Revisjon Midt-Norge

IT-SIKKERHET

Rennebu kommune

Forvaltningsrevisjon

2023

FR2112

FORORD

Revisjon Midt-Norge SA har gjennomført denne forvaltningsrevisjonen på oppdrag fra kontrollutvalget i Rennebu kommune i perioden desember 2022 til april 2023.

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

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

Steinkjer, 22.05.2023

Margrete Haugum

Oppdragsansvarlig revisor

Merete Lykken

Prosjektmedarbeider

SAMMENDRAG

Revisjon Midt-Norge SA har gjennomført forvaltningsrevisjon om informasjonssikkerhet på oppdrag fra kontrollutvalget i Rennebu kommune. Forvaltningsrevisjonen er gjennomført i henhold til standarden RSK 001. Datainnsamlingen ble avsluttet 30.03.2023 og har omfattet intervjuer, dokumentgjennomgang og tilgang til kvalitetssystemet QM+.

System for informasjonssikkerhet

Rennebu kommune gjennomfører og dokumenterer risikovurderinger på ulike nivå i organisasjonen. Kommunen har en ROS-analyse på cyberangrep. Det er uklart om risikovurderingene er systematiske og om de er grunnlag for informasjonssikkerhetstiltak. Det finnes overordnede sikkerhetsmål, men det mangler en strategi for informasjonssikkerhet. Kommunen har ingen sikkerhetsorganisasjon hvor roller og ansvar for informasjonssikkerhet framgår.

Rennebu kommune holder på å bygge opp et internkontrollsystem med grunnlag i prosedyrebeskrivelser i Teams og risikoanalyser og avvikssystem i QM+. Informasjonssikkerhet inngår i internkontrollsystemet.

Det finnes en rutine for tildeling og fjerning av tilganger i datasystemet, men det er ikke alltid fjerning blir fulgt opp i praksis. Det skjer jevnlige oppryddinger flere ganger i året.

Rennebu kommune har tatt i bruk NanoLearning, som med jevne mellomrom gir alle ansatte korte opplæringssekvenser på nett. Det stilles også krav til opplæring i informasjonssikkerhet for nyansatte. Hendelser på IKT-området evalueres som en del av internkontrollen, men det er ikke noe system for å evaluere og dokumentere hendelser innenfor informasjonssikkerhet.

Tekniske og organisatoriske tiltak

Rennebu kommune har oversikt over enheter i datasystemet og programvare som brukes. Det finnes dokumentasjon av IKT-infrastrukturen med ulike sikkerhetstiltak. Det er sentral styring med sikkerhetsoppdateringer og det finnes en plan for sikkhetskopiering, som følges.

Rennebu kommune har systemer for overvåkning av sikkerheten og til en viss grad analysers data fra overvåkningen. Det gjennomføres jevnlig inntrengningstester på kommunens datasystem. Kommunen har verken plan for håndtering av IKT-hendelser eller en plan for gjenoppretting.

Konklusjon

Rennebu kommune har sentrale mangler i styringssystemet for informasjonssikkerhet. Det mangler spesifikke sikkerhetsmål, sikkerhetsstrategi og en tydelig sikkerhetsorganisasjon.

Rennebu kommune har flere tekniske og organisatoriske tiltak for å ivareta informasjons-sikkerheten, men mangler kritiske planer for hendelser og gjenoppretting.

Anbefalinger

- Iverksette et arbeid med identifisering av informasjonsverdier, vurdering av trusler og sårbarheter som grunnlag for spesifikke sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganiseringen. Dette arbeidet kan munne ut i en overordnet plan for IKT og IKT-sikkerhet.
- Avklare og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
- Vurdere å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
- Vurdere behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
- Utarbeide en planer for hendelseshåndtering og gjenoppretting.

INNHOLDSFORTEGNELSE

Tabell

Figurer

1 INNLEDNING

1.1 Bestilling

Kontrollutvalget i Rennebu kommune har bestilt en forvaltningsrevisjon om IT-sikkerhet, den 21.09.2022, sak 34/22.

Bakgrunnen for bestillingen er et vedtak i kontrollutvalget 16.03.2022, sak 19/22, hvor kontrollutvalget ber om en orientering om IKT-sikkerheten i kommunen, og hvilke risiko- og sårbarhetsvurderinger som er knyttet til vurderingen. I kontrollutvalgsmøtet 03.05.2022, sak 24/22, orienterte IKT-rådgiver og personal- og stabssjef om hvordan den digitale sikkerheten ivaretas i Rennebu kommune. I denne saken vedtok kontrollutvalget følgende:

> *Kontrollutvalget tar informasjonen om kommunens digitale sikkerhet til orientering.*
>
> *Ut fra en generell risiko- og vesentlighetsvurdering mener kontrollutvalget at det bør gjennomføres en forvaltningsrevisjon innenfor IT-sikkerhet. Også Nasjonal Sikkerhetsmyndighet har kommet med klare råd til virksomheter om å forebygge og avverge cyberangrep. Forvaltningsrevisjon innen IT-sikkerhet står ikke i plan for forvaltningsrevisjon. På den bakgrunn ber kontrollutvalget om at en forvaltningsrevisjon på dette området blir prioritert og gjennomføres utenom planen.*
>
> *Kontrollutvalget oversender saken til kommunestyret med følgende forslag til vedtak: Kommunestyret ber kontrollutvalget om å gjennomføre en forvaltningsrevisjon innenfor IT-sikkerhet utenom gjeldende plan for forvaltningsrevisjon.*

Kommunestyret behandlet saken 16.06.2022, sak 22/2022, og ba om at det det gjennomføres en forvaltningsrevisjon innenfor IT-sikkerhet.

Dette vedtaket er bakgrunn for kontrollutvalgets bestilling 21.09.2022.

Kontrollutvalget vedtok prosjektplanen i sak 41/22, den 09.11.2022. IT-sikkerhet henger tett sammen med bestemmelser i personopplysningsloven. Personopplysningsloven stiller spesifikke krav til behandlingen av personopplysninger. Denne forvaltningsrevisjonen avgrenses bort fra å se på de spesifikke kravene som omhandler behandling av personopplysninger, men har en mer overordnet tilnærming til informasjonsverdier, hvor personopplysninger er en bestemt type informasjonsverdi.

1.2 Problemstillinger

Følgende problemstillinger besvares i rapporten:

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

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 Rennebu kommune, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3. Denne forvaltningsrevisjonen er basert på intervjuer og dokumentgjennomgang. Datainnsamlingen har skjedd i perioden november 2022 til 30.03.2023.

Intervju

Det er gjennomført et oppstartsmøte med kommunedirektør, personal- og stabssjef, IKT-rådgiver og controller. Oppstartsmøtet var en gjensidig informasjon hvor revisor fikk høre om organiseringen og arbeidet med informasjonssikkerhet i kommunen, og revisor orienterte om den planlagte forvaltningsrevisjonen.

I det videre arbeidet er intervju brukt for å samle inn data. Intervju er valgt fordi revisor ønsket å få fram detaljer om informasjonssikkerhet. I oppstartsmøtet ble det klart at kommunens deltakere i møtet jobbet med informasjonssikkerhet fra litt ulike ståsted, slik at det var naturlig å ha separate intervju med dem i etterkant.

Det er gjennomført separate intervju med controller og IKT-rådgiver på Teams. Det ble gjennomført et felles intervju på Teams med kommunedirektør og personal- og stabssjef. Når det presenteres data fra dette intervjuet henvises det generelt til ledelsen og i noen tilfeller til personal- og stabssjef. Til alle intervjuene ble det laget en tilpasset intervjuguide. Det er skrevet referater fra intervjuene, som er godkjent av de som ble intervjuet. Litt senere ut i revisjonen har det vært separate Teams-møter med controller og IKT-rådgiver. Controller hadde en gjennomgang av kommunens kvalitetssystem og mappestruktur på Teams, i tillegg til å utdype noen av de tidligere svarene. Møtet med IKT-rådgiver var en gjennomgang av supplerende spørsmål som var oversendt på epost i forkant. IKT-rådgiver har fått oversendt kapittel 4.3 til 4.6 for å sikre at beskrivelsene i rapporten ikke utgjør noen sikkerhetsrisiko for kommunen.

Dokumentgjennomgang

Revisor har fått tilgang til kommunens kvalitetssystem QM+. Der har det vært mulig å se på systemet for risikovurderinger og avviksmeldinger. Revisor har også etterspurt dokumentasjon av rutiner og andre dokumenter som er blitt oversendt. Revisor ønsket tilgang til Teams for å undersøke dokumentasjonen der, men fikk ikke det. Revisor har blitt vist filoversikten i deler av Teams og fått tilsendt dokumenter som revisor oppfattet å være av interesse. Revisor har også lagt til grunn politiske dokumenter og de månedlige informasjonsskrivene fra kommunedirektøren.

Vurdering av metode

Revisor har intervjuet de sentrale personene i kommunen som har en rolle innen informasjonssikkerhet. I tillegg er det samlet inn og gjennomgått sentrale dokumenter på området. Det kan være relevante dokumenter som revisor ikke har klart å etterspørre fordi de kan ha andre betegnelser enn hva revisor har brukt. Revisor anser disse datakildene som tilstrekkelige for å gjøre vurderinger og konkludere.

1.4 Uttalelse om rapport

En foreløpig rapport ble sendt til kommunedirektøren for uttalelse, 30.03.2023. Revisjon Midt-Norge SA mottok svar 27.04.2023. Uttalelsen er vedlagt rapporten (vedlegg 2).

Sammen med uttalelsen fra kommunedirektøren fikk revisor tilbake foreløpig rapport med korrigeringer i henhold til beskrivelsen i uttalelsen fra kommunedirektøren. Der går det fram at direkte feil er merket med gjennomstreking av tekst, mens tilføyelser er skrevet i rødt. Revisor har gått gjennom forslagene til korrigeringer. I korrigeringene kommer det delvis ny informasjon, som revisor har bedt om mer dokumentasjon på og revisor stilte i tillegg noen oppfølgingsspørsmål i epost 04.05.2023. Revisor mottok dokumentasjon og svar 10.05.2023. Svarene fra 10.05.2023 er gjengitt i vedlegg 3.

Korrigeringer i uttalelsen fra kommunedirektøren som er påpekninger av feil er rettet.

1.4.1 Håndtering av korrigeringene

Korrigeringer som revisor oppfatter som språklige nyanser er vurdert og tatt til følge når det bidrar til å gi en bedre framstilling av fakta. Disse er ikke kommentert videre.

I tilbakemeldingen er personen som revisor har omtalt som innkjøpsansvarlig endret tittel til controller. Revisor hentet tittelen fra kommunens hjemmeside.

Kommunedirektøren har gjort endringer i revisors vurderinger. Dette har revisor ikke tatt hensyn til. Korrigering av data som er feil i foreløpig rapport har ført til endring i revisors vurderinger. Dette gjelder:

- Risikoanalyser ved IKT-anskaffelser
- Sikkerhetsorganisasjon
- Sikkerhetsmål

De resterende korrigeringene består av:

- Nye data etter at datainnsamlingen ble avsluttet. Dette gjelder personvernombudets årsmelding for 2022, som er datert 30.03.2023 og opprettelsen av IKT-arbeidsutvalg som er opprettet etter at kommunedirektøren fikk foreløpig rapport til uttalelse. Den foreløpige rapporten ble sendt 30.03.2023 og nye data etter den tid tas ikke inn i selve rapporten.
- Nye supplerende opplysninger til teksten, som bidrar til utdypende forklaring, er tatt inn.
- Supplerende opplysninger som har vært vanskelig å håndtere til tross for oppfølgingsspørsmål. Antakelig snakkes det forbi hverandre og avsnittet er tatt bort. Det gjelder følgende avsnitt i foreløpig rapport:

Personal- og stabssjef opplyser at det er oversiktlig hvem som har tilgang til hva. Ledere har administratorrettigheter og legger inn og skal slette sine ansatte ved endringer i Qm+. Roller og tilganger følger organisasjonskartet. ~~sine systemer.~~

- Tilleggsopplysninger som revisor delvis er kjent med, men som ble utelatt fordi de ble vurdert til å være mindre relevant. Dette gjelder også tilleggsopplysninger som revisor vurderer som lite relevant. Disse er samlet i vedlegg 4.
- Korrigeringer som er dekket av annen tekst i samme kapittel eller andre kapittel. Disse er ikke tatt med i teksten. Disse framgår også av vedlegg 4.
- Korrigeringer av direkte feil er endret. Dette er blant annet knyttet til at responsavtalen med Atea er kommet på plass, sikkerhetsorganisasjon og omtalen av ROS i anskaffelse av IT-system. Den siste har ført til en endret vurdering.
- Korrigeringer som viser at teksten bør utdypes for å skape en bedre forståelse. Slike korrigeringer har ført til endringer i teksten, men ikke i vurderingene.

Flere av korrigeringene er av intervjudata som tidligere er godkjent av den som ble intervjuet. Revisor har derfor måtte kontakte de som ble intervjuet for å få klarhet i om de står bak de korrigeringene av data som de tidligere har godkjent. Dette har gjort prosessen noe uryddig.

2 INFORMASJONSSIKKERHET

2.1 Sikkerhet på nasjonalt nivå

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for forebyggende nasjonal sikkerhet. Direktoratet gir råd om og gjennomfører tilsyn og kontrollaktiviteter på sivil og militær side knyttet til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. NSM har et nasjonalt ansvar for å avdekke, varsle og koordinere håndtering av alvorlige IKT-angrep. NSM har gitt ut rapporten *Risiko 2022* (NSM 2022) og *Nasjonal digitalt risikobilde for 2021* (NSM 2021). Begge rapportene beskriver forhold omkring informasjonssikkerhet i samfunnet og informasjonen i dette kapitlet er hentet fra disse to rapportene.

Samfunnet har blitt mer digitalisert. Ny teknologi endrer måten vi jobber på og hvordan vi behandler data. Det oppstår flere og større avhengigheter mellom ulike digitale systemer og dette skaper sårbarheter. Det er bekymringsverdig at stadig flere samfunnsverdier flyttes over i det digitale domenet, uten at det først er gjennomført tilstrekkelig verdi- og risikovurderinger. Når en risikovurdering foreligger med risikoer identifisert og evaluert, må beslutningstaker håndtere risikoen på en god måte. (NSM 2021)

I dag understøttes samfunnet av en rekke digitale kritiske funksjoner som må fungere til enhver tid. En uønsket hendelse mot en eller flere av disse kan få store konsekvenser og føre til synlige og negative samfunnseffekter. Det gjøres mye godt sikkerhetsarbeid i mange virksomheter, og stadig flere får opp bevisstheten rundt og fokuset på digital sikkerhet. Men arbeidet må forsterkes betydelig. Det kreves et taktskifte i forebyggende arbeid og beredskap. (NSM 2021)

Flere og flere virksomheter erkjenner at cyberoperasjoner kan ramme alle og Nasjonalt cybersikkerhetssenter[1] erfarer at stadig flere prioriterer det digitale sikkerhetsarbeidet. Vi ser likevel at mange norske virksomheter ikke har et forsvarlig sikkerhetsnivå for å beskytte viktige verdier. Økt bevissthet om digital risiko har ofte ikke blitt omsatt i handling. Dette bør være et tema i alle styrerom og ledergrupper. (NSM 2021)

Risikovurderingen bygger på forholdet mellom verdi, trussel og sårbarhet. Virksomheten og ledelsen har alltid ansvaret for sikring av egne verdier. Risikovurdering og risikohåndtering er helt nødvendig for å oppnå et forsvarlig sikkerhetsnivå i egen virksomhet. (NSM 2021) Mange

[1] Nasjonalt cybersikkerhetssenter (NCSC) er en del av nasjonal sikkerhetsmyndighet og samtidig et partnerskap mellom NSM og ulike offentlige og private virksomheter. Sentret skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberoperasjoner.

virksomheter sikrer seg mot driftsforstyrrende hendelser som innbrudd eller nedetid på systemene. Men disse sikringstiltakene beskytter ikke nødvendigvis mot målrettede trussel-aktører. Et tilstrekkelig sikkerhetsnivå avhenger av at virksomheter oppdaterer sin kunnskap, blir mer sikkerhetsbevisste og tilpasser sikringstiltak etter endringer i trusselbildet. (NSM 2022)

I *Risiko 2022* (NSM 2022), beskrives det at trussel-aktørene viser stor kapasitet til å gjennomføre cyberangrep. Siden 2019 har NSM sett en tredobling i antall cyberhendelser som får alvorlige konsekvenser for virksomheter i Norge. Det siste året har kartleggingsaktivitet, phishing[2], digital utpressing og sabotasje, og utnyttelse av digitale sårbarheter hos et stort antall virksomheter preget cyberbildet. Kartleggingsaktivitet kan innebære kartlegging av tekniske sårbarheter, hvilken informasjon som ligger på åpne nettsider og kartlegging av personer eller organisasjoner. Vi må være oppmerksomme på at dette kan være forberedelser til neste fase i et cyberangrep.

Phishingforsøkene er ofte svært godt tilpasset til hvert enkelt mål. Vi er kjent med at trussel-aktører bruker offentlig tilgjengelig informasjon for å skreddersy e-poster som sendes virksomheter. Virksomheter bør derfor vurdere hvor mye informasjon om ansatte som skal ligge tilgjengelig på internett. (NSM 2021)

Utnyttelse av tekniske programvaresårbarheter er den vanligste veien inn for få uautorisert tilgang til en virksomhets digitale systemer. Utnyttelse av nulldagssårbarheter har preget det internasjonale risikobildet det siste året. En nulldagssårbarhet er en sårbarhet som ikke er kjent for leverandøren av programvaren, og som kan utnyttes av en trussel-aktør. (NSM 2021) Det betyr at trussel-aktøren oppdager sårbarheten først.

Norske virksomheter blir jevnlig rammet av krypteringsvirus med krav om løsepenger, såkalt løsepengevirus. Løsepengevirus har blant annet som formål å hindre virksomheten i å bruke sitt eget IT-system, slik at virksomheten presses til å betale angriperen for å kunne opprettholde ordinær drift. Bruken av løsepengevirus fortsetter å øke både i omfang og antall, og har i flere tilfeller ført til store systemlammelser med utilgjengeliggjøring av funksjoner, varer og tjenester, samt sensitiv informasjon på avveie. Internasjonalt rapporteres det om en dramatisk økning i summen av løsepengekrav. (NSM 2021)

Programvare- og tjenesteleverandører kan også utnyttes av trussel-aktører for å få innpass i systemene til selskapets kunder i såkalte leverandørkjedeangrep. Trussel-aktører kan skjule skadevare i programvare som leverandøren selger videre til sine kunder. På denne måten kan

[2] Phishing er en form for sosial manipulering hvor en angriper forsøker å lure noen til å gjøre en handling, eksempelvis trykke på en lenke. (Phishing - hvordan beskytte virksomheten | Datatilsynet, lastet ned 0707.2022)

en trussel-aktør enkelt etablere brohoder hos mange nye virksomheter. Skadevaren kommer inn i nye virksomheters systemer i form av en ordinær anskaffelse eller oppgradering, og slike sårbarheter kan være vanskelig å oppdage. Kartlegging av egne digitale avhengigheter og verdikjeder, samt å stille krav til tjenesteleverandørenes IT-sikkerhet er helt essensielt for en virksomhet for å redusere konsekvensene av en cyberoperasjon mot tjenesteleverandøren. (NSM 2021)

Gjenoppretting er både tid- og ressurskrevende og komplisert. Full stans i virksomheten og tap av sensitiv informasjon kan vise seg å bli vesentlig mer kostbart enn å investere i forebyggende sikkerhetsarbeid. Det bør derfor stå høyt på agendaen hos alle å sikre seg mot dette. (NSM 2021)

Den 09.03.2022 sendte KS ut et brev til alle landets kommuner om sikkerhetstiltak i norske kommuner i forbindelse med Russlands invasjon i Ukraina. Her opplyses det at norske sikkerhetsmyndigheter forventer økt aktivitet med svindel, phishing og sosial manipulering, og at kommune derfor må prioritere å innarbeide en god sikkerhetskultur. Brevet viser til Nasjonal sikkerhetsmyndighet (NSM) sine råd til virksomheter om å forebygge og avverge cyberangrep. KS anbefaler kommunene å iverksette undersøkelser og vurdere iverksetting av tiltak på følgende områder:

- Sikkerhetsovervåkning
- Sikring av kritiske funksjoner og tjenester
- Beskytte tjenester som er tilgjengelige på internett
- Årvåkenhet og teknologi

2.2 Erfaringer fra dataangrepet i Østre Toten kommune i 2021

Østre Toten kommune ble 09.06.2021 utsatt for et løsepengevirusangrep som rammet store deler av kommunens tjenesteproduksjon. Kommunedirektøren bestilte en rapport fra KPMG for å bidra til å belyse forholdet rundt årsak og konsekvens for berørte parter. Formålet med rapporten var å legge til rette for læring og komme med innspill til arbeidet med digital sikkerhet i framtiden. (KPMG, 2021)

I rapporten gis det anbefalinger til Østre Toten kommune som også er relevant for andre kommuner. Anbefalingene innledes med (KPMG 2021, s. 26)[3]:

[3] offentlig-versjon.pdf (ototen.no)

Et forsvarlig sikkerhetsnivå for informasjon og IKT-systemer oppnås ved å redusere risiko for uønskede hendelser til at akseptabelt nivå. For å lykkes er det nødvendig at kommunen har velfungerende og helhetlig sikkerhetsstyring som er en integrert del av virksomhets-styringen og samtidig må det gjøres kontinuerlig vurdering av risiko knyttet til egne verdier og håndtering av tilhørende risiko. Risikovurderingene må omfatte vurdering av verdier, identifisering av trusler og avdekking av sårbarheter. Risikovurderingene vil definere hva som er forsvarlig sikkerhetsnivå for kommunen og danner grunnlag for videre risikohåndteringsarbeid.

Noen av anbefalingene som ble gitt til Østre Toten kommune er gyldig for mange kommuner (forkortet versjon):

- Oppdatere kommunedirektørens internkontroll på IKT-sikkerhet i samsvar med anerkjente standarder.
- Gjennomføre jevnlige risikovurderinger, både overordnet, på IKT-avdelingen og tjenesteområdene.
- Innføre og styre etter NSMs grunnprinsipper.

Etter dataangrepet mot Østre Toten kommune sendte KS brev til kommunedirektørene og kommunenes IT-ansvarlig/IT-sikkerhetsansvarlig i februar 2021. I brevene ga KS råd og anbefalinger som kommunen burde vurdere, og at det er nødvendig at kommunene vurderer egen sikkerhets- og sårbarhetssituasjon. I brevet pekes det på følgende alvorlige konsekvenser av et dagangrep.

- Kommunen blir totalt lammet over lengre tid
- Kostnaden for å komme tilbake til normal drift vil kunne beløpe seg til 10-talls millioner
- Sensitive data på avveie kan innebære nasjonal risiko og eller brudd på personvern og rettssikkerhet til den enkelte borger, og som kan utløse erstatningskrav
- Andres IT-systemer kan bli rammet
- Tapt tillit til data og systemer

2.3 IT i Rennebu kommune

Rennebu kommune har en IKT-avdeling med to ansatte. En IKT-rådgiver og en IKT-konsulent. IKT-avdelingen er en del av staben ledet av personal- og stabssjef. Rennebu kommune kjøper tjenesten som personvernombud fra Midtre Gauldal. Vedkommende har 40 prosent stilling som personvernombud fordelt på fire kommuner.

2.4 Begreper

IT-området inneholder en del begreper og forkortelser som det kan være nyttig å ha oversikt over. Under er noen av IT-begrepene og begrepsdefinisjonene fra personvernforordningen[3] gjengitt.

Informasjonssikkerhet - Denne rapporten tar utgangspunkt i informasjonssikkerhet, og omhandler da både digital og analog informasjon. Hovedvekten er lagt på digital informasjon, men ikke avgrenset bort fra analog informasjon.

IT og IKT – forkortelsen IT – informasjonsteknologi og IKT – informasjons- og kommunikasjonsteknologi er forkortelser som brukes litt om hverandre. Begrepene brukes i dagligtale noe unøyaktig om hverandre. I denne rapporten brukes fortrinnsvis IT, men hvis dokumenter henviser til IKT, så er IKT brukt.

Tofaktorautentisering – betyr at det benyttes to ulike trinn for å bekrefte identitet.

Switch – nettverkskomponent som styrer datatrafikk mellom ulike noder i et nettverk, slik som PC, server[4], skriver og Internett-forbindelse. (Wikipedia, 07.05.2022.)

Ransomware – er på norsk omtalt som løsepengevirus, utpressingsprogramvare eller gisselvare. Det er skadelig programvare (datavirus) som krypterer hele eller deler av innholdet i en infisert datamaskin slik at den blir utilgjengelig for brukeren, for så å be om løsepenger.

QM+ - dette er navnet på kommunens kvalitetssystem.

DPIA – personvernkonsekvensvurdering. Datatilsynet forklarer at dersom det er sannsynlig at en type behandling av personopplysninger vil medføre høy risiko for folks rettigheter og friheter, skal den behandlingsansvarlige vurdere hvilke konsekvenser den planlagte behandlingen vil ha for personvernet. (, lest 21.02.2023)

GDPR – general data protection regulation. På norsk omtales GDPR som personvernforordningen. Dette er en lov som er vedtatt i EU og som er tatt inn i den norske lov om personopplysninger. Personvernforordningene skal styrke og harmonisere personvernet ved behandling av personopplysninger.

Ekomtjenester – er en forkortelse for elektronisk kommunikasjonstjenester.

Inntrengingstest (penetrasjonstest) – metode for å teste den digitale sikkerheten.

3 SYSTEM FOR INFORMASJONSSIKKERHET

3.1 Problemstilling

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

3.2 Revisjonskriterier

Følgende revisjonskriterier er utledet for denne problemstillingen:

- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen skal ha sikkerhetsmål og sikkerhetsstrategi.
- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjons-sikkerhet framgår.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen må ha rutiner med tilhørende praksis for tildeling og fjerning av tilganger og jevnlig kontrollere identiteter og tilganger.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.
- Kommunen bør vurdere og dokumentere IKT-risiko ved anskaffelser av datasystemer.
- Kommunen bør evaluere og lære av hendelser.

Utledningen av revisjonskriteriene finnes i vedlegg en.

3.3 System for informasjonssikkerhet i kommunen

Dette kapitlet handler om hvilke styringssystemer Rennebu kommune har bygd opp omkring informasjonssikkerhet.

3.3.1 Risikovurderinger

Rennebu kommune har en overordnet risiko- og sårbarhetsanalyse (ROS) og en beredskapsplan som ble vedtatt i kommunestyret 16.12.2021 (datert 07.12.2021). I ROS-analysen er svikt i ekomtjenester[4] og cyberangrep identifisert som farer. Cyberangrep omtales

[4] Ekomtjenester er en forkortelse for elektroniske kommunikasjonstjenester.

i forbindelse med svikt i ekomtjenester. Det er gjort risikovurdering av 22 hendelser i ROS-analysen og supplert med cyberangrep senere, forteller personal- og stabssjefen.

Selve dokumentasjonen av risikoanalysen for cyberangrep er ikke datert. Risikoanalysen for cyberangrep er beskrevet som et angrep hvor noen trenger seg inn i et nettverk eller datasystem på ulovlig vis. Risikobildet er illustrert med et scenario om løsepengevirus. Risikoen beskrives som høg på fire av fem områder. I risikoanalysen er det identifisert risikoreduserende tiltak. Det er:

- Beredskapsplaner for aktuelle hendelser innenfor informasjonssikkerhet
- Øvelser med evaluering
- Kommune-CSIRT
- Obligatorisk kursing i informasjonssikkerhet for alle ansatte
- Tilgangskontroller og økt internkontroll
- Offline back-up
- Penetrasjonstester

Ansvaret for de risikoreduserende tiltakene er lagt til kommunedirektøren med personal- og stabssjef og for noen tiltak også kommunalsjefer.

I kommunens beskrivelse av overordnet internkontroll og kvalitetsstyring står det at risiko-vurderinger skal dokumenteres og revideres etter gjeldende plan. Kommunen har gjennomført flere risikovurderinger på overordnet nivå og av kommunale tjenester og prosesser. Kommunen har etablert system for standardisert risikostyring som kan brukes av alle tjenesteområdene.

Ledergruppa er nøkkelen til arbeidet med risikovurderinger og er synlige i arbeidet med internkontroll og helse, miljø og sikkerhet, forteller ledelsen. Protokoller og referater legges ut slik at alle ansatte kan lese dem. Ledere som deltar i ledergruppen, tar med informasjon videre til avdelingsmøter.

Controller forteller at alle ansatte i kommunen har fått innføring i ROS om hva det betyr for ansatte og jobben de gjør. ROS-analysen er brukt som en mal for risikovurderinger på lavere nivå i organisasjonen. Det kan være utfordrende å bruke denne, spesielt når det gjelder ansattes forståelse av begrepene og sammenheng mellom sannsynlighet, konsekvens og risiko.

Personal- og stabssjef forteller at det er gjort en risikovurdering av det viktigste planverket og dette oppbevares også på papir. Det er den enkelte leder som må vurdere hva som er viktigst å ha i papirutgaver. Det er tatt opp i ledergruppa og der har kommunedirektøren informert om

at ledere må vurdere hva som er viktig å ha papirkopier av. Det skal stå i referatene fra ledergruppen.

I kommunens kvalitetssystem, QM+, kan det gjøres ROS-analyser for de enkelte tjenesteområdene. I QM+ er det mulig å gjøre risikovurderinger når det gjelder beredskap, informasjonssikkerhet, HMS (helse, miljø og sikkerhet) og i tjenesteytingen. Risikovurderingene innenfor beredskap er koblet opp til de områdene som er angitt i den overordnede ROS-analysen, også det 23. området som er cyberangrep. Innenfor informasjonssikkerhet er det følgende risiko eller mulige uønskede hendelser identifisert:

- Brudd på taushetsplikt
- Dokumenter er ikke arkivert, mistet eller ødelagt
- Risikovurdering av fagprogram
- Sensitiv informasjon er frigitt
- Sikkerhetsbrudd (innbrudd, hacking osv.)
- Utilgjengelige data

I personvernombudets årsmelding for 2021 står det at kommunen har gjennomført en del risikovurderinger fra tidligere år, men arbeidet er omfattende og de er fremdeles langt unna å være i mål.

Nå står risikovurdering av tjenesteområdenes kjøp av apper for tur, forteller personal- og stabssjefen. Personvernombudet bistår kommunen i risikovurderinger innenfor personvern. Det er månedlige møter med personvernombudet hvor personal- og stabssjefen og controller deltar.

IKT-rådgiver har ikke vært spesielt involvert i den overordnede ROS-analysen, og det er ikke utarbeidet egne risikovurderinger innenfor IT-området.

Ledelsen i kommunen har en årlig gjennomgang av overordnet beredskapsplan og beredskapsarbeidet, gyldig fra 16.06.2022, datert 20.06.2022. Til stede var kommunedirektør, kommunalsjefer, personal- og stabssjef, økonomisjef og saksbehandler.

3.3.2 Sikkerhetsmål og sikkerhetsstrategi

Ledelsen forteller at det ikke er utarbeidet målsettinger eller etablert egne styringsplaner for informasjonssikkerhet. Kommunen har ingen egne styringsdokumenter som for eksempel IKT-sikkerhetsplan. I tilsvaret på foreløpig rapport opplyser ledelsen at det er utarbeidet målsettinger og etablert egne styringsplaner for informasjonssikkerhet, men at kommunen ikke har etablert overordnede styringsdokumenter som for eksempel IKT-strategiplan. Etter at uttalelsen forelå stilte revisor et spørsmål til kommunedirektøren om å få tilsendt disse planene. I svaret (vedlegg 3) vises det til vedlagte dokumenter. Dette er:

- Varsling til Datatilsynet ved sikkerhetsbrudd
- Personvern og informasjonssikkerhet
- ROS-analyse, 07.12.2021

Rennebu kommune har en rutine for overordnet internkontroll, gyldig fra 18.02.2022. I rutinen er sikkerhetsmålet omtalt slik:

> *Sikkerhetsmålet er rett informasjon til rette vedkommende til rett tid for å sikre forsvarlige tjenester til kommunens innbyggere, herunder pasienter og øvrige brukere. Dette innebærer at informasjonen må sikres tilfredsstillende med høy grad av:*
>
> - *Konfidensialitet*
> - *Tilgjengelighet*
> - *Integritet*
> - *Kvalitet*
>
> *Data som registreres og behandles i våre datasystemer skal være:*
>
> - *Beskyttet mot uvedkommende*
> - *Tilgjengelig når det er tjenstlig behov for dem*
> - *Korrekte*

Det finnes etablerte overordnede styringsdokumenter for internkontroll i kommunen, men det mangler en overordnet strategi for informasjonssikkerhet, forteller controller. Kommunen har foreløpig ikke etablert personvernkonsekvensvurdering (DPIA) for noen av sine systemer. Controlleren har vært i kontakt med KS for å få innspill til blant annet mal for ROS-analyser og DPIA. Kommunen har behandlingsprotokoller som ligger samlet i QM+. I personvernombudets årsmelding for 2021 står det at Rennebu kommune har kommet langt i arbeidet for å få på plass protokoller over behandlinger som innehar personopplysninger som loven påkrever. Protokoller skrives fortløpende som nye program tas i bruk og nye behandlinger oppdages eller tas i bruk.

Når det gjelder prioriteringer internt på hvilke verdier som skal beskyttes er det IKT-rådgiver som kan svare best på det, forteller ledelsen. Det er mest IKT-rådgiver som vurderer hva som skal prioriteres.

IKT-rådgiver kunne tenkt seg økt fokus på mål og strategier, men har selv ikke kapasitet til ekstra arbeid med overordnet styring. IKT-rådgiver forteller at han har etablert egne mål i forbindelse med økonomiplanarbeidet, og lager innspill til budsjettet ut fra sitt ståsted. Det er ikke etablert noen rutine ut over dette. Flere av de foreslåtte budsjettpostene handler om utskifting av utstyr på grunn av alder eller tiltak for å øke sikkerheten. Hendelser på IKT-

området kan oppstå plutselig og må prioriteres, forteller IKT-rådgiver. IKT-rådgiver savner mer overordnede styringsdokumenter for hele området, inkludert mål og strategier for samhandling med andre enheter i kommunen. Pandemien utløste et oppgraderingsbehov, men etterpå har budsjettet normalisert seg.

IKT-rådgiver har prioritert hvilke informasjonsverdier som er viktigst å beskytte, eksempelvis at helseprogram er tilgjengelig i sikker sone, i påvente av en overordnet bestemmelse. IKT-rådgiver forteller at han sporadisk har tatt opp med ledelsen og enhetene om at de må lage en beredskapsplan for hva de skal gjøre om systemene er nede, eksempelvis hva de må ha på papir. Det er ikke etablert noen skriftlig prosedyre eller forankret i en overordnet plan. IKT-rådgiver har informert om dette i ledermøtet og forventer at kommunalsjefene formidler det videre til sine avdelingsledere.

I prosedyren for anskaffelse av IT-system, programvare eller app har sikkerhetsleder ansvar for å sørge for at kommunens sikkerhetsmål og -strategi for informasjonssikkerhet etterleves i driftsfasen.

3.3.3 Sikkerhetsorganisasjon

I praksis er det strategisk ledergruppe som er IKT-sikkerhetsutvalg, forteller ledelsen. Kommunen har ikke etablert eget IKT-sikkerhetsutvalg eller annen rutine som kun har fokus på informasjonssikkerhet. Revisor har fått tilgang på noen protokoller fra strategisk ledergruppe. Eksempler på informasjonssikkerhetssaker er følgende:

- Informasjon fra IKT-rådgiver om at totrinns pålogging på Office 365 er ikke like sikker lengre. Forslag om å etablere et system som sikrer pålogging kun via autorisert utstyr.
- Beredskap hacking. IKT-rådgiver orienterer. Omtaler blant annet papirkopier av viktige dokumenter, ber avdelingsledere tenke gjennom hva vi gjør hvis vi kommer på jobb og ikke noe fungerer. IKT-rådgiver sender ut mail til de som ikke har gjennomgått/fullført kurs i informasjonssikkerhet.
- Dataangrep. IKT-rådgiver informerer om konsekvenser av ikke å ha responsavtale eller overvåkningsavtale. Spørsmålet om responsavtale og overvåkningsavtale tas opp i strategisk lederteam når kommunedirektøren er tilbake. (Saken tas opp i ledermøte senere og der avventes det forvaltningsrevisjon)

IKT-rådgiver opplever å bli hørt og at innspill i stor grad blir fulgt opp. Samtidig opplever han at IKT blir sett på som de tekniske løsningene. Oppfatning av IKT har endret seg de siste årene når alle ansatte i mer eller mindre grad benytter IKT i det daglige arbeidet. Alle ansatte burde fått økt informasjon om når IKT-avdelingen bør inkluderes, for å gi ansatte økt innsikt i hvilke utfordringer det er i datasystemene og bruken av dem. Det er ingen faste rapporteringsrutiner

for rapportering til ledelsen, men IKT-rådgiver har mulighet til å legge fram saker for strategisk ledergruppe, forteller IKT-rådgiver.

IKT-rådgiver er stort sett fornøyd med arbeidsoppgavene IKT-avdelingen har i kommunen. De samarbeider også noe med IKT-avdelingen i Oppdal kommune. Atea[5] er samarbeidspartner og leverandør av tjenester og utstyr. Dette er kompetente folk som kan hjelpe IKT-avdelingen ved behov. Det har ikke vært noen formaliserte avtaler med Oppdal kommune eller Atea. IKT-rådgiver synes det er utfordrende å få forankret dette samarbeidet i kommunen. I mars 2023 ble en responsavtale med Atea formalisert.

Rennebu kommune har et personvernombud som er felles for kommunene Rennebu, Midtre Gauldal, Holtålen og Oppdal. Vedkommende er ansatt i Midtre Gauldal kommune. Personvern-ombudet har månedlige Teams-møter hvor kommunen har mulighet til å stille spørsmål om, og få tips og råd angående endringer i lovverk, forteller controller. IKT-rådgiver opplyser at han har deltatt i noen av disse møtene i saker om behandlingsprotokoller i fagsystemer, samt fagdagene med gjennomgang av GDPR. Ut over det, er han lite involvert i personvern-ombudets arbeid.

IKT-rådgiver opplever at han kan ta aktuelle kurs. Utviklingen innenfor IKT går så raskt at det er lite relevant med faglig fordypning på alle områder, men i stedet være opptatt av gjennomføringsevne og bruke konsulenter ved behov. Det viktigste er å forsøke å ha oversikt over behovet og stadig utvikle systemene, forteller IKT-rådgiver.

I prosedyren for anskaffelse av IT-system, programvare og app er det henvist til at IKT-rådgiver er sikkerhetsleder og sikkerhetsansvarlig.

3.3.4 Internkontroll

Rennebu kommune holder på å utarbeide et dokument om *ledelse og styring i Rennebu kommune*. Revisor har fått et utkast av dokumentet som etter planen skal behandles politisk. I dokumentet beskrives de overordnede retningslinjene for styring og ledelse som grunnlag for hvordan internkontroll og kvalitetssikring skal fungere. Dokumentet beskriver organisasjon, oppgaver og virksomhetsstyringen. I årsmeldingen for 2021 rapporteres det at administrasjonen har startet arbeidet med å etablere et omfattende, forsvarlig og gjennom-gående internkontrollsystem. Som en del av internkontrollsystemet skal kommunens

[5] Atea er et IT-selskap som jobber med behovskartlegging, rådgiving, utvikling av produkter og tjenester, drift og vedlikehold.

administrative ledelse foreta en gjennomgang av kvalitetssystemet, HMS-systemet og systemet for informasjonssikkerhet og overordnet beredskap.

Personal- og stabssjef forteller at internkontroll er tema på alle møter i strategisk ledergruppe. Det er gjort en kartlegging av rutiner for arbeidet med informasjonssikkerhet i 2021 og 2022. Controller forteller at fagdagene innenfor GDPR alltid inkluderer internkontroll. Dette er en årlig gjennomgang av blant annet behandlingsprotokoller. I personvernombudets årsmelding for 2021 er det oppsummert at kommunen har 161 ferdigstilte behandlingsprotokoller og i 19 av disse er risiko vurdert.

Ledelsen forteller at i kommunens kvalitetssystem QM+, finnes risikoanalyser og avviks-håndtering. Controller sier at alle styrende dokumenter skal ligge i QM+, mens planer, rutiner og retningslinjer skal ligge tilgjengelig i Teams. Unntaket her er de styrende dokumentene som følger meldinger i QM+. De ligger både i Teams og QM+.

Avvik legges inn og behandles i QM+, forteller ledelsen. Det arbeides med økt bevisstgjøring av avvikshåndtering. Avvikshåndteringen fungerer ikke optimalt for alle tjenesteområdene, men helse og omsorg er flinke til å bruke avvikssystemet. Skole og barnehage har også kommet godt i gang med avviksprosedyrer. Det skal generelt meldes avvik på 15 avviks-kategorier, inkludert brudd på informasjonssikkerhet. Avviksmelding i QM+ går til nærmeste leder og vurderes av leder, også avviksmeldinger om brudd på informasjonssikkerhet. Kommunedirektøren kan se alt og i tillegg kan personal- og stabssjef se meldinger om brudd på informasjonssikkerhet i avvikssystemet. Avvikssystemet følger organisasjonskartet, forteller ledelsen.

I QM+ er det mulig å melde avvik i forhold til risikoanalysen for tjenester, HMS og beredskap, samt ROS – GDPR/personvern. Innenfor tjenester, HMS og beredskap er det en kategori for informasjonssikkerhet, som har følgende risikoer eller mulighet for uønskede hendelser:

- Brudd på taushetsplikten
- Dokumenter er ikke arkivert, mistet eller ødelagt
- Risikovurdering av fagprogram
- Sensitiv informasjon er frigitt
- Sikkerhetsbrudd (innbrudd, hacking osv.)
- Utilgjengelige data

På området ROS – GDPR/personvern er det mulig å kategorisere meldingene i følgende tema:

- Integritet
- Konfidensialitet

- Tilgjengelighet
- Annet

Innenfor de tre første kategoriene finnes det en sjekkliste med flere kategorier som kan være med å definere avviket. For perioden 01.01.2023 til 30.03.2023 finnes det 18 meldinger på ROS – GDPR/personvern.

Blant de siste fem avviksmeldingene i QM+ per 21.02.2023 var et brudd på informasjons-sikkerhet. I personvernombudets årsmelding for 2021 er det totale antallet registrerte avvik 170 og to av dem gjelder personvern. To avvik er meldt til Datatilsynet.

Ledelsen forteller at det fortsatt finnes situasjoner hvor det ikke meldes avvik. Systemet er fortsatt under oppbygging og kan brukes mer enn i dag. Det arbeides med å inkludere ansatte i sikkerhetstankegangen, og de ansatte er blitt flinkere til ikke å trykke på lenker. Hvis noen trykker på en lenke de ikke skal, er prosedyren at IKT-avdelingen kontaktes for videre oppfølging. Revisor har ikke funnet noen skriftlig prosedyre på dette.

Ledelsen forteller at kommunen planlegger å sette av mer tid framover for å bedre internkontrollen på de ulike fagområdene. Dette skal ses i sammenheng med de lovverk som gjelder for tjenesteområdene i kommunen. Controller opplever at kommunedirektøren forstår at det må brukes ressurser til internkontrollarbeidet i kommunen, inkludert risikoanalyser.

Controlleren har opplevd ansatte som mener at internkontroll er et ikke-tema, men som etter nærmere informasjon får forståelse av internkontroll, og at mange allerede har internkontroll uten at de er klar over det. I Rennebu kommune arbeides det spesielt med å få avdelings-lederne til å ta i bruk internkontroll mer bevisst. Det ble gjennomført en enkel vurdering (ROS) på ledernivået i 2022, for å bevisstgjøre ledere på risikoer knyttet til det enkelte nivået. ROS-analysen er tilgjengelig for alle på fellesområdet i Teams.

Denne vurderingen av helheten i internkontrollen er gyldig fra 21.06.2022 (Tittel: enkel vurdering av helheten i internkontrollen). I denne vurderingen er et av seks punkt om informasjonssikkerhet og personvern. I vurderingen heter det:

> *GDPR er vi godt i gang med og dokumentert. IT sikkerhet jobbes godt med opplæring av alle ansatte i forhold til kursing og informasjon.*

Som tiltak står det at på IT-sikkerhet må kommunen vurdere backup ved eventuelle virus-angrep, samt å fortsette arbeidet med GDPR.

Når det gjelder evaluering og læring i internkontrollarbeidet utarbeides dokumentet *Ledelsens gjennomgang*, som er et årlig administrativt dokument med evaluering. Ledelsens gjennomgang er en del av den samlede informasjonen som kommunedirektøren opplyser om i sin årsmelding. Ute i organisasjonen er det avdelingslederne som skal gjennomføre dette på sine områder, forteller controller.

I dokumentet overordnet internkontroll og kvalitetsstyring står det at kommunen hvert år skal gjennomgå kvalitetssystemet, HMS-systemet og systemet for informasjonssikkerhet og overordnet beredskapsplan.

Årsmelding 2021 fra personvernombudet ble lagt fram sammen med sak 33/2022 Regnskapsavleggelse for 2021, den 16.06.2022. Innenfor dette området rapporteres det at avvik bør registreres i avvikssystemene uansett størrelse. Det gjelder ikke bare hendelser som har skjedd, men også ting som kan skje. Det handler ikke bare om å gjøre skadebegrensning i etterkant, men komme avvikene i forkjøpet. Videre rapporteres det at rapporterte avvik som er personvernrelatert forekommer sjeldent i kommunen. Det vil fremdeles være behov for å øke kunnskapen innad i kommunen for hva som anses som et avvik og hvilke regler og rutiner som gjelder.

Det er to ansatte på IKT-avdelingen og de deler kunnskap med hverandre, og nødvendig dokumentasjon blir skrevet ned og lagret på et felles område IT-ansatte har tilgang, forteller IKT-rådgiver. Det varierer hvor mye IKT-avdelingen er involvert i QM+. IT har egen helpdesk der brukerne melder inn behov, men når det gjelder sikring av data på enhetene, kan enhetene selv rapportere avvik i QM+. Det hender at lederne som skal håndtere avvikene tar kontakt med IT når de trenger hjelp. For eksempel på skole, rapporterte brukerne tidligere ofte direkte til helpdesken på IT. Nå er rutinen at det skal rapporteres til rektor først. Mange avvik blir derfor håndtert av rektor nå. Avvikshåndtering følger rutinene i avvikssystemet generelt.

I kommunens månedlige informasjonsrundskriv informeres det om status i arbeidet med internkontroll. For desember 2022 står det blant annet at:

> *Din nærmeste leder vil i samarbeid med deg finne hvordan Rennebu kommune best mulig kan bygge en god kultur for internkontrollarbeidet, slik at ditt arbeid følger aktuelle lover og forskrifter.*

3.3.5 Tilgangsstyring

Det er utarbeidet en rutine for alle nytilsatte, som må gjennomføres før de får tilgang til systemene og starte i arbeidet i kommunen, forteller controller. Dette handler om IKT-sikkerhet og at den nyansatte må gjøre seg kjent med kommunens rutiner og datasystemene. Dette er

ledernes ansvar å følge opp. Rutinen er forholdsvis ny og det kan være grunnlag for å forbedre den, men den følges i dag, sier controller. Det er beskrevet i rutinen at det skal gå melding til IKT-avdelingen når det kommer en nytilsatt.

Det er leder som gir tilganger til fagsystemer etter at nyansatte har fått opplæring i IT- sikkerhet, forteller ledelsen.

Rutine for den nytilsatte er gyldig fra 27.06.2022. Her er nærmeste leder gitt ansvaret for å følge opp rutinen. Sjekklistens del en for alle nyansatte handler om bestillinger fra leder før oppstart, for å sørge for at nødvendig utstyr og bestilling av tilganger er på plass. Dette omfatter IT-utstyr og passord til mailsystemet, kurs i informasjonssikkerhet og tilgang til fagprogrammer. Bestillingsfrist for tilganger er en uke. Del to er første arbeidsdag hvor IT-reglement, sikkerhets-kurs og taushetserklæring skal gjennomgås, samt at tilgang til data- og fagprogrammer er avklart og klargjort.

I kommunens IT-reglement står det at epost og personlig filområde blir slettet når brukeren har fratrådt sin stilling. Før fratreden skal brukeren rydde opp i sin epost og filer på hjemmeområdet og sørge for at opplysninger som fortsatt skal lagre overføres til rett person i Rennebu kommune.

IKT-rådgiver forteller at utfordringen oppstår når ansatte bytter avdelinger og skal ha nye tilganger eller rettigheter. Da er det en risiko for at gamle tilganger og rettigheter ikke slettes. IKT-rådgiver rydder i tilganger flere ganger i året, men det er muligens ikke strengt nok.

Det er ingen skriftlige rutiner på bruk av passord, men alle brukerkontoer som logger seg på datanettverket har systemkrav til kompleksitet og antall tegn. Passord er omtalt i kommunens IT-reglement, men det sies ikke noe om krav til selve passordet eller rutine for endring av passord. Det er etablert tofaktor-tilgang på skyløsninger der det er mulig, forteller IKT-rådgiver.

Kommunen er i ferd med å etablere et nytt system med passord. Ved første innlogging på datasystemet må brukerne logge inn via ID-porten for å sette personlig passord. Det jobbes også med en rutine for skifte av passord, med synkronisert skifte. Det er en vurdering hvor sikkert det skal være i forhold til brukervennligheten. Jo flere åpninger i et system, jo flere sikkerhetsrutiner må etableres, sier IKT-rådgiveren.

Tilgangskontroller og økt internkontroll er et av de risikoreduserende tiltakene i risiko-vurderingen på cyberangrep.

3.3.6 Opplæring

Fra 2022 har IT-sikkerhet hatt økt prioritert fra myndighetene, forteller ledelsen. Kommunen informerer og har innført opplæring og egne digitale kurs. Det er ikke utarbeidet egne planer

for opplæring innenfor informasjonssikkerhet. Kommunedirektøren henviser til opplæring i planen for nytilsatte, men det kan være behov for en plan for alle ansatte, alle har behov for oppdateringer.

Opplæring er stadig tema i ledergruppen og ledelsen mener at de blir bedre og bedre på IT-sikkerhet. Ledelsen er bevisst på at det er en balansegang når det er nok opplæring. Opplæringen handler om at ansatte må være observante, forlate PC i hvilemodus og låse døra der det oppbevares sensitive personopplysninger i papirform som ikke er innlåst. Kommunehuset i Rennebu er åpent for alle, servicetorget er strategisk plassert og bidrar til å stoppe og registrere besøkende, forteller ledelsen. Controller forteller at ledermøtene brukes bevisst til å videreformidle informasjon om opplæring. Det må være et eierskap hos lederteamet, sier controller.

Kommunen har jobbet mye med bevisstgjøring av databruk med kommunens ansatte. IKT-avdelingen har en plan for ansattes gjennomføring av NanoLearning. Denne opplæringen er en oppfrisking og bevisstgjøring. Alle ansatte har behov for slik oppdatering for å henge med, forteller controller. Ledelsen forteller at kommunen vil fortsette med NanoLearning, som er korte digitale kursmoduler, som kommunen kjøper og tilbyr ansatte som opplæring. IKT-rådgiver forklarer at NanoLearning er et kort opplæringsprogram som alle brukere får hver tredje uke. I programmet gis det informasjon og etter hver bolk stilles det spørsmål om informasjonen som er gitt. IKT-rådgiver ser også behov for å kjøpe opplæringspakker for generell bruk av PC og støttesystemer som Office-programmer, eksempelvis Teams.

IKT-rådgiver opplever at det er opp til han å sette i gang en prosess for å øke oppmerksomheten omkring informasjonssikkerhet. Det er generelt et behov for å øke bevisstheten blant ansatte og ledelsen om temaet. Samtidig har sikkerhetshendelsene som har vært i media den siste tiden økt bevisstheten hos brukerne.

Kommunedirektøren sender ut månedlige rundskriv til alle ansatte. Disse arkiveres i QM+ slik at alle ansatte har tilgang til dem. Fra januar 2023 legges disse ut i Teams, forteller ledelsen. I informasjonsrundskrivet for oktober 2022 informeres det om at kommunen gjennomfører bevisstgjøringskurs innen IT-sikkerhet.

IKT-rådgiver sier at den største utfordringen innenfor informasjonssikkerhet er å bli utsatt for hackerangrep. For å forebygge dette er det viktig å jobbe med brukerne og hvordan de skal håndtere systemene.

Obligatoriske kurs i informasjonssikkerhet for alle ansatte er et av de risikoreduserende tiltakene i risikoanalysen på cyberangrep.

Rennebu kommune har et kurs for ansatte om IT-sikkerhet på området for rutiner på IT, som er gyldig fra 08.09.2021. Formålet med kurset er en bevisstgjøring av digitale trusler og hvilke verktøy som kan benyttes for å ta gode digitale valg i hverdagen. Det står blant annet at informasjonssikkerhet ikke er kun et teknologiproblem, men 20 prosent teknologi og 80 prosent holdninger. I dokumentet ligger en systematisk gjennomgang av ulike informasjonssikkerhets-risikoer.

I det siste året har det vært fokus på å få en solid grunnmur i IKT-systemet. Det er gjennomført flere oppgraderinger og forbedringer av IKT-infrastrukturen på initiativ fra IKT-rådgiver. IKT-rådgiver har vurdert dette som viktig i forhold til økt sannsynlighet for angrep utenfra. På bakgrunn av dette har det praktiske arbeidet med det tekniske systemet blitt prioritert på bekostning av administrativt arbeid på informasjonssikkerhet.

3.3.7 IT-risiko ved anskaffelser

Rennebu kommune har en rutine for anskaffelse av IT-system, programvare eller app som er gyldig fra 01.01.2021. Rutinen er bygd opp med aktiviteter knyttet til ulike roller i organisasjonen. De rollene som omtales er bestiller, sikkerhetsleder, ansvarlig for teknisk løsning, personvernombud, arkiv og superbruker/systemansvarlig. Alle disse rollene har to eller flere av disse kategoriene med ytterligere beskrivelse:

- Stilling
- Rolle
- Ansvarsområde
- Myndighet
- Rapporterer til

Ansvaret for å gjennomføre DPIA (ROS i henhold til GDPR) før systemet blir anskaffet er lagt til sikkerhetsleder. Sikkerhetsleder er IKT-rådgiver. Et annet sted i prosedyren omtales IKT-rådgiver som sikkerhetsansvarlig. IKT-rådgiver er også den som skal ivareta funksjonen som ansvarlig for teknisk løsning. Ansvarlig for teknisk løsning har ansvar for å følge opp prosjektet og har direkte kontakt med tekniker fra leverandøren og som bistår sikkerhetsansvarlig ved ROS/DPIA. Personvernombudet er også ansvarlig for å bistå ved ROS/DPIA av programvaren.

Rutinen er tilgengelig på fellesområde på Teams og i QM+.

Formålet med prosedyren er at Rennebu kommune gjør bare gode og nødvendige innkjøp av programvare og apper, og at arkivlov og lov om behandling av personopplysninger og annen informasjonssikkerhet er ivaretatt i systemet som kjøpes inn, i prosessen mot drift og i drift. Prosedyren skal også bidra til at IKT-avdelingen kan planlegge sitt arbeid og dermed bistå best

mulig i etableringsprosessen. Bestiller har ansvar for at prosedyren blir iverksatt. Prosedyren beskriver blant annet følgende:

> **Bestiller:** IKT-rådgiver/sikkerhetsansvarlig/kommunalsjef/avdelingsleder/ personvern-ombud.
>
> **Bestillers ansvarsområde:** blant annet å kalle sammen gruppa bestående av ansvarlig for anskaffelsen, IT-rådgiver, arkivleder, sikkerhetsansvarlig (IT-rådgiver), systemansvarlig for systemet og personvernombud.
>
> **Sikkerhetsleder:** Sikkerhetsleder er IT-rådgiver. Leder som har det overordnede ansvar (kommunaldirektøren) for at organisasjonen følger de krav som stilles til informasjonssikkerhet.
>
> **Sikkerhetsleders ansvarsområde:** blant annet gjennomføre DPIA (ROS i henhold til GDPR) før systemet anskaffes. Sørge for at kommunens sikkerhetsmål og -strategi for informasjonssikkerhet etterleves i driftsfasen.

Ledelsen forteller at innkjøp av teknisk IKT-utstyr utføres i hovedsak av IKT-rådgiver, men at det skjer noe innkjøp på tjenesteområdene og avdelingene. Når det gjelder anskaffelser av IKT-utstyr og programvare er det controller som er ansvarlig for å kvalitetssikre innkjøpet med IKT-avdelingen, for eksempel ved kjøp av apper. Dette følger av delegert myndighet selv om det ikke er spesifikt nevnt i økonomireglementet. Controller jobber med anskaffelser sentralt i kommunen. Kommunen har innkjøpsavtale med fylkeskommunen og sektorene har i tillegg egne avtaler. IKT-rådgiver forteller at han har ansvar for alt kjøp innen IKT, og at flere kunne vært informert om ansvaret for innkjøp og IKT-avdelingen sin rolle. Det er lederne som har hovedansvaret for innkjøp i samsvar med delegert myndighet, forteller ledelsen. IKT-rådgiver setter ulike krav, så det er viktig at lederne spør. Dette kan svikte, og IKT-rådgiver har tatt opp i ledergruppa at IKT-avdelingen bør kontaktes før innkjøp av programvare.

Videre forteller ledelsen at kommunen har et eget telefonreglement og de følger systemet *Skytreck Control* via Telenor, som sikrer at telefonreglementet følges og det trekkes for private tjenester som er definert i reglementet.

IKT-rådgiver opplyser at det arbeides med rutiner for anskaffelser. Før var det kjøp av programmer som ble installert på kommunens servere, men nå er det mye mer skybaserte programmer. Det betyr at avdelingene i utgangspunktet har mulighet til å kjøpe og få tilgang til programvare uten å involvere IT, ettersom det ikke installeres på lokale servere.

Det er de enkelte enhetene i samarbeid med IKT-avdelingen som må følge opp at programvare som ikke lengre er i bruk avinstalleres. Enhetene har stort sett kontroll på dette, forteller IKT-rådgiver.

3.3.8 Evaluering og læring av hendelser

Evaluering av hendelser inngår i rapportgjennomgang av internkontrollen, forteller personal- og stabsleder. Dette skal med i årsrapporten for 2022. På personvern legges det årlig fram en rapport for kommunestyret, som i 2022 ble lagt fram sammen med sak 33/2022 Regnskapsavleggelse for 2021, den 16.06.2022. Foreløpig er det ingen egen evaluering av IT- hendelser.

Ledelsen forteller at det utarbeides evalueringsrapporter når kommunen gjennomfører beredskapsøvelser. Det kan tas ut rapporter for meldinger om brudd på informasjonssikkerhet i QM+. Det samme gjelder databehandleravtalene som er lagret i kommunens sak- og arkivsystem, Elements.

Ledelsen forteller at det har vært to meldinger til Datatilsynet i løpet av de siste årene. Den ene saken gjaldt et system over ledningsnettet til vann og avløp, hvor eieren av programvaren oppfordret kommunen til å melde saken i tillegg til dem selv. Den andre meldingen var knyttet til et pasientregistersystem, som ikke var i bruk, men som kommunen ble oppfordret til å melde av programvareleverandøren.

IKT-rådgiver forteller at de evaluerer hendelser og har da kontakt med personal- og stabssjef samt IT i Oppdal kommune. Det er ingen rutiner for å dokumentere dette, og det har vært lite hendelser hittil. Det føres ingen egen logg på hendelser og det dokumenteres ikke hvor ofte hendelsene skjer. Det er ulike typer hendelser og IKT-rådgiver opplyser at det kan være vanskelig å klassifisere typer hendelser.

3.4 Vurderinger

3.4.1 Risikovurdering

Revisor vurderer at Rennebu kommune gjennomfører og dokumenterer risikovurdering på ulike nivåer, men det er ikke gjennomført systematiske risikovurderinger og det er uklart hvilket grunnlag de gir for informasjonssikkerhetstiltak.

Kommunen har en overordnet risiko- og vesentlighetsvurdering fra 2021. Etterpå er det laget en ROS på cyberangrep. I QM+ er det mulig å gjøre risikovurderinger i forhold til informasjons-sikkerhet. Revisor finner liten sammenheng mellom risikovurderinger og informasjons-sikkerhetstiltak. Når systematiske risikovurderinger er gjennomført må kommunen ta stilling til

hvilke informasjonssikkerhetstiltak som prioriteres. I ROS på cyberangrep er det laget en beredskapsplan med risikoreduserende tiltak, men begrunnelsen for disse tiltakene mangler og det er uklart hvordan denne planen følges opp. Etter revisors forståelse er det bare tiltakene obligatorisk kursing i informasjonssikkerhet for alle ansatte og tilgangskontroller og økt internkontroll, som er risikoreduserende tiltak.

3.4.2 Sikkerhetsmål og sikkerhetsstrategi

Revisor vurderer at Rennebu kommune har generelle overordnede sikkerhetsmål, men mangler en sikkerhetsstrategi.

I rutinen om personvern og informasjonssikkerhet finnes det generelle sikkerhetsmål som er knyttet til konfidensialitet, integritet, tilgjengelighet og kvalitet. Revisor oppfatter at disse er sterkt knyttet til ivaretakelse av personopplysninger og mindre fokusert på bakenforliggende forhold som skal sikre ivaretakelse av personopplysninger. Eksempelvis vil system for tilgang på sikkerhetskopier ha betydning, og det kan være avveininger mellom hvor enkelt det er å ta i bruk systemer og flertrinns pålogginger.

Kommunen mangler overordnede styringsdokumenter for informasjonssikkerhet. Dette fører til at IKT-rådgiver får mye ansvar for å jobbe med informasjonssikkerheten uten mye hjelp fra resten av organisasjonen til å finne ut hva som er viktig å beskytte. Nasjonal sikkerhets-myndighet (2021) peker på behovet for å kartlegge organisasjonens informasjonsverdier, trusler og sårbarheter som en del av risikovurderingen. Dette er et arbeid som hele organisasjonen må involveres i. Når risikovurderingen er gjort må kommunen sette noen mål for hvor stor grad av sårbarhet som kan aksepteres i forhold til at systemer skal være brukervennlige og fungere i det daglige. Videre vil mål og strategier gi føringer for hva som skal beskyttes og hvordan. Når denne overordnede systematiske vurderingen mangler, kan det for eksempel være områder som IKT-avdelingen ikke klarer å følge opp.

I prosedyren for anskaffelse av IT-system, programvare eller app, henvises det både til sikkerhetsmål og sikkerhetsstrategi. Revisor har ikke funnet noe sikkerhetsstrategi og dette svekker denne prosedyren.

3.4.3 Sikkerhetsorganisasjon

Rennebu kommune har ikke fastsatt noen sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.

Kommunen har ikke fastsatt noen egen sikkerhetsorganisasjon for informasjonssikkerhet. Det henvises til at strategisk ledergruppe i kommunen er IKT-sikkerhetsutvalg. Revisor har ikke

funnet at strategisk ledergruppe har satt informasjonssikkerhet på dagsorden ut over enkeltsaker som IKT-rådgiver løfter til strategisk ledergruppe.

Kommunens kriseledelse slik den er definert i beredskapsplanen kan håndtere en krisesituasjon, men en sikkerhetsorganisasjon har andre roller og ansvar som må klarlegges og tildeles.

I prosedyren for anskaffelse av IT-system er IKT-rådgiver gitt rollen som sikkerhetsleder og sikkerhetsansvarlig, men dette er ikke forankret i en overordnet avklaring av rollene. Revisor stiller også spørsmål med begrepsbruken og om dette er to ulike roller som IKT-rådgiver har. Mye tyder på at beskrivelsen i prosedyren ikke er implementert fullt ut. En sikkerhets-organisasjon med definerte roller er et av Nasjonal sikkerhetsmyndighets grunnprinsipp for sikkerhetsstyring. Revisors inntrykk er at IKT-rådgiver får myndighet til å håndtere informasjonssikkerhetsspørsmål som burde vært håndtert av ledelsen i kommunen. IKT-rådgiver følger opp arbeidet med utgangspunkt i sitt ståsted.

3.4.4 Internkontroll

Revisor vurderer at Rennebu kommune holder på å bygge opp og implementere internkontrollsystemet og at informasjonssikkerhet inngår i internkontrollsystemet.

Rennebu kommune holder på å bygge opp et internkontrollsystem og ledelsen informerer jevnlig til organisasjonen om arbeidet. QM+ er kommunens kvalitetssystem som håndterer risikovurderinger og avvik, mens rutiner og prosedyrer er samlet i en mappestruktur på Teams. Informasjonssikkerhet inngår i internkontrollsystemet. Det gjenstår å komplettere med rutiner og få organisasjonen til å ta i bruk systemet. Slik det er i dag er det ingen systematikk i at IKT-avdelingen får informasjon om avvik på informasjonssikkerhet. Unntaket er når de blir kontaktet av ledere for å få hjelp til å håndtere avviket.

3.4.5 Tilgangsstyring

Revisor vurderer at Rennebu kommune har en rutine for tildeling og fjerning av tilganger, men at den ikke alltid følges opp i praksis. Det skjer jevnlige oppryddinger i tilganger.

Kommunen har en rutine som beskriver tildeling og avvikling av tilganger. I praksis vil det være en kontroll med tilganger for nyansatte fordi de trenger dette for å kunne gjøre jobben. Utfordringen er når det skjer endringer eller at de slutter i jobben. Det er et ledelsesansvar å følge opp at tilgangene endres når det er grunnlag for det. Funnene tyder på at praksisen med avvikling av tilganger ikke alltid følger rutinen, ettersom IKT-rådgiver må rydde i tilgangene. Vanligvis er det slik at kommunene betaler for alle tilganger slik at det også er kostnadsbesparende å ha kontroll på tilganger.

3.4.6 Opplæring

Revisor vurderer at kommunen gir ansatte opplæring i informasjonssikkerhet.

I kvalitetssystemet finnes det en opplæring i IT-sikkerhet som er obligatorisk for nyansatte og er omtalt i rutinen for nyansatte. Denne opplæringen er også aktuell for alle ansatte i organisasjonen. Rennebu kommune har satt i gang opplæring i informasjonssikkerhet gjennom å tilby ansatte NanoLearning moduler hver tredje uke samt at ledelsen informerer om informasjonssikkerhet. Dette er i tråd med risikoreduserende tiltak i risikovurderingen for cyberangrep. Det finnes ingen overordnet plan for denne opplæringen og det kan gjøre at opplæringen blir litt tilfeldig og kanskje ikke behovsprøvd. IKT-rådgiver peker på behovet for en generell opplæring i Office og tilhørende programmer.

3.4.7 IT-risiko ved anskaffelser

Revisor vurderer at Rennebu kommune har en rutine for anskaffelse av IT-system, programvare og app, hvor risikovurderinger skal inngå, men det er foreløpig ikke laget noen DPIA.

Rennebu kommune har en rutine for anskaffelse av IT-system, programvare og app, som beskriver framgangsmåten ved anskaffelser. Revisor har avdekket at prosedyren henviser til roller og dokumenter som ikke er avklart eller finnes.

Rutinen omtaler personvernkonsekvensvurdering (DPIA), som kun er en del av informasjons-sikkehetsområdet. Kommunen har ikke kommet i gang med DPIA. Intervjudataene tyder på at det er litt ulike forståelser av rollene i innkjøp av IT-utstyr og programvare og at rutinene ikke alltid følges. Uklarheter om ansvaret for innkjøp av IT-utstyr og programvare kan skyldes at behovet, budsjettet og informasjonssikkerheten er fordelt på ulike roller i organisasjonen.

3.4.8 Evaluering og læring av hendelser

Revisor vurderer at hendelser evalueres som en del av internkontrollen, men at det ikke er noe system for å dokumentere og evaluere hendelser innenfor hele informasjonssikkerhets-området.

Hendelser skal evalueres som en del av kommunens internkontroll som grunnlag for læring og forbedring. Internkontrollsystemet er under oppbygging og følgelig vil ikke rutiner og praksis for evaluering og læring være til stede på alle enheter og nivå i organisasjonen, herunder på IKT-avdelingen.

Rennebu kommune har ikke mange hendelser innenfor informasjonssikkerhet. De som er håndteres av IKT-rådgiver, men de dokumenteres ikke og det skjer ingen loggføring. De

bruddene på informasjonssikkerhet som registreres i kvalitetssystemet håndteres i utgangspunktet av nærmeste leder og kan forbli ukjent for IKT-rådgiver.

4 TEKNISKE OG ORGANISATORISKE TILTAK

4.1 Problemstilling

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

4.2 Revisjonskriterier

Følgende revisjonskriterier er utledet for denne problemstillingen:

Identifisere og kartlegge

- Kommunen må ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.

Beskytte og opprettholde

- 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

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

Håndtere og gjenopprette

- Kommunen bør ha en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon, gjenopprettingsplan og loggføring).
- Kommunen må ha en plan for gjenoppretting.

Utledningen av revisjonskriteriene finnes i vedlegg en.

4.3 Identifisere og kartlegge

Rennebu kommune har et IT-reglement som er gyldig fra 09.09.2021. Det er lagt opp til at IT-reglementet skal signeres av den enkelte medarbeider når det er lest. Revisor har ikke undersøkt eller fått bekreftet om det er gjort.

4.3.1 Datautstyr

I IT-reglementet står det at det ikke er tillatt å koble til private maskiner eller annet utstyr til datanettverket uten godkjenning fra IT-tjenesten. I hovedsak er det IKT-rådgiver som setter opp alt utstyret som kobles til kommunens nett. IKT-rådgiver forteller at det finnes en sperre, som hindrer at ikke-registrert datautstyr blir koblet på kommunens nettverk. Kommunen har egne nettverk for forskjellig type utstyr. Egne nett for teknisk utstyr for varme/ventilasjon, TV, mobiler og nettbrett.

IKT-avdelingen har ansvaret for innkjøp av teknisk utstyr, som servere, nettverksutstyr og sentralt IT-utstyr, PC, laptop og nettbrett, forteller IKT-rådgiver. Alt utstyr merkes og meldes inn i datasystemet. Samtidig dokumenteres utstyret i en egen oversikt. Skolen leaser PC-er, mens det kjøpes PC-er til administrasjonen. Dette oppleves som en ryddig løsning da det er ulik bruk. Det kan være behov for å kjøpe inn PC-er løpende gjennom året. Kommunen er med i fylkeskommunens innkjøpsavtale for innkjøp av datautstyr.

Basert på vurderingen til IKT-avdelingen er det nødvendig å ha en egen serverpark, for å ha nødvendige tjenester i drift, forteller IKT-rådgiver. Drift og vedlikehold av serverparken er en del av arbeidet til IKT-avdelingen. Det har ikke vært behov for å se på andre løsninger.

Etter hvert skal kommunens IKT-system oppgraderes slik at den ansatte kun får logget seg på skytjenester med utstyr godkjent av IKT-avdelingen. Dette arbeidet er nå i startfasen.

IKT-rådgiver mener det er enhetenes ansvar at IT-utstyr leveres inn når noen slutter. IKT-avdelingen har ikke mulighet til å følge opp dette, og dette kunne vært tydeliggjort mer. Det står i IT-reglementet at Rennebu kommune sitt datautstyr skal leveres tilbake til nærmeste leder, som igjen skal levere til IKT-avdelingen. Når kommunen tar i bruk det nye systemet for brukerhåndtering, får kommunen bedre styring med rettigheter og kan sperre all pålogging på systemet.

Rennebu kommune har en rutine for håndtering av lagringsmedier inkludert mobilt/bærbart utstyr, gyldig fra 01.01.2021. Formålet med rutinene er å ivareta kravene til personvern og informasjonssikkerhet. Det er egen nettbutikk for kommunens ansatte for kjøp av telefon, som baserer seg på et eget telefonreglement, forteller IKT-rådgiver.

I telefonreglementet, gyldig fra 01.12.2020, står det at IKT-avdelingen er ansvarlig for innkjøp av alt nytt utstyr i henhold til rammeavtaler. Reglementet har et kapittel om bruk og datasikkerhet. Mobilen skal sikres med PIN-kode eller tilsvarende som slås på automatisk. Det skal ikke installeres applikasjoner som kommer fra andre kilder enn de offisielle app-butikkene tilknyttet mobiloperativsystemet, med mindre dette er eksplisitt avklart og godkjent av arbeidsgiver. Når en brukt telefon, bytter eier/kjøpes av ansatte skal det kjøres en sikker

sletting. I reglementet finnes det også bestemmelser i forhold til permisjon og at avtalen opphører når arbeidstaker slutter i stillingen.

4.3.2 Programvare

I IT-reglementet står det at alt av programvare skal godkjennes av IT-ansatte før det installeres på maskiner. IKT-rådgiver forteller at det er en systemsperre slik at ingen brukere har rettigheter til å installere på arbeids-PC.

Rennebu kommune har de siste årene benyttet seg av mulighetene til å flytte tjenester over i sky, forteller IKT-rådgiver. Dette er en vurdering som gjøres for hvert enkelt system. Skyløsninger gjør kommunen mindre sårbare i forhold til driftsstans, oppdateringer skjer kontinuerlig og det gir mer fleksibilitet. Sikkerheten vurderes nøye, og det etableres tofaktorautentisering på tjenestene som ligger i sky.

Ulike enheter i kommunen har ulike behov, for eksempel har skole skybaserte programmer. Rektor har vært pådriver for skybaserte programmer på skole og IKT-avdelingen har lagt til rette for skybaserte tjenester. Dette kunne gjerne vært nedskrevet i et overordnet planleggings-dokument, forteller IKT-rådgiver. Premissene for gjennomføring gjøres i fellesskap mellom skole og IKT-avdelingen.

Det er gjennomført informasjonsmøter for alle avdelingsledere og strategisk lederteam om GDPR og hvordan kommunen skal fører protokoller for behandling av personopplysninger og hensikten med protokollene, forteller controller. Det er gjennomført fire fagdager for oppfølging av registrerte protokoller.

Behandlingsprotokoller er i stor grad utarbeidet og de er i hovedsak oppdatert. Det er avdelingslederne som skal føre protokollene, og dobbeltsjekke at databehandleravtalene eksisterer, forteller controller. Kommunen har etablert noen protokoller på personopplysninger i forbindelse med digitalisering av arkiv og annet arkiv. Fysisk lagring av personopplysninger blir også håndtert. Alle protokoller er lagret i QM+.

I personvernombudets årsmelding for 2022 står det at Rennebu kommune har kommet langt i arbeidet for å få på plass protokoller over behandlinger som innehar personopplysninger som loven påkrever. Protokoller skrives fortløpende når nye program tas i bruk og nye behandlinger oppdages eller tas i bruk.

4.4 Beskytte og opprettholde

4.4.1 Sikker IKT-arkitektur

IKT-rådgiver forteller at IKT-avdelingen har segmentert kommunens datasystem mye i det siste, strammet inn sikkerhet på servere og fjernet internett-tilgang fra servere. Utstyr som kun trenger internett-tilgang, er plassert i et eget nettverk. Før lå servere og PCer i samme nett. Nå ligger PCer i eget nettverk. Segmenteringen har økt sikkerheten både for bruker-PC og servere når det gjelder antivirusbeskyttelse og annen sårbarhet.

I kommunens nett er det to brannmurer til henholdsvis ytre og indre nettverk. På indre nett ligger data som trenger ekstra beskyttelse. Nettet er satt opp slik at ting ikke kan spres side-veis. Atea har bistått kommunen i å brygge opp IKT-infrastrukturen. Det er sikkerhetsløsninger for servere og klienter. Det er en egen vasking av epost og kommunens brannmur er streng i forhold til vedlegg i epost. I brannmuren ligger det sperrer for nettsider som anses å ha høy risiko.

IKT-rådgiver har et papirbasert konfigurasjonskart, som er innelåst et sted som bare ansatte på IKT-avdelingen kjenner til. Konfigurasjonskartet finnes i tillegg på en PC som ikke er koblet til nett og på en minnepinne. IKT-rådgiver føler at konfigurasjonskartet er oversiktlig, men det er alltid en utfordring å vedlikeholde konfigurasjonskartet løpende. Personal- og stabssjef blir orientert, men har ikke kjennskap til innholdet i dokumentet. Han har uttalt at han stoler på at IKT-avdelingen har kontroll og gjør de riktige vurderingene.

Personal- og stabssjef forteller at kommunen samarbeider med Atea og Atea sier at kommunen har en bra grunnmur i datasystemet sitt.

Det er gjort flere tiltak for å bedre sikkerheten, slik som segmentering av nettverk, skille forskjellige brukertyper i forskjellige nettverk og stenge internett-tilgang på servere, forteller IKT-rådgiver.

4.4.2 Sikkerhetsoppdateringer

IKT-rådgiver forteller at han gjør vurderinger om når oppdateringene skal installeres. Ved behov kan han stenge ned for å installere oppdateringer. Han har ikke opplevd motforestillinger fra ledelsen for dette. De fleste sikkerhetsoppdateringer kommer automatisk, fra HelseCERT, generell IT-informasjon og fra Atea.

Microsoft gjør månedlige oppdateringer på Windows, som er viktig å få installert. Når det kommer oppdateringer på antivirusporteføljen i sky, pushes den ut til klienter. Utstyret må være koblet på det kommunale nettverket for å få oppdateringene. Hvis ansatte er mye på

hjemmekontor får de ikke disse oppdateringene. Denne utfordringen blir løst med nytt system for klienthåndtering.

IKT-rådgiver forteller at sikkerhetsoppdateringer skjer automatisk for programmer som ligger i skytjenester.

4.4.3 Sikkerhetskopiering

Det er ingen skriftlig policy for hvordan lagringen skal foregå, men det er etablert rutiner for sikkerhetskopiering, forteller IKT-rådgiver. Revisor har fått en orientering om rutinene for sikkerhetskopiering, men de beskrives ikke her av hensyn til sikkerheten.

I ROS på cyberangrep er offline back up et av de risikoreduserende tiltakene.

4.5 Oppdage

4.5.1 Overvåkning

Det er overvåking av systemene som hele tiden gir status på servere og utstyr i nettverket, forteller IKT-rådgiver. Det er satt forskjellige terskelverdier i overvåkningsprogrammer. IKT-avdelingen får varsel på eposter når terskelverdiene brytes, og da må saken undersøkes. Det hender også at samarbeidspartnere varsler om eksterne trusler de er kjent med.

De fleste systemer logger aktivitet. Det er forskjellige overvåkingssystemer som IKT-avdelingen ser på daglig, forteller IKT-rådgiver. Det er programmer som overvåker trafikken på nettet og disse programmene logger hendelser. For å undersøke en hendelse må IKT-avdelingen inn på loggen, noe som er komplisert og kan ta lang tid.

IKT-rådgiver forteller at Atea har spesialkompetanse og kan fange opp og raskt tyde informasjon i logger om det oppstår en hendelse. Det er mulig å inngå en avtale med Atea om overvåkning av kommunens nett. Med en slik avtale kan de fange opp og unngå en uønsket hendelse før den inntreffer. En slik avtale er et kostnadsspørsmål. Det hender at kommunen får varsler fra Atea, uten å ha en slik avtale.

IKT-avdelingen følger med hva som skjer, forteller IKT-rådgiver. Han deltar i møter med Atea og oppdaterer seg mest på datasikkerhet og teknisk løsninger gjennom møter, kurs, kontakt med andre kommuner.

Kommunens datasystem er bra, forteller IKT-rådgiver. Utfordringen er at IKT-avdelingen ikke har tid nok til å lese loggene. Denne tjenesten er mulig å kjøpe fra Atea og når de leser logger kan de arbeide med preventivt. Atea tar mange trusler gjennom lesing av logger. Kommunen

kunne sysselsatt en person med å lese logger og vedkommende hadde kanskje ikke klart å ta unna alt, og det er ikke realistisk.

4.5.2 Inntrengningstester

IKT-rådgiver forteller at Atea har gjennomførte en inntrengningstest for å se på kommunens tjenester som er eksponert mot internett. Denne ble gjennomført for 1,5 år siden.

Rennebu kommune er medlem av Norsk helsenett og har tilgang til HelseCERT som har et Nasjonalt beskyttelsesprogram (NBP) hvor de tilbyr en rekke sikkerhetstjenester. I medlemskapet ligger det inntrengingstester som gjøres jevnlig, og kommunen får rapporter som viser resultatet, forteller IKT-rådgiver.

I ROS på cyberangrep er inntrengningstester nevnt som et av de risikoreduserende tiltakene.

IKT-rådgiver forteller at disse testene har vist lav sikkerhetsrisiko og har ikke ført til store endringer i kommunens system. Kommunen har lite tjenester som er eksponert mot internett og derfor er det begrenset hvor mye en test utenfra kan avdekke.

4.6 Håndtere og gjenopprette

4.6.1 Hendelseshåndtering

Rennebu kommune har en beredskapsplan datert 07.12.2021. I saksframlegget i behandlingen av planen i kommunestyret 16.12.2021 står det at enkelte fagområder bør ha en egen plan for å håndtere situasjoner ut fra sitt ansvars- og oppgaveområde, i tillegg til beredskapsplanen.

I ROS-analysen på cyberangrep er beredskapsplaner for aktuelle hendelser innenfor informasjonssikkerhet et av de risikoreduserende tiltakene.

Det har vært samtaler om hva som skal gjøres ved eventuelle angrep. IKT-avdelingen har en egen skriftlig beredskapsplan, men overordnet planlegging med ledelsen mangler, forteller IKT-rådgiver.

IKT-rådgiver forteller at han ikke har fått delegert myndighet, men tar beslutningen om det er kritisk og vil stenge ned med en gang uten å spørre, og vil informere ledelsen om handlingen etterpå. IKT-rådgiver har blitt kontaktet av Atea om en hendelse og da stengte han av epost-serveren midt på dagen for å løse hendelsen. Det er de to ansatte på IKT-avdelingen som kan gjøre dette. De har arbeidstid fra 8-15.30, og det er ikke etablert noen vaktordning for beredskap. Det har vært få hendelser utenfor arbeidstid, og med tanke på dagens bemanning er ikke vaktordning noe tema. Det er mulig for IKT-rådgiver å stenge ned kommunens

datasystem uten å være på rådhuset, men det er en fordel å være der. I slike situasjoner er det viktig å være i forkant.

IKT-avdelingen vil i praksis kontakte kommunedirektøren hvis noe oppstår, men i en svært prekær situasjon vil IKT-avdelingen kunne avgjøre selv, men kommunedirektøren er alltid den ansvarlige, forteller ledelsen. I den administrative organiseringen er myndighet delegert fra kommunedirektør til personal- og stabssjef og videre til IKT-avdelingen.

Det er ikke etablert rutiner for rapportering fra IKT-avdelingen og det er lite krav om rapportering fra IKT-avdelingen, for eksempel hva de arbeider med, hendelser og status. Hendelser håndteres løpende, forteller IKT-rådgiver. IKT-rådgiver presiserer at det er god dialog mellom IKT og ledelsen. IKT-rådgiver opplever å bli hørt og tatt på alvor når han kommer med innspill.

Kommunen har en rutine for melding til Datatilsynet, sist oppdatert 18.02.2022. Her er behandlingsansvarlig gitt ansvaret for å melde til Datatilsynet, mens leder/virksomhetsleder er ansvarlig for å gjennomføre prosedyren. Prosedyrens aktivitet/beskrivelse er slik:

1. *Virksomhetsleder/leder skal umiddelbart informere personvernombudet og eller behandlingsansvarlig:*
    a. *Ved brudd på personopplysningssikkerheten*
    b. *Ved mistanke om brudd på personopplysningssikkerheten*
2. *Virksomhetsleder skal dokumentere brudd og mistante om brudd på personvernsikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre de. Denne dokumentasjonen skal være lett tilgjengelig for tilsynsmyndigheten.*
3. *Organisasjonen skal dokumentere (hendelse, oppfølging og korrigering) i intern-kontrollsystemet.*

IKT-rådgiver har ikke vært involvert i de to varslene som er sendt til Datatilsynet, men ble orientert.

4.6.2 Gjenoppretting

Det er ingen sentrale føringer på prioritering av rekkefølge om det oppstår hendelser, forteller IKT-rådgiver. IKT-rådgiver har sin egen beredskapsplan, basert på det IKT-tekniske, men den er ikke forankret politisk. I og med at det mangler en overordnet strategiplan eller beredskaps-plan for IT-sikkerhet, vil det i en krisesituasjon bli mangel på kommunikasjon mellom kommuneorganisasjonen og IKT-avdeling om hva som skal gjøres, forteller IKT-rådgiver. IKT-avdelingen vil ha fullt opp med å håndtere hendelsen og vil ikke ha tid til å følge opp brukere

og innbyggere, forteller IKT-rådgiveren. Hvis det skjer et dataangrep kan det bli utfordrende for kommunen, sier IKT-rådgiveren. IKT-avdelingen vil måtte håndtere systemene, og det er ingen overordnede planer for hva andre i kommunen må gjøre. Det er mange systemer som vil rammet ved en hendelse, eksempelvis varme, ventilasjon, signalanlegg ved sykehjem til sentrale fagsystemer. Mange ansatte vil i en slik situasjon ha spørsmål som noen må besvare og følge opp.

I uttalelsen til foreløpig rapport opplyser kommunedirektøren at det foreligger beredskapsplan og fagplaner ved uønskede hendelser, som sikrer gjennomføring av den løpende driften. Revisor har bedt om å få tilsendt planer for gjenoppretting for ulike type hendelser og har fått til svar at det vises i første omgang til gjeldende ROS der dette tematiseres.

Det er ingen plan for gjenoppretting, eller andre overordnede planverk i kommunen som omhandler IKT og gjenoppretting. IKT-avdelingen har definert hva de har behov for å ha utskrevet i papir og har manuelle backup i manuelt system, forteller IKT-rådgiver. Selv om det ikke foreligger skriftlige overordnede planer, er det sagt at helse skal ha det vesentlige på utskrevet på papir.

Gjenoppretting av sikkerhetskopier har ikke blitt testet i stort omfang, forteller IKT-rådgiver.

IKT-rådgiver har en uformell avtale med Atea om at de bidrar med konsulenthjelp og kompetanse når de er tilgjengelig. Basert på dagens bemanning og IKT situasjonen i Rennebu kommune, er kommunen helt avhengig av bistand ved en alvorlig hendelse. Alt vil være utilgjengelig helt til kommunen får hjelp.

Kommunen har i mars 2023 fått på plass en responsavtale med Atea. Den gir kommunen prioritert hjelp til å gjenopprette data i løpet av fire timer, forteller IKT-rådgiver. Uten responsavtale kan det ta måneder før kommunen får gjenopprettet systemene sine. Kommunen er helt avhengig av andre hvis noe skjer.

4.7 Vurderinger

4.7.1 Identifisere og kartlegge

Revisor vurderer at Rennebu kommune har en oversikt over enheter i IKT-systemet.

IKT-avdelingen har en oversikt over enheter og utstyr som brukes i datasystemet. Det kan være en svakhet i at datautstyr ikke blir levert tilbake når ansatte slutter.

Revisor vurderer at kommunen har oversikt over programvaren som brukes i kommunens systemer.

Kommunen har et regelverk som regulerer ansattes mulighet til å legge inn programmer og apper. Kommunen har en systemsperre slik at det ikke er mulig å laste ned programvare på kommunens utstyr uten at det er klarert med IKT-avdelingen.

4.7.2 Beskytte og opprettholde

Revisor vurderer at kommunen har dokumentasjon på IKT-arkitekturen med ulike sikkerhetstiltak.

IKT-avdelingen har et konfigurasjonskart som viser oppbyggingen av kommunens IKT-system med ulike sikkerhetstiltak. Revisor har ikke beskrevet dette ytterligere fordi det kan være en sikkerhetstrussel. Revisor har fått en redegjørelse for dokumentasjonen.

Revisor vurderer at kommunen har en sentral styring med sikkerhetsoppdateringer.

IKT-rådgiver har ansvaret for sikkerhetsoppdateringer og kan iverksette disse umiddelbart hvis det er behov. Det er sentral styring med oppdatering av skybaserte tjenester. Inntil kommunen har fått på plass nytt system for klienthåndtering, er det en utfordring at sikkerhets-oppdateringene ikke skjer når ansatte er på hjemmekontor.

Revisor vurderer at kommunen har en plan for sikkerhetskopiering og tar sikkerhetskopier.

IKT-avdelingen sørger for at det blir tatt sikkerhetskopier og har en rutine for dette som ikke er dokumentert. Rutinen burde vært dokumentert slik at det det finnes et grunnlag for å vurdere forbedringer hvis en uønsket hendelse skulle oppstå. Revisor har fått en redegjørelse for hvordan sikkerhetskopieringen foregår, men den er ikke beskrevet her av sikkerhetshensyn.

4.7.3 Oppdage

Revisor vurderer at Rennebu kommune har et system for å overvåke sikkerheten og til en viss grad analysere data fra overvåkningen.

Rennebu kommune har ulike systemer for å overvåke aktivitet. Det genereres logger som kan være tidkrevende å følge opp. Det betyr at tiden ikke strekker til for å undersøke alle meldinger som logges. Gjennomgang av logger er en tidkrevende prosess.

Revisor vurderer at det gjennomføres jevnlig inntrengingstester på kommunens IT-system.

Revisor finner at både HelseCERT og Atea gjennomfører inntrengningstester på kommunens IT-systemer.

4.7.4 Håndtere og gjenopprette

Revisor vurderer at Rennebu kommune ikke har noen plan for håndtering av hendelser.

En plan for håndtering av hendelser er et av de risikoreduserende tiltakene i ROS-analysen av cyberangrep. Et forhold er det som må følges opp teknisk ved en hendelse, noe annet er at for eksempel kommunes tjenesteproduksjon kan bli rammet. Så lenge det ikke rapporteres på hendelser kan det være vanskelig å se behovet for en beredskapsplan som strekker seg til andre enheter i kommunen enn bare IKT-avdelingen. En manglende plan gjør at ulike deler av kommunen heller ikke har kunnskap om behovet for å iverksette enkle risikoreduserende tiltak.

Revisor vurderer at Rennebu kommune ikke har noen plan for gjenoppretting.

Funnene viser at Rennebu kommune vil være avhengig av hjelp fra andre hvis det oppstår en hendelse og det blir behov for å gjenopprette kommunens IT-systemer. Det er ikke nødvendigvis så enkelt som å legge tilbake en sikkerhetskopi. Angrep på datasystemer er i stadig utvikling og de aller fleste vil være avhengig av ekstern kompetanse for å klare jobben. I tillegg viser erfaring at dette kan ta lang tid. Responsavtalen med Atea er et tiltak for å sikre rask hjelp til kommunen med gjenopprettingen.

5 KONKLUSJONER OG ANBEFALINGER

5.1 Konklusjon

Revisor konkluderer at Rennebu kommune har sentrale mangler i styringssystemet for informasjonssikkerhet. Det mangler spesifikke sikkerhetsmål, sikkerhetsstrategi og en tydelig sikkerhetsorganisasjon.

Selv om det ikke er et helhetlig styringssystem for informasjonssikkerhet finnes det elementer av et overordnet system for informasjonssikkerhet, men de blir litt fragmentert og ikke alltid satt i sammenheng. Kommunen har risikovurderinger og et internkontrollsystem under oppbygging. Det er utarbeidet flere rutiner som berører informasjonssikkerhet, men rutinene kan bygge på forutsetninger som ikke er til stede eller at de ikke blir fulgt i praksis. Kommunen har tatt grep og satt fokus på opplæring.

Informasjonssikkerhet berører alle deler av en kommuneorganisasjon og det er de ansatte på de ulike enhetene som kjenner til hvilke informasjonsverdier de har, hvilke trusler de kan bli utsatt for og hvor sårbare de vil være hvis informasjonen ikke blir tilgjengelig. Selv om en IKT-avdeling kjenner til de tekniske løsningene, må det til et samarbeid for å vurdere hvilken grad av beskyttelse er hensiktsmessig for ulike informasjonsverdier. Som det står i kommunens kurs i IT-sikkerhet, er informasjonssikkerhet 20 prosent teknologi og 80 prosent holdninger. I tillegg må teknologi og holdninger henge sammen.

Revisor konkluderer med at Rennebu kommune har flere tekniske og organisatoriske tiltak for å ivareta informasjonssikkerheten, men mangler kritiske planer for hendelser og gjenoppretting.

Rennebu kommune har et IT-system med ulike tekniske tiltak for å ivareta informasjons-sikkerheten. Det er et ressursspørsmål hvor mye tid som skal brukes på å lese logger fra overvåkningen fordi det genereres mye data fra dem.

5.2 Anbefalinger

Revisor anbefaler kommunedirektøren å:

- Iverksette et arbeid med identifisering av informasjonsverdier, vurdering av trusler og sårbarheter som grunnlag for spesifikke sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganiseringen. Dette arbeidet kan munne ut i en overordnet plan for IKT og IKT-sikkerhet.
- Avklare og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
- Vurdere å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
- Vurdere behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
- Utarbeide en planer for hendelseshåndtering og gjenoppretting.

KILDER

CISA (2015) CISA Review Manual 26th Edition. CISA.

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

KMPG (2021) IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021.Kartlegging og ekstern vurdering. KPMG 2021.

KS 09.03.2022. Brev til kommunene. Til landets kommunedirektører og ordførere. Sikkerhetstiltak i norske kommuner i forbindelse med Russlands invasjon av Ukraina.

Nasjonal sikkerhetsmyndighet, udatert, Veileder i sikkerhetsstyring. Versjon 1. Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet (2020) NSMs grunnprinsipper for IKT-sikkerhet, versjon 2.0. 15.04.2020.

Nasjonal sikkerhetsmyndighet (2021) Nasjonalt digitalt risikobilde 2021.

Nasjonal sikkerhetsmyndighet (2022) Risiko 2022. Økt risiko kraver økt årvåkenhet.

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.

Problemstillingen om informasjonssikkerhet er knyttet til at Rennebu kommune samler inn og lagrer informasjon, både elektronisk og på andre medier. Personvernforordningens artikkel 32 b knytter sikkerhet for personers rettigheter og friheter til evnen til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og –tjenestene.

- Konfidensialitet – informasjonen blir ikke kjent for uvedkommende
- Integritet – informasjonen ikke blir endret utilsiktet eller av uvedkommende
- Tilgjengelighet – at informasjonen er tilgjengelig for autoriserte ved behov
- Robusthet – summen av konfidensialitet, integritet og tilgjengelighet

Disse prinsippene for personopplysninger er også relevante for annen informasjon som en kommune lagrer, eksempelvis at informasjonen er gjenfinnbar i sin opprinnelige form. Det at informasjonen er tilgjengelig når kommunen trenger den er vesentlig for mye av tjeneste-utøvelsen i en kommune.

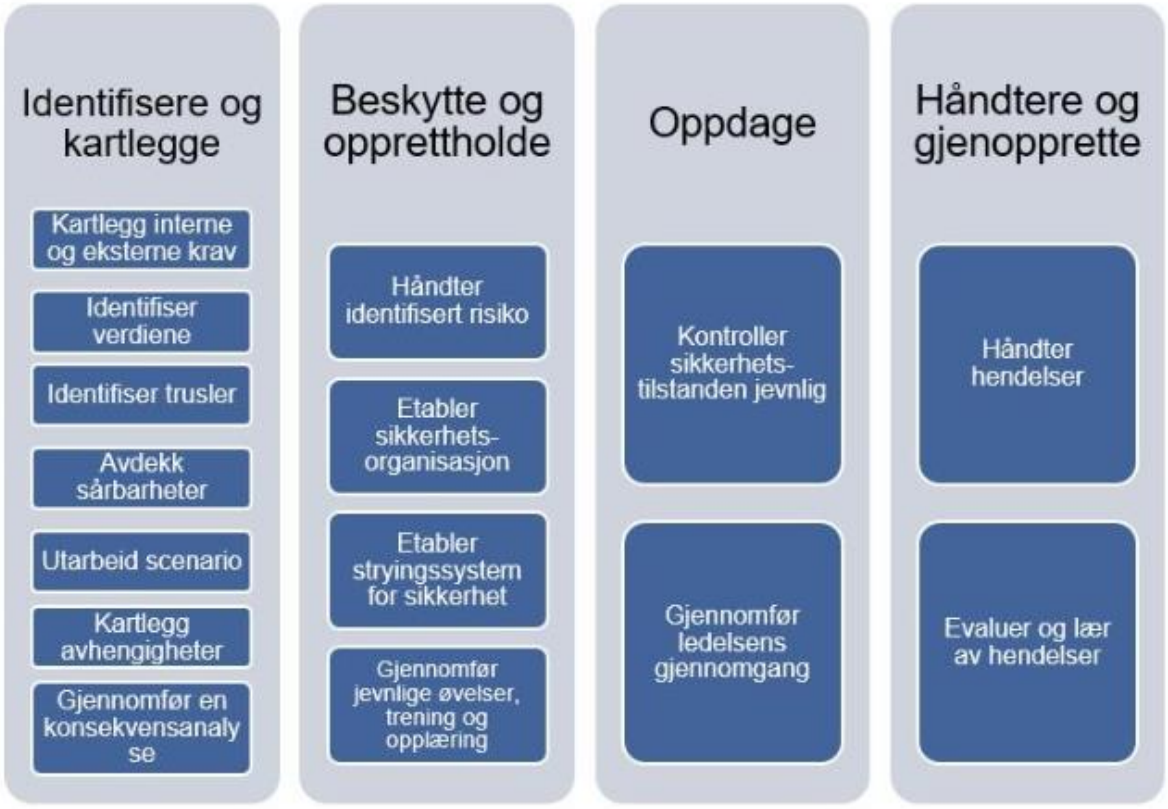
I denne forvaltningsrevisjonen er det to aktuelle tilnærminger til informasjonssikkerhet.

1. eForvaltningsforskriften, § 15 om internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan.
2. Sikkerhetsloven, kapittel 4 om krav til forebyggende sikkerhetsarbeid.

Nasjonal sikkerhetsmyndighet har grunnprinsipper innenfor fagområdene digital sikkerhet (IKT-sikkerhet), fysisk sikkerhet, personell sikkerhet og sikkerhetsstyring.

Sikkerhetsstyring

Grunnprinsippene for sikkerhetsstyring skal bidra til at virksomheten tenker helhetlig på sikkerheten og skal være en overbygning til de mer fagspesifikke sikkerhetsområdene som IKT-sikkerhet. (NSM 2020) Figur en viser grunnprinsippene for sikkerhetsstyring.



Kilde: NSM, 2020

Figur 1. NSM grunnprinsipper for sikkerhetsstyring

Både sikkerhetsloven og eForvaltningsforskriften peker på ledelsens ansvar, som først og fremst er på det strategiske nivået. Sikkerhetsloven stiller krav om at sikkerhetsstyringen skal gjennomføres planlagt og systematisk i et sikkerhetsstyringssystem som samordnes med virksomhetens styringssystem. Nasjonal sikkerhetsmyndighet har utarbeidet en veileder i sikkerhetsstyring[6] basert på kravene i sikkerhetsloven. Styring av informasjonssikkerhet består av å definere strategiske målsettinger av informasjonssikkerhet, sørge for at disse blir oppnådd, styre sikkerhetsrisikoen ved bruk av organisatoriske ressurser og påse at

[6] veileder-i-sikkerhetsstyring.pdf (nsm.no)

ledelsessystemet for informasjonssikkerhet fungerer hensiktsmessig og at resultater følger forventinger og målsettinger (Jøsang 2021). *Information systems audit and control association* (ISACA) har fem hovedmålsettinger for styring av informasjonssikkerhet:

- Strategisk tilpasning av aktiviteter til informasjonssikkerhet – informasjonssikkerhet er ikke et mål i seg selv, men skal bidra til virksomhetens mål.
- Risikostyring
- Effektiv bruk av ressurser – ledelsessystem og -prosesser må standardiseres så langt som mulig for å redusere administrasjons- og opplæringskostnader.
- Verdiskaping – optimal verdiskaping oppstår når strategiske mål for informasjonssikkerhet oppnås, juridiske krav etterleves og sikkerhetstrusler balanseres med akseptabel risiko, alt til lavest mulig kostand.
- Målbarhet – Måling er viktig for å vurdere om målsettinger oppnås. Metoder for å måle aktiviteter og hendelser relaterte til informasjonssikkerhet på tvers av organisasjonen må utvikles.

Sikkerhetslovens § 4-1 pålegger virksomhetens leder ansvaret for det forebyggende sikkerhetsarbeidet og at dette skal være en del av virksomhetens styringssystem. Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres. § 4-1 andre ledd sier at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. § 4-2 handler om vurdering av risiko og sier at en virksomhet skal regelmessig gjennomføre vurdering av risiko og at vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak. I § 4-4 står det at virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene.

Ledelse av informasjonssikkerhet er å opprette, drifte og vedlikeholde et sett med prosesser og aktiviteter som på en fornuftig måte beskytter organisasjonens informasjonsverdier mot sikkerhetstrusler, og som dermed kan opprettholde sikkerhetsmålene om konfidensialitet, tilgjengelighet og integritet (Jøsang 2021). Videre sier Jøsang (2021) at ledelse av informasjonssikkerhet bør være basert på et ledelsesinformasjonssystem bygd opp av et sett med prosesser og aktiviteter definert av et utvalg av standarder, rammeverk og egendefinerte retningslinjer og policyer, eksempelvis ISO 27001.

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

I § 15 andre ledd står det at internkontrollen skal basere seg på anerkjente standarder for styringssystem og være en integrert del av virksomhetens helhetlige styringssystem. § 15 tredje ledd sier at omfang og innretning på internkontrollen skal være tilpasset risiko. Revisor legger til grunn at det skal være gjennomført en risikovurdering som grunnlag for internkontroll-systemet.

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

IKT-sikkerhet

Nasjonal sikkerhetsmyndighet sine grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. (NSM 2020) Grunnprinsippene er delt i fire kategorier og er gjengitt i tabellen under.

Tabell 1. Grunnprinsipper for IKT-sikkerhet

1. Identifisere og kartlegge	**2. Beskytte og opprettholde**
Kartlegge styringsstrukturer, leveranser og under-støttende system Kartlegge enheter og programvare Kartlegge brukere og behov for tilgang	Ivareta sikkerhet i utviklings- og anskaffelsesprosesser 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 Etablere evne til gjenoppretting av data Integrere sikkerhet i prosess for endringshåndtering
3. Oppdage	**4. Håndtere og gjenopprette**
Oppdage og fjerne kjente sårbarheter og trussel Etablere sikkerhetsovervåkning Analysere data fra sikkerhetsovervåkning Gjennomføre inntrengningstester	Forbered virksomheten på håndtering av hendelser Vurder og klassifiser hendelser Kontroller og håndter hendelser

Kilde: NSM 2020

Hovedinndelingen av grunnprinsippene for IKT-sikkerhet er i stor grad sammenfallende med CISAs (2015) inndeling i forebyggende, oppdagende og korrigere tiltak. (CISA 2015).

Administrasjon og drift av informasjonssikkerhet er en samling ulike aktiviteter, slik som eksempelvis brannmurer, konfigurering, overvåkning, sårbarhetsskanning, forebygge tap og gjenoppretting av data (Jøsang 2021).

Kommunen bør ha oversikt over alle enhetene i informasjonssystemet. (NSM 2020) Denne bør være basert på hva kommunen har behov for av enheter og retningslinjer for godkjenning av enheter.

Kommunen skal ha et system for tilgangsstyring, som ivaretar at behandlingen av person-opplysninger begrenses til det som er nødvendig for formålene de behandles for (artikkel 5, 1 punkt, bokstav c). I dette ligger det at bare de som har bruk for informasjonen har tilgang til den. Begrensning av tilganger henger sammen med at eventuelle inntrengeres muligheter blir mindre. En virksomhet må derfor har kontroll på de ulike brukerne, kontoene de disponerer og hvilke rettigheter en gitt konto har (NSM, 2020).

Enheter, programvare og brukere er sentrale elementer i et informasjonssystem som inngår i den overordnede IKT-arkitekturen. Kommunen bør bygge en sikker IKT-arkitektur med sentral styring og automatiserte prosesser hvor det er hensiktsmessig (NSM, 2020). En slik IKT-arkitektur kan visualiseres i et konfigurasjonskart som viser ulike soner for tilganger, brannmurer med mer.

Denne IKT-arkitekturen bør beskyttes med brannmurer, kryptering og antivirusprogram.

Det er mulig å konfigurere både utstyr og programvare, slik at det legges inn begrensninger i bruken for å ivareta sikkerheten. En viktig del av dette er å sikre at sikkerhetsoppdatering installeres når de foreligger og at dette er sentralt styrt (NSM 2020).

Selv om mange sikkerhetstiltak kan bygges inn i systemer vil det alltid være en risiko for at autoriserte brukere er inngangen for mange som vil bryte seg inn i informasjonssystemer, eksempelvis gjennom å trykke på lenker som kommer på epost. Opplæring av ansatte og informasjon om sikkerhetstiltak som den enkelte kan følge opp er viktig for å bygge en sikkerhetskultur i virksomheten. Samtidig er det viktig at ansatte får beskjed når det dukker opp phishing-kampanjer, slik at ingen aktiverer lenken.

Til tross for at systemer kan beskyttes teknisk vil det alltid være steder som er mer sårbare enn andre. Noe av dette kan også være bevisst for at systemene skal være mer brukervennlig. Det betyr at det må finnes tiltak for å gjenopprette informasjon gjennom for eksempel sikkerhetskopier. Kommunen må ha system som sikrer tilstrekkelig sikkerhet for person-opplysninger, herunder vern mot utilsiktet tap, skade eller ødeleggelse (artikkel 5, punkt 1, bokstav f)

Gjennom skyløsninger for programvare og for eksempel samarbeidsparter vil kommunen kunne utveksle data med andre, såkalte databehandlere. Artikkel 4, punkt 8 definerer data-behandler som en fysisk eller juridisk person som behandler personopplysninger på vegne av den behandlingsansvarlige. Artikkel 28 punkt 3 omhandler databehandleravtale som skal være en skriftlig avtale som er bindende for databehandleren med hensyn til den behandlings-ansvarlige, og der gjenstanden for og varigheten av behandlingen, behandlingens art og

formål, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt. I bokstav a til h er det oppgitt hva databehandleravtalen særlig skal inneholde, hvor punkt c henviser til artikkel 32 om sikkerhet ved behandling av personopplysninger. Kommunen bør vurdere sikkerheten i forbindelse med inngåelse av databehandleravtaler.

Moderne skadevare utvikles for å unngå enkelte sikkerhetstiltak, eller for å angripe eller deaktivere tiltakene. Selv de beste produkter har feil og sårbarheter som kan utnyttes av angripere (NSM 2020). Kommunen bør ha et system for sikkerhetsovervåking. Data fra sikkerhetsovervåkningen bør analyseres med tanke på å oppdage uautoriserte handlinger og sikkerhetstruende hendelser. IKT-systemer er under konstant endring og utvikling og utfordres jevnlig av angrepsaktører. Virksomheter bør derfor jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Dette kan gjøres gjennom jevnlige inntrengningstester. (NSM 2020)

Nasjonal sikkerhetsmyndighet (2020) skriver at dataangrep har blitt en del av dagliglivet. Når hendelsen inntreffer er det for sent å utarbeide gode prosedyrer, rapporteringsrutiner, datainnsamling, ledelsesansvar og kommunikasjonsstrategier. Kommunen må derfor ha en plan for hendelseshåndtering som oppdateres minst en gang i året.

Følgende revisjonskriterier legges til grunn:

System for informasjonssikkerhet

- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen skal ha sikkerhetsmål og sikkerhetsstrategi.
- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen må ha rutiner med tilhørende praksis for tildeling og fjerning av tilganger og jevnlig kontrollere identiteter og tilganger.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.
- Kommunen bør vurdere og dokumentere IKT-risiko ved anskaffelser av datasystemer.
- Kommunen bør evaluere og lære av hendelser.

Tekniske og organisatoriske tiltak

Identifisere og kartlegge

- Kommunen må ha en oversikt over enheter i IKT-systemet.
- Kommunen bør ha en oversikt over programvare.

Beskytte og opprettholde

- Kommunen bør etablere og dokumentere en sikker IKT-arkitektur.
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer.
- Kommunen må ha en plan for sikkerhetskopiering.

Oppdage

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

Håndtere og gjenopprette

- Kommunen bør ha en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon, gjenopprettingsplan og loggføring).
- Kommunen må ha en plan for gjenoppretting.
- Kommunen må ha en beredskapsplan som omfatter IKT hendelser.

VEDLEGG 2 – UTTALELSE FRA KOMMUNEDIREKTØREN

RENNEBU KOMMUNE

REVISJON MIDT-NORGE SA
Brugata 2

7715 STEINKJER

Off. § 5

Deres ref:	Vår ref 2022/1478	Saksbehandler Per Øivind Sundell	Dato 27.04.2023

Rapport til uttalelse - informasjonssikkerhet - u.off., jfr. offl. § 5 (2)

Vi viser til tilsendt utkast til forvaltningsrevisjonsrapport om informasjonssikkerhet i Rennebu kommune. Kommunedirektøren ønsker å benytte seg av retten til å gi en uttalelse om utkastet. Vår uttalelse følger under og som eget vedlegg.

Administrasjonen ønsker å takke for en fyldig rapport som på en oversiktlig måte klargjør status for kommunens IT-sikkerhet. Administrasjonen ser positivt på at et slikt dypdykk kan bidra til å avdekke de svakheter som måtte finnes – da som i et ledd i å stadig bli bedre. Vi ønsker selvsagt å bli best mulig forberedt, noe rapporten kan bidra positivt godt til.

Administrasjonen vil likevel benytte muligheten til å påpeke enkelte feil og mangler i den foreløpige rapporten som med fordel bør endres i endelig rapport. Vi har ved gjennomgang av foreløpig rapport følgelig funnet flere forhold vi mener bør korrigeres og utdypes for å gi et mest mulig korrekt bilde av status. Da vårt innspill til endringer er spredt rundt kring hele rapporten (nær på alle sider f.o.m. kap. 3), finner vi det ikke hensiktsmessig å svare ut med å her gjengi hver endring for seg, men har heller valgt her å vise behov for endringer gjennom følgende grep direkte i teksten som foreligger:

~~Overstreking~~ i forslaget: For det vi mener er direkte feil.

Rød skrift i forslaget: Diverse tilføyelser og korrigeringer.

Annen generell kommentar/avklaring til forslaget: Har revisor kjennskap til de mange ulike avviksmeldinger i Qm+, som omhandler IT- sikkerhet? Vi mener at eksempelvis melding IT – GDPR som handler om integritet, konfidensialitet, tilgjengelighet og annet, med sjekklister, ivaretar i stor grad rutiner for krav om informasjons-/sikkerhetssystem.

Med vennlig hilsen
Rennebu kommune

Per Øivind Sundell
Kommunedirektør
485 95 970
per.sundell@rennebu.kommune.no

Postadresse:	Epostadresse:	Telefon:	Bankkonto:
Myrveien 1, 7391 Rennebu	postmottak@rennebu.kommune.no	947 86 930	4260 70 73915
Besøksadresse:	Web adresse:		Organisasjonsnummer:
Myrveien 1	www.rennebu.kommune.no		940 083 672

Dette dokumentet er elektronisk godkjent og har derfor ingen signatur.

Vedlegg

1 230329 IKT-sikkerhet Rennebu - tilsvar fra kommunedirektøren

VEDLEGG 3 – KOMMUNEDIREKTØRENS SVAR PÅ OPPFØLGINGSSPØRSMÅL

Hei, vårt lokale IKT-arbeidsutvalg har gått gjennom de punkter som er listet opp av revisor og svarer her ut som følger (*markert i blå kursiv skrift*):

- Det henvises til årsmelding for 2022 fra personvernombudet, s. 17. Revisor ønsker denne tilsendt.
  Denne ligger vedlagt.

- Det henvises til at det er utarbeidet målsettinger og egne styringsplaner for informasjonssikkerhet, s. 17. Disse ønsker revisor tilsendt.
  Disse ligger vedlagt.

- Det opplyses om et IKT-arbeidsutvalg, s. 19. Når ble dette opprettet? Finnes det en beskrivelse av dette, eksempelvis hvilket mandat IKT-arbeidsutvalg har.
  IKT-arbeidsutvalg ble formelt opprettet av kommunedirektøren i april 2023 som en følge av konklusjoner fra foreløpig rapport for forvaltningsrevisjonsprosjektet samt opplevd behov for et mindre og hurtigarbeidende utvalg utover det ordinære IKT-utvalget (strategisk ledergruppe).

- Et nytt spørsmål: Har dere eksempler på IKT-saker som er behandlet i strategisk ledergruppe? Dokumentert med møtereferat.
  Slike saker har vært på agendaen til ledergruppen i flere omganger siden denne ble opprettet i 2019. Med ukentlige møter med unntak av sommermånedene blir antall gjennomførte møter gjennom året stort – dermed også mange saker totalt. Protokoll fra møtene skal være gjort tilgjengelig for revisor i teams – jfr. «Strategisk lederteam – Ledermøter – Årstall – Møtedato». Vi legger ved ***et utvalg*** *referat her der det det er protokollert temaer knyttet til IKT. Se f.eks. notat fra møte 17.01.22 – sak 2, notat fra møte 09.05.22 – sak 7 og 14, notat fra møte 17.10.22 – sak 1 + m.fl.*

- Nest siste avsnittet s. 23: Er korrigeringene her riktige? Jeg leser det slik at QM+ styrer tilganger??
  Nei - dette følger organisasjonskartet. Det er kommunedirektøren som styrer tilganger gjennom QM+.

- Dere har tilføyd ordet overordnet (første setning s. 24), i forbindelse med skriftlige rutiner for bruk av passord. Betyr det at det finnes andre skriftlige rutiner for bruk av passord?
  Nei, det har vi ikke. Men vi har jo føringer for dette i IT-reglementet. IKT-arbeidsutvalg har plan/ønske om enda større detaljfokus på dette fremover.

- Dere har tilføy at det har blitt gjennomført flere oppgraderinger og forbedringer av IKT-infrastrukturen s. 25. Kan dere være litt mer presise på hvilke oppgraderinger og forbedringer?
  Det er oppgraderinger og forbedringer av infrastrukturen som er nevnt tidligere i dette dokumentet – herunder:
  - ✓ *Forbedret sikkerhet i forhold til anti-virus på servere*
  - ✓ *Segmentering av nettverk*
  - ✓ *Ny hardware som gjør at programvare er oppdatert og i vedlikehold.*
  - ✓ *Forbedret brannmur mtp. sikkerhet*
  - ✓ *Forbedret sikkerhet på servere i forhold til tilganger.*

- Det er tilføy at det foreligger beredskapsplan og fagplaner ved uønskede hendelse som skal sikre gjennomføring av den løpende driften s. 38. Revisor ønsker å få tilsendt planer som gjelder gjenoppretting for ulike typer IKT-hendelser.
  Vi henviser da i første omgang til gjeldene ROS der dette tematiseres.

Vi håper med dette at de spørsmål revisor har reist er svart ut tilfredsstillende i denne omgang. Dersom behov for ytterligere presiseringer av ovennevnte og/eller ønske om kommentarer/forklaringer/dokumentasjon mht. andre IKT-relaterte forhold, er vi selvsagt klare for å svare ut dette.

Med vennlig hilsen

Per Øivind Sundell
Kommunedirektør
Rennebu kommune
Mobil: 48 59 59 70
www.rennebu.kommune.no

RENNEBU KOMMUNE

VEDLEGG 4 – TEKST SOM ER UTELATT ELLER SOM ER DEKKET AV ANNEN TEKST

3.3.1 - utelatt

Controller forteller at alle ansatte i kommunen har fått innføring i ROS, og om hva det betyr for ansatte og jobben de gjør. ROS-analysen er et lederansvar i organisasjonen. Det kan være utfordrende å bruke denne, spesielt når det gjelder ansattes forståelse av begrep.

3.3.2 - utelatt

Kommunen har foreløpig ikke etablert personvernkonsekvensvurdering (DPIA) for noen av sine systemer. ~~Innkjøpskoordinator har vært i kontakt med KS for å få innspill til blant annet ROS- analyser og DPIA.~~ Controller har vært med i et nettverksamarbeid ledet av KS hvor dette er utredet, men foreløpig er det kun på pilot stadiet og Bergen kommune prøver ut. Controller har vært i kontakt med KS for å få innspill til blant annet når mal for ROS-analyser og DPIA vil bli offentliggjort for alle andre kommuner, uten å få bekreftelse. Derfor står Rennebu på lik linje med mange andre kommuner på stedet hvil, i forhold til DPIA.
Kommunen har behandlingsprotokoller som ligger samlet i QM+. I personvernombudets årsmelding for 2021 står det at Rennebu kommune har kommet langt i arbeidet for å få på plass protokoller over behandlinger som innehar personopplysninger som loven påkrever. Protokoller skrives fortløpende som nye program tas i bruk og nye behandlinger oppdages eller tas i bruk.

3.3.2 - utelatt

IKT-rådgiver kunne tenkt seg økt fokus på mål og strategier, men har selv ikke kapasitet til ekstra arbeid med overordnet styring. IKT-rådgiver forteller at han har etablert egne mål i forbindelse med økonomiplanarbeidet, og lager innspill til budsjettet ut fra sitt ståsted. Det er ikke etablert noen rutine ut over dette. Flere av de foreslåtte budsjettpostene handler om utskifting av utstyr på grunn av alder eller tiltak for å øke sikkerheten. Hendelser på IKT-området kan oppstå plutselig og må prioriteres, forteller IKT-rådgiver. IKT-rådgiver savner mer overordnede styringsdokumenter for hele området, inkludert mål og strategier for samhandling med andre enheter i kommunen. Pandemien utløste et akutt oppgraderingsbehov, men deretter ble det normalisert, ~~men etter pandemien har det stagnert litt.~~ Administrasjonen viser forøvrig til gjeldende reglement for budsjett og økonomiplan i Rennebu kommune (økonomireglement).

3.3.3 - utelatt

IKT-rådgiver er stort sett fornøyd med arbeidsoppgavene IKT-avdelingen har i kommunen. De samarbeider også noe med IKT-avdelingen i Oppdal kommune. Rennebu har forsøkt å utrede nærmere formelt samarbeid over kommunegrensen til Oppdal innen mange tjenesteområder - herunder også IKT, men dette har dessverre strandet etter at Oppdal har trukket seg fra videre drøftinger (jfr. at de stiller ultimatum om legevaktsamarbeid for å vurdere samarbeid på andre tjenesteområder). Atea[5] er samarbeidspartner og leverandør av tjenester og utstyr. Dette er kompetente folk som kan hjelpe IKT-avdelingen ved behov. Det er ingen formaliserte avtaler med Oppdal kommune eller Atea. IKT-rådgiver synes det er utfordrende å få forankret dette samarbeidet i kommunen. ~~Det burde vært en formalisert avtale med Atea i forhold til beredskap, og i mars 2023 ble en responsavtale med Atea formalisert.~~ Responsavtale med Atea ble inngått i mars 2023.

3.3.4 - utelatt

Avviksmelding i QM+ går til nærmeste leder og vurderes av leder, også avviksmeldinger om brudd på informasjonssikkerhet. Kommunedirektøren kan se alt og i tillegg kan personal- og stabssjef se meldinger om brudd på informasjonssikkerhet samt ledere og ansatte som gis roller. Avvikssystemet følger organisasjonskartet, forteller ledelsen.

3.3.4. - utelatt

Ledelsen forteller at kommunen planlegger å sette av mer tid framover for å bedre internkontrollen på de ulike fagområdene. Dette skal ses i sammenheng med de lovverk som gjelder for tjenesteområdene i kommunen. Controller opplever at kommunedirektøren forstår og aksepterer at det må brukes ressurser til internkontrollarbeidet i kommunen, inkludert risikoanalyser.

3.3.4 - utelatt

Det er to ansatte på IKT-avdelingen og de deler kunnskap med hverandre, og nødvendig dokumentasjon blir skrevet ned og lagret på et felles område IT-ansatte har tilgang, forteller IKT-rådgiver. Det varierer hvor mye IKT-avdelingen er involvert i QM+. IT har egen helpdesk der brukerne melder inn behov. Når det gjelder sikring av data på enhetene kan enhetene rapportere avvik selv i QM+. Det hender at lederne som skal håndtere avvikene tar kontakt med IT når de trenger hjelp. For eksempel på skole, rapporterte brukerne tidligere ofte direkte til helpdesken på IT. Nå er rutinen at det skal rapporteres til rektor først. Mange avvik blir derfor håndtert av rektor nå. Avvikshåndtering følger rutinene i avvikssystemet generelt. Qm+ har melding avvik/ uønskede hendelse hvor brudd på informasjonssikkerhet kan meldes og melding IT - GDPR hvor det foreligger sjekkliste for integritet, konfidensialitet, tilgjengelighet og annet. Viser til 4 avsnitt i 3.3.4.

3.3.4 – ivaretatt av annen tekst

Presiserer at kommunedirektøren har internkontroll som fast spalte i sine informasjonsskriv. Som i form, innhold og volum varierer i forhold til fokusområder.

3.3.6 - ivaretatt av annen tekst

Fra ~~I løpet av~~ 2022 har IT-sikkerhet hatt økt ~~vært~~ prioritet fra myndighetene, forteller ledelsen. Kommunen informerer og har innført opplæring og egne digitale kurs. Det er ikke utarbeidet egne planer for opplæring innenfor informasjonssikkerhet. Kommunedirektøren henviser til opplæring i planen for nytilsatte, men det kan være behov for en plan for alle ansatte, alle har behov for oppdateringer. IT informerer alle om sikkerhetsmessige presiseringer. Dette utføres jevnlig.

3.3.7 - utelatt

Ledelsen forteller at innkjøp av teknisk IKT-utstyr utføres i hovedsak av IKT-rådgiver, men at det skjer noe innkjøp på tjenesteområdene og avdelingene. Når det gjelder anskaffelser av IKT-utstyr og programvare er det innkjøper som er ansvarlig for å kvalitetssikre innkjøpet med IKT-avdelingen, for eksempel ved kjøp av apper. Dette følger av delegert myndighet selv om det ikke er spesifikt nevnt i økonomireglementet (selv om det ikke er spesifisert i gjeldende økonomireglementet, vil dette fremgå av eget anskaffelsesreglement, som har vært under utarbeidelse det siste halvåret og vil bli fremmet politisk når den er endelig klar - se for øvrig gjeldende delegeringsreglement). Controller jobber med anskaffelser sentralt i kommunen. Kommunen har innkjøpsavtale med fylkeskommunen og sektorene har i tillegg egne avtaler.

4.3.1 - utelatt

IKT-rådgiver mener det er enhetenes ansvar at IT-utstyr leveres inn når noen slutter. IKT-avdelingen har ikke mulighet til å følge opp dette, og dette kunne vært tydeliggjort mer. Det står i IT-reglementet at Rennebu kommune sitt datautstyr skal leveres tilbake til nærmeste leder, som igjen skal levere til IKT-avdelingen. ~~Inntil videre er det slik at det er mulig å logge på PC, men ikke på kommunens systemer.~~ Når kommunen tar i bruk det nye systemet for brukerhåndtering, får kommunen bedre styring med rettigheter og kan sperre all pålogging på systemet.

4.4.2 - utelatt

De fleste systemer logger aktivitet~~, men IKT-avdelingen har ikke noe sentralisert system som leser alle loggene~~. Det er forskjellige overvåkingssystemer som IKT-avdelingen ser på daglig, forteller IKT-rådgiver. Det er programmer som overvåker trafikken på nettet og disse programmene logger hendelser. For å undersøke en hendelse må IKT-avdelingen inn på loggen, noe som er komplisert og kan ta lang tid.

4.5.2 – utelatt

IKT-rådgiver forteller at disse testene har vist lav sikkerhetsrisiko og har ikke ført til store endringer i kommunens system. Kommunen har lite tjenester som er eksponert mot internett og derfor er det begrenset hvor mye en test utenfra kan avdekke. ~~Kanskje burde systemet blitt testet fra innsida.~~

4.6.1 - utelatt

Det har vært samtaler om hva som skal gjøres ved eventuelle angrep. IKT-avdelingen har en egen skriftlig beredskapsplan, men overordnet planlegging med ledelsen mangler, forteller IKT-rådgiver. Merknad: kommunedirektøren mener at kriseledelsen ut fra erfaring (pandemien) ved behov, er raskt i stand til å prioritere. Selv om dette vil ta noe tid, vil det være tidsnok for IT når de får prioriteringen. Det er en selvfølge at datasystemer som ivaretar liv og helse vil ha prioritet. Det vil uansett være fornuftig å ha utarbeidet en slik liste i forkant.

4.6.2 - utelatt

Det er ingen sentrale føringer på prioritering av rekkefølge om det oppstår hendelser, forteller IKT-rådgiver. IKT-rådgiver har sin egen beredskapsplan, basert på det IKT-tekniske, men den er ikke forankret politisk. I og med at det mangler en overordnet strategiplan eller beredskaps-plan for IT-sikkerhet, vil det i en krisesituasjon bli mangel på kommunikasjon mellom kommuneorganisasjonen og IKT-avdeling om hva som skal gjøres. IKT-avdelingen vil ha fullt opp med å håndtere hendelsen og vil ikke ha tid til å følge opp brukere og innbyggere, forteller IKT-rådgiveren. Hvis det skjer et dataangrep kan det bli utfordrende ~~vil det blir kaos,~~ sier IKT-rådgiveren. IKT-avdelingen vil måtte håndtere systemene, og det er ingen overordnede planer for hva andre i kommunen må gjøre. Det foreligger beredskapsplan og fagplaner ved uønskede hendelser, som sikrer gjennomføring av den løpende driften. Det er mange systemer som vil rammet ved en hendelse, eksempelvis varme, ventilasjon, signalanlegg ved sykehjem til sentrale fagsystemer. Mange ansatte vil i en slik situasjon ha spørsmål som noen må besvare

og følge opp. Som løses gjennom lederskapet, og at eventuelle situasjoner blir tillagt kriseledelsen.

Revisjon Midt-Norge

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no