Rapport fra forvaltningsrevisjon - Digital sikkerhet

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Trøndelag fylkeskommune	17.11.2026	101/26

Saksbehandler Ragnhild Aashaug
Arkivkode FE-217
TI-&58
Arkivsaknr 25/378 - 7

Forslag til vedtak
Kontrollutvalget slutter seg til revisors anbefalinger og oversender rapport fra forvaltningsrevisjon til fylkestinget med følgende innstilling:

1. Fylkestinget ber fylkesdirektøren om å:
    a. Styrker arbeidet med å sikre at rutiner og prosedyrer for informasjonssikkerhet er kjent og tas i bruk i relevante deler av organisasjonen.
    b. Sikrer mer fullstendig og oppdatert dokumentasjon av internkontrollen for informasjonssikkerhet, herunder oversikten over informasjonssystemer og behandling av personopplysninger.
    c. Styrker den systematiske bruken av avvik, sikkerhetshendelser og risiko som grunnlag for læring og forbedring av internkontrollen.
    d. Etablerer en mer systematisk og risikobasert oppfølging av tilganger, herunder kontroll av tilgangslogger der dette er nødvendig.
2. Fylkestinget ber fylkesdirektøren om å orientere kontrollutvalget skriftlig og muntlig om hvordan fylkeskommunen arbeider med å innarbeide anbefalingene i punkt 1 i fylkeskommunens rutiner og praksis innen utgangen av august 2027.

Vedlegg
Rapport - Digital sikkerhet

Saksopplysninger
Kontrollutvalget bestilte forvaltningsrevisjon av digital sikkerhet i sak , se kontrollutvalgets sak 55/25, den 7. oktober 2025 og møteprotokollen til møtet. Bestillingen bygger på planen for forvaltningsrevisjon 2024–2028 vedtatt av fylkestinget. Revisor utarbeidet en prosjektplan som beskriver hvordan forvaltningsrevisjonen skal gjennomføres, se kontrollutvalgets vedtak i sak 2/26 den 19. januar 2026 og møteprotokollen til møtet.

I denne saken legges endelig rapport fra forvaltningsrevisjonen frem til behandling i kontrollutvalget.

Hovedproblemstilling som skal besvares i rapporten er om fylkeskommunen har etablert og gjennomført et forsvarlig arbeid med digital sikkerhet. Det er utarbeidet delproblemstillinger for å konkretisere det som skal undersøkes for:

- Styringssystemer og rutiner:
- Avvik og forbedringsarbeid:
- Kompetanse og opplæring:
- Tilgangsstyring:
- Etterlevelse av personvernregelverket i tjenesteområdene:

Avgrensning
Det er undersøkt hvordan fylkeskommunen arbeider med digital sikkerhet gjennom styring, internkontroll og utvalgte personvernområder. Det har **ikke** vært et formål å kontrollere alle

behandlinger, systemer eller enkeltsaker innen de undersøkte tjenesteområdene. Dokumentasjon, utvalgte avtaler og opplysninger om systemer er benyttet for å belyse fylkeskommunens ordninger og beskrevne praksis på de undersøkte områdene. Utvalgte krav til behandlingsprotokoller, informasjon til de registrerte og databehandleravtaler er undersøkt innen tannhelse, personal og elevområdet.

Det er ikke gjennomført tekniske tester eller en fullstendig kontroll av etterlevelsen av regelverket.

Metode
Revisjonen bygger på dokumentgjennomgang, oppstartsmøte, intervjuer og supplerende informasjon innhentet underveis i gjennomføringen. Intervjuene omfatter sentrale funksjoner og utvalgte tjenesteområder med ansvar eller oppgaver innen informasjonssikkerhet, personvern og internkontroll. Revisjonen har brukt dette til å belyse hvordan styringssystemer, rutiner og ansvarsforhold forstås og praktiseres. Det er også brukt til å innhente erfaringer med avvikshåndtering, opplæring, tilgangsstyring og personvernarbeid.

Disse er intervjuet:
- Seksjonsleder organisasjon
- Fylkestannlege
- Leder kvalitet og internkontroll
- Seksjonsleder eksamen og støttetjenester
- Seksjonsleder jus og anskaffelser
- Seniorrådgiver digitalisering
- Informasjonssikkerhetskoordinator
- Sikkerhets- og beredskapsleder
- Direktør organisasjon og økonomi
- Seksjonsleder arkiv
- Personvernombud
- Seksjonsleder IKT
- Seksjonsleder kommunikasjon
- IKT sikkerhetskoordinator

Omtalen i rapporten er på rolle- og funksjonsnivå.

Problemstillingen - Har fylkeskommunen har etablert og gjennomført et forsvarlig arbeid med digital sikkerhet?

Det er utarbeidet delproblemstillingene for å svare ut spørsmålet. I saksfremlegget har vi ikke tatt inn revisors vurderinger for de enkelte delproblemstillingene. Revisors oppsummerende konklusjoner er lagt til grunn.

<u>Delproblemstilling 1 – Styringssystemer og rutiner</u>
For å besvare denne problemstillingen har revisor utarbeidet revisjonskriterier, som revisor knytter vurderinger til. Revisjonskriteriene er angitt som kulepunkter mens vurderingene er gjengitt med *kursiv skrift* rett etter revisjonskriteriet.

Fylkeskommunen skal:
- ha dokumenterte mål og strategi for informasjonssikkerhet i digitale tjenester og systemer – *oppfylt.*
- ha avklart og dokumentert roller, ansvar og myndighet for informasjonssikkerhet og personvern – *i hovedsak oppfylt***.**
- ha nødvendige rutiner og prosedyrer for informasjonssikkerhet - *oppfyl*t.
- sikre at rutiner og prosedyrer for informasjonssikkerhet er gjort kjent, tilgjengelige og tatt i bruk i relevante deler av organisasjonen - *delvis oppfylt*.

- dokumentere internkontrollen for informasjonssikkerhet i den formen og det omfanget som er nødvendig - *delvis oppfylt*.

Delproblemstilling 2 – Avvik og forbedringsarbeid
For å besvare denne problemstillingen har revisor utarbeidet revisjonskriterier, som revisor knytter vurderinger til. Revisjonskriteriene er angitt som kulepunkter mens vurderingene er gjengitt med *kursiv skrift* rett etter revisjonskriteriet.

Fylkesdirektøren skal:
- ha skriftlige rutiner for å avdekke, registrere, klassifisere, behandle og følge opp avvik og sikkerhetshendelser knyttet til informasjonssikkerhet - *oppfylt*.
- ha rutiner som sikrer at brudd på personopplysningssikkerheten vurderes og dokumenteres – *i hovedsak oppfylt*.
- bruke avvik, sikkerhetshendelser og risiko for avvik som grunnlag for forbedring av internkontrollen for informasjonssikkerhet - *delvis oppfylt*.

Delproblemstilling 3 – Kompetanse og opplæring
For å besvare denne problemstillingen har revisor utarbeidet revisjonskriterier, som revisor knytter vurderinger til. Revisjonskriteriene er angitt som kulepunkter mens vurderingene er gjengitt med *kursiv skrift* rett etter revisjonskriteriet.

Fylkeskommunen skal:
- sikre at ansatte og andre brukere som får tilgang til digitale systemer og personopplysninger, får nødvendig opplæring om sikker bruk, konfidensialitet, tilgangsstyring, avvikshåndtering og behandling av personopplysninger – *i hovedsak oppfylt.*
- sikre at ansatte som behandler elevdata, pasientdata eller personaldata får nødvendig informasjon og opplæring om relevante krav i regelverk og interne rutiner – *i hovedsak er oppfylt.*
- dokumentere gjennomførte opplærings- og informasjonstiltak i det omfanget som er nødvendig for å kunne følge opp internkontrollen - *i hovedsak er oppfylt.*

Delproblemstilling 4 – Tilgangsstyring
For å besvare denne problemstillingen har revisor utarbeidet revisjonskriterier, som revisor knytter vurderinger til. Revisjonskriteriene er angitt som kulepunkter mens vurderingene er gjengitt med *kursiv skrift* rett etter revisjonskriteriet.

Fylkeskommunen skal:
- ha rutiner for tilgangsstyring i digitale systemer som behandler eller gir tilgang til personopplysninger og annen beskyttelsesverdig informasjon – *i hovedsak oppfylt.*
- sikre at tilganger tildeles på bakgrunn av tjenstlig behov– *i hovedsak oppfylt.*
- ha rutiner for logging og oppfølging av tilgang der dette er nødvendig for å avdekke eller følge opp urettmessig tilgang, eller følger av særskilt regelverk - *delvis oppfylt*.

Delproblemstilling 5 – Etterlevelse av utvalgte personvernkrav
For å besvare denne problemstillingen har revisor utarbeidet revisjonskriterier, som revisor knytter vurderinger til. Revisjonskriteriene er angitt som kulepunkter mens vurderingene er gjengitt med *kursiv skrift* rett etter revisjonskriteriet.

Fylkeskommunen skal:
- ha oversikt over behandling av personopplysninger og dokumentere behandlingsaktivitetene i behandlingsprotokoller i samsvar med personvernregelverket. – *i hovedsak oppfylt.*

- gi de registrerte informasjon om hvordan personopplysningene deres behandles – *i hovedsak oppfylt.*
- inngå databehandleravtale når eksterne leverandører behandler personopplysninger på fylkeskommunens vegne - *oppfylt*.

Revisors konklusjon og anbefalinger
Revisor konkluderer med at Trøndelag fylkeskommune i hovedsak har etablert og gjennomført et forsvarlig arbeid med digital sikkerhet innenfor de områdene revisjonen har undersøkt.

Revisor vurderer at fylkeskommunen i stor grad har etablert et styringssystem for informasjonssikkerhet og personvern. Det foreligger mål og strategier for arbeidet, og roller, ansvar og myndighet er i hovedsak dokumentert og forankret i organisasjonen. Videre er det etablert rutiner og prosedyrer for blant annet risikostyring, systemforvaltning, avvikshåndtering og håndtering av brudd på personopplysningssikkerheten.

Samtidig viser revisjonen variasjoner i kjennskap til og bruk av rutiner, mangler ved dokumentasjonen av internkontrollen og behov for mer systematisk bruk av avvik og sikkerhetshendelser i forbedringsarbeidet. Det er også identifisert
- svakheter ved oppfølging av enkelte tilganger og kontroll av tilgangslogger.
- Innen personvern er det behov for å videreutvikle den samlede oversikten over behandlinger av personopplysninger og tydeliggjøre enkelte rutiner.

Revisor anbefaler at fylkeskommunen:
1. Styrker arbeidet med å sikre at rutiner og prosedyrer for informasjonssikkerhet er kjent og tas i bruk i relevante deler av organisasjonen.
2. Sikrer mer fullstendig og oppdatert dokumentasjon av internkontrollen for informasjonssikkerhet, herunder oversikten over informasjonssystemer og behandling av personopplysninger.
3. Styrker den systematiske bruken av avvik, sikkerhetshendelser og risiko som grunnlag for læring og forbedring av internkontrollen.
4. Etablerer en mer systematisk og risikobasert oppfølging av tilganger, herunder kontroll av tilgangslogger der dette er nødvendig.

Høringssvar og uttalelse fra fylkesdirektøren
Fylkesdirektøren har avgitt høringssvar til rapporten, og mener rapporten gir nyttige innspill. Samtidig understrekes det at innføringen av det overordnede internkontrollsystemet skal gjøre styrende informasjon bedre kjent i organisasjonen. Høringssvaret er vedlagt rapporten, se side 72. Fylkesdirektøren har i tillegg anledning til å uttale seg når kontrollutvalget tar saken opp til behandling og før vedtak fattes.

Vurdering og konklusjon
Rapporten er i tråd med kontrollutvalgets bestilling og prosjektplanen. Det betyr at forvaltningsrevisjonen er avgrenset til fylkeskommunens arbeid med digital sikkerhet, når det gjelder styring, organisering, internkontroll, informasjonssikkerhet og utvalgte områder innen personvern. Det er ikke gjennomført tekniske sikkerhetstester eller en fullstendig kontroll av etterlevelsen av regelverket.

Sekretariatet vurderer at revisjonen gir kontrollutvalget et godt grunnlag for å vurdere fylkeskommunens arbeid med digital sikkerhet innenfor de undersøkte områdene. Revisjonen avdekker ikke grunnleggende mangler i styringssystemet, men viser at flere sentrale tiltak ikke er tilstrekkelig innarbeidet og fulgt opp i hele organisasjonen.

Sekretariatet merker seg særlig revisors vurderinger knyttet til behovet for helhetlige risikovurderinger, bedre dokumentasjon av internkontrollen, mer systematisk bruk av avvik i forbedringsarbeidet og styrket oppfølging av personvern- og tilgangsstyringsarbeidet. Dette

vurderes som sentrale forhold for å sikre en tilfredsstillende utvikling av fylkeskommunens arbeid med digital sikkerhet.

Forvaltningsrevisjon gir god og nyttig informasjon som bør kunne bidra til læring og forbedring, noe fylkesdirektøren bekrefter i høringssvaret.
Sekretariatet anbefaler at kontrollutvalget slutter seg til revisors anbefalinger, og oversender rapporten til behandling i fylkestinget.