Revisjon Midt-Norge

INFORMASJONSSIKKERHET

Melhus kommune

Forvaltningsrevisjon

FR1256

2024

FORORD

Revisjon Midt-Norge SA har gjennomført denne forvaltningsrevisjonen på oppdrag fra Melhus kommunes kontrollutvalg i perioden september 2023 til mai 2024.

Vi vil takke alle som har bidratt med informasjon i prosjektet.

Alle rapporter fra Revisjon Midt-Norge SA publiseres på www.revisjonmidtnorge.no.

Bodø, 30. mai 2024

Hanne Marit Ulseth Bjerkan

Oppdragsansvarlig revisor

Margrete Haugum

Prosjektmedarbeider

SAMMENDRAG

Revisjon Midt-Norge SA har gjennomført denne forvaltningsrevisjonen på oppdrag fra kontrollutvalget i Melhus kommune. Revisor har undersøkt kommunens arbeid med informasjonssikkerhet.

I **første problemstilling** konkluderer revisor med at Melhus kommune har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller 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.

I **andre problemstilling** konkluderer revisor 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.

Revisor anbefaler at rådmannen:

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

INNHOLDSFORTEGNELSE

Tabell

Figurer

1 INNLEDNING

1.1 Bestilling

Kontrollutvalget i Melhus kommune bestilte den 16. februar 2023, sak 06/23 en forvaltningsrevisjon om datasikkerhet. Bestillingen er gjort med utgangspunkt i *Plan for forvaltningsrevisjon 2020-2024*.

Under behandlingen kommer det frem at kontrollutvalget ønsker svar på følgende spørsmål:

- *Hva gjør kommunen for å forebygge, oppdage og håndtere digitale angrep?*
- *Hva gjør kommunen hvis systemene blir helt utilgjengelige eller ikke til å stole på?*
- *Hvordan forvaltes kommunens kontroll over persondata?*
- *Hvordan forvaltes teknologien og hvordan understøtter den kommunale tjenester på kort og lang sikt?*
- *Hvilke rutiner er etablert for sikring av kommunes data?*
- *Hvordan følger kommunens sikkerhetstiltak lover, forskrifter og annet regelverk med tanke på backup, personvern, kriseløsninger, hacking med mer?*
- *Hvordan fungerer de fastlagte rutinene for informasjonssikkerhet i praksis?*
- *I hvilken grad er organiseringen av informasjonssikkerhetsarbeidet tilfredsstillende og i tråd med lovkrav?*
- *Hvilke systemer har kommunen for kontroll og etterprøving av informasjonssikkerhet?*
- *Hvordan blir kontroll og etterprøving gjennomført?*

Revisor har hensyntatt kontrollutvalgets ulike spørsmål i utformingen av problemstillinger, med den ambisjon om at utvalgets spørsmål blir besvart gjennom revisor sine problemstillinger.

Prosjektplanen var lagt fram til behandling under sak 18/23 i kontrollutvalgets møte den 4. mai 2023. På bakgrunn av brevtilsyn fra Datatilsynet vedtok kontrollutvalget å avvente behandlingen av prosjektplanen til Datatilsynet hadde avgjort hvilke kommuner som skulle inngå i fase to av tilsynet. Melhus kommune inngikk ikke i fase to av tilsynet. Resultat fra tilsynet omtales i kapittel 1.5.2.

Prosjektplanen ble vedtatt i sak 40/23 i kontrollutvalgets møte den 7. september 2023.

1.2 Problemstillinger

Følgende problemstillinger besvares i rapporten:

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

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

1.2.1 Avgrensing

Melhus kommune inngår i vertskommunesamarbeidet ITMidt mellom Melhus og Skaun kommune. Melhus kommune er vertskommune. Revisjonen omhandler kun arbeidet Melhus kommune gjør innenfor informasjonssikkerhet, selv om ITMidt også inkluderer Skaun kommune.

Personopplysningsloven stiller krav til behandling av personopplysninger. Revisjonen har ikke mulighet til å se på alle de spesifikke kravene som omhandler behandling av person-opplysninger. Revisjonen vil ikke se på behandlingsgrunnlaget som ligger til grunn for behandling av hver enkelt personopplysning til hvert enkelt formål, for eksempel om det er innhentet samtykke.

1.3 Metode

Forvaltningsrevisjonen er gjennomført i henhold til NKRF - kontroll og revisjon i kommunenes standard for forvaltningsrevisjon, RSK 001. Revisor har vurdert egen uavhengighet overfor Melhus kommune, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3.

Revisor har brukt flere metoder for å samle inn data til dette prosjektet. Nærmere beskrivelse blir gitt nedenfor.

Intervju

Revisor gjennomførte et oppstartsmøte med rådmann, beredskapskapsrådgiver og IT-sjef. Beredskapsrådgiver er også kommunens personvernombud og informasjonssikkerhets-ansvarlig.

Revisor gjennomførte intervju med IT-sjef og IT teknisk sikkerhetsansvarlig (omtales som sikkerhetsansvarlig i rapporten) hos ITMidt sammen. Driftsleder på IT var forhindret fra å delta på intervjuet. Revisor har vurdert at det ikke var behov for å følge opp intervju med driftsleder IT, da både IT-sjef og sikkerhetsansvarlig har svart ut revisors spørsmål. Vi har også til slutt gjennomført et digitalt oppfølgingsintervju med IT-sjef og sikkerhetsansvarlig for å få avklart spørsmål som har kommet til underveis i arbeidet med sammenstilling av informasjon.

Revisor har også gjennomført et digitalt intervju med beredskapsrådgiver.

I forkant av intervjuene laget revisor en strukturert intervjuguide. I etterkant av alle intervjuene er det skrevet referat som er verifisert av informantene. Rapporten benytter kun verifisert intervjudata.

Dokumentgjennomgang

Revisor har fått tilsendt dokumenter knyttet til kommunens rutiner, prosedyrer, policyer og planer som omhandler informasjonssikkerhet i Melhus. Overordnede planer revisor har fått tilsendt er Digitaliseringsstrategien til kommunen, overordnet beredskapsplan og overordnet risiko- og sårbarhetsanalyse. Kommunen har også oversendt hvordan internkontroll er beskrevet i årsmeldingen for 2022.

Videre har kommunen oversendt rutiner knyttet til melding av avvik og avvikshåndtering ved brudd på informasjonssikkerhet/personopplysningsloven. Vi har også fått tilsendt protokoller over behandlingsaktiviteter.

Revisor har også fått tilsendt svarene og dokumentasjonen kommunen oversendte til Datatilsynet knyttet til brevkontrollen av personopplysningssikkerhet i kommunen.

Videre har revisor fått oversendt sikkerhetshåndboken til Melhus kommune som består av tre hefter. Revisor har fått oversendt to av tre hefter. Revisor har ikke mottatt hefte 3 som omhandler IT-løsning på drift. Revisor anser heftet som ikke relevant for å svare ut problemstillingene siden det omhandler tekniske IT-løsninger.

I tillegg har revisor fått oversendt en mappe knyttet til beredskap på IT med flere dokumenter. Mappen med dokumenter er inndelt i tre deler; styrende del, kontrollerende del og gjennomførende del, og inneholder til sammen ca. 60 dokumenter. Dokumentene er under utarbeidelse og ikke endelige. Dokumentene har ved utgangen av april 2024 ikke vært behandlet i kommunens strategiske ledergruppe.

Mange av dokumentene revisor har mottatt er unntatt offentligheten. Dokumenter som er unntatt offentligheten skal merkes med hvilken hjemmel som er brukt for å begrunne dette. Revisor har ikke undersøkt eller fokusert på om kommunen har hjemmel til å unnta informasjon eller om det er brukt riktig hjemmel.

Observasjon

Revisor (prosjektleder og prosjektmedarbeider) deltok som observatør under Statsforvalteren sin beredskapsøvelse, SODD, der Melhus kommune deltok. Øvelsen ble arrangert i mars 2024 og omhandlet cyberangrep. Revisor ønsket å delta på denne øvelsen siden temaet de skulle øve på var direkte rettet mot temaet i denne forvaltningsrevisjonen, og revisor hadde et ønske

om å observere hvordan kommunen håndterte og jobbet med beredskap innenfor informasjonssikkerhet.

I etterkant av øvelsen har revisor skrevet et observasjonsnotat, som vi oversendte til orientering til kommunedirektør og beredskapskoordinator.

Vurdering av metode

Valg av intervju som metode er grunnet ut ifra behovet for mer kunnskap og detaljert informasjon knyttet til kommunens arbeid med informasjonssikkerhet.

Revisor har benyttet dokumentgjennomgang til å svare ut problemstillingene. Kommunens overordnede dokumenter er brukt for å finne ut hvordan arbeidet med informasjonssikkerhet i kommunen er forankret i kommunens planverk. Videre har revisor fått tilgang til kommunens planer, prosedyrer og policyer innenfor informasjonssikkerhet, som svarer ut hvordan kommunen har lagt opp arbeidet med informasjonssikkerhet i kommunen.

Siden mange av dokumentene revisor har brukt til å svare ut problemstillingene, er unntatt offentligheten, har det medført at revisor ikke kan gjenta alt av informasjon og fakta i rapporten. Revisor har sett alle dokumentene, men på grunn av sikkerhetshensyn og sikkerheten til kommunen kan ikke dette gjentas. Det har medført at revisor ikke har beskrevet innholdet i dokumentene nærmere, men beskrevet hovedtrekkene eller hva dokumentet sier noe om.

Å delta på beredskapsøvelsen i kommunen var nyttig for revisor for å få innsikt i hvordan ledelsen i kommunen tenker og reflekterer rundt uønskede hendelser og hvordan de potensielt vil håndtere en slik hendelse som cyberangrep. I forkant av øvelsen laget revisor en liste over elementer vi skulle se etter under øvelsen. Under øvelsen skrev vi hver vår oppsummering og vurdering. Dette ble gjort siden vi som revisor kan oppfatte ting ulikt, og vi vurderte at det var nyttig for vår del å se om det var noe ulik oppfattelse mellom oss to revisorer. I etterkant sammenstilte vi notatet, slik at vi fikk en felles oppsummering som vi sendte til kommunedirektør og beredskapskoordinator. Hensikten med å oversende det til kommunen var at våre notater kan være nyttig for dem i sitt videre arbeidet med beredskap, som evaluering av øvelsen og videre oppfølging av tiltak i etterkant av øvelsen.

Revisor har ikke gjennomført intervju med andre ansatte på ITMidt enn de som er nevnt. Revisor har vurdert at det ikke har vært hensiktsmessig med tanke på informasjonsbehovet og bruk av ressurser i prosjektet. Videre har vi ikke undersøkt hvordan informasjonssikkerhet er forankret ute på enhetene i kommunen. Vi har vurdert at dette ikke har vært nødvendig for å svare ut problemstillingene, der fokuset er å undersøke kommunens systematiske arbeid innenfor informasjonssikkerhet på et overordnet nivå.

Revisor vurderer at innsamlet data gir et godt grunnlag for å gjøre vurderinger og besvare problemstillingene.

1.4 Uttalelse om rapport

En rapport med faktagrunnlaget ble sendt til rådmannen for gjennomsyn i epost den 2. mai 2024. Formålet med oversendelsen av faktagrunnlaget var å gi rådmannen mulighet til å vurdere opplysningene revisor har brukt opp mot sensitiv informasjon og informasjon som er unntatt offentlighet, samt å korrigere eventuelle faktafeil. Revisor mottok tilbakemelding den 14. mai 2024. På bakgrunn av tilbakemeldingene har revisor gjort små korrigeringer av faktaopplysninger.

En foreløpig rapport ble sendt til rådmannen for uttalelse den 21. mai 2024. Revisor mottok uttalelsen fra rådmannen den 30. mai 2024. Uttalelsen er vedlagt rapporten i vedlegg 2. Uttalelsen har ikke ført til endringer i faktagrunnlaget, vurderinger eller konklusjon.

1.5 Bakgrunn

1.5.1 Informasjonssikkerhet

Direktoratet for forvaltning og økonomistyring (DFØ) skriver i sin miniveileder[1] at informasjon behandles i et samspill mellom mennesker, prosesser og teknologi. Det er denne informasjonsbehandlingen informasjonssikkerhet handler om; å sikre og beskytte informasjonsverdier mot skade. En informasjonsverdi kan være selve informasjonen, men også ressurser for representering og behandling av informasjonen. Eksempler på informasjonsverdier er data, fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og til og med menneskelige ressurser (Jøsang 2021). DFØ skriver at informasjonssikkerhet også handler om kompetanse og kultur i virksomheten.

Informasjonssikkerhet omfatter:

- konfidensialitet (sikre at informasjonen ikke blir kjent for uvedkommende)
- integritet (sikre at informasjonen ikke blir endret utilsiktet av uvedkommende)
- tilgjengelighet (sikre at informasjonen er tilgjengelig ved behov).

[1] https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/miniveileder-om-oppfolging-av-informasjonssikkerhet-i-styringsdialogen/hva-og-hvorfor-er-det-viktig

Robusthet er også en del av informasjonssikkerhet. Det handler om at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser. [2] Jøsang (2021) skriver at det ikke er noen tydelig avgrensning av hva som kan være informasjonsverdi. Derimot er det en klar definisjon på hvordan informasjonsverdier kan skades, nemlig gjennom brudd på konfidensialitet, integritet og tilgjengelighet.

1.5.2 Informasjonssikkerhet i kommuner

Norske kommuner behandler store mengder personopplysninger om sine innbyggere og ansatte, og har ansvaret for å ivareta opplysningen på en forsvarlig måte. I tillegg har norske kommuner samfunnskritiske oppgaver og sitter på opplysninger om sin egen virksomhet, blant annet informasjon om kommunalt vann og avløp. Betydningen av å ivareta kommunens informasjonsbehov- og beskyttelse er stor.

I en rapport fra Digdir[3] i 2020 finner de at fylkeskommuner og kommuner ikke har tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet, og særlig gjelder dette små og mellomstore kommuner. Figuren under viser at norske kommuner ikke er beskyttet mot uønskede hendelser innenfor informasjonssikkerhet.

Kilde: Computerworld, Lyngdal kommune og NRK.

I 2023 gjennomførte Datatilsynet kontroll med et stort antall norske kommuner om personopplysningssikkerheten. Melhus kommune var en av 100 kommuner som besvart spørsmålene i Datatilsynets første runde av tilsynet.

[2] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

[3] Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner, 2020, Digitaliseringsdirektoratet

Noen av funnene til Datatilsynet er at norske kommuner, til tross for begrensende ressurser, jobber godt med personvernarbeidet og at det er stor forståelse for at personvern og informasjonssikkerhet er viktige verdier som må ivaretas. Samtidig viser kontrollene at mange kommuner mangler overordnede retningslinjer og praktiske rutiner/prosedyrer innenfor temaene som ble kontrollert.[4] Blant annet skriver Datatilsynet at majoriteten av kommunene mangler tilstrekkelig overordnede retningslinjer for arbeidet med vurdering av risiko, men mange kommuner har rutiner og skjema for hvordan gjennomføre en risiko- og sårbarhetsanalyse. Resultatet viser at 60 av 94 kommuner har svært mangelfulle eller mangler en overordnet sikkerhetsstrategi. I sin presentasjon av rapporten[5] forteller Datatilsynet at mye av ansvaret for informasjonssikkerhet er lagt til de som jobber med IKT i kommunen, og ikke overordnet ledelse.

Digitaliseringsdirektoratet skriver at arbeidet med informasjonssikkerhet er del av styringsarbeidet som leder av offentlige virksomheter har ansvaret for. Formålet med styring og kontroll av informasjonssikkerhet er å medvirke til at informasjonsbehandlingen gjennomføres på en best mulig måte som realiserer virksomhetens samlede mål samtidig som det er kostnadseffektivt og i tråd med lov og regelverk.[6]

1.5.3 Regelverk

Det er minst tre juridiske tilnærmeringer til sikkerhetsarbeidet. Disse er:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), § 15 om internkontroll på informasjonssikkerhetsområdet.

Sikkerhetsloven stiller generelle krav til forebyggende sikkerhetsarbeid i kapittel 4. Sikkerhetsstyring er hjemlet i § 4-1; forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Virksomhetsikkerhetsforskriften definerer i § 3 kravet om at virksomheter som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.

Personopplysningsloven gir bestemmelser om hvordan personopplysninger skal behandles. Loven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom

[4] https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/funn-fra-tilsyn-i-kommuner-og-fylkeskommuner/

[5] Basert på revisors notater fra presentasjonen den 9. november 2023, opptak tilgjengelig på https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/seminar-om-kommunetilsyn/

[6] https://www.digdir.no/informasjonssikkerhet/styring-av-informasjonssikkerhet/2693

behandling av personopplysninger. Loven gjennomfører EUs personvernforordning i norsk rett. Personopplysningsloven er bygget på noen grunnleggende prinsipper, og alle som behandler personopplysninger må følge disse prinsippene.

I eForvaltningsforskriften er internkontroll på informasjonssikkerhetsområdet regulert. Forskriften krever at forvaltningsorganet skal ha en internkontroll på informasjons-sikkerhetsområdet og som bør være integrert som en del av virksomhetens helhetlige styringssystem. eForvaltningsforskriften krever blant annet at mål og strategier for informasjonssikkerhet er beskrevet gjennom sikkerhetsmål og sikkerhetsstrategi, som skal danne grunnlaget for internkontrollen på området.

Norge har et eget ekspertorgan for informasjons- og objektsikkerhet, Nasjonal sikkerhetsmyndighet (NSM), som er det nasjonale fagmiljøet for IKT-sikkerhet. NSM har utarbeidet en veileder i sikkerhetsstyring som beskriver sikkerhetsstyring som systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier.

Figuren nedenfor viser sammenhengen for sikkerhetsstyringsarbeidet, og er basert på nasjonal sikkerhetsmyndighets veileder i sikkerhetsstyring.

Kilde: Revisjon Midt-Norge SA

Figur 1. Sammenhenger for sikkerhetsstyring

Skjermingsverdige verdier er definert i sikkerhetslovens § 6-1 første ledd:

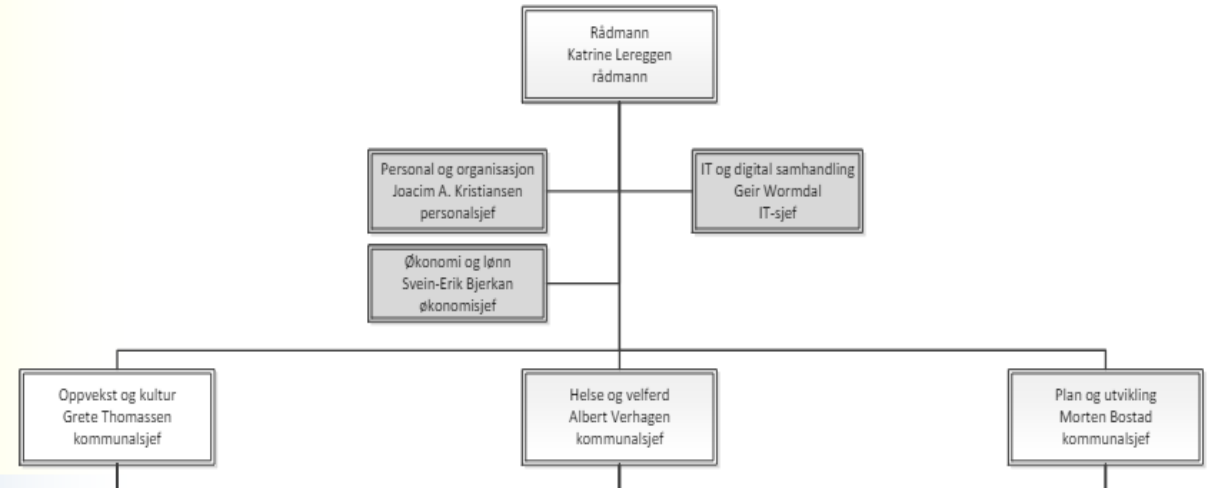
> *Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.*

Utgangspunktet for sikkerhetsstyringen er risikovurderinger, som omfatter informasjon om verdier, identifisering av trusler og avdekking av sårbarheter. Risikovurderingene danner grunnlaget for risikohåndteringen. Risikohåndtering omfatter etablering av sikkerhetstiltak,

tilpasset de skjermingsverdige verdiene en virksomhet forvalter. Sikkerhetstiltak kan være både organisatoriske tiltak og tekniske tiltak. Organisatoriske tiltak kan være roller og ansvar, retningslinjer, prosedyrer og rutiner. Tekniske tiltak er eksempelvis IKT-løsninger, IKT-utstyr, programvare, skap, dører, rom og bygninger.

1.5.4 Melhus kommune

Melhus kommune har en egen enhet, IT og digital samhandling, som er en del av kommunens sentraladministrasjon. Enheten består av ITMidt (drift, support og tjenesteutvikling), kommunikasjon og dokumentasjon (arkiv og innsyn), og politisk sekretariat.



Kilde: Melhus kommune

Figur 2. Utklipp fra Melhus kommune sitt organisasjonskart

ITMidt er et interkommunalt IT-samarbeid mellom kommunene Melhus og Skaun som ble etablert i 2018, da som interkommunalt samarbeid organisert etter (da gjeldende) kommunelovens § 27. ITMidt ble 1. januar 2022 organisert som et administrativt vertskommunesamarbeid etter kommunelovens § 20-2, hvor Melhus kommune er vertskommune. ITMidt har som formål å ivareta oppgaver knyttet til drift, service, forvaltning og utvikling av informasjons- og kommunikasjonsteknologi, inngåelse og oppfølging av avtaler, samt å ivareta digitalisering og tjenesteutvikling. ITMidt har også ansvar for å ivareta informasjonssikkerhet og internkontroll i henhold til lov og forskrift. IT-sjef er leder av ITMidt og deltar fast i strategisk ledergruppe i Melhus kommune, men deltar også i strategisk ledergruppe i Skaun kommune en gang i uka. Strategisk ledergruppe i Melhus består i tillegg av rådmann, kommunalsjefer, økonomi og personal.

2 STYRINGSSYSTEM

2.1 Problemstilling

Det er utarbeidet følgende problemstilling:

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

Problemstillingen besvares med bruk av både dokumentasjon fra det nåværende og eksisterende styringssystemet og dokumentasjon fra det nye styringssystemet som er under etablering.

Nåværende styringssystem består av hefte 1 om ansatte og sikkerhetskultur og hefte 2 om informasjonssikkerhet.

Det nye styringssystemet som er under etablering består av ulike planer, prosedyrer og policyer innenfor informasjonssikkerhet. Det refereres til titlene på dokumentene fra det nye styringssystemet.

2.2 Rammeverk

2.2.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen bør legge et rammeverk til grunn for sitt informasjonssikkerhetsarbeid.

2.2.2 Funn

IT-sjef og sikkerhetsansvarlig forteller at Melhus kommune har bygget opp sine rutiner og prosedyrer etter kravene i standarden for informasjonssikkerhet, ISO/IEC 27002:2002. Standarden er en global standard for IT-sikkerhet, og benyttes av virksomheter både i Norge og i utlandet.[7]

Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet et regneark som viser sammenhengen mellom NSM sine grunnprinsipper for IKT-sikkerhet 2.0 og ISO/IEC 27002, som er tilgjengelig på deres hjemmeside. Regnearket kan benyttes av virksomheter som ønsker å bruke prinsippene aktivt for sitt sikkerhetsarbeid, skriver NSM på hjemmesiden. Bakgrunn for koblingen er laget for å vise sammenhengen mellom de to sikkerhetsrammeverkene, samt

[7] Koblingstabell mellom NSMs grunnprinsipper for IKT-sikkerhet 2.0 og ISO/IEC 27002:2022, NSM

hvorfor det er ulikheter i rammeverkene. Regnearket viser også en tredelt prioritering av sikkerhetstiltakene. Prioriteringsgruppe 1 er de høyest prioriterte sikkerhetstiltakene. NSM skriver i om prioriteringsgruppe 1 at:

> «*Mangelen på implementering av flere av disse tiltakene er som oftest «rot-årsaken» til vellykkede data-angrep*».

Melhus kommune har brukt koblingstabellen som NSM har utarbeidet, og sikkerhetsansvarlig forteller at de har gjennomgått de fleste grunnprinsippene i regnearket (totalt 118 sikkerhetstiltak fordelt på 21 prinsipper og fire kategorier). Revisor har fått tilsendt Melhus kommunes versjon av regnearket. Kommunen har i regnearket blant annet lagt til en kolonne som beskriver status på tiltaket i kommunen. Av de totalt 118 sikkerhetstiltakene, har kommune fylt ut status for 23 tiltak. Sikkerhetsansvarlig forteller at det fortsatt gjenstår arbeid med gjennomgangen av grunnprinsippene, eksempelvis er det ikke begrunnet hvorfor punktene er ok. Kommunen har prioritert NSM sin gruppe 1 i sitt arbeid, og har begynt på prioriteringsgruppe 2 og 3.

Melhus kommune har utarbeidet en sikkerhetshåndbok for kommunes styringssystem for informasjonssikkerheten. I sikkerhetshåndboken skriver kommunen at styringssystemet skal bidra til å sikre et felles nivå på informasjonssikkerhet på tvers av virksomhetene i kommunene, og gir en felles føring for de ansatte i kommunen, eksterne brukere, borgere og samarbeidspartnere. Sikkerhetshåndboken består av tre hefter:

- Hefte 1: Ansatte og sikkerhetskultur
- Hefte 2: Informasjonssikkerhet i Melhus kommune
- Hefte 3: IT-løsning-drift

Hefte 2 om informasjonssikkerhet omtaler hvorfor det er viktig med informasjonssikkerhet i kommunen. Det skyldes blant annet at kommunen har tilgang på store mengder personopplysninger om sine innbyggere og andre som er i kontakt med kommunen. I tillegg er ivaretagelse av personvern viktig for å ivareta enkeltes integritet og befolkningens tillit til kommunen. Kommunen skriver videre:

> «*Melhus skal sørge for å samle inn de personopplysningene kommunen trenger for å levere sine tjenester og utføre lovpålagte oppgaver, men skal samtidig jobbe for å minimere bruke av personopplysninger der det er mulig*.»

Videre skriver kommunen at den, i tillegg til personopplysninger, behandler annen informasjon som er skjermingsverdig. Dette er blant annet kommunal infrastruktur, konkurransesensitive opplysninger fra leverandører og informasjon om egen organisasjon.

Om arbeidet med sikkerhet i Melhus, skriver kommunen i heftet at:

> «*Sikkerhetsnivået i Melhus skal bygge på risikovurderinger som sikrer kjennskap til ulike trusler for ulike informasjonselementer, og at sikkerheten rundt informasjonen er tilpasset den risikoen som er identifisert. For å redusere risikoen for sikkerhets-hendelser skal Melhus jobbe med å ha gode systemer, god internkontroll for oppfølging og avdekking av sikkerhetsbrudd, og bygge en god sikkerhetskultur i kommunen.*»

ITMidt opplyser at sikkerhetshåndboken og styringssystemet for informasjonssikkerhet i Melhus er under revidering og skal erstattes. Strategisk ledergruppe vil bli involvert i dette arbeidet i løpet av høsten 2024.

ITMidt jobber med å bygge opp et nytt system basert på tilpasninger etter EU sitt direktiv NIS2-direktivet (erstatter NIS1-direktivet). Departementet skriver at formålet med NIS2-direktivet blant annet er å øke motstandsdyktigheten i nettverks- og informasjonssystemer og å forbedre den felles bevisstheten og kapasiteten knyttet til motstandsdyktighet.[8] ITMidt forteller at direktivet er et krav som vil komme til Norge, og kommunen forsøker derfor å tilpasse sine styringssystem til disse kravene.

Kommunen benytter seg også av arbeidet foreningen Kommunal Informasjonssikkerhet (KiNS)[9] gjør knyttet til informasjonssikkerhet og oppbygging av maler knyttet til standarden ISO/IEC 27002. KiNS tilbyr blant annet forhåndsutfylte maler og forslag til prosedyrer innenfor informasjonssikkerhet.

Revisor har fått tilsendt det nye systemet for informasjonssikkerhet som er under utarbeidelse i kommunen. Dokumentene i det nye systemet er bygget opp etter tre kategorier, og inneholder planer, prosedyrer og policyer innenfor informasjonssikkerhet. ITMidt forteller at sikkerhetshåndboken skal erstattes av policyer og prosedyrer, hvor policyer er mer regler og prosedyrer er det som skal etterleves. ITMidt forteller videre at de skal vurdere om innholdet i sikkerhetshåndboken skal videreføres med tanke på aktualitet, men dokumentene blir ikke med videre.

De tre kategoriene i det nye styringssystemet er:

- Gjennomførende del
- Kontrollerende del
- Styrende del

[8] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/

[9] Foreningen har som formål å bidra til økt informasjonssikkerhet i kommuner og fylkeskommuner.

Under styrende del er det utarbeidet en egen policy for informasjonssikkerhet. Policyen er det overordnede styringsdokumentet for informasjonssikkerhetsområdet, og har som formål å beskrive overordnede mål, rammer og føringer for alt arbeidet med informasjonssikkerhet i kommunen. Videre skal policyen gi uttrykk for ledelsens holdning til sikring av informasjon og tjenester. Kommunedirektørens ledergruppe er ansvarlig for å sikre at styringssystem for informasjonssikkerhet er etablert.

Nærmere detaljer om de ulike delene av styringssystemet til Melhus kommune vil bli beskrevet i kapitlene nedenfor.

2.2.3 Revisors vurdering

Revisor vurderer at kommunen har lagt et rammeverk til grunn for sitt informasjonssikkerhetsarbeid.

Melhus kommunen bruker en anerkjent standard (ISO/IEC 27002:2002) som sitt rammeverk for arbeid med informasjonssikkerhet. I tillegg har kommunen gjennomgått NSM sine grunnprinsipper, men det gjenstår noe arbeid med dette. Kommunen benytter seg også av KiNS og deres arbeidet med informasjonssikkerhetsarbeid.

Et overordnet rammeverk gir kommunen et system å arbeide etter og bidrar til å sikre at relevante deler fanges opp. Melhus kommune er i ferd med å skifte over til et nytt system. Dette systemet bygger på EU direktivet NIS2, som forventes å komme. Kommunen bruker ulike rammeverk for sitt arbeid. Det kan være krevende å følge flere rammeverk, men samtidig gir det kommunen ulike innfallsvinkler til å bygge opp og tilpasse systemet til kommunens behov.

Revisor vurderer kriteriet som oppfylt.

2.3 Sikkerhetsmål og strategi

2.3.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen skal ha etablert sikkerhetsmål og sikkerhetsstrategi.

2.3.2 Sikkerhetsmål

Hefte 2 om informasjonssikkerhet presenterer sikkerhetsmålene for kommunen. Sikkerhetsmålene beskriver kommunens overordnede mål for beskyttelse av kommunens informasjonsbehandling mot interne og eksterne trusler og hendelser, tilsiktet og utilsiktet.

Kommunen har definert 15 sikkerhetsmål. Revisor har sett disse målene, men velger å ikke gjengi dem konkret. Målene definerer blant annet forankring av sikkerhet i ledelsen i kommunen, tilgang til systemer, rutiner knyttet til uønskede hendelser og kompetanse blant de ansatte for å ivareta kommunens sikkerhetsbehov.

Det nye dokumentet *policy for informasjonssikkerhet* inneholder også tre overordnet informasjonssikkerhetsmål som skal gjelde for alt arbeid med informasjonssikkerhet i kommunen. I tillegg inneholder dokumentet grunnleggende informasjonssikkerhetsprinsipper for arbeidet. Revisor velger å ikke gjenta målene eller prinsippene her.

2.3.3 Strategi

Digitaliseringsstrategi

Melhus kommune vedtok den 28. juni 2019 «*Digitaliseringsstrategi Smartere Melhus 2019-2023*». I oppstartsmøte ble det opplyst at strategien skal revideres, men at kommunen avventer ny nasjonal strategi som er ventet å bli presentert i juni 2024. ITMidt forteller at de rapporterer på oppfølgingen av digitaliseringsstrategien til rådmann og politisk nivå.

Digitaliseringsstrategien omfatter hele organisasjonen, men den har vært lettest å forankre hos ledelsen i kommunen, forteller informantene. Videre forteller de at den politiske forankring av arbeidet med strategien har ført til at det er avsatt tilstrekkelig ressurser i kommunens budsjett. Det er blant annet bevilget midler til to stillinger til sikkerhetsarbeid, hvor en av dem er stillingen som IT-teknisk sikkerhetsansvarlig.

Digitaliseringsstrategien omhandler kommunens systematiske og strukturerte tilnærming til digitalisering. Melhus kommune har i strategien valgt fem områder som skal være førende for arbeidet med digitalisering i strategiperioden:

1. Vi skal sette brukernes behov i sentrum når vi skal vurdere digitale løsninger
2. Vi skal utvikle tjenester, og øke produktiviteten i våre tjenester gjennom bruk av digitale verktøy
3. Vi skal sikre at alle brukere av digitale verktøy klarer å benytte seg av disse
4. Vi skal sikre at digitaliseringsprosjekter gjennomføres på en effektiv måte
5. Vi skal sørge for å ha sikre IT-systemer, og behandle personopplysninger på en forsvarlig måte

Kilde: Melhus kommune

Figur 3. Utklipp fra digitaliseringsstrategien 2019-2023 – fem førende områder

Det siste området i strategien omhandler informasjonssikkerhet, personvern og dokumentasjonsforvaltning. Overordnet føring innenfor dette områder er blant annet at kommunen skal behandle personopplysninger på en måte som ivaretar den enkeltes

personvern, og at slike opplysninger kun skal være tilgjengelig for ansatte med tjenstlig behov for det. På grunn av mye skjermingsverdig informasjon i kommunen, må systemene i kommunen være godt sikret mot ekstern inntrengning og legge til rette for sikker informasjonsbehandling internt. Videre står det:

> «*Nivået på informasjonssikkerheten i Melhus kommune skal være tilpasset den informasjonen kommunen behandler, slik at det er en balanse mellom hensynet til sikring og deling av informasjon. Melhus må unngå å sette seg i en situasjon der sikkerhetsnivået er så strengt at kommunen ender opp med bruk av "skygge-IT" - at brukere tar i bruk andre systemer, for å omgå hindringer som ligger i kommunens systemer*.»

Det står også at personvern og informasjonssikkerhet skal være en integrert del av utviklingen og bruken av IKT. Informasjonssikkerhet skal ivaretas med utgangspunkt i risikovurderinger basert på trussel- og sårbarhetsvurderinger og følges opp gjennom god internkontroll. Kommunen skal ha gode systemer, god internkontroll for oppfølging og avdekking av sikkerhetsbrudd, og bygge en god sikkerhetskultur i kommunen for å redusere risikoen for sikkerhetshendelser.

Et kapittel i strategien sier noe om målbildet for arbeidet med digitalisering, både på overordnet nivå og innenfor hver sektor. På overordnet nivå skal blant annet hver sektor ha eierskap til egne IT-systemer og data skal flyte automatisk mellom systemene for å sikre samhandling og unngå behov for dobbeltregistrering. E-læring skal være en del av kompetanseutvikling. Innenfor sentraladministrasjonen skal IT-støtte gis i størst mulig grad gjennom selvbetjenings-løsninger. Brukere skal selv kunne tilbakestille passord og bestille IT-utstyr i tråd med fullmakter.

Sikkerhetsstrategi

Heftet 2 om informasjonssikkerhet inneholder kommunens sikkerhetsstrategi som beskriver hvilke virkemidler kommunen velger å bruke for å nå sikkerhetsmålene. Sikkerhetsstrategien dekker 15 områder. Et av områdene som strategiene sier noe om, er organisering av sikkerhet. Dette vil bli omtalt i kapittel 2.5. De resterende områdene sikkerhetsstrategien dekker er:

- Egenkontroll
- Personell
- Leverandører
- Fysisk sikkerhet
- Tilgang til IT-løsninger
- Dokumentsikkerhet

- Endringskontroll
- Beredskap
- Avvikshåndtering
- Systemteknisk sikkerhet (hefte 3)
- Anskaffelser av IT-verktøy og IT-løsninger
- Epost
- Risikovurderinger (hefte 3)
- Ledelsen gjennomgang.

Strategien gjør rede for organisatoriske og tekniske valg knyttet til disse områdene og hvordan sikkerhetsarbeidet skal gjennomføres.

2.3.4 Revisors vurdering

Revisor vurderer at kommunen har etablert sikkerhetsmål og sikkerhetsstrategi.

Melhus kommune har definert sikkerhetsmål i sikkerhetshåndboken, som gir overordnede mål for informasjonssikkerhet i kommunen. Digitaliseringsstrategien sier også noe om målbildet, men målene er mer rettet mot digitalisering. Samtidig vurderer revisor at noen av disse målene er relevant for arbeidet med informasjonssikkerhet, blant annet at e-læring skal være en del av kompetanseutvikling.

Kommunene har definert strategier gjennom digitaliseringsstrategien og egen strategi for sikkerhet. Sikkerhetsstrategien beskriver hvordan kommunen skal nå sikkerhetsmålene.

Revisor vurderer kriteriet som oppfylt.

2.4 Sikkerhetsorganisasjon

2.4.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.

2.4.2 Funn

Sikkerhetsorganisasjon i Melhus kommune er både beskrevet i hefte 2 om informasjons-sikkerhet og i et nyere dokument som beskriver roller og ansvar for implementering og vedlike-hold av informasjonssikkerheten i kommunen. Begge dokumentene omtaler organisering av sikkerhet i kommunen og hvem som er medlemmer av sikkerhetsorganisasjonen.

Medlemmene er de som er ansvarlig for å utvikle, implementere, overvåke og forvalte styringssystemet for informasjonssikkerhet. Roller og ansvar er spesifisert, og det skal samarbeides for å sikre at kommunen har et effektivt styringssystem.

Medlemmer av sikkerhetsorganisasjonen, jamfør hefte om informasjonssikkerhet er:

- Rådmann (behandlingsansvarlig)
- Kommunalsjef, enhetsleder, systemeier og systemansvarlig
- Sikkerhetsleder (Denne rollen ligger til beredskapsrådgiver)
- Personvernombud
- Arkivleder
- Leder med personalansvar
- Bruker/medarbeider
- IT-drift/databehandler

Kilde: Melhus kommune

Figur 4. Sikkerhetsorganisering, hefte 2

Medlemmer av sikkerhetsorganisasjonen jamfør nyere dokument er:

- Kommunedirektørens ledergruppe (representant fra gruppen)
- Informasjonssikkerhetsansvarlig (CISO)
- Sikkerhetsarkitekt
- Sikkerhetsrådgiver
- Opplæringsansvarlig
- Personvernombud

I nyere dokument om roller og ansvar står det at det i tillegg til de nevnt ovenfor vil flere ansatte være involvert i arbeidet med informasjonssikkerhet, blant annet gjennom arbeid med risikovurderinger, gjennomføring av sikkerhetstiltak eller at ansatte må forholde seg til sikkerhetsinstrukser.

Roller og tilhørende ansvar er beskrevet i begge dokumentene. I det nyeste dokumentet er også flere roller og ansvar beskrevet enn det som følger av medlemmer av sikkerhetsorganisasjonen, blant annet ansvaret til brukerstøtte, fagledere og ledere med personalansvar. Rådmannens ledergruppe har ansvaret for at styringssystem for informasjonssikkerhet er etablert og årlig gjennomgang av status. De skal også sikre at sikkerhetsorganisasjon er definert og fungerer og at policyen for informasjonssikkerhet er i samsvar med kommunens strategiske mål. De har også ansvar for å sikre nødvendige ressurser til forvaltning av styringssystemet for informasjonssikkerhet.

ITMidt opplyser om at beskrivelse av sikkerhetsorganisasjonen i det nye dokumentet ikke er ferdig utarbeidet, og at de må se på hvilke roller og titler som brukes i dokumentet.

I oppstartsmøte forteller informantene at kommunens ledelse er involvert i overordnet policy, rutiner og tiltak knyttet til informasjonssikkerhet, og at mye har vært tatt opp i kommunens strategiske ledergruppe. IT-sjefen forteller at han deltar i kommunens strategiske ledergruppe, også tilsvarende i Skaun kommune (siden interkommunalt samarbeid). Arbeidet med informasjonssikkerhet er forankret i møter med enhetsledere, opplyses det i oppstartsmøtet.

I intervju med ITMidt og beredskapskoordinator får revisor informasjon om at beredskapsrådgiver har rollen som informasjonssikkerhetsansvarlig og har det overordnede sikkerhetsansvaret i kommunen. Sikkerhetsansvarlig hos ITMidt har rollen som IT-teknisk sikkerhetsansvarlig. ITMidt opplyser om at det har vært viktig for dem å ha det overordnede sikkerhetsansvaret plassert utenfor ITMidt, og at det overordnede ansvaret for informasjonssikkerhet ligger til kommunen og ikke IT.

Beredskapsrådgiverrollen innebærer det overordnede ansvaret for samfunnssikkerhet og beredskap. Beredskapsrådgiver jobber mye på tvers i kommunen, og gjennomfører blant annet intern opplæring i risikoanalyser og risikovurderinger ute på enhetene. Beredskapsrådgiver er også kommunens personvernombud. Organisatorisk er beredskapsrådgiver plassert på enhet plan, under plan og utvikling.

Beredskapsrådgiver forteller at hun skal være mer involvert i arbeidet med informasjonssikkerhet enn det hun har vært så langt etter at hun begynte i stillingen august 2023. Beredskapsrådgiver uttaler at skifte i beredskapsrådgiver kan ha påvirket at arbeidet med informasjonssikkerhet har blitt mindre enn det som er tiltenkt, og at arbeidet har blitt lagt mer til ITMidt. Beredskapsrådgiver forteller at ITMidt er flinke til å holde henne oppdatert, og særlig på arbeidet som er gjort knyttet til ny beredskapsplan på IT.

2.4.3 Revisors vurdering

Revisor vurderer at kommunen har en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet er beskrevet.

Flere dokumenter beskriver kommunens sikkerhetsorganisasjon med roller og ansvar, men roller og ansvar er ikke konsistent. Når beskrivelser finnes i flere dokumenter er det krevende å følge opp at de er identiske. Derfor vurderer revisor at det er viktig at roller og ansvar blir tydelig i de nye styringsdokumentene for informasjonssikkerhet som er under utarbeidelse.

Melhus kommune har organisert arbeidet med informasjonssikkerhet slik at beredskapsrådgiver har rollen som informasjonssikkerhetsansvarlig og det overordnede sikkerhetsansvaret i kommunen. Revisor vurderer dette som positivt med tanke på forankring av arbeidet med informasjonssikkerhet. Informasjonssikkerhet gjelder hele kommunen og ikke bare de som jobber med IKT. På bakgrunn av at arbeidsoppgaver og rolle i informasjonssikkerhetsarbeidet spenner over hele organisasjonen, vurderer revisor at det kan være uheldig at beredskapsrådgiver er plassert ute på en enhet og ikke i en stabsfunksjon under rådmannen. Dette handler om at beredskapsrådgiver jobber tverrsektorielt i kommunen og skal bistå alle enheter.

Revisor merker seg, med bakgrunn i dokumenter og informasjon fra intervju, at arbeidet med informasjonssikkerhet framstår som godt forankret hos ledelsen i kommunen.

Revisor vurderer kriteriet som oppfylt.

2.5 Internkontroll

2.5.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.

2.5.2 Overordnet system

Melhus kommune benytter EQS som kvalitetssystem, både for internkontroll og avviksmeldinger. I oppstartsmøte opplyser informantene om at rutiner og prosesser skal ligge i EQS, men at det fortsatt er en jobb for å få alt på plass. ITMidt har sine rutiner og prosedyrer bygget opp i Teams og Sharepoint. Revisor får opplyst fra ITMidt at sikkerhetshåndboken med hefte 1 og hefte 2 er tilgjengelig for de ansatte. Hefte 3 er unntatt offentligheten.

I det nye styringssystemet for informasjonssikkerhet (som er under arbeid) er det utarbeidet et dokument for «dokumentstruktur i styringssystemet for informasjonssikkerhet». Dokumentet legger rammer og føringer for strukturen for dokumentene som inngår i styringssystemet for informasjonssikkerhet. Det er definert prinsipper for hvordan dokumentene skal utformes. Den overordnede strukturen av dokumentene er presentert og består av den styrende, den gjennomførende og den kontrollerende delen. Dokumentet referer til ISO 27003 standarden.

Hefte 2 om informasjonssikkerhet inneholder en del om ledelsens gjennomgang av styringssystemet for informasjonssikkerhet. Ledelsen skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av sikkerhet for å kontrollere at disse er i samsvar med kommunens behov. Rutinen for gjennomgangen er beskrevet i heftet. I gjennomgangen deltar

representanter fra kommunens øverste ledelse sammen med sikkerhetsleder og IT-leder, hvor ledelsen har ansvaret for at gjennomgangen blir gjennomført. Rutinen inneholder hva som skal vurderes og hensikten med evalueringen. På bakgrunn av gjennomgangen blir det utarbeidet forbedringstiltak, som skal godkjennes av rådmannen. Det skal skrives referat fra disse gjennomgangene. Revisor har ikke etterspurt dette.

Under kontrollerende del i det nye styringssystemet er det utarbeidet en prosedyre for ledelsens gjennomgang av styringssystemet for informasjonssikkerhet. Prosedyren er knyttet opp til at ledelsen skal med planlagte mellomrom gjennomgå styringssystemet for å sikre at systemet er velegnet, tilstrekkelig og virkningsfullt. I tillegg er det utarbeidet en prosedyre for internrevisjon. Prosedyren regulerer hvordan internrevisjon av kommunens styringssystem for informasjonssikkerhet skal gjennomføres med hensyn til blant annet omfang og prioriterte områder for internrevisjon. Prosedyren beskriver også forberedelse av internrevisjonen, selve gjennomføringen og avslutning av internrevisjonen. Krav til internrevisor er spesifisert, og at informasjonssikkerhetsleder er ansvarlig for internrevisjonen.

Kommunen har også en prosedyre for overvåking, måling, analyse og evaluering der formålet er at styringssystemet overvåkes, måles, analyseres, evalueres og kontinuerlig forbedres. Prosedyren inneholder en oversikt over relevante nøkkelindikatorer. Det er informasjonssikkerhetsleder som er ansvarlig for dette arbeidet.

2.5.3 Avvik

Avdekke og følge opp avvik og risiko for avvik er en del av kravet til internkontroll. Melhus kommune har et eget skjema i EQS for å melde avvik knyttet til brudd på informasjonssikkerhet/personvernopplysningsloven som alle ansatte kan benytte. Revisor fikk systemet demonstrert under datainnsamlingen.

Tidligere mottok personvernombudet avviksmeldingen og videresendte den til rådmann. Nå er praksisen at avvik som meldes i EQS skal gå til nærmeste leder. Ved avvik om brudd på informasjonssikkerhet/personopplysningsloven mottar IT-sjefen, rådmannen og personvernombudet en kopi. IT-sjef forteller at dette er et bevisst valg, siden det er nærmeste leder som har ansvaret dersom avviket omhandler databehandleravtale[10] og som kjenner til hvilke data enheten behandler. IT-sjef forteller at styring av avvikene fungerer nå.

[10] Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale. Avtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysninger. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/hvordan-lage-en-databehandleravtale/

Melhus kommune har to rutiner/prosedyrer knyttet til avvikshåndtering. Sikkerhetsansvarlig forteller at rutinene ikke er sammenstilt enda. Den ene, som er en rutine, er tilgjengelig i EQS. Den andre er en prosedyre som er tilgjengelig i dokumentstrukturen hos ITMidt. Rutinen som er tilgjengelig i EQS inneholder en beskrivelse av formål, grunnlagsinformasjon, ansvar og arbeidsbeskrivelse. Arbeidsbeskrivelsen sier noe om hvem som skal behandle avviket og på hvilken måte, samt en vurdering av om avviket skal meldes til Datatilsynet.

I prosedyren er definisjonen av et avvik inkludert. Videre er det definert prinsipper for avvikshåndtering og prosess for håndtering av avvik. Metode for rotårsaksvurdering er også inkludert, med formål om å identifisere den grunnleggende årsaken til et avvik. Også ansvarlig for prosedyrer er gitt, og ansvaret er lagt til informasjonssikkerhetsleder.

Tabellen nedenfor viser omfanget av antall avvik som er meldt knyttet til brudd på informasjonssikkerhet/personopplysningsloven i perioden fra 2018 og så langt i 2024.

Tabell 1. Antall avvik meldt knyttet til brudd på informasjonssikkerhet/personopplysningsloven for 2018-2024 i Melhus kommune.

År	2018	2019	2020	2021	2022	2023	2024
Antall avvik	3	11	6	4	2	6	5

Kilde: Melhus kommune

Tabellen viser at det var i 2019 flest meldte avvik, mens færrest meldte i 2022.

2.5.4 Revisors vurdering

Revisor vurderer at informasjonssikkerhet inngår i kommunens internkontrollsystem.

Revisor har ikke sett på kommunens internkontrollsystem, men hatt fokus på internkontroll knyttet til informasjonssikkerhet.

Styringssystemet for informasjonssikkerhet, gjennom hefte 1 og 2, er tilgjengelig for alle ansatte. Rutiner og prosedyrer skal være tilgjengelig i EQS, men kommunen opplyser at ikke alt er på plass. ITMidt har sine rutiner tilgjengelig gjennom sine systemer. Evaluering og oppdatering av rutiner er beskrevet gjennom ledelsen gjennomgang av styringssystemet i hefte 2. Revisor har ikke undersøkt hvordan dette gjennomføres i praksis.

Avvik i kommunen meldes i EQS, og det er et eget skjema for å melde avvik knyttet til brudd på informasjonssikkerhet/personopplysningsloven. Ved brudd på informasjonssikkerhet-/personopplysningsloven mottar både rådmann, IT-sjef og personvernombud en kopi. Kommunen har egne rutiner og prosedyrer for avvikshåndtering.

Revisor vurderer kriteriet som oppfylt.

2.6 Risikovurderinger

2.6.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.

2.6.2 Funn

Melhus kommunen har utarbeidet en overordnet og helhetlig risiko- og sårbarhetsanalyse (ROS-analyse) fra mars 2023. Kommunestyret vedtok ROS-analysen med vedlegg i sak 23/23. ROS-analysen inneholder blant annet kommunens utvalg av uønskede hendelser som kan ramme kommunesamfunnet. I analysen skriver kommunen at:

> «*Analysen vil videre være nyttig for fag- og sektorområdene i kommunen, og den vil også fungere som et kunnskaps- og beslutningsgrunnlag for kommunens ledelse og deres oppfølging av samfunnssikkerhet- og beredskapsarbeid i Melhus.*»

En av de uønskede hendelsene som Melhus kommunen har inkludert i sin ROS, er cyberangrep. Kommunen skriver i analysen at hendelsen er valgt med bakgrunn i hendelser valgt av Trøndelag fylke sin ROS-analyse, det nasjonale sikkerhetsbildet, og at kommunen selv anser hendelsen som sentral.

Uønskede hendelser er nærmere beskrevet og beskrivelsen av cyberangrep er unntatt offentlighet. Revisor har sett hvordan cyberangrep er beskrevet i dokumentet, men gjengir ikke informasjonen i detalj. Beskrivelsen av hendelsen inneholder blant annet risikovurdering, oversikt over eksisterende og nye tiltak, og sårbarhetsvurdering før og etter implementering av nye tiltak.

Med utgangspunkt i ROS-analysen skal kommunen utarbeide en overordnet beredskapsplan. Revisor har fått tilsendt en overordnet beredskapsplan, datert 1. februar 2024. Melhus kommune har en egen beredskapsplan for informasjonssikkerhet, som omtales nærmere i kapittel 3.5.

Hefte 2 om informasjonssikkerhet inneholder et eget kapittel om risikostyring. Heftet sier at Melhus kommune skal gjennomføre risikovurderinger ved endringer i forhold som kan påvirke informasjonssikkerhet, både endringer i informasjonssystemet og i trusselbildet. Formålet med risikovurderinger er å undersøke om avdekt risiko er innenfor akseptkriteriene som kommunen

har fastlagt. Akseptkriteriene blir presentert i heftet. Risikovurderingen vil danne grunnlag for iverksetting av nødvendige sikkerhetstiltak, og inngå som en del av informasjon knyttet til ledelsen gjennomgang av informasjonssystemet og informasjonssikkerhet.

Melhus kommune har utarbeidet tre dokumenter som omhandler risiko knyttet direkte til informasjonssikkerhet, og inngår som en del av det nye styringssystemet for informasjonssikkerhet:

- Prosedyre for risikostyring
- Risikoregister
- Risikohåndteringsplan

Prosedyren for risikostyring definerer hvordan risikovurderinger og sikkerhetstiltak skal gjennomføres, mens risikoregisteret viser en oversikt over alle identifiserte og analyserte risikoer. Risikohåndteringsplanen inneholder oversikt over hvordan risikoer nevnt i risikoregisteret håndteres med tiltak.

Prosedyren for risikostyring gir føringer for at risikovurderinger skal gjennomføres ved alle typer planlagte endringer og i situasjoner med vurdert sårbarhet eller endret trusselbilde. Prosedyren gir eksempler på slike situasjoner:

- Informasjonssystemer som inneholder personopplysninger (behandlinger)
- Endringer i relevante lover og forskrifter
- Endringer i tjenestekatalogen
- Organisasjonsendringer
- Innføring av nye IT-systemer
- Flytting av infrastruktur og tjenester til skyen
- Flytting til nye lokaler
- Etablering av nye leverandører
- Endringer av trusselbildet

Videre står det at alle risikovurderinger skal dokumenteres og arkiveres, herunder må det gjøres vurderinger og beslutninger om sikkerhetstiltak. Prosedyren gir en beskrivelse av fasene ved gjennomføring av risikostyring. Risikostyring består av risikovurdering (inkluderer fasene identifisering, analyse og evaluering) og risikohåndtering (fasen for sikkerhetstiltak). De ulike fasene er beskrevet i prosedyren.

Risikoregisteret revisor har fått tilsendt er ikke utfylt, men gir en beskrivelse av hvilke kolonner med hvilken informasjon et slikt register bør inneholde. Her nevnes blant annet beskrivelse av uønsket hendelse, sannsynlighet, konsekvens, og hvem som er ansvarlig i kommunen for å håndtere risikoen. Tilsvarende gjelder for risikohåndteringsplan; versjonen revisor har fått

tilsendt inneholder ikke en oversikt over hvordan risikoer håndteres med tiltak. Dokumentet skisserer hvilken informasjon en slik plan bør inneholde, blant annet risikoeier, tiltak og frist for gjennomføring av tiltak.

Revisor har fått tilsendt rutine for risiko- og sårbarhetsvurdering i Melhus kommune som gjelder for hele kommunens virksomhet. Rutinen inneholder en beskrivelse av formålet med ROS, grunnlagsinformasjon og arbeidsbeskrivelse. Under arbeidsbeskrivelse, står det at ROS-modulen i CIM (kommunens kommunikasjonssystem i beredskapsarbeid) skal brukes som verktøy ved ROS-vurdering. I oppstartsmøte opplyste informantene om at CIM ikke lengre er i bruk og at kommunen fra 1. oktober 2023 bruker RAYVN som nytt krisehåndteringssystem. Melhus kommune hadde brukt 2-3 år på å bygge opp ROS og tiltakskort i CIM. RAYVN inneholder ikke tilsvarende mulighet for å gjennomføre ROS-analyser. Beredskapskoordinator opplyser at gjennom avtalen mellom direktoratet for sikkerhet og beredskap (DSB) og RAYVN fikk kommunene mulighet til å gjøre avrop på ROS-programmet Dmaze[11]. Melhus kommune har nettopp begynt å ta i bruk Dmaze for å gjennomføre ROS-analyser på sektornivå. IT-sjef opplyser om at risikovurderinger fra CIM er eksportert og tatt vare på enhetsvis.

IT-sjef forteller at tidligere personvernombud var ute i organisasjonen og gjennomgikk risikovurderinger da GDPR ble innført. Det ble da gjort en risikovurdering til bruken og databehandling på hvert system. IT-sjef forteller at nå gjøres denne risikovurderingen på den tekniske delen også. ITMidt har utarbeidet en prosjektveiviser hvor alle prosjekter som initieres i kommunen skal kjøres gjennom. I prosjektveiviseren ligger det et krav om at det skal være utført ROS-analyse tilhørende prosjektet. IT-leder forteller at dersom prosedyren ikke følges, sendes den tilbake med beskjed om å gjennomføre alle trinnene.

I rutinen for risikovurderinger, som er tilgjengelig i EQS, refereres det til behandling av personopplysninger (DPIA) og en klikkbar link til når det må gjennomføres DPIA (revisor er ikke kjent med om denne linken fungerer eller hva det linkes til). Videre står det at:

«*Personvernombud kontaktes der det er behov for bistand til DPIA/risikovurdering ved behandlingsaktiviteter/personvernvurderinger.»*

Beredskapsrådgiver forteller at hun ikke har mottatt noen henvendelser knyttet til DPIA.

Når det gjelder risikovurderinger knyttet til sensitive personopplysninger og personvernkonsekvenser, har revisor fått tilsendt behandlingsprotokoll (nærmere omtalt i kapittel 2.7). I behandlingsprotokollen er det på flere av systemene, også systemer som

[11] https://www.dmaze.com/dsb?lang=no

behandler sensitive personopplysninger, svart nei på personvernkonsekvenser. På system for kameraovervåkning kommunale bygg henvises det til ROS på personvernkonsekvenser. Et annet eksempel er registrering og oppfølging av sosialhjelpsmottakere hvor det for personvernkonsekvensvurdering henvises til ROS-analyse og at personvern og informasjonssikkerhet er en risiko i HMS-ROS-analysen. Innenfor helseområdet framgår det at det er gjennomført enkle risikoanalyser for systemene.

2.6.3 Revisors vurdering

Revisor vurderer at kommunen gjennomfører og dokumenterer risikovurderinger som grunnlag for informasjonssikkerhetstiltak.

Melhus kommunen har en overordnet ROS-analyse fra mars 2023 der cyberangrep er en av de uønskede hendelsene. På bakgrunn av ROS-analysen er det utarbeidet en overordnet beredskapsplan. Kommunen har også en egen beredskapsplan for IT (omtales i kapittel 3.5).

I kommunen sitt kvalitetssystem er rutine for utarbeidelse av ROS-analyser tilgjengelig. Kommunen har en prosjektveiviser som inneholder en risikovurdering. Hvis noen i kommunen skal anskaffe et nytt dataprogram eller annet IKT-system, må trinnene i denne prosjektveiviseren gjennomgås. Revisor vurderer at denne praksisen ivaretar kravet om at det skal utarbeides ROS-analyser som grunnlag for informasjonssikkerhetstiltak.

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at kommunen gjennomfører risikovurderinger og dokumenterer vurderinger av personvernkonsekvenser.

Behandlingsprotokollene viser at det er vurdert personvernkonsekvenser for de ulike systemene. For noen av systemene vises det til risikovurderinger. Rutinen for risikovurderinger inkluderer informasjon om vurdering av personvernkonsekvenser. Revisor har ikke sett på om det er gjennomført risikovurderinger og vurderingene av personvernkonsekvenser er dokumentert knyttet til data og informasjon som oppbevares i papirform.

Revisor vurderer kriteriet som oppfylt.

2.7 Behandlingsoversikt

2.7.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.

2.7.2 Funn

Artikkel 30 i personvernforordningen stiller krav til at det skal føres protokoll over behandlingsaktiviteter og hva protokollen skal inneholde. På kommunens hjemmeside opplyses det følgende:

> *Rådmannen i Melhus kommune er behandlingsansvarlig, bestemmer formålet med behandlingen av personopplysninger som innhentes og er ansvarlig for at de behandles i tråd med gjeldende lover og forskrifter.*[12]

Melhus kommune sin behandlingsoversikt ligger i kvalitetssystemet EQS i pdf-format. ITMidt har en oversikt over ulike systemer og applikasjoner som er bygd opp i SharePoint.

Revisor har fått tilsendt en protokoll over behandlingsaktiviteter, hvor endringshistorikken viser at den er sist oppdatert 31.03.2023. Det er uklart hvordan protokollen over behandlingsaktiviteter oppdateres, fortelles det i oppstartsmøtet. Rådmann er oppført som behandlingsansvarlig. Personvernombudet som er oppført, har sluttet i kommunen. På kommunens nettside om personvernerklæring er det et annet navn på personvernombudet enn hva som står i behandlingsprotokollen, og begge er forskjellig fra den som har rollen som personvernombud i dag.

I behandlingsprotokollen finnes det 41 systemer med hver sin registrering. Revisor har ikke undersøkt om protokollen er fullstendig. Noen bokser henviser til flere systemer. For hvert system er det lagt inn opplysninger som artikkel 30 krever. I flere tilfeller er Melhus kommune lagt inn som databehandler.

Kommunen har rutiner som fanger opp oppfølging av databehandleravtaler. ITMidt behandler ikke databehandleravtalene. Det er ledere ute på enhetene som bruker systemene som gjennomgår dem og rådmannen signerer.

ITMidt har systemoversikt over hvem som er systemansvarlig, eier og superbrukere på ulike systemer og applikasjoner. På intranettet framgår det hvem som har roller i de ulike systemene. ITMidt har oversikt over hvem som er teknisk ansvarlig, men dette deles ikke med alle på grunn av sikkerhetshensyn.

ITMidt forteller at kommunen skal ta i bruk FIKS Digiorden, som vil erstatte den behandlingsprotokollen kommunen har i dag og den systemoversikten som ITMidt har.

---

[12] Personvernerklæring - Melhus kommune, 17.04.2024.

2.7.3 Revisors vurdering

Revisor vurderer at Melhus kommune har en protokoll over hvilke personopplysninger kommunen behandler, men at det ikke er noe system for oppdatering av den.

Registreringene i behandlingsprotokollen er noe mangelfull. Melhus kommune er oppført som databehandler flere steder i behandlingsprotokollen. Datatilsynet skriver at det er den behandlingsansvarlige som bestemmer over personopplysningene, mens databehandleren opptrer på vegne av den behandlingsansvarlige. Databehandleren kan derfor bare behandle personopplysninger etter instruks fra den behandlingsansvarlige. Revisor vurderer at det er uheldig at rollene brukes feil for det kan for eksempel oppstå misforståelser.

Opplysninger om hvem som er personvernombud er ikke oppdatert i behandlingsprotokollen og kommunens hjemmeside.

Oversikten ITMidt har over datasystemene og behandlingsprotokollen har mange likheter, men ITMidt sin oversikt er ikke bygd opp for å være en behandlingsprotokoll. Melhus kommune skal ta i bruk FIKS Digiorden som blant annet ivaretar behandlingsprotokoll.

Revisor vurderer kriteriet som delvis oppfylt.

2.8 Opplæring

2.8.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

2.8.2 Funn

Ansatte i Melhus kommune må signere en sikkerhetsinstruks ved ansettelse og oppdateringer av den. Sikkerhetsinstruksen er tilgjengelig i EQS og utgjør ett av heftene i sikkerhetshåndboken til kommunen. Revisor har fått den demonstrert i EQS, samt oversendt. IT-sjef opplyser at sikkerhetsinstruksen må revideres for å være tilpasset dagens sikkerhetsbilde og gjeldende prosedyrer. Alle ansatte må signere ny sikkerhetsinstruks når den er på plass.

Sikkerhetsinstruksen inneholder beskrivelse av retningslinjer for bruk av IKT-tjenester i Melhus. Instruksen inneholder 11 viktige punkter for bedre informasjonssikkerhet, blant annet at taushetsplikten overholdes, være på vakt knyttet til eksterne eposter og vedlegg, ivaretagelse og behandling av personopplysninger og at brudd og andre avvik knyttet til informasjonssikkerhet skal meldes. Det er også påpekt at det ikke gis anledning til lagring av

bilder, film og musikkfiler grunnet at slike filer krever stor lagringsplass og kan hindre nødvendig sikkerhetskopiering. Instruksen inneholder også de viktigste sikkerhetstiltakene i IKT-løsningen, blant annet informasjon om brukeradministrasjon, passord, nettverk delt i soner og enheter (mobil, smarttelefon og nettbrett). Instruksen beskriver også kommunens regler for internett og media. Siste kapittelet i instruksen omhandler avvik og sikkerhetsbrudd.

Under intervju opplyser ITMidt at kommunen skal i gang med en sikkerhetskulturkampanje fra KS. Kampanjen er besluttet i strategisk ledergruppe og hadde oppstart i mars 2024 for alle ansatte, unntatt ansatte innenfor helse som starter kampanjen i september 2024 grunnet innføring av Helseplattformen i slutten av april 2024.

IT-sjefen opplyser at opplæringen fra KS er en holdningskampanje som skal gjennomføres både i Melhus og Skaun. Det er gjennomført et webinar som oppstartsmøte. Opplæringen blir ikke et tradisjonelt kurs, men mer tid til refleksjoner og diskusjoner. Kommunen har gjennomført løpende sikkerhetsopplæring i flere runder fra 2022 i form av nettbaserte kurs for de ansatte. Kommunen har ikke vært fornøyd med pedagogikken i kursene og kursene ble stoppet i mars 2024. Innholdet i kurset var greit det første året, men det ble for teknisk det andre året. Nå planlegges det å legge opplæring av de ansatte ut på anbud og spesifisere nærmere hva kommunen ønsker. Tidligere kurs nådde heller ikke alle ansatte, opplyser ITMidt. Opplæringen må gjøres enkel og forståelige for de ansatte.

ITMidt forteller at de også har gjennomført tester for å undersøke om brukere avgir brukernavn og passord sammen med læringsleksjoner. Det er stor interesse for antallet som avgir slik informasjon, men ITMidt sier at en bruker er en for mye. Slike tester ble sendt ut fra oktober 2023 til mars 2024. I perioden registrerte ITMidt at trenden gikk nedover. Testene dannet også grunnlag for refleksjoner ute på enhetene i kommunen. ITMidt ser at det er behov for å øve på sikkerhetskulturen, og brukeren er det svakeste leddet. KS sin holdningskampanje passer fint, mener ITMidt.

Testene som ITMidt har brukt for å sjekke om brukere avgir informasjon, er stoppet nå på grunn av sikkerhet. Testene og kurset var noe dynamisk, slik at brukere som hadde trykket på lenker fikk tilpasset kurset.

2.8.3 Revisors vurdering

Revisor vurderer at Melhus kommune sørger for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

Melhus kommune legger til rette for at ansatte skal få tilstrekkelig opplæring i informasjonssikkerhet gjennom at ansatte må signere en sikkerhetsinstruks og at kommunen

nå gjennomfører KS sin holdningskampanje. Kommunen har tidligere gjennomført nettbasert opplæring med jevne mellomrom om informasjonssikkerhet. Det er positivt at kommunen er kritisk til innholdet i opplæringen og ønsker å være tydeligere på hva den skal inneholde. ITMidt har også gjennomført tester blant de ansatte for å undersøke hva og hvilken informasjon de ansatte avgir, samt hvor mange som avgir slik informasjon.

Revisor vurderer kriteriet som oppfylt.

2.9 Hendelser

2.9.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen bør evaluere og lære av hendelser.

2.9.2 Funn

I oppstartsmøtet kommer det fram at kommunen hadde to uønskede hendelser våren 2020. De ble oppdaget gjennom logger, hvor epostsystemet sendte ut tusenvis av eposter. Det medførte at kommunens e-postsystem ble svartelistet, og e-poster fra kommunen kom ikke fram. Politikerne ble også rammet, noe som gjorde at de ble oppmerksomme på informasjonssikkerhet og konsekvensene av hendelser. Informantene forteller at hendelsene ble brukt både internt og politisk som læring knyttet til konsekvenser. Kommunen har også brukt eksemplet fra Østre-Toten kommune, som ble rammet av et stort dataangrep i 2021.

ITMidt forteller at tidligere hendelser har ført til umiddelbare tiltak. Teknisk sikkerhet er et fast punkt i driftsmøtene hos ITMidt hver uke. ITMidt får også varslinger fra sine samarbeidspartner som igjen kan føre til tilpasninger, og gjerne før det skjer en uønsket hendelse.

2.9.3 Revisors vurderinger

Revisor vurderer at Melhus kommune evaluerer og lærer av hendelser.

Informasjon indikerer at kommunen bruker hendelser og varslinger fra sine samarbeidspartnere til å evaluere og lære. Blant annet medfører det igangsetting av umiddelbare tiltak.

Revisor vurderer kriteriet som oppfylt.

2.10 Konklusjon

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

Revisor konkluderer med at Melhus kommune har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller 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.

3 ORGANISATORISKE OG TEKNISKE TILTAK

3.1 Problemstilling

Det er utarbeidet følgende problemstilling:

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

3.2 Identifisere og kartlegge

3.2.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen må ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.
- Kommunen må ha et system for styring av tilganger.

3.2.2 Oversikt over enheter i IT-systemet

Melhus kommune har en policy for bruk og sikring av brukerutstyr som PCer, nettbrett og mobiltelefoner. Policyen skal bidra til å sikre at brukerutstyret har en sikker konfigurasjon som innebærer at det er gjennomført relevante tekniske sikkerhetstiltak på utstyret. Dette omfatter blant annet at kommunen skal en oppdatert oversikt over hvilket utstyr som til enhver tid er i bruk. I policyen er det også regler for brukernes ansvar for å sikre brukerutstyret. Inntil policyer og prosedyrer er iverksatt, er ikke brukerne kjent med disse kravene.

I hefte 1 om ansatte og sikkerhetskultur, som er gjeldende i dag, står det eksempelvis at

- PC, smarttelefon, nettbrett, lagringsmedier og annet portabelt utstyr skal konfigureres av IKT-enheten.
- All maskinvare og lagringsmedia/harddisk skal være registeret hos IKT-enheten.

Heftet omtales også som sikkerhetsinstruks og skal signeres av den ansatte.

ITMidt har en oversikt over alle enheter i IT-systemet gjennom et egnet verktøy. ITMidt forteller at de har god kontroll på enheter som er koblet til nettet ute på enhetene. Etter hvert blir mobiler også lagt inn i det samme verktøyet.

Det er ikke mulig koble på trådløst nett med ekstern enhet. For å komme på kommunens nett må maskiner være oppdatert. Det skjer en årlig kartlegging av klienter for å identifisere enheter som bør skiftes ut og når. Da går det melding til enhetsledere slik at de kan budsjettere fornyelse.

3.2.3 Oversikt over programvare

Revisor har fått demonstrert ITMidt sin oversikt over systemer og applikasjoner som er bygd opp i SharePoint. Oversikten viser alle applikasjoner og hvem som har ulike roller i de forskjellige applikasjonene.

Kommunens policy for bruk og sikring av brukerutstyr, regulerer blant annet at brukerne ikke skal kunne installere programvare på egne maskiner.

I hefte 1 om ansatte og sikkerhetskultur står det eksempelvis at IKT-enheten skal kontaktes hvis noen har bruk for annen programvare. ITMidt har tatt i bruk prosjektveiviseren for anskaffelse av ny programvare. Dette er nærmere beskrevet i kapittel 3.3.2.

Gjennom FIKS Digiorden håper kommunen å få en enkel oversikt over avhengigheter som finnes mellom systemer, forteller ITMidt.

3.2.4 Tilgangsstyring

I hefte 2 om informasjonssikkerhet i Melhus kommune beskrives rutiner for tilgangsstyring. Et av målene, spesielt i forhold til personopplysninger, er robusthet. Det innebærer at kommunen skal ha sikre IT-systemer som er motstandsdyktige og behandler personopplysninger på en forsvarlig måte. Videre at det er mulig å gjenopprette normaltilstand etter en fysisk eller teknisk hendelse. To av delmålene er:

- Det må sikres at kun autorisert personell har adgang til det enkelte fagsystem.
- Sensitive personopplysninger sikres mot uautorisert tilgang.

En av strategiene for å følge opp målene er at det skal gjennomføres tilgangskontroll til fagsystemene hvert kvartal. Videre står det at områder hvor personopplysninger lagres skal sikres med adgangskontroll. Et av tiltakene er tildeling, sletting og kontroll av autorisasjon.

Tilgangen til IT-løsninger er nærmere beskrevet slik:

- Enhetsleder er ansvarlig for å klarlegge og autorisere den ansattes behov for tilganger og formidle dette til IT-drift ved ansettelse eller endringer i ansvar.
- Enhetsleder er ansvarlig for å melde til IT-seksjonen at personell slutter slik at tilgangsrettigheter fjernes.

- IT-drift er ansvarlig for å vedlikeholde tilgangsrettigheter samt holde oversikt over de tilgangsrettigheter som er gitt.

Kommunen har en policy for tilgangsstyring. Her står det blant annet at autentiseringsstyrken skal ta utgangspunkt i informasjonens klassifiseringsnivå. Det er også en egen passordpolicy som setter krav til ansattes brukerkontorer og passord. I policyen listes det opp en rekke krav til selve passordet og bruken av det.

ITMidt har gjort vurderinger på at de har kontroll på identiteter og tilganger. I den sammenhengen er det viktig å minimere tilgangen til sluttbrukere og spesialbrukere. Videre er det et prinsipp om ikke å tildele administratorrettigheter til sluttbruker og retningslinjer for hvordan håndtere spesialbrukere som unntaksvis har behov for utvidede rettigheter.

I oppstartsmøtet fortelles det at tilgangskontrollen er digitalisert og bestemmes gjennom roller og tilhørighet i HR-systemet. Tilgangen er predefinert ut fra arbeidssted, hvor bruker får tildelt standardsystemer og lisenser. I HR-systemet blir det tildelt startdato og selve brukeren opprettes 14 dager før vedkommende starter i jobben. Hvis den ansatte får en annen organisatorisk tilhørighet i organisasjonen fører det til at den ansatte mister tilganger og rollestyring. Tilgangene reverseres med stoppmelding på ansatte. Noen stillinger fanges ikke opp. Systemet med rollestyring koblet til HR-systemet gjør tilgangsstyringen dynamisk.

ITMidt har systemoversikt over hvem som er systemansvarlig, eier og superbrukere. På intranettet presenteres det hvem som har roller i de ulike systemene, noe revisor fikk demonstrert i oppstartsmøtet. ITMidt har oversikt over hvem som er teknisk ansvarlig, men dette deles ikke med alle.

Kommunen har selv vurdert at den har kontroll på identiteter og tilganger, noe som NSM har ansett som høyt prioriterte sikkerhetsprinsipper.

ITMidt forteller i intervjuet at de har vært restriktive til å la eksterne få tilganger i kommunens systemer. Kommunen har nå fått på plass et bra system for tilganger for tredjeparter. Leverandører har ofte egne enheter som er koblet på VPN mot leverandør. ITMidt holder på å lage et årshjul for å følge opp leverandører.

Hefte 1 ansatte og sikkerhetskultur forteller at kommunen har totrinns pålogging samt regler for passord.

3.2.5 Revisors vurdering

Revisor vurderer at Melhus kommune har oversikt over enhetene i IKT-systemet.

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at Melhus kommune har oversikt over programvaren som benyttes på kommunens IT-system.

ITMidt har en systemoversikt over programvare og applikasjoner som inngår i kommunens informasjonssystem.

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at Melhus kommune har et dynamisk system for styring av tilganger.

Revisor finner at Melhus kommune har knyttet tilgangsstyringen til HR-systemet. Dette gjøre at tilganger stopper når det blir gjort endringer i ansettelsesforholdet. Tilknytningen til HR-systemet gjør at tilgangene vil være dynamiske og automatiserte. Kommunen antyder at systemet ikke er fullstendig slik det er i dag.

Revisor vurderer kriteriet som oppfylt.

3.3 Beskytte og opprettholde

3.3.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.
- Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer.
- Kommunen må ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

3.3.2 Anskaffelser

ITMidt har utviklet en prosjektveiviser for henvendelser om ny programvare og digitaliserings-muligheter. Dette er en digitalisert løsning hvor den som ønsker en ny applikasjon eller løsning må gjennom alle trinnene i et innføringsprosjekt. Dette innføringsprosjektet krever at det er forankret og at det er avsatt ressurser. Trinnene omfatter også risikovurderinger og gevinstrealisering. Alle prosjekter ligger åpent i prosjektveiviseren. Kommer det forespørsler utenom prosjektveiviseren, blir de henvist til å bruke den. Underveis i kommunens beredskapsøvelse kom det opp en planlagt anskaffelse, som ikke hadde gått trinnene i prosjektveiviseren.

Kommunen har selv vurdert at de oppfyller de to høyest prioriterte tiltakene sikkerhetsprinsippene fra NSM innenfor anskaffelse av IKT-produkter med henvisning til beredskapsplanverket.

Kommunen har en egen policy for anskaffelse og forvaltning av programvarelisenser. Denne policyen sier at kommunen skal ha en liste over lisensene og at lisensavtalene skal arkiveres, tilgangssikres og sikkerhetskopieres. Ansvaret for denne policyen er lagt til innkjøpsansvarlig.

Melhus kommune har en policy for informasjonssikkerhet i leverandørforhold. Den er en overbygning for prosedyre for kontroll av leverandører (datert 23.02.2024). Det framgår av prosedyren at alle databehandlere skal ha en databehandleravtale. Alle leverandører skal registreres og risikovurderes. Det skal gjennomføres kontroll med utgangspunkt i risikovurderingene.

3.3.3 IKT arkitektur

ITMidt forteller at de har en systemoversikt i tillegg til oversikt over fagprogrammer og applikasjoner. ITMidt har full systemoversikt med den er ikke samlet i eget system for virksomhetsarkitektur. Dette blir ivaretatt når Fiks Digiorden tas i bruk. ITMidt har oversikt over alle serverne og brannmurer som kommunen benytter. Denne oversikten finnes også på en usb-pinne. Nettverksverktøyet IMS tegner et kart. Nettverksansvarlig tar det ut hvis det gjøres endringer.

Det skal lages et årshjul som skal ivareta ulike gjøremål, blant annet oppfølging av sertifikatskifter og lignende som må gjøres.

Kommunen har selv vurdert at de oppfyller det høyest prioriterte NSM sikkerhetsprinsipp om IKT-arkitektur, nærmere bestemt å dele opp virksomhetens nettverk etter virksomhetens risikoprofil. Det er etablert egne soner for servere samt egen brannmur for soner med sensitiv informasjon.

3.3.4 Sikkerhetsoppdatering

Hefte 1 om ansatte og sikkerhetskultur sier at all maskinvare skal være registrert hos IKT-enheten. For å komme på kommunens nett må maskiner være oppdatert, forteller ITMidt. Det fortelles at skole og barnehage nå begynner å lease utstyr blant annet for å ivareta sikkerheten.

Dette handler om å ivareta en sikker konfigurasjon og her avgrenset til om kommunen har en sentral styring med sikkerhetsoppdateringer. NSM har vurdert dette som et høyt prioritert sikkerhetsprinsipp. ITMidt har vurdert at dette de oppfyller dette prinsippet og har henvist til to ulike verktøy for å ivareta dette.

I prosedyren for sårbarhetskartlegging går det fram at identifiserte sårbarheter håndteres i henhold til sårbarhetens alvorlighet. Sårbarhetene kan håndteres med forebyggende tiltak eller avbøtende tiltak. ITMidt forteller at det gjøres tilpasninger i systemet når det blir kjent at det er sårbart. ITMidt kan få beskjed om sikkerhetsoppdateringer fra eksterne og noen beskjeder kan komme i forbindelse med overvåkning av systemer, noe som er nærmere omtalt i kapittel 3.4.2.

Ifølge det interne dokumentet om roller og ansvar for implementering og vedlikehold av informasjonssikkerhet i kommunen, er det systemansvarlig som skal gjennomføre oppdatering og vedlikehold av det enkelte system.

3.3.5 Sikkerhetskopier

Hefte 1 om ansatte og sikkerhetskultur har et punkt om sikkerhetskopiering rettet mot ansatte, med blant annet regler om at all jobbrelatert informasjon lagres slik at det blir omfattet av kommunen sikkerhetskopiering.

Melhus kommune har en policy for sikkerhetskopiering og gjenoppretting. Policyen gir prinsipper for sikkerhetskopiering og et eksempel er at sikkerhetskopieringen skal ta utgangspunkt i hvor kritisk de enkelte deler av systemet er. Det skal utarbeides en egen prosedyre for sikkerhetskopiering med oversikt over hvilke systemer det skal tas sikkerhetskopi av og hvordan. Sikkerhetskopiering vurderes i forhold til RPO (Recovery Point Objective), som er et mål på hvor langt tilbake i tid kommunen må kunne gjenopprette data, altså det maksimale datatapet som tillates. I tillegg må RTO (Recovery Time Objective) vurderes. Dette er et tidsmål på hvor raskt kommunen må kunne gjenoppta driften av systemene etter uforutsette hendelser.

I intervjuet har ITMidt redegjort for systemet med sikkerhetskopiering. Dette er ikke gjengitt her av sikkerhetsmessige årsaker. All sikkerhetskopiering skjer automatisk og lagres lokalt. ITMidt har organisert systemet med sikkerhetskopiering etter rutiner som en ekstern samarbeidspart har gode erfaringer med. Samarbeidsparten har hjulpet ITMidt å sette opp systemet med sikkerhetskopiering. ITMidt opplever at de har systemer som fungerer veldig bra og de oppdateres jevnlig. I sikkerhetskopiene er at lagt vekt på at det ikke skal være mulig å endre dataene som ligger der.

3.3.6 Revisors vurdering

Revisor vurderer at Melhus kommune har etablert en digital prosjektveiviser som er med å sikre nødvendige sikkerhetsvurderinger ved anskaffelse av programvare.

Melhus kommune har satt anskaffelse av programvare i system gjennom bruken av prosjektveiviseren. Det kan tyde på at den ikke er godt nok kjent i organisasjonen. Revisor oppfatter at fasen med risikovurdering i prosjektveiviseren er en mulighet for å ivareta kravet om risikoanalyse om personvern (DPIA, se kapittel 2.7).

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at Melhus kommune har etablert og dokumentert en sikker IKT-arkitektur.

ITMidt har ikke en samlet oversikt over IKT-arkitekturen, men den er oppdelt og dokumentert. FIKS Digiorden vil bidra til å samle oversikten over IKT-arkitekturen. Det er revisors inntrykk at ITMidt har gode oversikter gjennom ulike verktøy. Trusselbildet kan gjøre at IKT-arkitekturen vil måtte endres.

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at Melhus kommune ved ITMidt har sentral styring med sikkerhetsoppdateringer.

ITMidt har sentral styring med sikkerhetsoppdateringer. Oppdatering av hvert enkelt system er det systemansvarlig som skal gjennomføre.

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at Melhus kommune har en prosedyre for sikkerhetskopiering og at det tas sikkerhetskopier.

Revisor finner at ITMidt har en gjennomtenkt og bevisst rutine for sikkerhetskopiering og at dette gjennomføres etter rutinen.

Revisor vurderer kriteriet som oppfylt.

3.4 Oppdage

3.4.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.
- Kommunen bør gjennomføre inntrengningstester.

3.4.2 Overvåke systemene

Melhus kommune har en policy for logging med det formål å sikre dokumentasjon av hendelser og sikre digitale bevis. Policyen inneholder prinsipper for logger, blant annet hvor lenge og hvordan logger skal oppbevares. Alle logger bør sendes til en sentral enhet som kan sammenstille informasjon fra flere logger. Videre er det angitt hvor i systemet det bør genereres hendelseslogger og hvilke typer hendelser som skal logges.

ITMidt har vurdert at de oppfyller de to høyest prioriterte sikkerhetsprinsippene fra NSM på …samt et av tiltakene med prioritet to. Alle logger er satt opp automatisk og håndteres eksternt i SOC (Security Operation Center). Dette er en 24/7 overvåkning. Det er regler for hvor lenge logger skal oppbevares.

ITMidt gjør i tillegg egne analyser gjennom et egnet verktøy, som fungerer som en mini SOC. Det omfatter antivirus, mailvask og logger. Systemet lager en trendportefølje som deles med ekstern samarbeidspart. Kommunen kan også få meldinger fra andres SOC. Det er ganske omfattende det kommunen varsles om. I tillegg kommer det også ukentlige meldinger fra HelseCert og KommuneCert, som er to ordninger for norske kommuner. Dette er en tosidig tjeneste. Det er en nyttig tjeneste som varsler angrep og svakheter. Det er betryggende å ha i tillegg.

Både kommunen og den eksterne samarbeidsparten har mulighet til å gjennomføre manuelle søk i siner SOC.

3.4.3 Inntrengningstester

ITMidt forteller at det er gjennomført inntrengingstester på eget initiativ. HelseCert gjør jevnlige tester på kommunens systemer og kommunen får påfølgende rapporter. Inntrengningstester blir en del av beredskapsplan IT når den er ferdig, forteller ITMidt.

3.4.4 Revisors vurdering

Revisor vurderer at Melhus kommune har et system for å overvåke sikkerheten og analysere data fra overvåkningen.

Melhus kommune benytter eksterne kontakter og er i et nettverk hvor sikkerhetstrusler og hendelser deles. Dette er betryggende for å kunne håndtere situasjoner raskt og være i forkant. Det er positivt at overvåkningen av logger er satt opp automatisk.

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at Melhus kommune gjennomfører inntrengningstester.

Revisor vurderer kriteriet som oppfylt.

3.5 Håndtere og gjenopprette

3.5.1 Revisjonskriterier

Følgende revisjonskriterier er utledet:

- Kommunen bør ha en plan for hendelseshåndtering.
- Kommunen må ha en plan for gjenoppretting.

3.5.2 Plan for hendelseshåndtering

Melhus kommune har en beredskapsplan IT, som skal sikre at Melhus og Skaun kommune kan opprettholde sine tjenester, og redusere skadevirkningene av eventuelle uforutsette og uønskede hendelser. Beredskapsplan IT knytter kommunens kriseledelse til eventuelle hendelser på IT området og angir roller og ansvar. Planen beskriver hvilken IT-drifts-dokumentasjon som skal finnes utenfor kommunens systemer og som skal være tilgjengelig hvis det skjer en hendelse.

Denne planen er forankret i kommunens overordnede beredskapsplan og henviser videre til hendelseshåndteringsplanen og omtaler arbeidet med gjenoppretting. Melhus kommune har en hendelseshåndteringsplan under arbeid.

Planen inneholder en oversikt over hendelseshåndteringsteamet og støttesystemer og utstyr som er tilgjengelig. I hendelseshåndteringsplanen beskrives prosessen med hendelses-håndteringen inndelt i ni faser og en nærmere beskrivelse av alle fasene med mål og aktiviteter. En av fasene er rapportering, som henviser til:

- Prosedyre for varsling av brudd på personopplysningssikkerheten, hvis hendelsen involverer personopplysninger og sikkerhetsbruddet innebærer en risiko for de registrerte så skal Datatilsynet varsles.
- Prosedyre for varsling av brudd på personopplysningssikkerheten, hvis hendelsen innebærer en høy risiko for de registrerte, så skal de registrerte varsles.
- Prosedyre for rapportering av signifikante hendelser, hvis det er en signifikant hendelse som har betydelig innvirkning på kommunens leveranser så skal NCSIR eller kompetent nasjonal myndighet varsles.

I tillegg har hendelseshåndteringsplanen tre andre prosedyrer under arbeid, som bygger opp under selve planen.

- Prosedyre for rapportering av signifikante hendelser
- Prosedyre for å vurdere og melde brudd på personopplysningssikkerheten (avvik) til Datatilsynet.
- Prosedyre for varsling av brudd på personopplysningssikkerheten (avvik)

Melhus kommune har en responsavtale med ekstern samarbeidspart, hvor kommunen ved hendelser har en avtalt responstid for å få hjelp.

3.5.3 Plan for gjenoppretting

I planen for hendelseshåndtering er en av fasene gjenoppretting. Der beskrives at formålet er gjenoppretting av det tekniske miljøet slik det var før sikkerhetshendelsen oppstod. I tillegg vises det til fem aktiviteter for gjenoppretting til normalsituasjon.

I beredskapsplan IT er det nærmere beskrevet en systemoversikt samt en oversikt over applikasjoner. Det er også vurdert hvor kritisk disse systemene er og en prioriteringsliste for gjenoppretting. I systemoversikten er det også gjort vurderinger av hvor langt tilbake i tid kommunen må kunne gjenopprette data etter en uforutsett hendelse. (RPO – Recovery Point Objective). Dette er et uttrykk for det maksimale datatapet kommunen kan tillate. RPO setter dermed krav til sikkerhetskopiering og gjenoppretting.

Melhus kommune har en beredskapsplan IT, som skal sikre at Melhus og Skaun kommune kan opprettholde sine tjenester, og redusere skadevirkningene av eventuelle uforutsette og uønskede hendelser. Denne planen er forankret i kommunens overordnede beredskapsplan og henviser videre til hendelseshåndteringsplanen.

Det er også vurdert hvor raskt kommunen må kunne gjenoppta driften av systemene etter uforutsette hendelser. (RTO - Recovery Time Objective). Dette beskriver hvor raskt kommunen må kunne gjenoppta driften av systemene etter uforutsette hendelser, altså den maksimale tillatte tid det skal ta å gjenopprette systemene. RTO legger grunnlag for prioriteringer for gjenopprettingsarbeidet.

I intervjuet forteller ITMidt at beredskapsplan IT angir en prioritert rekkefølge for gjenoppretting. Dette er en grov plan og vil være avhengig av hva som er omfattet av hendelsen. Denne prioriteringen har vært behandlet i strategisk ledergruppe.

Kjernen i gjenopprettingen er sikkerhetskopier og hva det innebærer vet ikke kommunen før det har prøvd det, eksempelvis hva som kreves hvis bare deler av systemet er rammet. Kommunen har en beredskapskoffert med PC, ruter, minnepinner og annet utstyr samt noe skriftlig dokumentasjon. Beredskapskofferten inneholder at de trenger av trendverktøy og det

er eksempelvis mulig å få tak i mail via det systemet. Beredskapsplan IT er et av dokumentene som finnes i beredskapskofferten.

3.5.4 Revisors vurdering

Revisor vurderer at Melhus kommune har en plan for hendelseshåndtering.

Revisor vurderer kriteriet som oppfylt.

Revisor vurderer at Melhus kommune har en plan for gjenoppretting.

Melhus kommune har en beredskapsplan IT. Den er koblet til kommunens øvrige beredskapsarbeid og kommunens kriseledelse er kriseledelse på IT. IT beredskapsplan dekker både håndtering av en hendelse og gjenoppretting av en hendelse. Når det gjelder gjenoppretting er det ingen egen plan, men den er en del av beredskapsplan IT. Beredskapsplan IT gir kommunen et godt planverk for å håndtere hendelser og gjenopprette normal drift i IT systemene.

Revisor vurderer kriteriet som oppfylt.

3.6 Konklusjon

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.

4 ANBEFALINGER

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.

KILDER

Lov og forskrift

Lov om nasjonal sikkerhet (Sikkerhetsloven)

Lov om behandling av personopplysninger (Personopplysningsloven)

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhetsforskriften)

Litteratur, veiledere og lignende

Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet

NMSs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet

Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet

Personvernprinsippene, Datatilsynet

Jøsang, A. (2021) Informasjonssikkerhet. Teori og praksis. Universitetsforlaget, Oslo

Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner, 2020, Digitaliseringsdirektoratet

Koblingstabell mellom NSMs grunnprinsipper for IKT-sikkerhet 2.0 og ISO/IEC 27002:2022, NSM

Internett

Melhus kommune sin hjemmeside

https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/miniveileder-om-oppfolging-av-informasjonssikkerhet-i-styringsdialogen/hva-og-hvorfor-er-det-viktig

https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/funn-fra-tilsyn-i-kommuner-og-fylkeskommuner/

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/hvordan-lage-en-databehandleravtale/

https://www.digdir.no/informasjonssikkerhet/styring-av-informasjonssikkerhet/2693

https://www.dmaze.com/dsb?lang=no

VEDLEGG 1 – UTLEDNING AV REVISJONSKRITERIER

Ifølge forskrift om kontrollutvalg og revisjon (§15) skal det etableres revisjonskriterier for gjennomføring av forvaltningsrevisjon. Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal revideres/vurderes i forhold til. Disse kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. Slike autoritative kilder kan være lov, forskrift, forarbeider, rettspraksis, politiske vedtak (mål og føringer), administrative retningslinjer, samt statlige føringer og praksis. I denne forvaltningsrevisjonen har vi benyttet oss av følgende kilder til revisjonskriterier:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhetsforskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet
- NMSs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet

Problemstilling 1: Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket

Overordnet styringssystem og rammeverk

Sikkerhetsloven stiller generelle krav til forebyggende sikkerhetsarbeid i kapittel 4. Sikkerhetsstyring er hjemlet i § 4-1; forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Virksomhetsikkerhetsforskriften definerer i § 3 kravet om at virksomheter som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.

Nasjonal sikkerhetsmyndighets veileder i sikkerhetsstyring skriver at sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Skjermingsverdige verdier er definert i sikkerhetslovens § 6-1 første ledd: *Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.*

Videre skriver veilederen at sikkerhetsstyring omfatter alle aktiviteter som har betydning for det forebyggende sikkerhetsarbeidet og skal gjennomføres planlagt og systematisk i form av et sikkerhetsstyringssystem som omfatter planlegging, etablering, gjennomføring og forbedring av det forebyggende sikkerhetsarbeidet. Utformingen av styringssystemet for sikkerhet skal omfatte følgende prinsipper:

- Risikostyring
- Sikkerhetsledelse
- Sikkerhetsorganisering
- Sikkerhetstiltak og prosedyrer
- Forhold til andre virksomheter
- Sikkerhetsoppfølging
- Sikkerhetsdokumentasjon

Datatilsynet anbefaler i sin veileder om virksomhetens plikter at anerkjente standarder, rammeverk og veiledere som beskriver styringssystem for informasjonssikkerhet benyttes.

Sikkerhetsmål og sikkerhetsstrategi

Forskriften fastsetter krav om sikkerhetsmål i § 5. Virksomheten skal fastsette hvordan kravene til et forsvarlig sikkerhetsnivå skal oppfylles og kriterier og å evaluere om kravene er oppfylt.

eForvaltningsforskriften omhandler internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan i § 15. Første ledd krever at mål og strategier for informasjonssikkerhet er beskrevet (sikkerhetsmål og sikkerhetsstrategi). Dette skal danne grunnlaget for forvaltningsorganets internkontroll på området for informasjonssikkerhet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. Kravene i personvernforordningen vil være aktuelle å innarbeide i en slik sikkerhetsstrategi.

Datatilsynet skriver at sikkerhetsstrategien skal omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette gjelder blant annet fordeling og avklaring av arbeidsoppgaver mellom ledelse og driftspersonell, men også beslutning om eventuelt å ta i bruk eksterne leverandører i sikkerhetsarbeidet. Videre skal sikkerhetsstrategien gjøre rede for organisatoriske og tekniske strategiske valg. Strategien beskriver hvilke virkemidler virksomheten velger å bruke for å nå målene.

Sikkerhetsorganisasjon

Jamfør sikkerhetsloven § 4-1 er det er virksomhetens leder som har ansvaret for det forebyggende sikkerhetsarbeidet. I forskriften om virksomhetens sikkerhet, framgår det i § 4

krav om styringsdokument. Leder av virksomheten skal fastsette et styringsdokument som beskriver hvilke deler av sikkerhetsloven som gjelder for virksomheten, roller og ansvar i virksomhetens forebyggende sikkerhetsarbeid og prinsipper for virksomhetens sikkerhetsarbeid. Styringsdokumentet skal gjøres kjent og tilgjengelig for blant annet alle ansatte. Virksomhetsforskriften § 6 definerer videre krav til roller og ansvar for det forebyggende sikkerhetsarbeidet. Det er leder sitt ansvar å fordele roller og ansvar, og at disse gjøres kjent i virksomheten.

Internkontroll

Internkontroll er hjemlet i kommuneloven § 25, der det står at internkontrollen skal være systematisk og tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Kommunedirektøren er ansvarlig for internkontrollen og skal:

a. utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
b. ha nødvendige rutiner og prosedyrer
c. avdekke og følge opp avvik og risiko for avvik
d. dokumentere internkontrollen i den formen og det omfanget som er nødvendig
e. evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Andre ledd i § 15 i eForvaltningsforskriften krever at det skal være etablert internkontroll på området for informasjonssikkerhet. Internkontrollen skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være integrert som en del av virksomhetens helhetlige styringssystem. Tredje ledd § 15 krever at omfang og innretning på internkontroll skal være tilpasset risiko.

I fjerde ledd bokstavene a til h, § 15, gis det eksempler på hvilke forhold sikkerhetsstrategien og internkontrollen bør adressere, herunder prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Risikovurderinger

Sikkerhetsloven § 4-2 krever at virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen danner grunnlaget for iverksetting av forebyggende sikkerhetstiltak. Videre skal virksomheten kartlegge, som en del av vurderingen, om hvilke virksomheter den er avhengig av for å fungere som den skal. Vurderingen skal gjennomgås jevnlig og om nødvendig revideres. Kravet om vurdering av risiko er videre utdypet i

virksomhetsikkerhetsforskriften § 12. Forskriften skriver i andre ledd at behovet for å gjennomføre en ny helhetlig vurdering av risikoen skal vurderes årlig.

Personopplysninger

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven gjennomfører EUs personvernforordning i norsk rett. Personopplysningsloven er bygget på noen grunnleggende prinsipper, og alle som behandler personopplysninger må følge disse prinsippene.

Datatilsynet har laget informasjon om pliktene en virksomhet har etter personvernregelverket. En av pliktene Datatilsynet referer til er vurdering av personvernkonsekvenser (DPIA – Data Protection Impact Assessment) (artikkel 35 i personopplysningsloven). Artikkel 35 krever at virksomheten gjennomfører en vurdering av personvernkonsekvenser ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter. Datatilsynet skriver følgende om DPIA:

«*En vurdering av personvernkonsekvenser er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak*.»

DIPA skal som minimum inneholde:

a) En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.
b) En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.
c) En vurdering av risikoene for de registrertes rettigheter og friheter
d) De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes.

En av pliktene er at alle virksomheter som behandler personopplysninger, skal føre protokoll over behandlingsaktivitetene de har ansvar for (artikkel 30 i personopplysningsloven). Protokollen skal inneholde formålet med behandlingen, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Dersom det er aktuelt, skal eventuelle databehandlere så oppført i protokollen.

Datatilsynet skriver at personvernforordningen skiller mellom begrepene behandlingsansvarlig og databehandler. Den behandlingsansvarlige bestemmer over personopplysningene, mens

databehandleren opptrer på vegne av den behandlingsansvarlige. Databehandleren kan derfor bare behandle personopplysninger etter instruks fra den behandlingsansvarlige.

Opplæring

Sikkerhetsloven definerer i § 4-1 at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. Kravet om ressurser og kompetanse er videre utdypet i virksomhetsforskriften § 7. Forskriften krever blant annet at de ansatte som får tilgang til skjermingsverdige verdier, får tilstrekkelig kompetanse om sikkerhet og kartlegge at personene kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser. Veilederen fra NSM skriver at riktig kompetanse oppnås og opprettholdes gjennom planmessig opplæring, kvalifisering og kompetansevedlikehold.

Datatilsynet skriver at målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt. Brukerne må være gitt muligheten til å etterleve dette i ditt daglige arbeid gjennom tilpasset opplæring ut ifra behov. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.

Hendelser

Virksomhetsforskriften § 8 sier at ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet skal en virksomhet gjennomføre umiddelbare tiltak for å redusere skadeomfanget og gjenopprette et forsvarlig sikkerhetsnivå. Virksomheten skal vurdere konsekvensene av den sikkerhetstruende virksomheten eller avviket.

NSM sine grunnprinsipper (versjon 1) sier at etter en uønsket hendelse det det forebyggende sikkerhetsarbeidet i virksomheten evalueres. Virksomheten må forsikre seg om at tiltakene som er etablert fungerer etter hensikten og vurdere om hendelsen ble håndtert tilfredsstillende. NSM skriver at dette er viktig fordi:

«*Når en hendelse er ferdig håndtert og akseptabelt sikkerhetsnivå gjenopprettet, er det viktig at virksomheten hurtig identifiserer og lærer fra det inntrufne og sørger for at konklusjoner blir gjennomgått og tatt tak i. Dersom dette ikke gjøres vil kunnskap og erfaring forsvinne, og man kan gjøre de samme feilene om igjen neste gang en uønsket hendelse oppstår. Det kan være at det oppdages nye sårbarheter, eller behov for nye eller forbedrede sikringstiltak som kan forhindre at fremtidige situasjoner oppstår.*»

På bakgrunn av redegjørelsen over, er følgende revisjonskriterier utledet for styringssystem:

- Kommunen bør legge et rammeverk til grunn for sitt informasjonssikkerhetsarbeid.

- Kommunen skal ha etablert sikkerhetsmål og sikkerhetsstrategi.
- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.
- Kommunen bør evaluere og lære av hendelser.

Problemstilling 2: Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Nasjonal sikkerhetsmyndighet har utgitt en veileder om grunnprinsipper for IKT-sikkerhet for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene fokuserer på teknologiske og organisatoriske tiltak, og hovedfokuset er på tilsiktende handlinger.

Grunnprinsippene er delt inn i fire kategorier og er gjengitt i tabellen under.

1. Identifisere og kartlegge	**2. Beskytte og opprettholde**
Kartlegge styringsstrukturer, leveranser og understøttende systemer Kartlegge enheter og programvare Kartlegge brukere og behov for tilgang	Ivareta sikkerhet i anskaffelses- og utviklingsprosesser Etablere en sikker IKT-arkitektur Ivareta en sikker konfigurasjon Beskytte virksomhetens nettverk Kontroller dataflyt Ha kontroll på identiteter og tilganger Beskytt data i ro og i transitt Beskytt e-post og nettleser Etabler evne til gjenoppretting av data Integrer sikkerhet i prosess for endringshåndtering
3. Oppdage	**4. Håndtere og gjenopprette**
Oppdage og fjerne kjente sårbarheter og trusler Etablere sikkerhetsovervåkning Analysere data fra sikkerhetsovervåkning Gjennomfør inntrengingstester	Forberede virksomheten på håndtering av hendelser Vurdere og klassifisere hendelser Kontrollere og håndtere hendelser Evaluere og lære av hendelser

Identifisere og kartlegge

NSM skriver at kartlegging av enheter og programvare er viktig for å få oversikt over hva som befinner seg i kommunen. Det er viktig at kommunen selv får oversikt over enheter, programvare og deres sårbarheter før angripere gjør det.

Videre skriver NSM at risikobildet må vurderes knyttet opp til valget mellom sikkerhet og behovet for leveranser til kommunen. Det kan hende at kommunen må godta enheter med lavere sikkerhetsnivå enn ønsket, og det er derfor viktig at kommunen er bevisst på strategier som velges og vurderer de funksjonelle behovene opp mot risiko. Anbefalt tiltak fra NSM er å kartlegge enheter og programvare.

Det er også viktig at kommunen har oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i en kommune. En angriper har ofte som mål å økte tilgangen ved et angrep på informasjonssystemet. Mange brukere kan ha tilganger og rettigheter til systemer og tjenester de egentlig ikke har behov for. Derfor bør tilganger og rettigheter begrenses slik at skaden fra en potensiell angriper eller utro ansatt reduseres. Derfor bør kommunen kartlegge brukere og behov for tilgang.

Utledet revisjonskriterier:

- Kommunen må ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.
- Kommunen må ha et system for styring av tilganger.

Beskytte og opprette

NSM har et prinsipp som sier at sikkerheten i anskaffelse- og utviklingsprosesser må ivaretas. Målet med prinsippet er å minimere risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter.

Et av prinsippene under denne kategorien er å etablere en sikker IKT-arkitektur. Et IKT-system består av mange sikkerhetsfunksjoner og ulike IKT-produkter fra ulike produsenter som skal fungere godt og sikkert sammen. Hvis ikke så kan dette økte sårbarheten og som en angriper kan utnytte. Videre skriver NSM at drift og sikkerhetskonfigurasjon bør skje sentralt og likt per type enhet, hvis ikke økes risikoen for dobbeltarbeid, menneskelige feil og flere sårbarheter. IKT-systemet bør videre deles opp i forskjellige deler avhengig av tillitsnivå for å begrense risiko.

Under prinsippet om å ivareta en sikker konfigurasjon kommer NSM med et anbefalt tiltak om å etablere et sentralt styrt regime for sikkerhetsoppdatering. I dette ligger det blant annet at kommunen bør installere sikkerhetsoppdatering så fort som mulig. Videre bør kommunen ha

en prioriteringsliste for oppdateringer og etablere en rutine med klare ansvarsforhold for hvor ofte oppdateringer skal utføres og hvem som er ansvarlig dersom en oppdatering ikke kan gjennomføres eller må utsettes.

NSM skriver at et av prinsippene er å etablere en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap. Et av de anbefalte tiltakene er å lage en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.

Utledet revisjonskriterier:

- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser.
- Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer.
- Kommunen må ha en plan for sikkerhetskopiering og ta sikkerhetskopier.

Oppdage

NSM har et prinsipp som omhandler etablering av sikkerhetsovervåkning for å overvåke og samle inn relevante data for å oppdage sikkerhetshendelser og legge et grunnlag for å analysere data. Dette for at kommunen kan oppdage sikkerhetshendelser tidlig som mulig for å minimere skadeomfang eller forhindre hendelser. Det er viktig at kommunen har tilgang på tilstrekkelig data siden det kan være avgjørende for at kommunen skal gjenopprette normaltilstand og hindre gjentagelse av en hendelse. NSM anbefaler derfor at kommunen etablerer sikkerhetsovervåkning.

Videre anbefaler NSM at kommunen analyserer data fra sikkerhetsovervåkningen. Gjennom analyse av sikkerhetsrelevante data kan kommunen oppdage aktiviteter som påvirker informasjonssystemer, data og tjenester. NSM skriver at systematisert prosessering, gjennom sammenstilling og analyse av innhentet data vil bidra til å øke sannsynligheten for å avdekke hendelser.

Et prinsipp til under kategorien oppdage, er at kommunen bør gjennomføre inntrengningstester. Kommunen bør jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Angripere utnytter ofte svakheter i virksomhetens rutiner.

Utledet revisjonskriterier:

- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen.
- Kommunen bør gjennomføre inntrengningstester.

Håndtere og gjenopprette

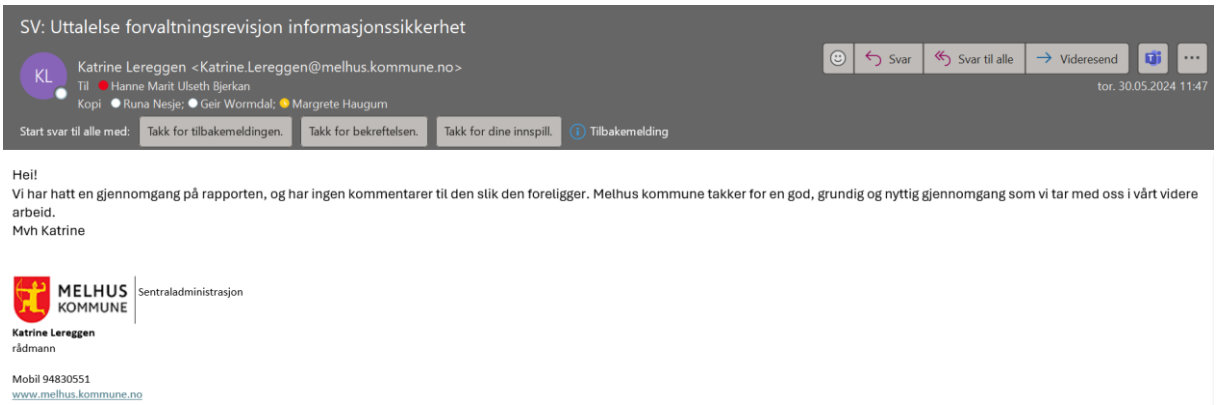
For å forberede kommunen på håndtering av hendelser anbefaler NSM at kommunen etablerer et planverk for hendelseshåndtering. Uten en plan og en prosess for hendelseshåndtering vil det være vanskelig for kommunen å begrense skaden og gjenopprette normal tilstand.

Ved en hendelse er det viktig at kommunen håndtere hendelsen korrekt og med riktige ressurser slik at spredning og konsekvenser minimeres og normaltilstand opprettholdes eller gjenopprettes effektivt. For å få til dette er det viktig at kommunen har en plan for gjenoppretting som iverksettes i løpet av eller i etterkant av hendelsen.

Utledet revisjonskriterier:

- Kommunen bør ha en plan for hendelseshåndtering.
- Kommunen må ha en plan for gjenoppretting.

VEDLEGG 2 – UTTALELSE



SV: Uttalelse forvaltningsrevisjon informasjonssikkerhet

KL Katrine Lereggen <Katrine.Lereggen@melhus.kommune.no>
Til Hanne Marit Ulseth Bjerkan
Kopi Runa Nesje; Geir Wormdal; Margrete Haugum

Svar | Svar til alle | Videresend | tor. 30.05.2024 11:47

Start svar til alle med: Takk for tilbakemeldingen. | Takk for bekreftelsen. | Takk for dine innspill. | Tilbakemelding

Hei!
Vi har hatt en gjennomgang på rapporten, og har ingen kommentarer til den slik den foreligger. Melhus kommune takker for en god, grundig og nyttig gjennomgang som vi tar med oss i vårt videre arbeid.
Mvh Katrine

MELHUS KOMMUNE | Sentraladministrasjon
Katrine Lereggen
rådmann

Mobil 94830551
www.melhus.kommune.no

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no