



Rapport 7/2025-RE

Etterlevelseskontroll IT - roller og tilganger for utvalgte systemer



Forord

Trondheim kommunerevisjon har i denne etterlevelseskontrollen undersøkt roller og tilganger i It-systemer for å sikre at rettigheter i systemet er i samsvar med tjenestlig behov og regelverk. Arbeidet med rapporten har foregått fra 28.08.24 til 02.04.25. Byrådet har hatt rapporten til verifisering og uttalelse i perioden 02.04.25 til 19.05.25.

Dette er en forenklet etterlevelseskontroll med økonomiforvaltningen. Kontrollen skal skje i forlengelsen av revisjonen av regnskapet og skal rette seg mot de delene av økonomiforvaltningen som går ut over å uttale seg om årsregnskapet.

Kommunelovens §24-9 forutsetter at revisor gir en egen uttalelse om kontrollen som er utført. Kontrollen skal gjennomføres med såkalt moderat sikkerhet. Kravene til denne kontrollen er definert gjennom god kommunal revisjonsskikk¹ og revisjonsstandarden RSK 301 "Forenklet etterlevelseskontroll med økonomiforvaltningen". Etterlevelseskontrollen formaliseres gjennom en uttalelse fra revisor til kontrollutvalget.

Arbeidet er utført av Elin Haarsaker (prosjektleder), Anne-Margit Eide Schjølberg og Elin Ingeborg Vassmo.

Trondheim, 26. mai 2025

Per Olav Nilsen
revisjonsdirektør

Elin Haarsaker
statsautorisert revisor

¹ Med god kommunal revisjonsskikk menes at revisjonen skal utføres i samsvar med den oppfatning av etiske og revisjonstekniske prinsipper for revisjon av kommuner som til enhver tid er alminnelig anerkjent og praktisert av dyktige og ansvarsbevisste utøvere av yrket.

Uavhengig revisors attestasjonsuttalelse om etterlevels kontroll IT - roller i og tilganger til utvalgte systemer

Vi har utført et attestasjonsoppdrag som skal gi moderat sikkerhet for at Trondheim kommune har etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemer.

Problemstillinger

Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemer for å sikre at ansattes rettigheter i systemene er i samsvar med tjenstlig behov og gjeldende regelverk?

Revisjonskriterier

- Kommunen skal ha overordnede skriftlige retningslinjer som definerer hvordan tjenesteforvalter² skal utøve sitt ansvar for roller og tilganger.
- Roller i IT-systemene skal være satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet.
- Kommunen skal ha rutiner for tildeling, endring og sletting av tilganger.
- Tilganger til IT-systemer skal følge prinsippet om minst mulig privilegium, brukere skal kun ha tilgang til det de trenger for å utføre sine arbeidsoppgaver.
- Kommunen skal jevnlig evaluere tilganger for å sikre at de er nødvendige og oppdaterte.
- Kommunen bør sørge for opplæring av tjenesteforvaltere i informasjonssikkerhet og personvern.
- Loggføring av bruk av IT-systemer skal gjennomgå jevnlig for å avdekke eventuelt misbruk.

Revisjonskriteriene er utledet fra følgende kilder:

- NSM Grunnprinsipper for IKT-sikkerhet
- Kvaliteket
 - 15741-4, IT-tilganger for ansatte og vikarer i Trondheim kommune
 - 16018-1 Årlig revisjon av tilganger til fagprogram med egen tilgangskontroll i Trondheim kommune
- Lov om behandling av personopplysninger, GDPR artikkel 25 og 32

Ledelsens ansvar for etterlevelse av bestemmelser og vedtak for økonomiforvaltningen

Byrådet er ansvarlig for å etablere administrative rutiner som sørger for at økonomiforvaltningen utøves i tråd med bestemmelser og vedtak, og at økonomiforvaltningen er gjenstand for betryggende kontroll.

² En tjenesteforvalter er en person som har fagkompetanse om et tjenesteområde og har ansvar for den daglige driften av et IT-system knyttet til dette tjenesteområdet.

Vår uavhengighet og kvalitetskontroll

Vi har utført oppdraget i samsvar med etiske retningslinjer for kommunerevisjonen, som inneholder uavhengighetskrav og andre krav basert på grunnleggende prinsipper om integritet, objektivitet, faglig kompetanse og tilbørlig aktsomhet, fortrolighet og profesjonell opptreden. I samsvar med internasjonal standard for kvalitetskontroll (ISQM 1 Kvalitetskontroll for revisjonsfirmaer som utfører revisjon og forenklet revisorkontroll av regnskaper samt andre attestasjonsoppdrag og beslektede tjenester) har Trondheim kommunerevisjon et tilstrekkelig kvalitetskontrollsystem, herunder dokumenterte retningslinjer og rutiner for etterlevelse av etiske krav, faglige standarder og krav i gjeldende lovgivning og annen regulering.

Våre oppgaver og plikter

Vår oppgave er å avgi en uttalelse om etterlevelse av bestemmelser og vedtak for økonomiforvaltningen på grunnlag av bevisene vi har hentet inn. Vi har utført vårt attestasjonsoppdrag med moderat sikkerhet i samsvar med kommunelovens regler og RSK 301 Forenklet etterlevelseskontroll med økonomiforvaltningen. Standarden krever at vi planlegger og gjennomfører oppdraget for å oppnå moderat sikkerhet for hvorvidt det foreligger vesentlige feil eller mangler ved etterlevelse av bestemmelser og vedtak i kommunens økonomiforvaltning på det området vi har foretatt forenklet etterlevelseskontroll.

Vi baserer oppgaven på en risiko- og vesentlighetsvurdering.

Utføring av et attestasjonsoppdrag som skal gi moderat sikkerhet i henhold til RSK 301, innebærer å utføre handlinger for å innhente bevis for at bestemmelser og vedtak for økonomiforvaltningen etterleves. Typen, tidspunktet for og omfanget av de valgte handlingene er gjenstand for revisors skjønn. Moderat sikkerhet har klart lavere sikkerhetsgrad enn betryggende sikkerhet, og vi gir derfor ikke uttrykk for samme nivå av sikkerhet som i en revisjonsberetning.

Vi mener at vi har innhentet tilstrekkelig og hensiktsmessig bevis som grunnlag for vår konklusjon.

Grunnlag for konklusjon

Vi viser til vårt brev til byrådet 14. april 2025 og tilsvaret 19. mai 2025.

Konklusjon med forbehold

Finansbyråden har i sitt tilsvare av 19. mai 2025 gitt en overordnet tilbakemelding på funnene i vår rapport. Han opplever rapporten som ryddig og nyttig, og den vil være et praktisk og godt arbeidsverktøy i videre oppfølging av rutiner og tilganger for IT-systemene som forvaltes i ulike byrådsområder. Han mener at arbeidet de har startet er en god begynnelse som møter flere av revisjonens vurderinger og anbefalinger.

I tilbakemeldingen fra finansbyråden er det ikke gitt konkret tilbakemelding på hvordan funnene i rapporten skal følges opp. Rapporten viser at:

- kommunen har ikke etablert overordnede skriftlige retningslinjer for hvordan tjenesteforvaltere skal administrere roller i og tilganger til IT-systemer.
- det ikke er etablert skriftlige rutiner for oppretting, endring, sletting og jevnlig evaluering av roller i IT-systemene i kommunen for å sikre at rollene er satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet.
- ikke alle rollene for de fem systemene som inngår i undersøkelsen er satt opp med riktig omfang som bidrar til betryggende sikkerhet.
- byggesakskontoret ikke har skriftlige rutiner for hvordan tjenesteforvalter skal administrere tilganger til eByggesak.
- tilgangene til tre av systemene i undersøkelsen ikke har vært satt opp i henhold til prinsippene om minst mulig privilegium.
- tilganger til Visma Velferd og Visma Flyvo ikke evalueres årlig.
- retningslinjer som beskriver hvordan tjenesteforvalter skal ivareta ansvaret for kommunens personopplysninger (GDPR) for sine IT-systemer ennå ikke er implementert.
- det ikke er gitt opplæring i informasjonssikkerhet til tjenesteforvaltere for systemene Visma Velferd, Visma Flyvo, Vigilo og Modulus Barn.
- det for systemene Visma Velferd, Visma Flyvo, Vigilo og Modulus barn ikke er utarbeidet skriftlige rutiner for gjennomgang av loggføring av bruk av systemene. Disse fire IT-systemene inneholder sensitive personopplysninger.

Basert på de utførte handlingene, innhentede bevis og byrådets svar, kan vi ikke konkludere med at kommunen har hatt tilfredsstillende kontroll med roller og tilganger for systemene Flyvo og eByggesak.

Denne uttalelsen er utelukkende utarbeidet for å gi kontrollutvalget et bedre grunnlag for å ivareta sitt påse ansvar med økonomiforvaltningen og til Trondheim kommunes informasjon, og er ikke nødvendigvis egnet til andre formål.

Innholdsfortegnelse

1 Innledning	8
1.1 Bakgrunn	8
1.2 Problemstilling	9
1.3 Revisjonskriterier	9
1.4 Metode	10
2 Styring og kontroll med roller og tilganger	12
2.1 Skriftlige overordnede retningslinjer skal definere hvordan tjenesteforvalter administrerer roller og tilganger	12
2.2 Roller i IT-systemene skal være satt opp i henhold til kommunens behov og med betryggende sikkerhet	12
2.3 Rutiner for tildeling, endring og sletting av tilganger	18
2.4 Tilganger til IT-systemer skal følge prinsippet om minst mulig privilegium.	21
2.5 Jevnlig evaluering av tilganger for å sikre at de er nødvendige og oppdaterte	25
2.6 Opplæring i informasjonssikkerhet og personvern	27
2.7 Loggføring av bruk av IT-systemene skal gjennomgås jevnlig for å avdekke eventuelt misbruk	28
3 Konklusjon	31
4 Byrådets uttalelse	32
5 Uttalelse fra ledelsen	34

1 Innledning

1.1 Bakgrunn

Trondheim kommunerevisjon har de senere årene gjennomført årlige etterlevelseskontroller på IT-området i kommunen. Vår erfaring fra kontakt med tjenesteforvaltere³ i disse etterlevelseskontroller, samt beskrivelse i “Risiko- og sårbarhetsanalyse av IT-området til Trondheim kommune” fra 2022, indikerer at det kan være manglende avklaring og beskrivelse av ansvar for ulike IT-systemer.

Risiko- og sårbarhetsanalysen av IT-området til Trondheim kommune fra 2022 avdekket at mange av de identifiserte svakhetene fra denne analysen ligger utenfor Trondheim Digital⁴ sitt ansvarsområde. Svakhetene ligger innenfor de enkelte virksomhetsområdene⁵ i kommunen. Mange av svakhetene synes å kunne knyttes til funksjonen som tjenesteforvalter og mangelfulle rutiner for, og forventninger til denne funksjonen.

Revisjonens etterlevelseskontroll fra 2023 “Roller og ansvar til tjenesteforvalter, tjenesteeier⁶, virksomhetsområdet og IT-tjenesten” viste at det ikke var klart for tjenesteeierne og virksomhetsområdene hva deres ansvar var for å følge opp tilgangrettigheter til IT-systemene. Vi konkluderte da med at kommunen ikke hadde klare retningslinjer som beskriver hvordan tjenesteforvalter, tjenesteeier og virksomhetsområdene skulle ivareta ansvaret for kommunens personopplysninger (GDPR) for sine IT-systemer.

Vi har i denne undersøkelsen valgt ut fem IT-systemer som brukes ved ulike fagområder som har betydning for økonomi i Trondheim kommune. Systemene er valgt ut på grunnlag av at det er store systemer som har stor grad av sensitiv informasjon og revisjonens erfaring fra tidligere undersøkelser.

³ En tjenesteforvalter er en person som har fagkompetanse knyttet til tjenesteområdet og som har ansvar for den daglige forvaltningen av hele eller deler av et IT-system, herunder å administrere tilganger til IT-systemet. Tjenesteforvalter er et bindeledd på operativt nivå mellom leverandør og kommunen.

⁴ Trondheim kommune sin IT-tjeneste

⁵ Kommunen har åtte virksomhetsområder: Helse- og omsorg, sosiale tjenester, oppvekst og utdanning, byutvikling, finans, miljø, næring og samferdsel, kultur, idrett og friluftsliv og byrådsleders avdeling

⁶ Tjenesteeier: Systemeier, dette er ofte en enhet i Trondheim kommune

1.2 Problemstilling

Prosjektets problemstilling er:

Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemer for å sikre at ansattes rettigheter i systemene er i samsvar med tjenstlig behov og gjeldende regelverk⁷?

Roller som er definert i et IT-system styrer hvilke rettigheter brukeren har i systemet.

Tilganger til et IT-system gis til ansatte med behov.

1.3 Revisjonskriterier

- Kommunen skal ha overordnede skriftlige retningslinjer som definerer hvordan tjenesteforvalter skal utøve sitt ansvar for roller og tilganger.
- Roller i IT-systemene skal være satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet.
- Kommunen skal ha rutiner for tildeling, endring og sletting av tilganger.
- Tilganger til IT-systemer skal følge prinsippet om minst mulig privilegium, brukere skal kun ha tilgang til det de trenger for å utføre sine arbeidsoppgaver.
- Kommunen skal jevnlig evaluere tilganger for å sikre at de er nødvendige og oppdaterte.
- Kommunen bør sørge for opplæring av tjenesteforvaltere i informasjonssikkerhet og personvern.
- Loggføring av bruk av IT-systemer skal gjennomgås jevnlig for å avdekke eventuelt misbruk.

Revisjonskriteriene er utledet fra følgende kilder:

- NSM Grunnprinsipper for IKT-sikkerhet
- Kvaliteket
 - 15741-4, IT-tilganger for ansatte og vikarer i Trondheim kommune
 - 16018-1 Årlig revisjon av tilganger til fagprogram med egen tilgangskontroll i Trondheim kommune
- Lov om behandling av personopplysninger, GDPR artikkel 25 og 32

⁷ Grunnprinsipper NSM, rutiner i Kvaliteket og GDPR

1.4 Metode

Metodisk baserer undersøkelsen seg på dokumentanalyse, spørreskjema og intervju med tjenesteforvaltere. I tillegg fikk vi for fire av systemene en presentasjon av oppsett av roller og tilganger i systemene. Tabellen under viser hvilke datasystemer som inngår i undersøkelsen

Tabell 1: Datasystemer som inngår i undersøkelsen

Systemnavn	IT-systemets oppgaver i kommunen	Antall roller	Antall brukere	Tjenesteeier	Tjenesteforvalter
Visma Velferd	IT-system for utbetalinger av økonomisk sosialhjelp. Saksbehandling og integrasjon mot økonomi- og lønnsystemet.	19 roller	347 brukere	Kommunalsjef sosiale tjenester	Fagleder H&V, Nav Lerkendal
Visma Flyvo	IT-system for utbetaling til flyktninger. Saksbehandling av introduksjonsstønad. Andre ytelser og integrasjon mot økonomisystemet.	11 roller	298 brukere	Kommunalsjef sosiale tjenester	Tjenesteutvikler, Nav Lerkendal
Vigilo	IT-system for administrasjon og kommunikasjon, barnehage og SFO. Utfaktureringskontingent og kostpenger, barnehage og SFO.	41 roller	6 100 brukere	Kommunalsjef skole	Rådgiver II, Stab - Kommunalsjef skole
Modulus barn	IT-system for saksbehandling og barnevernsutbetalinger.	26 roller	499 brukere	Kommunalsjef barne og familietjenesten	Rådgiver II, Stab - Kommunalsjef barne- og familietjenesten
eByggesak	IT-system for saksbehandling og fakturering av byggesaksgebyrer og tilknytningsavgift for VA.	7 roller	109 brukere	Bygningsjef, Byggesakskontoret	Avdelingsleder byggesak, Byggesakskontoret

Visma Velferd

Systemet ble tatt i bruk i 2013 til saksbehandling og utbetaling av sosiale tjenester og benyttes av Trondheim kommune og Nav i fellesskap. Vedtak fattes av de to forvaltningsenhetene Nav Falkenborg og Nav Lerkendal, mens utbetaling av sosiale ytelser gjøres av Sentralt behandlingskontor.

Visma Flyvo

Systemet ble tatt i bruk i 2017 og brukes til saksbehandling av introduksjonssøknad og andre stønader til flyktninger. Deltakere i introduksjonsprogrammet legges inn i lønssystemet på grunnlag av vedtak om introduksjonsstønad. For andre stønader er det integrasjon mot økonomisystemet. Systemet brukes av Flyktningeenheten, Enhet for voksenopplæring og administrasjonen.

Vigilo

Vigilo er et felles system for barnehager og skoler som ble tatt i bruk i 2019. Systemet håndterer hele søknadsprosessen fra foresatte søker om barnehageplass eller plass i SFO via søknadsportalen. I portalen kan foresatte endre og si opp plass. Systemet brukes også til barnehageadministrasjon med oversikt over barn og plasseringer, SFO administrasjon med oversikt over plasseringer per skole og skoleadministrasjon med oversikt over elever, basis- og faggrupper. Kommunikasjon med foresatte i skoler og barnehage gjøres i systemet. Fakturering av barnehage- og SFO-kontingent og moderasjonsbehandling av egenbetaling for barnehage og SFO gjøres i systemet. I Vigilo lages fakturagrunnlag som sendes over til økonomisystemet for fakturering.

Modulus Barn

Fagsystemet for barnevernet, Modulus Barn, ble tatt i bruk i 2023. Systemet brukes til saksbehandling av barnevernsaker og har en økonomimodul. Systemet er integrert mot kommunens økonomisystem og lønssystem. Modulus Barn brukes av Barne- og familietjenesten (BFT), BFT Heimdal, BFT Lerkendal, BFT Østbyen, BFT Midtbyen og BFT Omsorgsenheten.

eByggesak

Fagsystemet eByggesak ble tatt i bruk i 2017 for de som jobber med saksbehandling etter plan- og bygningsloven. Systemet ble tatt i bruk som forsystem for fakturering av byggesaksgebyr i 2023 og er integrert mot kommunens økonomisystem. eByggesak brukes av Byggesakskontoret, Byplankontoret, Enhet for kart og arkitektur, Trondheim Digital og byrådsavdeling for byutvikling.

2 Styring og kontroll med roller og tilganger

2.1 Skriftlige overordnede retningslinjer skal definere hvordan tjenesteforvalter administrerer roller og tilganger

Tjenesteforvaltere for de fem utvalgte systemene kjenner ikke til at det foreligger overordnede retningslinjer for hvordan tjenesteforvalter skal administrere roller og tilganger i kommunens systemer.

Trondheim kommunerevisjon sin etterlevelsesk kontroll for IT i 2023⁸ viste at rutinen "Tjenestestyring av IT-løsninger i Trondheim kommune" er overordnet og ikke beskriver tydelig hvilket ansvar tjenesteforvalter, tjenesteeier og virksomhetsområdet har for IT-systemer. Administrasjonen svarte på rapporten at den aktuelle rutinen ikke var oppdatert. Det er iverksatt arbeid for å oppdatere rutinen. Intranettsidene til [Trondheim Digital](#) viser at rutiner er under arbeid.

Revisjonens vurderinger

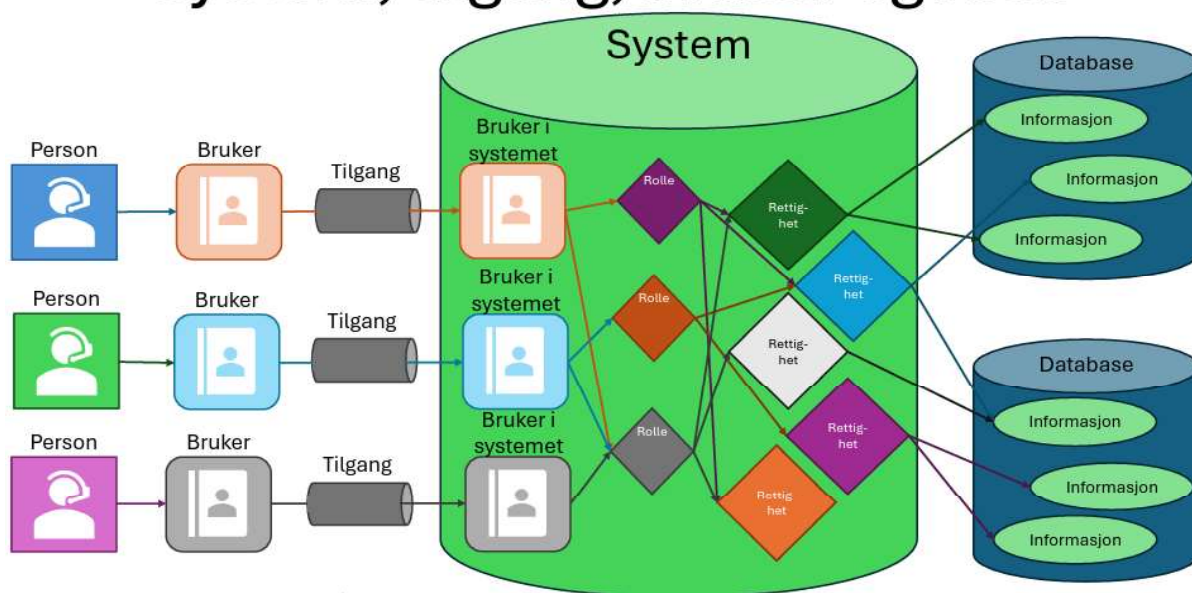
Revisjonen er kritisk til at kommunen ikke har etablert overordnede skriftlige retningslinjer for hvordan tjenesteforvaltere skal administrere roller i og tilganger til IT-systemer.

2.2 Roller i IT-systemene skal være satt opp i henhold til kommunens behov og med betryggende sikkerhet

Roller i IT-systemer definerer hvilke rettigheter brukere får i systemet. Ved implementering av nye IT-systemer er det vanligvis opprettet roller fra leverandørene.

⁸ "Roller og ansvar til tjenesteforvalter, tjenesteeier, virksomhetsområdet og IT-tjenesten". Behandlet i kontrollutvalget 08.04.2024, sak 12/24

System, tilgang, bruker og rolle



Kilde: Trondheim kommunerevisjon

Forklaring på figur:

En person er nyansatt i kommunen eller det kommer en konsulent som skal få opprettet en bruker i Trondheim kommunes intranett (TK-nett). Bruker er da den identiteten den ansatte/konsulenten får i TK-nettet. Basert på informasjon fra autorisert bestiller⁹ kan IT-brukerhjelp opprette en tilgang i det aktuelle IT-systemet. Den ansatte/konsulenten får da opprettet en bruker i systemet. For at man skal kunne se data eller utføre noe i systemet, må tjenesteforvalter legge til en eller flere roller til den ansattes/konsulentens bruker. Det er disse rollene som gir den ansatte/konsulenten rettigheter til å se data eller utføre oppgaver i IT-systemet. Alle data og informasjon i systemet ligger lagret i databaser. Tildelte roller gir brukeren tilgang til rettighetene de skal ha for å kunne utføre sin jobb i kommunen. Rollene i IT-systemer skal settes opp i henhold til kommunens behov og sikre at ansatte kun får tilgang til den informasjonen og de funksjonene de trenger for å utføre jobben sin. Roller skal være utformet slik at de sikrer at kommunen overholder lover og regler for informasjonssikkerhet og personvern. Det er derfor viktig å ha rutiner for håndtering og jevnlig evaluering av roller.

Tidlig i undersøkelsen ble det klart at det ikke er etablert skriftlige rutiner for håndtering av roller for de fem utvalgte IT-systemene. På bakgrunn av dette har vi sett på praksisen for administrering av roller og tilganger. Undersøkelsen viser at praksisen har vært ulik for de fem utvalgte systemene.

Revisjonen har ved tidligere gjennomgang av IT-systemer sett at noen roller har for vide rettigheter. Dette kan medføre risiko for at det blir utført handlinger som man ikke har fullmakt til og at man får innsyn i informasjon man ikke har behov for i sin stilling. Revisjonen har derfor valgt å se på hvordan roller er satt opp i de fem utvalgte IT-systemene. I tabellen

⁹ Autorisert bestiller: Person (ofte en enhetsleder) med fullmakt til å bestille tilgang til IT-systemer for sine ansatte.

under har vi oppsummert om rollene i systemene er satt opp i henhold til behov og betryggende sikkerhet.

Tabell 2: Er rollene i systemene satt opp i henhold til behov og riktig omfang som bidrar til betryggende sikkerhet?

Systemnavn	Ja / Nei	Kommentar
Visma Velferd	Usikker	Alle på samme enhet kan se samtlige saker og vi er usikker på om dette er betryggende sikkerhet
Visma Flyvo	Nei	De mest brukte rollene har alt for mange rettigheter.
Vigilo	Ja	Oppsettet av roller og nivå er i samsvar med tjenesteområdets behov.
Modulus barn	Ja	Oppsettet er satt opp i samsvar med tjenesteområdets behov.
eByggesak	Nei	Innsynsrollen har hatt registreringstilgang og saksbehandlerrolle har hatt mulighet for å godkjenne på ledernivå.

Kilde: Revisjonens analyse av oppsetting av roller basert på svar fra tjenesteforvaltere

Visma Velferd

Tjenesteforvalter opplyser at systemet er satt opp fra leverandør med de rollene som systemleverandør mener er riktig. Trondheim kommune har justert disse rollene slik at de er tilpasset kommunen sine behov og rutiner. Rollene er basert på de oppgaver som brukerne/ansatte skal utføre i systemet.

Tjenesteforvalter med team har ikke detaljkunnskap om roller og har ikke egne meninger rundt behov for roller. Tjenesteforvalter ser ikke behov for å endre, slette eller opprette nye roller i systemet. Det tas derfor ingen løpende vurderinger av de rollene som eksisterer.

Tjenesteforvalter opplyser at det er satt begrensinger slik at de ansatte kun ser de sakene som tilhører deres enhet. Trondheim kommune er delt mellom kontorene Nav Falkenborg og Nav Lerkendal. Systemet er gammelt og har sine begrensinger. Rollene er satt opp i henhold til arbeidsoppgaver og er begrenset etter hvilken stilling de ansatte har.

Revisjonen har, av tjenesteforvalter, fått presentert hvordan roller er bygd opp og hvilke rettigheter som er knyttet til ulike roller i fagsystemet. Presentasjonen avdekket ingen unormale roller eller rettigheter i roller.

Visma Flyvo

Systemet Flyvo benyttes av de to enhetene Flyktingetjenesten og Voksenopplæringen. Tjenesteforvalter opplyser at Flyvo er satt opp med roller fra systemleverandør. Disse rollene er basert på små kommuner, der det er få ansatte og mindre arbeidsdeling enn det Trondheim kommune har. Systemet er bygd opp hierarkisk¹⁰ fordi systemet skal kunne benyttes ulikt for de to enhetene. Dette betyr at brukere med samme rolle kun får rettighet innen sin egen enhet. Selv om roller er satt opp likt, får de ikke tilgang til samme funksjonalitet i systemet. Det er det overbygde hierarkiet som bestemmer hvilke rettigheter

¹⁰ Hierarki: Systemet er satt opp basert på brukere/tilgang, roller og enhet. Enhet bestemmer hvor du kan hente informasjon fra og rollen bestemmer hvilken informasjon du kan hente eller registrere.

de enkelte brukerne får i systemet på grunnlag av den rollen de er tildelt. Hierarkiet er satt opp fra leverandør og tjenesteforvalter er ikke kjent med hvordan dette er satt opp. Det vi si at ansatte som er tildelt samme rolle er gitt tilgang til ulike deler av systemet, basert på hvilken enhet de ansatte jobber i.

Tjenesteforvalter opplyser at roller endres i henhold til beskjed fra enhetene. Disse endringene har ikke vært vurdert opp mot behov for å opprette nye roller. Tjenesteforvalter har kun vært utførende og har ikke en funksjon med å vurdere behov for roller.

Det er ansatt en ny tjenesteforvalter i 2024 som har fått opplæring av tidligere tjenesteforvalter. Ny tjenesteforvalter mener det er stor usikkerhet om hvordan rollene faktisk fungerer. Tjenesteforvalter opplyser at rollene som er satt opp i systemet skal være basert på de oppgavene som brukerne skal utføre i systemet. Tjenesteforvalter ser imidlertid at rollene som er satt opp har alt for vide rettigheter i forhold til arbeidsoppgavene til de ansatte. Det er også satt koblinger på enkelte roller til andre roller. Det er uklart for tjenesteforvalter hvordan disse koblingen fungerer i praksis. Konsekvensen av dette er at enkelte har fått tilgang til flere roller og dermed for store rettigheter i systemet. Det er uklart for tjenesteforvalter hvem som har opprettet disse koblingen og hva som har vært hensikten med koblingene. Tjenesteforvalter opplyser at disse koblingene skal slettes, men det er feil i Visma Flyvo som leverandøren arbeider med å finne ut av før korrigeringen kan gjennomføres.

Revisjonen har fått presentert fagsystemet av tjenesteforvalter knyttet til de seks viktigste rollene av de elleve rollene fagsystemet har. I Flyvo har rollen "saksbehandler" en rettighet mer i systemet enn det rollen "superbrukere" har. Revisjonen fikk under presentasjonen av systemet se at det var superbrukere som hadde fått tildelt rollen som saksbehandler og at flere merkantile også var tildelt rollen som saksbehandler. For saksbehandlerrollen var det knyttet alt for mange rettigheter til rollen slik at tilgangen gir den ansatte rett til å utføre flere oppgaver enn det stillingen gir rett til. Vi fikk se at 22 aktive brukere var tildelt rollen admin¹¹, hvorav en av brukerne skulle vært slettet.

Det er uklart for tjenesteforvalter hvordan prosessen for endringer i roller skal være, det vil si hvem som skal være en del av prosessen med vurdering og gjennomføring av endringer og eventuelt opprettelse av nye roller. Systemet driftes av Sopra Steria som er en driftsleverandør til Trondheim Digital. Tjenesteforvalter opplyser at de må etablere en rutine for hvordan endringer skal meldes og gjennomføres.

Vigilo

Systemet Vigilo brukes av alle skoler, barnehager og administrasjonen i kommunen, det er mange brukere av systemet. For å sikre at informasjon begrenses, er det opprettet mange roller i systemet. Tjenesteforvalter opplyser at systemet er satt opp av leverandøren med 41 roller. Rollene er satt opp etter tjenestlig behov. Noen roller i Vigilo er tilpasset til bruk i barnehager, og andre roller er tilpasset til bruk i skoler.

Det finnes overordnede roller i systemet slik som rollene "Kommuneadministrator" og "Kildedata - Kommuneforvaltning". I disse rollene kan man administrere brukere og

¹¹ Rollen admin: I denne rollen ligger det utvidede rettigheter som bør begrenses til et absolutt minimum av brukere.

kildedata. De som har mulighet til å legge inn endringer av faste data, er kommuneadministrator, barnehageleder og SFO-leder. Det er en egen rolle som har rettigheter til moderasjonsbehandling av kontingent for SFO og barnehage som heter "Saksbehandler for redusert betaling".

Det er elleve personer som har kommuneadministratorrollen, åtte i kommunen og tre hos leverandør. I tillegg til tjenesteforvalter har flere i praksisteamet denne rollen i kommunen. Åtte personer i kommunen og fire personer hos leverandøren innehar rollen "Kildedata - Kommuneforvaltning". Rollene "Kommuneadministrator" og "Kildedata - Kommuneforvaltning" har rettighet til å vise konfidensielle adresser.

Etter revisjonens gjennomgang har praksisteamet tatt kontakt med leverandøren av systemet for å få vurdert om disse oppgavene kan ivaretas med andre roller. De har også vurdert om leverandøren kan ivareta kommunens behov for support med færre personer med rollen som kommuneadministrator. De har endret rollen "Kildedata kommuneforvaltning" til "Globalt barn- og elevsøk". Dette innebærer at færre personer kan få innsyn i konfidensielle adresser.

Tjenesteforvalter opplyser at det ikke har vært vurdert å begrense innholdet i rollene. Vurderinger har i større grad handlet om hvilken rolle som er hensiktsmessig ut fra den enkeltes arbeidsoppgaver og behov.

Tjenesteforvalter opplyser at det er leverandøren som kan opprette eller endre roller i systemet. Kommunen kan bestille roller ut fra sine behov. Tjenesteforvalter har et team "praksisfellesskap" som vurderer roller. Grunnlaget for å opprette eller endre eksisterende roller er ut fra tjenestelige behov slik at de dekker behovene for den enkelte brukergruppe. Mange roller på skole og barnehage er tilpasset behovet på enhetene. Mange av rollene må kombineres for å få riktig tilgangsnivå. De har ikke vurdert å opprette flere roller da behovene er dekket av de rollene som de har fått tilgang til fra leverandøren. Tjenesteforvalter opplyser at de ikke har hatt mistanke om at det har vært misbruk av roller i systemet. De har logging på innsyn i all sensitiv informasjon og kan dermed se hvem som har sett på sensitiv informasjon.

Modulus barn

Systemet Modulus barn ble tatt i bruk av barnevernet i 2023. Tjenesteforvalter opplyser at rollene i Modulus Barn er satt opp i henhold til en rollematrise med begrensninger på hva brukeren kan se. Systemet er bygd opp hierarkisk, slik at alle roller som settes opp i systemet har begrensninger som fastsettes av hierarkiet. I tillegg kan det settes opp begrensninger på enkelte rettigheter i roller. I enkelte roller er det lagt inn en begrensning slik at det kun gis tilgang til egne saker, enhetens saker eller egne og teamets saker. Roller er satt opp i henhold til hva som er behovet til Trondheim kommune basert på arbeidsoppgaver og arbeidsdeling. Modulus Barn er et nytt system som har et mer moderne programmeringsgrensesnitt¹², hvor det er enklere å sette begrensninger for hva enkelte brukere

¹² Programmeringsgrensesnitt er de metoder og tilhørende parametre (grensesnitt) som en applikasjon kan benytte i en annen applikasjon eller tjeneste. Applikasjon er programvare som benytter datamaskinens ressurser til en oppgave som brukeren ønsker utført.

kan få rettighet til. Tjenesteforvalter opplyser at rettigheter i roller er under løpende vurderinger og endringer gjøres når behov endres.

Tjenesteforvalter opplyser at det er hun som løpende vurderer om det er behov for endring av eksisterende roller eller om det må opprettes nye. Denne vurderingen baserer seg på informasjon fra ledere i kommunen. Systemet ble tatt i bruk i 2023 og man ser at det er behov for noen endringer eller oppretting av nye roller. Dette er ikke gjennomført pr i dag.

eByggesak

Systemet eByggesak ble tatt i bruk til saksbehandling av byggesaker i kommunen i 2017.

Tjenesteforvalter opplyser at det er systemadministrator/e-Team¹³ ved byggesakskontoret og dedikerte ansatte hos leverandør TietoEvry som kan opprette eller endre roller i eByggesak. Det skal ifølge tjenesteforvalter i utgangspunktet ikke rokkes ved rollene i systemet. Dersom kommunen skal endre roller, viser Tieto Evry hvordan systemadministrator kan endre dette selv. Tieto Evry kan gjøre endringer i roller etter forespørsel fra Trondheim kommune. Disse endringene logges.

Tjenesteforvalter opplyser at de i dag ikke har full oversikt over hvilke rettigheter som ligger i rollene i eByggesak. De mener at flere av rollene i systemet er for overlappende.

Tjenesteforvalter oppgir at "saksbehandlerrolle" i systemet har hatt mulighet for å godkjenne dokumenter som skal kreve "lederrolle". Alternativt at brukeren blir satt opp på ei liste over personer som skal ha mulighet til å godkjenne dokumenter. Denne feilen i rollen ble oppdaget da en saksbehandler på forespørsel fra en leder, fikk til å godkjenne et dokument som krevde ledergodkjenning. Det ble foretatt flere tester på andre saksbehandlere som også fikk til å godkjenne slike dokumenter. Feilen i rollen ble innrapportert til leverandøren TietoEvry. Det ble gjennomført testing på denne feilen den 23.01.25 i samarbeid med TietoEvry og man fant da ut hva som, rent teknisk, var problemet. Feilen er ifølge systemadministrator ikke korrigert per februar 2025.

Revisjonen fikk i møte med tjenesteforvalter 4.11.24 opplyst at de hadde oppdaget at rollen "Innsyn" i eByggesak også har hatt skrivetilgang. Rollen innsyn har derfor i realiteten vært en saksbehandlerrolle. Det står i den nasjonale kravspesifikasjonen til eByggesak at det skal være en innsynsrolle i systemet som ikke har registreringsmulighet. Tjenesteforvalter og systemadministrator opplyser at de ikke vet når eller hvorfor rollen har blitt endret. Trondheim kommune har ikke ønsket eller bedt om en slik endring. Risikoen ved at brukere med innsynsrolle har hatt skrivetilgang er at de dermed kunne se interne notater som skrives ved Byggesakskontoret som ikke skulle være tilgjengelige. Ansatte kunne derfor ifølge tjenesteforvalter blitt utsatt for utilbørlig press underveis i en byggesaksbehandling. Vi har fått opplyst fra systemadministrator at denne feilen er korrigert i systemet i januar 2025.

Det er ifølge tjenesteforvalter noen roller i eByggesak som ikke er i bruk. Tjenesteforvalter opplyser at det er rot i systemet og at de står overfor en ryddejobb der de ønsker å begrense roller og rettigheter i eByggesak.

¹³ E-Team er fire personer ved byggesakskontoret, tjenesteforvalter, systemadministrator og to personer som er systemstøtte og reserve for systemadministrator.

Revisjonens vurderinger

Revisjonen anbefaler at byråden vurderer om det bør etableres skriftlige rutiner for oppretting, endring, sletting og jevnlig evaluering av roller i IT-systemene i kommunen for å sikre at rollene er satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet.

Revisjonen er usikker på om roller i Visma Velferd er satt opp med riktig omfang som bidrar til betryggende sikkerhet. Vi ber byråden vurdere om rollene i systemet er satt opp med betryggende sikkerhet.

Revisjonen er kritisk til at roller i Visma Flyvo ikke er justert slik at de er tilpasset behovet til Trondheim kommune. Brukere kan ha mulighet til å gjøre endringer som de ikke skal ha tilgang til i tråd med sin stilling. Revisjonen anbefaler at roller knyttet til Flyvo gjennomgås og evalueres.

Revisjonen mener at rollene i Vigilo og Modulus Barn er satt opp i henhold til kommunens behov og med betryggende sikkerhet. Det gjøres jevnlig evalueringer av roller i disse systemene. I Vigilo er det gjort endringer i rollen "Kildedata kommuneforvaltning" som begrenser rettigheter til å se konfidensielle adresser.

Revisjonen er kritisk til at "saksbehandler-rollen" og rollen "Innsyn" i eByggesak har hatt større rettigheter i systemet enn det som var forutsetningen. Den interne kontrollen rundt systemet eByggesak har vært undergravet på grunn av at roller i systemet har hatt for store rettigheter. Revisjonen anbefaler at alle rollene i eByggesak gjennomgås for å sikre at rettighetene i rollene er i samsvar med de ansattes fullmakter. Vi har fått opplyst at rollen "Innsyn" er korrigert i 2025.

2.3 Rutiner for tildeling, endring og sletting av tilganger

I henhold til NSM Grunnprinsipper punkt 2.6 er det viktig at kommunen har retningslinjer for tilgangskontroll. Kommunen skal ha retningslinjer som sikrer at kun autoriserte personer har tilgang til IT-systemene.

Vi har stilt tjenesteforvalterne spørsmål om de har rutiner for tildeling, endring og sletting av tilganger for de fem systemene som inngår i denne undersøkelsen.

Tabell 3: Rutiner for tildeling, endring og sletting av tilganger

Systemnavn	Ja / Nei	Kommentar
Visma Velferd	Ja	Bestilles via Selvbetjeningsportalen. Enheten bestemmer.
Visma Flyvo	Ja	Bestilles via Selvbetjeningsportalen. Enheten bestemmer
Vigilo	Ja	Tilgang på ledernivå tildeles av tjenesteforvalter etter forespørsel i Selvbetjeningsportalen. Forvaltningen ¹⁴ administrerer roller til private barnehager og spesped-nettverkene i barnehagene. Enhetene på skoler og barnehager tildeler og fjerner ansatt-roller.
Modulus barn	Ja	Bestilles via Selvbetjeningsportalen.
eByggesak	Nei	Har ikke autorisert bestiller og bruker ikke skjema

Kilde: Revisjonens analyse basert på svar fra tjenesteforvaltere

Trondheim kommune har egne rutiner knyttet til registrering av ansatte/vikarer/brukere som skal koble seg på TK-nettet. Ansatte som skal ha tilgang til IT-systemer i Trondheim kommune må først få opprettet en bruker i TK-nettet. Rutinen for å få opprettet bruker i TK-nettet er at den nye brukeren først må registreres i HR-portalen¹⁵ av egen enhet. Alle tilganger til applikasjoner for ansatte i Trondheim kommune gis av IT-brukerhjelp gjennom Active Directory (AD¹⁶) til godkjente identiter.

Når det er gjort, kan autorisert bestiller¹⁷ bestille tilgang til TK-nettet via "Selvbetjeningsportalen" på intranett. Det er egne skjema som skal benyttes for ulike forhold, som autorisert bestiller må fylle ut. Dette gjelder både for nye ansatte/vikarer/endring av stilling og for de som slutter enten i Trondheim kommune eller vikarbyrå/Nav. Det er også utarbeidet egne rutiner for å håndtere tilganger til leverandørbruker¹⁸ i TK-nettet. Det er egne rutiner knyttet til Nav-ansatte, både de som er ansatt i kommunen og de i staten. Autorisert bestiller ved Nav-kontor/offentlig servicekontor kan opprette skjema på disse i Selvbetjeningsportalen.

Visma Velferd og Visma Flyvo

Tjenesteforvalter opplyser at når den ansatte har fått brukeridentitet i HR-portalen, kan autorisert bestiller sende skjema i Selvbetjeningsportalen. Med bakgrunn i sendt skjema oppretter IT-brukerhjelp tilgang til systemet. Da er bruker opprettet med tilgang til systemet, men har ikke mulighet til å få sett eller gjort noe i systemet. IT-brukerhjelp må sende bestillingen videre til aktuelle tjenesteforvaltere for å tildele roller til det aktuelle systemet.

¹⁴ Forvaltningen: Består av tjenesteforvalter og sitt praksisteam knyttet til systemet Vigilo.

¹⁵ HR-portalen: Er en nettportal for ansatte med direkte tilgang til lønn- og HR-relaterte oppgaver. Den delen av lønnsystemet som ansatte og enheter daglig benytter.

¹⁶ Active Directory (AD) er en kritisk applikasjon i tilgangshåndteringen i Trondheim kommune. På grunnlag av bestillingsskjema for tilganger fra autorisert bestiller kobler IT-brukeradministrasjon den nye identiteten i AD til de applikasjonene som er bestilt for den nyansatte. For at ny ansatt skal kunne få utført noe i applikasjonen, sender IT-brukeradministrasjonen e-post til tjenesteforvalter for at de skal sette på aktuelle roller iht bestilling fra autoriserte bestillere.

¹⁷ Autorisert bestiller: Person (ofte en enhetsleder) med fullmakt til å bestille tilgang til IT-systemer for sine ansatte.

¹⁸ Leverandørbruker: Ansatte fra leverandøren av IT-systemet som har tilganger i systemet.

Samme rutine gjelder også for Nav ansatte. De må registreres i HR portalen for å kunne få en e-postadresse som benyttes for å kunne gi vedkommende tilgang til ulike systemer. Tjenesteforvalter opplyser at de gir tilgang til den rollen som autorisert bestiller har oppgitt i skjema. Det gjøres ingen selvstendig vurdering av om det er riktige roller som tildeles brukeren.

Tjenesteforvalter opplyser at det hender at melding ikke blir videresendt fra IT-brukerhjelp når en person slutter i kommunen. Disse personene er likevel tatt ut av TK-nettet og har ikke lengre tilgang til kommunal pc og vil derfor ikke kunne logge seg på systemene.

Vigilo

Tjenesteforvalter opplyser at forvaltningen¹⁹ legger føringer for hvilke roller og rettigheter en ansatt skal ha. Skoler og barnehager tildeler og fjerner ansattroller selv. Forvaltningen tildeler lederroller og roller til ansatte i private barnehager. Kommunikasjon om dette går på e-post siden private barnehager ikke har tilgang til Selvbetjeningsportalen. I tillegg administrerer forvaltningen roller i forbindelse med de spesialpedagogiske nettverkene til barnehagene. Tilgang på ledernivå forøvrig tildeles av forvaltning gjennom Selvbetjeningsportalen.

Tjenesteforvalter med team oppgir at de har formidlet retningslinjer for tilganger til de ulike skolene og barnehagene i forbindelse med opplæring i systemet. På skolesiden er det viktig å vite at det å ha en rolle som ansatt ikke automatisk gir tilgang til elevopplysninger. De ansatte må i tillegg ha en knytning i systemet til eleven via timeplan eller en elevgruppe.

Tjenesteforvalter opplyser at kriteriene som legges til grunn for tildeling av tilgang til systemet er utfra tjenstlige behov. Tilganger registreres i en totalrapport over alle personer i systemet.

Modulus Barn

Tjenesteforvalter opplyser at det er autoriserte bestillere som melder inn nye personer, endringer i tilganger og personer som slutter via Selvbetjeningsportalen. Ut fra disse opplysninger gjøres det endringer av tilganger til systemet.

Vi har fått opplyst fra tjenesteforvalter at når det gjelder nye tilganger eller endringer i tilganger for ansatte som skal jobbe i Modulus Barn, får tjenesteforvalter videresendt aktuelt skjema fra IT-brukerhjelp. Dette er en manuell jobb som kan glippe. Ut fra opplysninger i skjema, foretar tjenesteforvalter innmelding eller endring i tilgang i henhold til ny stilling for den ansatte ut fra de roller som er opprettet. Det er tjenesteforvalter som bestemmer hvilke roller den enkelte får tilgang til.

eByggesak

Byggesakskontoret har ikke skriftlige rutiner for hvordan tjenesteforvalter skal administrere tilganger til systemet eByggesak. For eByggesak bruker Byggesakskontoret ikke autorisert bestiller og ikke skjema ved bestilling av tilganger. Systemadministrator foreslår hvilke tilganger ansatte skal ha til eByggesak, og tjenesteforvalter godkjenner disse. Det er tjenesteforvalter og systemadministrator som legger inn tilgangene i systemet. Endringer i brukernes eksisterende tilganger utføres av systemadministrator i samarbeid med

¹⁹ Forvaltningen: Består av tjenesteforvalter og praksisteam knyttet til systemet Vigilo.

tjenesteforvalter. Grunnlaget for å opprette eller endre eksisterende tilganger er endrede oppgaver og oppdateringer ved avgang og ansettelser.

Tilgangene tildeles til brukerne i administrasjonssystemet i eByggesak. Det er utarbeidet et regneark som viser en oversikt over ansatte som har tilgang til eByggesak med en beskrivelse av hvorfor brukerne skal ha hvilke tilganger.

Byggesakskontoret er ikke fornøyd med sikkerhetsnivået i eByggesak, og de har en dialog med leverandøren om saken.

Revisjonens vurderinger

Revisjonen mener at for systemene Visma Velferd, Visma Flyvo, Modulus Barn og Vigilo er det rutiner for håndtering av tilganger via Selvbetjeningsportalen. Det hender at mail blir avglemt sendt fra IT-brukerhjelp til tjenesteforvalter, men det har ingen kritisk konsekvens.

Byggesakskontoret benytter ikke Selvbetjeningsportalen med autorisert bestiller og skjema for eByggesak. De har heller ikke skriftlige rutiner for hvordan tjenesteforvalter skal administrere tilganger til eByggesak. Revisjonen mener byggesakskontoret bør vurdere om det skal etableres skriftlige rutiner for administrering av tilganger til eByggesak.

2.4 Tilganger til IT-systemer skal følge prinsippet om minst mulig privilegium.

I henhold til NSM sine grunnprinsipper pkt 2.6 skal det være etablert retningslinjer for tilgangskontroll. Retningslinjene bør følge prinsippet om minst privilegium.

Som tidligere beskrevet i punkt 2.1 - 2.3 i denne rapporten mangler Trondheim kommune skriftlige rutiner for de fem fagsystemene som inngår i denne undersøkelsen.

I tabellen under har vi oppsummert om tilgangene til IT-systemene følger prinsippet om minst mulig privilegium.

Tabell 4: Følger tilgangene til IT-systemene prinsippet om minst mulig privilegium?

Systemnavn	Ja /Nei	Kommentar
Visma Velferd	Nei	Ansatte har tilgang til alle saker på sin enhet, som enten er Nav Falkenborg eller Nav Lerkendal
Visma Flyvo	Nei	Flere brukere har fått tilgang til roller som har store rettigheter, og flere personer har fått tilgang til flere roller. Det er ingen kontroll i systemet av uforenelige roller
Vigilo	Ja	Praksisteamet har redusert hvor mange som har tilgang til rollen kommuneadministrator og kildedata kommuneforvaltning
Modulus barn	Ja	Ikke lenger godkjennerrolle til avdelingsleder

eByggesak	Nei	For mange ansatte har hatt tilgang til systemet. På grunn av at innsynsrollen har hatt registreringstilgang og saksbehandlerrollen har kunnet godkjenne saker på ledernivå har tilgangen til eByggesak ikke vært i henhold til minste privilegium
-----------	-----	---

Kilde: Revisjonens analyse basert på svar fra tjenesteforvaltere

Visma Velferd

Tjenesteforvalter opplyser at ansatte får tilgang til systemet basert på hva som er registrert i HR-portalen, knyttet til stillingskode og hvilken enhet de er ansatt i. De kan ikke logge seg på systemet uten å benytte kommunal PC. I tillegg opprettes det tilgang til ansatte i Nav som behandler saker i Velferd. Nav-ansatte får en rolle knyttet til sin stilling. Deres rolle er å behandle saker og fatte vedtak. Sentralt behandlingskontor foretar alle utbetalinger og eventuelt endrer kontonummer til mottakere av økonomisk sosialhjelp. Dette sikrer fire øyne prinsippet. Det er tre administratorer som gir tilganger basert på hva som er innmeldt fra autoriserte bestillere i Selvbetjeningsportalen.

Ansatte med tilgang til Visma Velferd får tilgang til alle saker på sin enhet, det er ingen begrensning til bare saker de selv jobber med.

Visma Flyvo

De elleve rollene i systemet Flyvo har for vide rettigheter. I tillegg har en del brukere fått tilgang til flere roller.

Ansatte får tilgang til systemet basert på hva som er registrert i HR-portalen, knyttet til stillingskode og hvilken enhet de er ansatt i. De kan ikke logge seg på systemet uten å benytte kommunal PC, med unntak av sju personer som har tilgang via Singel Sign On. Flyvo har for få roller til det som er behovet for Trondheim kommune. I tillegg har flere ansatte fått tildelt flere roller. Enkelte roller har vært koblet sammen med andre roller. Dette har medført at enkelte har fått altfor mange rettigheter i forhold til sin stilling. Kobling mellom roller er uheldig og tjenesteforvalter ønsker å få fjernet denne koblingen. Tjenesteforvalter sier det er uheldig at flere roller har rettighet til å endre bankkontonummer for utbetalinger til brukere.

Tjenesteforvalter vil ta kontakt med Trondheim Digital og eventuelt Sopra Steria/Visma Flyvo²⁰ for å få avklart hvordan de best kan få endret koblinger slik at det ikke blir problemer for brukerne.

Vigilo

Tjenesteforvalter opplyser at tilganger til roller tildeles ut fra tjenstlig behov. Forvaltningen som består av tjenesteforvalter med praksisteam ønsker å tildele tilganger på et så lavt nivå som mulig for at den enkelte ansatte skal få utført sine arbeidsoppgaver i systemet. Dersom det er personer som har mer spesielle behov, gjøres det individuelle vurderinger basert på de enkeltes behov. En vurderer da hvilke roller og kombinasjoner av roller som er nødvendige.

²⁰ Visma Flyvo driftes av driftsleverandøren Sopra Steria for kommunen som også drifter AD løsningen for kommunen.

Revisjonen har stilt spørsmål til tjenesteforvalter om hvorfor så mange personer i kommunen og hos leverandøren må ha tilgang til rollene "kommuneadministrator"²¹ og "kildedata kommuneforvaltning". Tjenesteforvalter svarer at noen ansatte har behandlet spørsmål rundt skoletilknytning og skoleskyss for barn og har derfor hatt behov for å kunne se adresser. Etter revisjonens gjennomgang er antall brukere med tilgang til rollen kommuneadministrator redusert fra 11 til sju. Dette innebærer at færre personer kan få innsyn i konfidensielle adresser.

Tjenesteforvalter opplyser at det finnes noen upersonlige tilganger i Vigilo. Dette er dedikerte brukerroller som har svært begrensede rettigheter. RobotRoger²² er eksempel på en upersonlig tilgang som utfører moderasjonsbehandling.

Modulus barn

Modulus barn er et nytt system i kommunen. Tjenesteforvalter opplyser at ved igangsetting av systemet, ble det gitt tilgang til flere roller enn behovet til enkelte ansatte skulle tilsi. Etter at oppstartsfasen var over, var det meningen at tilgang til enkelte roller skulle fjernes.

I årsbrev fra Regnskapsrevisjonen 2023²³ "punkt 3 Modulus Barn" stilte revisjonen spørsmål ved om det var for mange som hadde anvisningsmyndighet på økonomisk ramme²⁴. Tjenesteforvalter begrunnet dette med at det var nødvendig i forbindelse med oppstart av systemet. I svaret fra administrasjonen på revisjonens årsbrev skriver administrasjonen at de har hatt en gjennomgang av tilganger til godkjenning av økonomiske rammer. De svarte at det i hovedsak er barnevernsledere og kontorfaglig personell som godkjenner økonomiske rammer. Avdelingsledere/ teamledere innenfor barnevern, som er 44 personer, håndterer ikke økonomi i sine oppgaver. Tjenesteforvalter svarte på årsbrevet at de vurderte muligheten for å splitte opp avdelingslederrollen slik at de får skilt ut godkjenning av økonomiske rammer til kun de som har behov for dette. Etter revisjonens møte med tjenesteforvalter høsten 2024 er dette endret slik at avdelingsledere ikke lenger har godkjenningsfullmakt for økonomiske rammer.

eByggesak

Byggesakskontoret har hatt en risikogjennomgang og gjort en selektiv vurdering av behovet for tilgang til systemet eByggesak. Det er deres vurdering at de fleste som ikke er ansatt ved Byggesakskontoret kan finne tilstrekkelig informasjon om byggesaker ved å benytte kommunens innsynsløsning²⁵. Tjenesteforvalter har derfor i 2024 avviklet tilganger til eByggesak for brukere utenfor Byggesakskontoret som ikke har tilstrekkelig argumentasjon for hvorfor de trenger tilgang til systemet. Tidligere var det 210 personer som hadde tilgang til eByggesak. Etter Byggesakskontorets reduksjon av tilganger er det 109 personer som har tilgang. En utfordring med denne reduksjonen av tilganger for de som har mistet den, er at kommunens innsynsløsning ikke er oppdatert.

²¹ Kommuneadministrator: En overordnet rolle i systemet Vigilo som er begrenset til tjenesteforvalter og deres praksisteam.

²² RobotRoger er et dataprogram som automatiserer arbeidsoppgaver.

²³ Årsbrev Regnskapsrevisjon 2023: Revisjonens årlige rapportering av funn i regnskapsrevisjonen.

²⁴ En Økonomisk ramme opprettes under et vedtak og spesifiserer periode og omfang av tiltaket.

²⁵ Innsynsløsning: Digital innsynsløsning over bygg og plan på kommunens nettsider.

Vi har fått opplyst at i forbindelse med at mange brukere ble fratatt tilgangen til eByggesak ble det sendt ut en orientering om at sikkerhetsnivået i systemet ikke var tilstrekkelig ivarettatt. Utfordringen har som tidligere nevnt vært at roller i systemet har hatt for store rettigheter. De som har fått tilbake tilgangen i ettertid, har fått skriftlig beskjed om hva de har tillatelse til å gjøre og ikke gjøre inne i systemet. Det har også vært gjennomført ekstra opplæring av ansatte i kommunen som på forespørsel har fått tilbake tilgangen til eByggesak. Etter det vi har fått opplyst jobbes det sammen med leverandøren Tieto Evry med å få løst problemet.

For andre enn ansatte ved Byggesakskontoret skal de ifølge tjenesteforvalter være strengere med tilganger til eByggesak. Tildeling av tilganger til eByggesak dokumenteres i et regneark der det er beskrevet hvorfor brukerne skal ha tilgang til hvilke roller. Tjenesteforvalter får i samarbeid med TietoEvry en oversikt i TQM²⁶ som viser hvilke endringer som er gjort i tilganger og i systemet.

Det er kun systemleverandøren som har upersonlig tilgang til systemet som servicebrukere på håndtering av automatiske prosesser. Dette er oppgaver som ikke kan utføres av byggesakskontoret. Dersom kommunen ønsker endringer i systemet må dette bestilles via Tieto Evrys ServiceNow²⁷. Byggesakskontoret har ikke redigeringstilgang på det overordnede systemnivået i eByggesak. De kan kun gjøre små tilpasninger som systemadministrator og noen få ressurspersoner kan iverksette.

Revisjonens vurderinger

Revisjonen mener byrådet bør vurdere om rettigheter i Visma Velferd burde vært begrenset til den enkelte ansattes behov for å få utført sin jobb. Systemet er i dag satt opp slik at alle ansatte har tilgang til alle saker på sin enhet.

Revisjonen er kritisk til at tilganger til systemet Visma Flyvo ikke er i henhold til behovet for kommunen og minst mulig privilegium. Vi anbefaler at byrådet foretar en gjennomgang av tilganger til Visma Flyvo for å sikre at tilganger er i henhold til minst mulig privilegium.

Vi mener at tilganger i systemene Vigilo og Modulus Barn, etter endringer, er satt opp med minst mulig privilegium.

Det er uheldig at unødvendig mange ansatte i Trondheim kommune har hatt tilgang til eByggesak. Dersom kommunens innsynsløsning på nett hadde vært oppdatert, kunne denne vært et alternativ for mange av brukerne utenfor Byggesakskontoret. Det er spesielt uheldig at så mange ansatte har hatt tilgang til eByggesak samtidig som rollen "Innsyn" i systemet har hatt registreringstilgang og innsyn i dokumenter som ikke skulle vært tilgjengelige. Byggesakskontoret har redusert tilgangene til systemet.

²⁶ TQM: Total Quality Management. Total kvalitetsledelse

²⁷ ServiceNow er en skybasert administrasjonsplattform for blant annet IT-tjenester

2.5 Jevnlig evaluering av tilganger for å sikre at de er nødvendige og oppdaterte

Rutinen i Kvaliteket "Årlig revisjon av tilganger til fagprogram med egen tilgangskontroll i Trondheim kommune", beskriver at tjenesteforvalter minimum en gang per år skal ta ut en oversikt over brukerne av fagprogrammet og sende oversikten til aktuelle enheter. Enheten skal gjennomgå oversikten og sende bestilling på sletting av tilgang for de som ikke lenger skal ha denne. Tjenesteforvalter sletter deretter tilgangen i fagprogrammet.

Tabell 5: Evalueres tilganger jevnlig?

Systemnavn	Ja / Nei	Kommentar
Visma Velferd	Nei	Det er ingen løpende vurderinger av tilganger. De forholder seg til meldinger som kommer inn fra autorisert bestiller via IT-brukerhjelp
Visma Flyvo	Nei	Det er ingen løpende vurderinger av tilganger. De forholder seg til meldinger som kommer inn fra autorisert bestiller via IT-brukerhjelp
Vigilo	Ja	Årlig kontroll
Modulus barn	Ja	Jevnlig kontroll, flere ganger i året
eByggesak	Ja	De har halvårlig evaluering av tilganger

Kilde: Revisjonens analyse basert på svar fra tjenesteforvaltere

Visma Velferd

Tjenesteforvalter forholder seg til det som meldes via Selvbetjeningsportalen fra autoriserte bestillere. Det tas ingen egen vurdering av eventuelle endringer av behov for tilganger til ansatte i Trondheim kommune eller for Nav ansatte. Tjenesteforvalter er avhengig av at autorisert bestiller sender alle aktuelle opplysninger inn til Selvbetjeningsportalen og at disse sendes videre til tjenesteforvalter fra portalen. Det forekommer at sluttmeldinger ikke blir sendt til tjenesteforvalter fra Selvbetjeningsportalen. Da vil ikke endringer av tilganger bli gjennomført i systemet. Risikoen for misbruk av tilganger er liten da brukeren må ha tilgang på enten Nav pc eller kommunal pc for å få tilgang til systemet.

Visma Flyvo

Tjenesteforvalter forholder seg til det som meldes via Selvbetjeningsportalen fra autoriserte bestillere. Det tas ingen egen vurdering av eventuelle endringer av behov for tilganger til ansatte i Trondheim kommune. Tjenesteforvalter er avhengig av at autorisert bestiller sender alle aktuelle opplysninger inn til Selvbetjeningsportalen og at disse sendes videre til tjenesteforvalter fra portalen. Tjenesteforvalter opplyser at det forekommer at sluttmeldinger ikke blir sendt til tjenesteforvalter fra Selvbetjeningsportalen. Da vil ikke endringen bli gjennomført i systemet. Risikoen for misbruk av tilganger er liten da brukeren må ha tilgang på en kommunal pc.

Vigilo

Tjenesteforvalter opplyser at de årlig kontrollerer tilganger ved oppstart av nytt skole- og barnehageår. Tilganger som ikke lenger er nødvendige, slettes. På skole er det flere parametre som må på plass for at det faktisk gis en tilgang til elevopplysninger. Blant annet må den ansatte være registrert med en aktiv stilling på enheten, og ha en tilknytning til elever gjennom grupper eller timeplan.

Det er i hovedsak forvaltningen som har flere roller og tilganger i systemet. Den andre gruppen som har tilganger til flere enheter, er personer ansatt i de spesialpedagogiske teamene. De arbeider ved flere enheter og må ha tilgang til de enhetene som er relevante for den enkelte ansatte.

Generelt håndteres ansattetilganger til delegert person på skoler og barnehager og ledertilganger håndteres av forvaltningen. Ved opprettelse av nye ledertilganger stilles det spørsmål til enhetene om de gamle tilgangene skal slettes.

Modulus Barn

Tjenesteforvalter forholder seg til det som meldes via Selvbetjeningsportalen fra autoriserte bestillere. Ut fra opplysninger som blir gitt fra autorisert bestiller gir tjenesteforvalter ansatte tilgang til den/de roller de har behov for i sin stilling. Tilgang til Modulus Barn stoppes automatisk ved avslutning av ansattforholdet. Modulus Barn er et nytt system og inntil videre gjøres det i tillegg en manuell sjekk for å se om automatikken fungerer som den skal. Ansatte som har sluttet eller har endret stilling vil ikke bli slettet i systemet, men vil bli stoppet og de vil ikke få tilgang til systemet. Brukeren blir ikke slettet for at historikken skal beholdes i systemet. Modulus Barn er et nytt system for kommunen og er under kontinuerlig overvåking og evaluering.

eByggesak

Tjenesteforvalter opplyser at de har halvårslige gjennomganger av oversikten over tilganger til eByggesak for å sikre at tilgangene slettes når de ikke lenger er nødvendige. Det sendes e-post til den enkeltes enhetsleder med forespørsel om tilgangen til eByggesak fortsatt er relevant for hver enkelt bruker.

Byggesaksontoret har i 2024 tatt bort 100 tilganger til systemet, men arbeidet med jevnlig gjennomgang av tilganger vil likevel videreføres i mindre skala. På Byggesakskontoret følges dette opp av systemadministrator når folk slutter. HR-koordinator ved byggesakskontoret sender e-post til systemadministrator når ansatte sender inn sin oppsigelse. Det settes så en "slutt-dato" for den ansatte i systemet. Når man kommer til denne datoen, inndras brukertilgangen.

Vi har fått opplyst at bygningssjefen har besluttet at alle tilganger til eByggesak skal evalueres på ledernivå. Det vil si at det må sendes en e-post på ledernivå med systemadministrator som kopimottaker, der bygningssjefen beslutter om vedkommende skal få tilgang til systemet eller ikke.

Revisjonens vurderinger

Revisjonen mener at for systemene Vigilo, Modulus Barn og eByggesak er det jevnlig evalueringer av tilganger som sikrer at de er nødvendige og oppdaterte. Vi er kritisk til at tilganger til Visma Velferd og Visma Flyvo ikke evalueres årlig.

2.6 Opplæring i informasjonssikkerhet og personvern

Ifølge Datatilsynet inneholder informasjonssikkerhet tre hovedprinsipper:²⁸

- Konfidensialitet: at informasjon ikke blir kjent for uvedkommende.
- Integritet: at informasjon ikke blir endret utilsiktet eller av uvedkommende.
- Tilgjengelighet: at informasjon er tilgjengelig ved behov.

Bestemmelser knyttet til informasjonssikkerhet og GDPR finner vi i:

- NSM Grunnprinsipper for IKT-sikkerhet
- Lov om behandling av personopplysninger, GDPR artikkel 25 og 32

Fire av de fem utvalgte IT-systemer inneholder sensitive personopplysninger. I etterlevelseskontrollen for IT i 2023 tok revisjonen opp at kommunen ikke har klare retningslinjer som beskriver hvordan tjenesteforvalter, tjenesteeier og virksomhetsområdene skal ivareta ansvaret for GDPR i sine IT-systemer. Vi anbefalte at kommunedirektøren sikrer at kommunen har etablert retningslinjer som klart definerer hvilket ansvar tjenesteforvalter, tjenesteeier og virksomhetsområdene skal ha for GDPR for sine IT-systemer. Revisjonen observerer at det ikke foreligger retningslinjer på dette i Kvaliteket.

I tabellen under har vi oppsummert svarene fra tjenesteforvalterne på spørsmålet om de har fått opplæring i informasjonssikkerhet og personvern.

Tabell 6: Har tjenesteforvaltere fått opplæring i informasjonssikkerhet og personvern?

Systemnavn	Informasjonssikkerhet	Personvern
Visma Velferd	Nei	Ja
Visma Flyvo	Nei	Ja
Vigilo	Nei	Ja
Modulus barn	Nei	ja
eByggesak	Ja	Ja

Kilde: Revisjonens analyse basert på svar fra tjenesteforvaltere

²⁸ Informasjonssikkerhet - Kilde:

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/>

Visma Velferd, Visma Flyvo, Modulus Barn og Vigilo

Tjenesteforvalter opplyser at de har fått opplæring i personvern, men ikke god nok opplæring i informasjonssikkerhet.

eByggesak

Tjenesteforvalter opplyser at hun har fått opplæring i personvern, GDPR-forordningen og informasjonssikkerhet. Byggesakskontoret har ifølge tjenesteforvalter og systemadministrator en bevisst holdning til personvern og informasjonssikkerhet. Jurister på enheten vurderer personvernet og om dokumenter skal unntas offentlighet. Det holdes årlig gjennomgang av GDPR og habilitetsregler for alle ansatte ved Byggesakskontoret.

For å sikre at data i systemet ikke endres utilsiktet eller av uautoriserte personer har tjenesteforvalter i tillegg til oppfølging av ansattes tilganger også oppfølging av tilgangene til systemet for ansatte hos leverandøren.

Tilgjengeligheten til data fra eByggesak, for de autoriserte brukerne av systemet, skal sikres gjennom databehandleravtalen med leverandøren. Databehandleravtalen omhandler backup av data og sikkerheten rundt dette.

Revisjonens vurderinger

Revisjonen er kritisk til at retningslinjer som beskriver hvordan tjenesteforvalter skal ivareta ansvaret for kommunens personopplysninger (GDPR) for sine IT-systemer, som vi påpekte i vår etterlevelseskontroll for 2023, enda ikke er implementert.

Alle tjenesteforvalterne oppgir at de har fått opplæring i personvern. Revisjonen er kritisk til at det ikke er gitt opplæring i informasjonssikkerhet til tjenesteforvaltere for systemene Visma Velferd, Visma Flyvo, Vigilo og Modulus Barn.

2.7 Loggføring av bruk av IT-systemene skal gjennomgåes jevnlig for å avdekke eventuelt misbruk

Det er i henhold til NSM sine grunnprinsipper pkt. 3.2 viktig at uautoriserte handlinger, sikkerhetsbrudd og sikkerhetstruende hendelser kan oppdages så tidlig som mulig slik at skade kan minimeres, om ikke forhindres. Logger er viktige for hendelseshåndtering og rasjonell drift av informasjonssystemer.

Vi har spurt tjenesteforvalterne for de fem systemene om de har gjennomgang av loggføring i IT-systemene. Svarene er oppsummert i tabellen under.

Tabell 7: Gjennomgås loggføringer av IT-systemer jevnlig?

Systemnavn	Ja / Nei	Kommentar
Visma Velferd	Nei	Ingen egen kontroll er utført
Visma Flyvo	Nei	Ingen egen kontroll er utført
Vigilo	Ja	Ikke direkte tilgang til logg, men de sjekker logg ved mistanke om uautorisert tilgang.
Modulus barn	Ja	Alt logges. Må begrense spørring på grunn av mye informasjon.
eByggesak	Ja	Det er blitt gjennomført "jevnlige" kontroller i det siste halve året

Kilde: Revisjonens analyse basert på svar fra tjenesteforvaltere

Visma Velferd

Ansatte kommer ikke inn i systemet uten å logge seg på sin kommunale pc, eventuelt Nav pc som er satt opp for brukeren. Som vist i [kapittel 2.4](#), har bruker i systemet tilgang til å se mer enn prinsippet om minst mulig privilegium skulle tilsi. Tjenesteforvaltere har tilgang til noen logger i systemet, men det er ikke noe som benyttes aktivt.

Visma Flyvo

Ansatte må logge seg inn i Flyvo på sin kommunale pc ved innlogging via Active Directory. Det er et unntak for de som har Singel Sign On (SSO). På grunn av at innlogging i Flyvo via SSO ikke krever kommunal pc, er det større risiko for uautorisert tilgang fra eksterne. Tjenesteforvalter opplyser at de ikke kontrollerer loggføringer av bruk av systemet. Ved eventuell mistanke om autorisert bruk må de bestille logg fra leverandør.

Vigilo

Tjenesteforvalter opplyser at de ikke har direkte tilgang til en logg i systemet. De bestiller logg fra leverandøren ved behov. Unntaket er i de digitale mappene i systemet hvor det oppbevares sensitiv dokumentasjon for barnehagebarn og skoleelever. Alle handlinger og hvem som har sett i mappene logges. Disse loggene sjekkes ved mistanke om uautorisert tilgang. Det er imidlertid begrensninger på hvem som har tilgang til disse mappene.

Modulus Barn

Tjenesteforvalter opplyser at alt loggføres og de tar jevnlig kontroll av logger for å se etter mistenkelige hendelser. Tjenesteforvalter opplyser at de må begrense spørring i logg på grunn av datamengden. De har oppdaget at hvis en ansatt sletter noe forsvinner dette også fra loggene. Har de saksnummer, kan leverandør spore opp den slettede saken og få lagt det tilbake. De har tatt dette problemet opp med leverandøren, slik at data som slettes ikke skal slettes fra loggen for fremtiden.

eByggesak

Som vist i kapittel 2.2 har noen brukere gjennom sine roller i eByggesak hatt for store rettigheter i systemet. Systemadministrator har et støttesystem for å loggføre bruk av eByggesak. Tjenesteforvalter og systemadministrator opplyser at det er gjennomført stikkprøvekontroll på bruker- og saksnivå for å avdekke eventuelt misbruk av systemet det siste halve året. I støttesystemet har man mulighet til å se hvilke saker og filer hver enkelt

bruker har sett på og eventuelt har redigert i. Ifølge systemadministrator har de ikke funnet noe misbruk av systemet.

Revisjonens vurderinger

Revisjonen er kritisk til at det for Visma Velferd, Visma Flyvo, Vigilo og Modulus barn ikke er utarbeidet skriftlige rutiner for gjennomgang av loggføring av bruk av systemene. Vi understreker at disse fire IT-systemene inneholder sensitive personopplysninger.

Revisjonens undersøkelse viser at for systemene Visma Flyvo og eByggesak har brukere fått roller som har gitt for vide rettigheter. Dette understreker viktigheten av å ha en jevnlig gjennomgang av den loggførte bruken av systemet for å avdekke om det har vært misbruk av roller eller uautorisert tilgang til systemet.

3 Konklusjon

Har Trondheim kommune etablert tilfredsstillende styring og kontroll med roller og tilganger i IT-systemer for å sikre at ansattes rettigheter i systemene er i samsvar med tjenstlig behov og gjeldende regelverk?

Revisjonens undersøkelser viser at kommunen ikke har etablert overordnede skriftlige retningslinjer for hvordan tjenesteforvaltere skal administrere roller i og tilganger til IT-systemer.

Det er ikke etablert skriftlige rutiner for oppretting, endring, sletting og jevnlig evaluering av roller i IT-systemene i kommunen for å sikre at rollene er satt opp i henhold til kommunens behov og med riktig omfang som bidrar til betryggende sikkerhet.

Undersøkelsen viser at ikke alle rollene for de fem systemene som inngår i undersøkelsen er satt opp med riktig omfang som bidrar til betryggende sikkerhet.

For fire av systemene som inngår i undersøkelsen er det rutiner for håndtering av tilganger via Selvbetjeningsportalen. Byggesakskontoret benytter ikke Selvbetjeningsportalen med autorisert bestiller og skjema for eByggesak. De har ikke skriftlige rutiner for hvordan tjenesteforvalter skal administrere tilganger til eByggesak.

Tilgangene til tre av systemene i undersøkelsen har ikke vært satt opp i henhold til prinsippene om minst mulig privilegium. For de to siste systemene er tilgangene etter endring satt opp med minst mulig privilegium.

For systemene Vigilo, Modulus Barn og eByggesak er det jevnlig evalueringer av tilganger som sikrer at de er nødvendige og oppdaterte. Tilganger til Visma Velferd og Visma Flyvo evalueres ikke årlig.

Retningslinjer som beskriver hvordan tjenesteforvalter skal ivareta ansvaret for kommunens personopplysninger (GDPR) for sine IT-systemer, som vi påpekte i vår etterlevelseskontroll for 2023, er ennå ikke implementert.

Alle tjenesteforvalterne oppgir at de har fått opplæring i personvern. Det er ikke gitt opplæring i informasjonssikkerhet til tjenesteforvaltere for systemene Visma Velferd, Visma Flyvo, Vigilo og Modulus Barn.

For systemene Visma Velferd, Visma Flyvo, Vigilo og Modulus barn er det ikke utarbeidet skriftlige rutiner for gjennomgang av loggføring av bruk av systemene. Disse fire IT-systemene inneholder sensitive personopplysninger.

4 Byrådets uttalelse



TRONDHEIM KOMMUNE
Tråanten tjielte

Kommunerevisjonen

Vår saksbehandler
Berit Antonie Holmlimo

Vår ref.
2025/15818
oppgis ved alle henvendelser

Deres ref.
2024/25123

Dato
19.05.2025

Finansrådets uttalelse om etterlevelseskontroll IT 2025

Finansbyråden opplever rapporten om etterlevelseskontroll for IT 2024 som en ryddig og nyttig rapport. Revisjonen har gjort en grundig gjennomgang av rutiner, roller og tilganger for ulike IT-systemer for å se om rettigheter i systemet er i samsvar med tjenstlige behov og regelverk.

Systemene som revisjonen har gjennomgått ligger utenfor tjenesteeieransvaret og tjenesteforvalteransvaret for byrådsområde Finans. Samtidig er det viktig at styring og kontroll med roller og tilganger i IT-systemene sikrer ansattes rettigheter i systemene, er i samsvar med tjenstlig behov og gjeldende regelverk.

Finansbyråden oppfatter at rapporten har en systematisk gjennomgang av tema med en tydelig vurdering for hvert enkelt kriterium som berøres i rapporten. Dette gjør rapporten til et praktisk og godt arbeidsverktøy for byråden i videre oppfølging av rutiner og tilganger for IT-systemene som forvaltes i ulike byrådsområder. Trondheim Digital er en premissgiver og støttefunksjon for de som er tjenesteeiere og tjenesteforvaltere i de andre byrådsområdene.

Som en del av finansbyrådens ansvar med oppfølging av virksomhetsstyring i Trondheim kommune, arbeider organisasjonen med å utvikle gode systemer for gjennomgang av roller og rutiner. I dette ligger også rutiner med tilganger til ulike systemer. Trondheim Digital har påbegynt arbeidet med å tydeliggjøre retningslinjer og krav knyttet til rollene tjenesteeier og tjenesteforvalter. Dette arbeidet er en pågående prosess som enheten følger opp.⁴

I tillegg jobber Trondheim Digital med hvordan enheten kan bli en bedre premissgiver for bedre kvalitet for tjenesteforvaltningen i kommunen. Det jobbes blant annet med å ha en arena for tjenesteforvaltere med fokus på heving av felles kompetanse gjennom læring og erfaringsdeling. Trondheim Digital er i prosess med å planlegge kurs og opplæring knyttet til roller for de ulike systemene. I tillegg vurderes det å opprette en digital støttekanal for både systemeiere og

⁴ [IT tjenestestyring](#) - [Tjenesteforvalter](#) - [Tjenesteeier](#)

Postadresse:
Trondheim kommune
Byrådsavdeling for finans
Postboks 2300 Torgarden
7004 TRONDHEIM

Besøksadresse:
Munkegata 1

Telefon:
72 54 00 00

Organisasjonsnummer:
NO 942 110 464

E-postadresse: byradsleder.postmottak@trondheim.kommune.no
www.trondheim.kommune.no

tjenesteforvaltere for bistand og avklaringer fra Trondheim Digital.

Finansbyråden ser arbeidet som Trondheim Digital har begynt med som en god begynnelse som møter flere av revisjonens vurderinger og anbefalinger.

Med hilsen
Trondheim kommune

Kjetil Reinskou
byråd finans

Berit Antonie Holmlimo
seniorrådgiver

Dette er et digitalt dokument og har derfor ingen signatur

Kopi til:

Elin Haarsaker

5 Uttalelse fra ledelsen

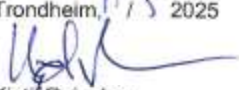
Uttalelse fra ledelsen

Til
Trondheim kommunerevisjon
v/oppdragsansvarlig revisor

Uttalelse fra ledelsen vedrørende "Etterlevelseskontroll IT 2024"

Ledelsens ansvar:

- Vi er kjent med, og har oppfylt vårt ansvar for å utforme og iverksette en hensiktsmessig intern kontroll for å sikre etterlevelse av lov, forskrift, egne reglement og vedtak.
- Vi bekrefter at vi har gitt revisor all informasjon som er relevant og vesentlig for "Etterlevelseskontroll IT 2024".
- Vi kjenner ikke til at det er manglende etterlevelse av lov, forskrifter, egne reglementer eller vedtak i kommunen.

Trondheim, 15. 5. 2025

Kjetil Reinskou

Trondheim kommunerevisjon
Postboks 2300 Torgarden
7004 Trondheim

www.trondheim.kommune.no/revisjon

Januar 2022

Forsidefoto:

Layout: Kommunikasjonsenheten, ghl

