Tilbakemelding til kontrollutvalget

Bakgrunn for tilbakemelding:

1. Kommunestyret tar forvaltningsrevisjonsrapport om informasjonssikkerhet til orientering.

2. Kommunestyret ber rådmannen følge opp anbefalingene i rapporten: • Fortsetter arbeidet med omlegging av styringssystemet for informasjonssikkerhet. • 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

Tilbakemelding på anbefalingene i rapportens to punkter

- *Fortsetter arbeidet med omlegging av styringssystemet for informasjonssikkerhet*

  Rådmannen viderefører implementering av nytt styringssystem basert på NIS2 i dagens internkontroll og kvalitetssystem EQS. Dokumenter er delt i ulike graderinger, og tilpasses med rollestyring for å ivareta nødvendig sikkerhet.

- *Vurder hensiktsmessig plassering av roller og ansvar i sikkerhetsorganisasjonen*

  Rådmannen har gjort en vurdering og laget en oversikt og gjennomgående beskrivelse og definisjon av roller og ansvar slik at den blir mer konsistent. Dette vil oppdateres i dokumenter og beskrivelser.

  Rolle *IT-sikkerhetsansvarlig* har gjennomgående tekniske ansvarsområder og legges til funksjon i ITMidt.

  Rolle *Fagansvar informasjonssikkerhet* er knyttet til informasjonssikkerhet og personvern, og funksjon er organisert under enhet Plan.

  Personvernombud er knyttet til forpliktelser som følger av personvernregelverket og er lagt til funksjon som er organisert under enhet Plan.

  Forvaltningsrevisjonen bemerker videre at beredskapsrådgiver er plassert i en enhet utenfor rådmannens stab e.l. og vurderer dette som uheldig. Rådmannen har vurdert hensiktsmessigheten, og ser at det praktisk og funksjonelt er den beste løsningen pt. Enhet Plan er lokalisert i nærhet til rådmann/kommunalsjefer og utøver allerede ulike funksjonsoppgaver som gjelder hele organisasjonen. Plasseringen er også i et etablert kompetanse- og fagmiljø, og rådmannen finner det derfor ikke som fordel å etablere en ny stabsenhet for å ivareta disse funksjonene nå.

Beskrivelse av roller og ansvar

IT-sikkerhetsansvarlig skal

- I tett samarbeid med Informasjonssikkerhet- og personvernansvarlig sikre at kommunens styringssystem for informasjonssikkerhet og personvern er i samsvar med ISO 27001-standarden.
- Overvåke kommunens informasjonssikkerhetsarbeid, og gripe inn der det er nødvendig.
- Identifisere risikoområder og foreslå sikringstiltak.
- Sikre at leverandører gjennomfører avtalte sikkerhetstiltak.
- Kommunisere sikkerhetsrisikoer og -trusler til ledelsen.

ITMidt er ansvarlig for tekniske sikkerhetstiltak (tiltaksleverandør), og er ansvarlig for å sørge for IT-faglig kompetanse inn i vurdering og håndtering av risiko. I tillegg er enheten ansvarlig for overvåking og hendelseshåndtering. ITMidt vil derfor være ansvarlig for å styre den teknsike aktiviteten. IT-leder vil være «risikoeier» for de arbeidsoppgavene som vedkommende er ansvarlig for. Dette innebærer også informasjonssikkerhetsrisiko.

Fagansvar informasjonssikkerhet skal

- Sikre at kommunens styringssystem for informasjonssikkerhet på overordnet nivå og personvern er i samsvar med ISO 27701-standarden og personvernregelverket.
- Bistå med vurderinger og tilsyn av databehandlere.
- Bistå i arbeidet med risikovurderinger (ROS og DPIA).
- Sikre at kompetanseplanen for informasjonssikkerhet og personvern er relevant i forhold til trusselbilde og kompetansebehov.

Fagansvarlig informasjonssikkerhet innebærer som hovedansvar å være pådriver og støtte til ledelsen og organisasjonen i informasjonssikkerhetsarbeidet. I tillegg skal fagansvarlig informasjonssikkerhet være en nøkkelressurs i Melhus kommunes kontinuerlige internkontrollarbeid på informasjonssikkerhetsområdet, blant annet ved å bistå i arbeidet med risikovurdering og -håndtering, evaluering og revisjon. Fagansvarlig vil sammen med ITMidt ha ansvaret for å planlegge og gjennomføre opplæring og bevisstgjøringsaktiviteter innen informasjonssikkerhet i Melhus kommune. Rollen ligger til enhet Plan, og enhetsleder Plan vil være «risikoeier» for de

arbeidsoppgavene som vedkommende er ansvarlig for. Dette innebærer også informasjonssikkerhetsrisiko.

Personvernombud

Et **personvernombud** er en person som er utnevnt for å overvåke og sikre at Melhus kommune overholder personvernlovgivning, som for eksempel EUs personvernforordning (GDPR) eller nasjonale personvernlovgivninger. Rollen ligger til enhet Plan. Personvernombudet fungerer som en rådgiver for Melhus kommune, og har ansvar for å:

1. **Informere og veilede** organisasjonen om personvernforpliktelser.
2. **Overvåke etterlevelse** av personvernregler og -praksis, og sikre at interne prosesser og retningslinjer er i samsvar med loven.
3. **Gi råd** om vurdering av personvernkonsekvenser.
4. **Være kontaktpunkt** for registrerte (de som er berørt av personvernet), og også for tilsynsmyndigheter som Datatilsynet.
5. **Holde seg oppdatert** om personvernlovgivning og eventuelle endringer i regelverket.

Personvernombudet skal være uavhengig i sitt arbeid og kan ikke instrueres om hvordan det skal utføre sine oppgaver, selv om de er ansatt i organisasjonen.