Revisjon Midt-Norge

INFORMASJONSSIKKERHET

Melhus kommune

Prosjektplan forvaltningsrevisjon

FR1256

2023

1 FAKTA OM OPPDRAGET

FORMÅL

Formålet med oppdraget er å svare ut kontrollutvalgets bestilling knyttet til informasjonssikkerhet i Melhus kommune. Oppdraget vil kunne identifisere mulige forbedringspotensial knyttet til informasjonssikkerhet i kommunen.

PROBLEMSTILLINGER

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

TIDS- OG RESSURSBRUK

Timeforbruk: Inntil 300 timer

Rapport til sekretær: Innen utgangen av februar 2024

OPPDRAGSANSVARLIG REVISOR

Hanne Marit Ulseth Bjerkan
hanne.bjerkan@revisjonmidtnorge.no

Tlf. 476 34 527

2 MANDAT

Kapittelet redegjør for bestillingen og gir informasjon om temaet.

2.1 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 forsøkt å ta hensyn til de ulike spørsmålene som kontrollutvalget har listet opp, og at disse besvares gjennom revisor sitt forslag til problemstillinger.

2.2 IT-sikkerhet

Kontrollutvalget har bestilt en forvaltningsrevisjon om «datasikkerhet», mens det er brukt «informasjonssikkerhet» i opplistingen av problemstillinger i bestillingen. Revisor vil først forklare og avklare bruk av begreper.

Datasikkerhet er et samlebegrep for metoder og verktøy som skal sikre at digitale tjenester eller digital informasjon ikke blir stjålet eller går tapt. Eksempel er brannmur, tofaktorautentisering, sikre passord. Begrepen IT-sikkerhet og IKT-sikkerhet brukes på samme

måte. I forvaltningsrevisjonen vil de ulike begrepene brukes uten at det gjøres noe prinsipielt skille mellom dem. [1]

Informasjonssikkerhet er å 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). Videre skriver Jøsang (2021) 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. Informasjonssikkerhet handler om hvordan en organisasjon sikrer informasjon og tjenester og hvilke rutiner og prosesser den bruker. Sentralt her er sikkerhetsledelse og risikostyring. En god sikkerhetskultur er viktig, siden angrep kan forekomme i hele virksomheten, ikke bare teknisk. [1]

Forvaltningsrevisjonen vil videre bruke begrepet informasjonssikkerhet.

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 krav om at sikkerhetsstyringen skal gjennomføres planlagt og systematisk i et sikkerhetsstyringssystem som samordnes med virksomhetens styringssystem. Personopplysningsloven gir bestemmelser om hvordan personopplysninger skal behandles. I eForvaltningsforskriften er internkontroll på informasjonssikkerhetsområdet regulert. Forskriften krever at forvaltningsorganet skal ha en internkontroll på informasjonssikkerhetsområdet og som bør være integrert som en del av virksomhetens helhetlige styringssystem.

Personopplysningsloven er bygget på noen grunnleggende prinsipper, og alle som behandler personopplysninger må følge disse prinsippene. Datatilsynet skriver at prinsippene gir ulike måter uttrykk for at behandling av personopplysninger skal skje på en måte som sikrer

[1] https://www.pwc.no/no/teknologi-omstilling/hva-er-cybersikkerhet.html

forutsigbarhet og forholdsmessighet for enkeltmenneske.[2] Tabellen nedenfor er basert på Datatilsynet sin gjennomgang av personvernprinsippene.

Tabell 1. Gjennomgang av personvernprinsippene

Prinsipp	Nærmere om prinsippene
Lovlig, rettferdig og gjennomsiktighet	Rettslig grunnlag for en planlagt behandling av personopplysninger. Behandlingen av personopplysninger skal være gjennomsiktig. Virksomhetene har en behandlingsansvarlig som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
Formålsbegrensing	Ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist.
Dataminimering	Begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet.
Riktighet	Korrekte opplysninger og skal oppdateres om nødvendig.
Lagringsbegrensning	Personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.
Integritet og konfidensialitet	Behandlingsansvarlig må sørge for å iverksette tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endring av personopplysninger.
Ansvarlighet	Punktet understreker ansvaret for å opptre i henhold til regelverket. Virksomhetene må kunne dokumentere at den har gjennomført tiltak for å etterleve personvernforordningen. Virksomheten må opptre proaktiv og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

Kilde: Datatilsynet

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[3]. Veilederen beskriver sikkerhetsstyring som

[2] Datatilsynet personvernprinsippene

[3] Veileder i sikkerhetsstyring (NSM)

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.* 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 er for eksempel roller og ansvar, retningslinjer, prosedyrer og rutiner. Tekniske tiltak er eksempelvis IKT-løsninger, skap, dører, rom og bygninger.

Figuren nedenfor illustrere sammenhengen i det som er beskrevet ovenfor.

Figur 1. Sammenhenger for sikkerhetsstyring.

NSM har også utarbeidet grunnprinsipper for IKT-sikkerhet[4] (NSM 2020) som er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene fokuserer på organisatoriske og teknologiske tiltak. Grunnprinsippene er inndelt i fire kategorier og er gjengitt i tabellen nedenfor.

Tabell 2. Grunnprinsipper for IKT-sikkerhet

1. Identifisere og kartlegge	2. Beskytte og opprettholde

[4] Grunnprinsipper for IKT-sikkerhet (NSM)

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

Kilde: NSM 2020

NSM skriver at hvert grunnprinsipp er en kontinuerlig aktivitet som må vurderes i hele informasjonssystemets levetid, fra planlegging og etablering til avhending. Flere av grunnprinsippene bygger på hverandre, og enkelte er en forutsetning for at andre prinsipper skal kunne implementeres effektivt.

2.3 Kommunens organisering

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

ITMidt er et interkommunalt IT-samarbeid mellom kommunene Melhus og Skaun, og er organisert som et vertskommunesamarbeid 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 ivareta digitalisering og tjenesteutvikling. ITMidt har også ansvar for å ivareta informasjonssikkerhet og internkontroll i henhold til lov og forskrift.

Melhus kommune har et eget personvernombud som skal påse at kommunen behandler personopplysninger etter bestemmelsene i personopplysningsloven. Melhus kommune har også en egen personvernerklæring som forteller hvordan kommunen samler inn og bruker opplysningene i sitt lovpålagte, daglig arbeid. Det er rådmann i kommunen som er

behandlingsansvarlig og bestemmer formålet med behandlingen av personopplysninger som innhentes og er ansvarlig for at de behandles i tråd med gjeldene lover og forskrifter.[5]

[5] Melhus kommunes hjemmeside

3 PROSJEKTDESIGN

Kapittelet redegjør for revisors forslag til løsning av oppdraget.

3.1 Problemstillinger

Problemstillingene som skal besvares i prosjektet er følgende:

1. Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?
2. Har kommunen tilfredsstillende organisatoriske og tekniske tiltak for å ivareta informasjonssikkerhet?

Den første problemstillingen tar utgangspunkt i hva som kreves av et styringssystem for informasjonssikkerhet. Risikovurderinger og risikohåndtering er sentralt her. Problemstillingen vil se på om kommunen har vurdert hvilke informasjonsverdier kommunen har, hvilke trusler som finnes og hvor sårbar kommunen er hvis denne informasjonen ikke blir tilgjengelig eller kommer på avveie. Revisor vil se på om informasjonssikkerhet er en del av kommunens internkontrollsystem. En del av problemstillingen vil også være å se om kommunen ivaretar personopplysninger i tråd med krav i regelverket; om kommunen har full oversikt over sin behandling av personopplysninger og om kommunen har etablert tiltak som sikrer at regelverket følges. Kommunen har blant annet plikt til å føre protokoller over behandlingsaktivitetene[6] de gjennomfører.

Den andre problemstillingen handler om konkret organisatoriske og tekniske tiltak for å ivareta informasjonssikkerheten. Rammene for problemstillingene vil være Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet. Nedenfor er de fire prinsippene listet opp og litt mer om hva revisor vil se på under hvert punkt.

- Identifisere og kartlegge
  - Om kommunen har oversikt over enheter i IKT-systemet og programvare
- Beskytte og opprettholde
  - Om kommunen har etablert og dokumentert en sikker IKT-arkitektur.
  - Om kommunen har styring med sikkerhetsoppdateringer og en plan for sikkerhetskopieringer og om de tar sikkerhetskopier.
- Oppdage

[6] Det må finnes et behandlingsgrunnlag for behandling av hver enkelt personopplysning til hvert enkelt formål. Et behandlingsgrunnlag er et rettslig grunnlag for å behandle personopplysninger, for eksempel samtykke. Kilde: Datatilsynet.

- Om kommunen har et system for å overvåke sikkerheten og analysere data fra overvåkningen.
- Om kommunen gjennomfører inntrengningstester.

- Håndtere og gjenopprette
  - Om kommunen har en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon og loggføring) og en plan for gjenoppretting.

For å vise at problemstillingene vil svare ut punktene kontrollutvalget har skissert, har revisor satt opp en oversikt over hvilke problemstillinger som svarer ut de ulike spørsmålene.

Spørsmål fra kontrollutvalget	Besvares i følgende problemstilling
Hva gjør kommunen for å forebygge, oppdage og håndtere digitale angrep?	Problemstilling 2
Hva gjør kommunen hvis systemene blir helt utilgjengelige eller ikke til å stole på?	Problemstilling 2
Hvordan forvaltes kommunens kontroll over persondata?	Problemstilling 1
Hvordan forvaltes teknologien og hvordan understøtter den kommunale tjenester på kort og lang sikt?	Problemstilling 1
Hvilke rutiner er etablert for sikring av kommunes data?	Problemstilling 2
Hvordan følger kommunens sikkerhetstiltak lover, forskrifter og annet regelverk med tanke på backup, personvern, kriseløsninger, hacking med mer?	Problemstilling 2
Hvordan fungerer de fastlagte rutinene for informasjonssikkerhet i praksis?	Problemstilling 2
I hvilken grad er organiseringen av informasjonssikkerhetsarbeidet tilfredsstillende og i tråd med lovkrav?	Problemstilling 1
Hvilke systemer har kommunen for kontroll og etterprøving av informasjonssikkerhet?	Problemstilling 1
Hvordan blir kontroll og etterprøving gjennomført?	Problemstilling 1

3.2 Avgrensing

Personopplysningsloven stiller krav til behandling av personopplysninger. Revisjonen har ikke mulighet til å se på alle de spesifikke kravene som omhandler behandling av personopplysninger. 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.

3.3 Kilder til kriterier

Aktuelle kilder til revisjonskriterier er:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)

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

3.4 Metoder for innsamling av data

Revisor vil innhente dokumentasjon fra kommunen for å besvare problemstillingene. Gjennomgang av kommunale dokumenter vil være en viktig datakilde for å undersøke hvordan kommunen jobber med informasjonssikkerhet. Eksempler på dokumenter er risikovurderinger, beredskapsplaner, politiske dokumenter som gir føringer, rutinebeskrivelser for ulike tiltak og ulike planer innenfor informasjonssikkerhet, dokumentasjon av behandling av personopplysninger med mer. Dokumentgjennomgang er en god metode for å finne frem til opplysninger som er nødvendige og relevante for kommunal oppgaveløsning og forvaltning. Det offentlige har i enkelte tilfeller plikt til å dokumentere sitt arbeid og sin regeletterlevelse.

Det vil bli gjennomført intervjuer med kommunens ledelse og ansatte innenfor IT for å få dybdekunnskap om hvordan arbeidet med informasjonssikkerhet foregår i kommunen og for å forstå sammenhengene. Revisor vil også intervjue personvernombudet i kommunen. Det kan være aktuelt å intervjue andre ansatte i kommunen.

4 PROSJEKTORGANISERING

4.1 Prosjektteam

Oppdragsansvarlig revisor	Hanne Marit Ulseth Bjerkan
Prosjektmedarbeider	Margrete Haugum
Kvalitetssikrer	Merete Montero
Kvalitetssikrer	Trine Holter

4.2 Milepælsplan

Bestillingsdato	16. februar 2023
Prosjektplan til sekretær	19. april 2023
Oppstartsmøte	Starten av september 2023
Datainnsamling ferdig	Starten av desember 2023
Rapport til uttalelse	Starten av februar 2024
Rapport til sekretær	Innen utgangen av februar 2024

Trondheim, 17.april 2023

Hanne Marit Ulseth Bjerkan

Oppdragsansvarlig revisor

Dokumentet er elektronisk godkjent og har derfor ingen signatur

KILDER

Lov om nasjonal sikkerhet (Sikkerhetsloven)

Lov om behandling av personopplysninger (Personopplysningsloven)

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

«Veileder i sikkerhetsstyring», Nasjonal sikkerhetsmyndighet

«NSMs Grunnprinsipper for IKT-sikkerhet», Nasjonal sikkerhetsmyndighet

Datatilsynet – personvernprinsippene

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

Melhus kommune sin hjemmeside

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no