



Trondheim kommunerevisjon

Vår saksbehandler  
Bjørn Jonny Villa

Vår ref.  
23/10121  
oppgis ved alle henv.

Deres ref.

Dato  
14.04.2023

### Svar - Uttalelse fra ledelsen vedrørende - Etterlevelseskontroll mot ansattilganger, systemtilganger og leverandørtilganger

I revisjonens etterlevelseskontroll har det blitt undersøkt om ansattilganger, systemtilganger og leverandørtilganger til IT-systemer i Trondheim kommune, kontrolleres på en tilfredsstillende måte.

Vi ønsker med dette å gi vår tilbakemelding på revisjonens konklusjoner og anbefalinger.

#### Kommunen skal ha retningslinjer for tilgangshåndtering til TK-nett og IT-systemer

Anbefalinger fra revisjon:

- Retningslinjene for tildeling av midlertidige passord samsvarer ikke med dagens praksis. Retningslinjene bør oppdateres.
- Revisjonen mener imidlertid det er viktig at kommunen følger opp at de får tilgangsrapporter fra Helseplattformen AS som gjør det mulig å følge opp at ansatte i Trondheim kommune har fått tilganger i henhold til tjenstlig behov.
- Det bør lages tydeligere beskrivelse av roller, ansvar og myndighet for tjenesteforvalter og tjenesteeier.

Svar:

- Retningslinjer for midlertidige pasord er nå oppdatert i aktuell rutine i kvaliteket
- Tilgangsrapporter fra Helseplattformen skal nå jevnlig etterspørres
- Arbeidet med å oppdatere rollebeskrivelser er igangsatt som del av en gjennomgang av hvordan Trondheim kommune utøver IT tjenestestyring.

#### Kommunen skal etterleve retningslinjer for tilgangshåndtering

Anbefalinger fra revisjon:

- Revisjonen mener det er svært viktig at bestilling av tilganger til systemet Helseplattformen blir gjort i henhold til gjeldende retningslinjer.

Svar:

- Bestilling av tilganger til systemet Helseplattformen blir nå gjort i henhold til gjeldende retningslinjer. De refererte innkjøringsproblemene på dette området er nå over.

#### Kommunen skal utføre en årlig kontroll av tilgangene til IT-systemer

Anbefalinger fra revisjon:

- Det mangler årlig gjennomgang av tilganger ved flere av IT-systemene som er kontrollert i undersøkelsen. Revisjonen mener at årlig gjennomgang bør gjennomføres i henhold til retningslinjene i kommunen.

Svar:

- Dette erkjenner vi at er et område hvor vi må legge ned mer innsats og tilstrebe at dette gjøres for alle systemene hvert år.

### **Kommunen skal ha kontroll og oppfølging av upersonlige tilganger**

Anbefalinger fra revisjon:

- For skysystemene Visma Multi og LIFT er det ikke satt spesifikke krav til oppfølging av upersonlige tilganger. Det er leverandøren av tjenesten som initierer behov for slike tilganger. Det må stilles krav til at leverandørene følger kommunens retningslinjer og at det rapporteres på håndtering av upersonlige tilganger. Kommunen bør også ha en årlig gjennomgang av behovet for de upersonlige tilgangene.

Svar:

- Vi erkjenner at vi må kravstille at våre leverandører håndterer denne typen tilganger på en god måte, men vi vil sannsynligvis ikke være istand til å kreve at leverandørene tilpasser intern praksis iht våre retningslinjer fullt ut. Dette som en naturlig konsekvens av at det er en skyleveranse hvor tjenester for flere kunder produseres.

### **Kommunen skal ha kontroll og oppfølging av leverandørtilganger**

Anbefalinger fra revisjon:

- Undersøkelsen viser at Trondheim kommune mangler gode rutiner for oppfølging av leverandørtilganger for systemleverandør. Revisjonen er enig med ROS-analysen sine anbefalinger om å etablere standardkontrakter og gode rutiner for kommunikasjon med leverandør.

Svar:

- Standardkontrakter/rutiner skal utarbeides og tilstrebes innført for alle leverandører der hvor leveransens art og avtaleform gir rom for dette.

### **Kommunen skal bruke sikkerhetslogger aktivt for å avdekke uønsket aktivitet i datatrafikken**

Anbefalinger fra revisjon:

- Gjennomført undersøkelse viser at det er svakheter knyttet til sikkerhetslogging og sikkerhetsovervåking for kommunens IT-systemer. Revisjonen slutter seg til ROS-analysens anbefalinger om å innføre sikkerhetslogging i alle systemer og etablere sikkerhetsovervåking.

Svar:

- Det arbeides aktivt med sikkerhetslogging og analyse. Omfang utvides hele tiden, og vi er således enig i fokuset på dette området. Men vi er samtidig relativt godt fornøyd med det nivået vi har kommet oss opp på gjennom et sterkere operativt miljø i egen organisasjon.

Med hilsen

Trondheim kommune

Trude Kristin Kjeldstad  
organisasjonsdirektør

Bjørn Jonny Villa  
it-sjef

*Elektronisk dokumentert godkjenning uten underskrift*

Vedlegg: Signert uttalelse fra ledelsen - Organisasjonsdirektør

Kopi: Trondheim kommunerevisjon v/Børge Sundli