er opplyst at tilgangsstyringen er automatisert. [redacted] Funn i undersøkelsen tilsier at IT-avdelingen har prosedyrer for overvåking som skal bidra til at nødvendige systemer til enhver tid er tilgjengelig for ansatte.

Revisor vurderer at Troms fylkeskommune har prosesser som sikrer at avvik som avdekkes gjennom iverksatte tiltak håndteres. Vi har fått opplyst at eventuelle avvik registreres og følges opp via fylkeskommunens avvikssystem. Alvorligheten i avvik vurderes, og dersom det er aktuelt skal avvik meldes til Datatilsynet.

Som beskrevet i kapittel 4 er ikke styringssystemet for informasjonssikkerhet ferdig utviklet. Fylkeskommunen har flere rutiner og dokumenter som beskriver prosesser som kan sikre evaluering av effektiviteten til styringssystemet for informasjonssikkerhet, det er identifisert risikoer og planlagt tiltak knyttet til IT-sikkerhet. IT-avdelingen er slik revisor oppfatter innforstått med at det tar tid i å iverksette alle planlagte sikkerhetstiltak, men har oppmerksomheten rettet mot viktigheten av å oppdage og respondere raskt på sikkerhetshendelser.

5.3 Revisors konklusjon

Har Troms fylkeskommune truffet tilfredsstillende tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet?

Revisor konkluderer med at Troms fylkeskommune i all hovedsak har truffet tilfredsstillende tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet.

Vi baserer vår konklusjon på at styringssystemet ikke fullt ut er ferdigstilt, og at alle planlagte sikkerhetstiltak opplyses å ikke være iverksatt.

6 ANBEFALINGER

Gjennom prosjektet *Helhetlig styring for informasjonssikkerhet og personvern* skal Troms fylkeskommune få på plass et styringssystem på området. Arbeidet med styringssystemet pågår. Vi anser det ikke som hensiktsmessig å gi særskilte anbefalinger knyttet til styringssystemets innhold da fylkeskommunen selv har laget en plan for videre arbeid. Det er beskrevet utfordring med deltakelse i opplæringstiltakene som gjennomføres. *Vi anbefaler derfor fylkeskommunen å vurdere å etablere pålagte opplæringstiltak for å øke sikkerhetskulturen i organisasjonen*.

Vår undersøkelse har avdekket at sentrale bestemmelser i personvernlovgivningen ikke ivaretas, og at fylkeskommunen derfor bør treffe tiltak for å lukke disse avvikene. *Vi anbefaler derfor Troms fylkeskommune å ferdigstille arbeidet med behandlingsprotokoll, og gjennomføre personvernkonsekvensvurderinger (DPIA) i hele organisasjonen.*

7 UTTALELSE

Vi sendte rapportutkast til Troms fylkeskommune v/fylkeskommunedirektør 01.04.2026, og mottok tilbakemelding 20.04.2026. Uttalelsen er gjengitt i sin helhet nedenfor, og har ikke medført endringer i rapporten.

Troms fylkeskommune
Romssa fylkkasuohkan
Tromssan fylkinkomuuni

Unntatt offentlighet
offl. § 24 tredje ledd

Fylkeskommunedirektøren

KOMREV NORD IKS
Sjøgata 3
9405 HARSTAD

Dato: 20.04.2026
Dok.nr: 26/07188-1
Deres ref:
Saksbehandler: Tor Arne Johansen Morskogen

Uttalelse revisjon digital sikkerhet

Fylkeskommunedirektøren har sett gjennom rapporten, og mener den i det overordnede peker på relevante utfordringer, samt prosesser Troms fylkeskommune står i.

Rapporten viser, etter fylkeskommunedirektørens syn, at Troms fylkeskommune er på rett vei med arbeidet innenfor digital sikkerhet og informasjonssikkerhet. Arbeidet med sikkerhet og beredskap har vært prioritert helt siden oppsplittingen fra Finnmark ble gjennomført i 2024.

Fylkeskommunedirektøren vil likevel knytte noen kommentarer til rapportens innhold, der vi mener rapporten legger til grunn et upresist bilde av organisasjonens nåværende nivå. Dette kan blant annet skyldes at dataene i rapporten er samlet inn i en periode der arbeidet med fagfeltet hadde store fremskritt.

Gjennomgang av anbefalinger og tilbakemeldinger

Innspillene under er en oppdatering av hvilke aktiviteter i prosjekt Helhetlig styring av informasjonssikkerhet og personvern som har direkte innvirkning på de anbefalinger og tilbakemeldinger som er gitt i rapporten.

- Behandlingsprotokoll (heretter behandlingsoversikt)

Troms fylkeskommune er i sluttfasen av delleveranse 6: Behandlingsoversikt og behandlingsoversikten er nå overført til vårt digitale verktøy i Samsvar. Det pågår nå et arbeid med å komplementere oversikten med behandlinger fra nivå 3 i organisasjonen: skolene. Dette gjelder behandling av personopplysninger i forbindelse med elev- og læringsaktiviteter.

Videre skal oversikten kvalitetssikres, og kobles med systemoversikt, slik at det gir et helhetlig bilde av hvor personopplysningene lagres. Det vil også være et gjenstående arbeid og vurdering med tanke på hvor lenge personopplysningene skal bevares vs. slettes, da dette må kvalitetssikres mot gjeldende bevarings- og kassasjonsplan.

- Personvernkonsekvensvurderinger (DPIA)

Som nevnt i rapporten vil arbeidet med å gjennomgå behandlingsoversikten med formål og identifisere hvilke behandlinger som krever konsekvensvurdering og hvorvidt disse er gjennomført. Det er også et mål at disse skal være dokumentert i vårt sak- og arkivsystem, samt i behandlingsoversikten
Den samme aktiviteten vil også gjelde for databehandleravtaler.

- Systemoversikt (applikasjonsforvaltning)

Postadresse:
Troms fylkeskommune
Postboks 6600, 9296 Tromsø

Kontakt:
E-post: postmottak@tromsfylke.no
Telefon: 77 78 80 00

Nettside:
tromsfylke.no

Troms fylkeskommune har i dag registrert over 220 systemer i dagen systemoversikt i Samsvar. Det er systemeier i dag som har ansvaret for oppfølging. Det vil derfor bli fremmet sak til styret i prosjektet om etablering av en ny delleveranse for forvalting av applikasjoner.

· Internkontroll og avviksoppfølging

Både internkontroll og avviksoppfølging er egne delleveranser i prosjektet. Til rapportens merknader om avviksoppfølging vil vi se på forbedringspunkter i dagens avvikshåndtering. Det er som nevnt i rapporten, og spesielt på saksbehandlingssiden, uklarheter i rutinene. Prosjektet vil jobbe med en prosessgjennomgang for å sikre at avvik blir behandlet i tråd med egne retningslinjer.
Avviksoppfølging vil videre få særskilt fokus til høsten 2026 gjennom planlagt opplæring og kompetanseheving.

· Sikkerhetsbevissthet (opplæring og kompetanse)

Prosjektets delleveranse 8: Opplæring og kompetanse har lyst ut bistand til etablering av en håndbok for informasjonssikkerhet og personvern. Leverandør er nå valgt og arbeidet vil starte innen kort tid. Håndboken vil være gjenstand for en planlagt «bevissthetsmåned» med fokus på profilering av denne, opplæring og kurs, foredrag o.l. for roller som har særskilt ansvar. Videre er prosjektet i gang med en kompetanseplan og informasjonsstrategi for å sikre at opplæring og kompetanseheving treffer fylkeskommunen. Videre vil det bli etablert obligatoriske kurs o.l. basert på disse planene. Disse er planlagt implementert høsten 2026.
Dette er et svært viktig prosjekt som vil ha direkte påvirkning på gevinstrealiseringen i prosjektet og de tilbakemeldingene i rapporten når det gjelder sikkerhetsbevissthet.

· Roller og ansvar

I rapporten er det en del gjengivelse rolle- og ansvarsbeskrivelsene. I noen tilfeller er en del av beskrivelsene misvisende, noe som kan gjør at det kan oppleves at roller og ansvar er uklart, og i noen tilfeller er dette reelt. Dette har sammenheng med modning av organisasjonen og implementering av prosjektets leveranser, samt nye lover og regler som fylkeskommunen må forholde seg til. Dette er oppdateringer som er og vil bli gjort fortløpende i prosjektet.

Selv om fylkeskommunedirektøren har flere innspill over mener jeg oppsummert at rapporten gir et godt bilde på tilstanden i organisasjonen på det tidspunktet dataene ble innsamlet. Svaret er for å tydeliggjøre hvilken utvikling som har vært i organisasjonen etter dataene ble samlet inn. Fylkeskommunedirektøren er av den formening at mange av de tiltakene som anbefales er igangsatt, og var igangsatt på det tidspunktet rapporten ble skrevet. Alt i alt oppfatter Fylkeskommunedirektøren rapporten støttende til det arbeidet som gjøres, og underbygger de valgene som er gjort etter Troms igjen ble eget fylke.

Avslutningsvis vil jeg takke revisjonen for godt samarbeid gjennom prosessen.

Med hilsen

Camilla Bjørn
Fylkeskommunedirektør

Tor Arne Johansen Morskogen
Fagleder sikkerhet

Dokumentet er elektronisk godkjent og har ingen signatur

2

8 REFERANSER

- Lov av 22. juni 2018 om kommuner og fylkeskommuner (kommuneloven)
- Lov av 1. juni 2018 om nasjonal sikkerhet (sikkerhetsloven)
- Lov av 15. juni 2018 om behandling av personopplysninger (personopplysningsloven)
- Lov av 20. desember 2023 om digital sikkerhet (digitalsikkerhetsloven)
- Forskrift av 23. juni 2025 om digital sikkerhet (digitalsikkerhetsforskriften)
- Forskrift av 25. juni 2004 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet. Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus
- Datatilsynet; En veiledning om internkontroll og informasjonssikkerhet
- Nasjonalt rammeverk for håndtering av digitale angrep og cyberhendelser
- ISO 27001
- NSMs grunnprinsipper for IKT-sikkerhet

Om selskapet og vår forvaltningsrevisjonskompetanse

KomRev NORD IKS utfører helhetlig revisjon av kommuner og fylkeskommuner, kommunale foretak, interkommunale selskaper, offentlige stiftelser, kirkeregnskap og legater. Selskapets eiere og oppdragsgivere er fylkeskommunene Troms, Finnmark og Nordland, samt 51 kommuner fordelt på de tre nordligste fylkeskommunene.

Vårt hovedkontor ligger i Harstad, og vi har avdelingskontorer i Alta, Bodø, Finnsnes, Hammerfest, Lakselv, Leknes, Narvik, Sortland, Svolvær og Tromsø.

Vi har 55 medarbeidere som samlet innehar lang erfaring fra og god kunnskap om offentlig sektor og revisjon.

Selskapet er uavhengig i forhold til kommuner, stat, privat næringsliv og andre institusjoner i samfunnet.

Vårt forvaltningsrevisjonsteam består av 17 medarbeidere med høyere utdanning innen ulike fag:

- Rettsvitenskap
- Sosiologi
- Statsvitenskap
- Samfunnsøkonomi

KomRev NORD har tidligere gjennomført følgende forvaltningsrevisjoner, eierskapskontroller og undersøkelser:

<u>Troms fylkeskommune</u>	
Oppfølging av politiske vedtak,	2025
Eierskapskontroll Troms fylkeskommune,	2025
Gjennomføring og frafall i videregående opplæring,	2025
Forvaltning av tilskuddsordninger,	2025
<u>Troms og Finnmark fylkeskommune</u>	
Anskaffelser i fylkeskommunens selskaper,	2024
Kvalitet og ressursbruk i tannhelsetjenesten,	2024
Undersøkelse av anskaffelse, MS Hollendaren,	2023
Tilsettinger i ledelsen,	2023
Oppfølging av budsjett- og regnskapsvedtak,	2023
Årøyasambandet,	2022
Offentlige anskaffelser,	2022
Kontraktsoppfølging kollektivtransport,	2022
Eierskapskontroll Alta Museum,	2022
Hålogaland teater,	2021
<u>Troms fylkeskommune</u>	
Bredbåndsfylket Troms AS,	2020
Behandling av klager på standpunktkarakterer,	2019
Bierverv i videregående skoler,	2019
Investeringsprosjekter,	2019
Fylkeskommunens internasjonale arbeid,	2019
VIGO IKS,	2018
Forvaltning, drift og vedlikehold,	2018
Barentssekretariatet IKS,	2017
FilmCamp AS,	2016
Iverksetting av politiske vedtak,	2016
Fylkesvegene,	2016
Ressursbruk og kvalitet i videregående skole,	2015
Kollektivtransport – oppfølging av bruttokontrakter,	2014
Offentlige anskaffelser,	2013