

Forvaltningsrevisjon av informasjonssikkerhet - rådmannens oppfølging av vedtak

Behandles i utvalg Kontrollutvalget i Melhus kommune	Møtedato 12.12.2024	Saknr 78/24
Saksbehandler Eva J. Bekkavik		
Arkivkode FE-217, TI-&58		
Arkivsaknr 23/94 - 18		

Forslag til vedtak

1. Kontrollutvalget tar rådmannens tilbakemelding til orientering.
2. Kontrollutvalget anser kommunestyrets vedtak som fulgt opp og avslutter forvaltningsrevisjonen.

Vedlegg

Rådmannens oppfølging av kommunestyrets vedtak i sak 91/2024 Forvaltningsrevisjon av informasjonssikkerhet

Saksopplysninger

På kontrollutvalgets møte 6. juni 2024 (sak 27/24) ble rapport fra forvaltningsrevisjon av informasjonssikkerhet behandlet.

Nedenfor kommer et kort utdrag fra forvaltningsrevisjonsrapporten.

Revisjon Midt-Norge SA formulerte følgende problemstillinger for prosjektet:

- Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstillende krav i regelverket?
- Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Revisjonens konklusjon

Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstillende krav i regelverket?

Revisor konkluderer med at Melhus kommune har etablert et styringssystem for informasjonssikkerhet som tilfredsstillende utvalgte krav i regelverket.

Kommunen er i ferd med å legge om styringssystemet for å tilpasse det til relevante standarder. Arbeidet med informasjonssikkerhet framstår som godt forankret i kommunen, både hos administrasjonen og politisk nivå.

Sikkerhetsorganisasjonen i Melhus er beskrevet i flere dokumenter, der bruken av roller og ansvar ikke er konsistente. Det er viktig at plassering av roller og ansvar i sikkerhetsorganisasjonen er tydelig og kjent for alle ansatte i kommunen. Kommunen må også sørge for at behandlingsprotokollen er oppdatert med riktig databehandler og personvernombud.

Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Revisor konkluderer med at Melhus kommune har satt i verk egnede organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten. Tiltak for å ivareta informasjonssikkerhet er ferskvare og vil hele tiden utfordres av trusselbildet som er i stadig endring. Kommunens tilgangssystem styres av HR-systemet og knytter de ansattes tilgang til den stillingen de har. Dette sikrer at tilganger fjernes når det sendes sluttmelding. Kommunen benytter seg av samarbeidspartnere som bidrar til at kommunen kan oppdage sikkerhetshendelser så tidlig som mulig for å minimere skadeomfang eller forhindre hendelser.

Videre har kommunen gode og gjennomtenkte planer for håndtering og gjenoppretting ved hendelser. Dette gjør at kommunen har en beredskap for å håndtere hendelser og en plan for hvem som gjør hva hvis noe oppstår.

Revisors anbefaling

Med bakgrunn i funn, anbefaler revisor at rådmannen:

- Fortsetter arbeidet med omlegging av styringssystemet for informasjonssikkerhet.
- Vurderer hensiktsmessig plassering av roller og ansvar i sikkerhetsorganisasjonen.

Politisk behandling

Kommunestyret hadde forvaltningsrevisjonsrapporten opp til behandling i sitt møte 10. september 2024 i sak 91/24 og gjorde følgende vedtak:

1. Kommunestyret tar forvaltningsrevisjonsrapport om informasjonssikkerhet til orientering.
2. Kommunestyret ber rådmannen følge opp anbefalingene i rapporten:
 - a. Fortsetter arbeidet med omlegging av styringssystemet for informasjonssikkerhet.
 - b. Vurderer hensiktsmessig plassering av roller og ansvar i sikkerhetsorganisasjonen.
3. Kommunestyret ber rådmannen gi kontrollutvalget skriftlig tilbakemelding om hvordan anbefalingene er fulgt opp innen 20.11.2024.

Rådmannens oppfølging

Rådmannen har i brev av 27. november 2024 gitt en skriftlig tilbakemelding til kontrollutvalget (sekretariatet ga rådmannen litt lenger frist enn det kommunestyret vedtok, fordi rådmannen trengte litt ekstra tid på oppfølging av vedtaket.) Tilbakemeldingen er lagt med som vedlegg til saken.

Vurdering

Rådmannen viderefører implementering av nytt styringssystem i dagens internkontroll og kvalitetssystem EQS.

Rådmannen har vurdert at per i dag så er det mest praktisk og funksjonelt at beredskapsrådgiver er plassert i Enhet plan fordi enheten er lokalisert i nærhet til rådmann/kommunalsjefer, og enheten har et kompetanse- og fagmiljø.

Rådmannen har utarbeidet en beskrivelse av rolle og ansvar for IT-sikkerhetsansvarlig, fagansvar informasjonssikkerhet og personvernombud.

Konklusjon

Kontrollutvalgets sekretariat er av den oppfatning at rådmannen har fulgt opp kommunestyrets vedtak punkt 2.

Sekretariatet anbefaler at kontrollutvalget tar rådmannens tilbakemelding til orientering og avslutter forvaltningsrevisjonen.