Revisjon Midt-Norge

Digital Sikkerhet

Trøndelag fylkeskommune,
17.11.26

Cathrine Berg-Mortensen



Problemstilling

- Har fylkeskommunen etablert og gjennomført et forsvarlig arbeid med digital sikkerhet?
- **Delproblemstillinger:**
  - **Styringssystemer og rutiner:** Har fylkeskommunen etablert rutiner og prosesser for å sikre informasjonssikkerhet, og i hvilken grad er disse gjort kjent og tatt i bruk i organisasjonen?
  - **Avvik og forbedringsarbeid:** Har fylkeskommunen etablert rutiner for håndtering av avvik og sikkerhetshendelser innen informasjonssikkerhet, og hvordan brukes avvik i arbeidet med å forbedre internkontrollen?
  - **Kompetanse og opplæring:** Har fylkeskommunen etablert og fulgt opp tiltak for å gi ansatte nødvendig informasjon, opplæring og kompetanseutvikling innen informasjonssikkerhet?
  - **Tilgangsstyring:** Har fylkeskommunen rutiner og ordninger for tilgangsstyring som ivaretar tjenstlig behov og nødvendig logging og oppfølging?
  - **Etterlevelse av personvernregelverket i tjenesteområdene**: Etterlever fylkeskommunen utvalgte krav i personvernregelverket ved behandling av pasientdata, elevdata og personaldata?

PM Revisjon Midt-Norge

Avgrensninger

- Revisjonen er avgrenset til utvalgte organisatoriske og styringsmessige forhold ved digital sikkerhet.
- Tekniske sikkerhetstiltak og IKT-infrastruktur er ikke testet.
- Etterlevelse av rutiner og faktiske brukertilganger er ikke kontrollert gjennom stikkprøver eller observasjon.
- Kompetanseområdet omfatter opplæringstiltak og oppfølging, ikke kartlegging av den enkelte ansattes kompetanse.
- Personvernområdet er avgrenset til utvalgte krav innen elev-, pasient- og personaldata.

PM Revisjon Midt-Norge

Styringssystemer og rutiner

- Fylkeskommunen **har** dokumenterte mål og strategier for informasjonssikkerhet i digitale tjenester og systemer
- Fylkeskommunen **har i hovedsak** avklart og dokumentert roller, ansvar og myndighet for informasjonssikkerhet og personvern
- Fylkeskommunen **har** nødvendige rutiner og prosedyrer for informasjonssikkerhet
- Fylkeskommunen **delvis** sikrer at rutiner og prosedyrer for informasjonssikkerhet er gjort kjent, tilgjengelig og tatt i bruk i relevante deler av organisasjonen
- Fylkeskommunen dokumenterer **delvis** internkontroll for informasjonssikkerhet i den formen og det omfanget som er nødvendig

PM Revisjon Midt-Norge

Avvik og forbedringsarbeid

- Fylkeskommunen **har** rutiner for å avdekke, registrere, klassifisere, behandle og følge opp avvik og sikkerhetshendelser knyttet til informasjonssikkerhet
- Fylkeskommunen **har** i hovedsak rutiner som sikrer at brudd på personopplysningssikkerheten vurderes og dokumenteres
- Fylkeskommunen **delvis** bruker avvik, sikkerhetshendelser og risiko for avvik som grunnlag for forbedring av internkontrollen for informasjonssikkerhet

PM Revisjon Midt-Norge

Kompetanse og opplæring

- Fylkeskommunen **sikrer i hovedsak** 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
- Fylkeskommunen **sikrer i hovedsak** at ansatte som behandler elevdata, pasientdata eller personaldata får nødvendig informasjon og opplæring om relevante krav i regelverk og interne rutiner.
- Fylkeskommunen dokumenterer **i hovedsak** gjennomførte opplærings- og informasjonstiltak i det omfanget som er nødvendig for å kunne følge opp internkontrollen.

PM Revisjon Midt-Norge

Tilgangsstyring

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

PM Revisjon Midt-Norge

Etterlevelse av utvalgte personvernkrav

- Fylkeskommunen har i hovedsak oversikt over behandlinger av personopplysninger og dokumenterer behandlingsaktivitetene i behandlingsprotokoller i samsvar med personvernregelverket.
- Fylkeskommunen gir i hovedsak de registrerte informasjon om hvordan personopplysningene deres behandles
- Fylkeskommunen inngår databehandleravtale når eksterne leverandører behandler personopplysninger på fylkeskommunens vegne

PM Revisjon Midt-Norge

Konklusjon

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

Fylkeskommunen har etablert sentrale rammer for styring og internkontroll, men det er behov for å styrke den systematiske gjennomføringen og oppfølgingen av sikkerhetsarbeidet.

PM Revisjon Midt-Norge

Anbefaling

Revisor anbefaler at fylkeskommunen:

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

PM Revisjon Midt-Norge