Rapport

RAKKESTAD KOMMUNE

08.09.2026

Forvaltningsrevisjon
Informasjonssikkerhet

Innhold

1 SAMMENDRAG

Revisjonens gjennomføring

I denne forvaltningsrevisjonen har vi undersøkt Informasjonssikkerhet i Rakkestad kommune, ved å se om kommune har etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket, og om kommunen har tilfredsstillende organisatoriske, tekniske og menneskelige tiltak for å ivareta informasjonssikkerheten.

Forvaltningsrevisjonen besvarer følgende problemstillinger:

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

Revisjonen har benyttet flere metoder for datainnsamling: dokumentanalyse, intervjuer med ledelse og ansatte, samt en spørreundersøkelse sendt ut til alle ansatte i kommunen. For mer utfyllende informasjon om metode, se rapportens kapittel 3.3.

Revisjonens funn og konklusjoner

Revisjonen finner at Rakkestad kommune i det vesentlige har etablert et styringsgrunnlag for informasjonssikkerhet som svarer på sentrale krav i regelverket. Kommunen har fastsatt sikkerhetsmål, etablert en sikkerhetsstrategi, definert roller og ansvar og innført et dokumentert styringssystem som er integrert i kommunens internkontroll. Kommunen har også etablert rutiner for håndtering og rapportering av sikkerhetshendelser og et omfattende dokumentasjonsgrunnlag for sikkerhetsarbeidet.

Samtidig viser revisjonen at informasjonssikkerhetsarbeidet ikke er tilstrekkelig forankret i hele organisasjonen. En betydelig andel ansatte kjenner ikke til kommunens sikkerhetsmål eller informasjonssikkerhetshåndboken, noe som kan svekke den praktiske etterlevelsen av styringssystemet. Revisjonen vurderer derfor at kommunen har et forbedringsbehov knyttet til implementering og intern forankring av sikkerhetsarbeidet.

Når det gjelder risikostyring, arbeider kommunen systematisk og risikobasert med informasjonssikkerhet. Det gjennomføres risikovurderinger på sentrale områder, og identifiserte risikoer knyttes til eksisterende og planlagte tiltak. Revisjonen vurderer likevel at oppfølgingen av risikoreduserende tiltak ikke er fullt ut etterprøvbar, fordi dokumentasjon av frister, status og gjennomføring ikke alltid fremgår tydelig nok. Kommunen har også et omfattende dokumentasjonsgrunnlag for sikkerhetsarbeidet og gjennomfører egenkontroller og ledelsens gjennomgang, men vi vil likevel påpeke at det ikke foreligger en mer uavhengig internrevisjon eller evaluering av informasjonssikkerhetsarbeidet.

Knyttet til organisatoriske, tekniske og menneskelige tiltak viser revisjonen at kommunen har etablert tilfredsstillende kontroll med IKT-ressurser og tilgangsstyring, dokumenterte løsninger for sikkerhetskopiering og gjenoppretting, samt et strukturert rammeverk for håndtering av sikkerhetshendelser. Kommunen har etablert en dokumentert IKT-arkitektur og rutiner som bidrar til å beskytte informasjon og digitale tjenester.

Kommunen har iverksatt flere opplærings- og bevisstgjøringstiltak, blant annet nyansattopplæring, e-læring, deltakelse i nasjonal sikkerhetsmåned og anskaffelse av nanolæring. Revisjonen vurderer likevel at opplæringen ikke har nådd alle ansatte i tilstrekkelig grad. I spørreundersøkelsen oppgir 1 av 5 i liten eller svært liten grad opplever å ha fått opplæring. Våre undersøkelser avdekker også enkelte risikofylte praksiser og usikkerhet blant ansatte, blant annet knyttet til låsing av PC, lagring av personopplysninger, bruk av privat utstyr og melding av avvik. Dette tilsier at kommunen fortsatt har et forbedringspotensial knyttet til sikkerhetskultur, kompetanse og praktisk etterlevelse.

Revisjonen finner videre at kommunen i begrenset grad har gjennomført systematiske og regelmessige inntrengingstester. Dette reduserer muligheten til å avdekke tekniske sårbarheter og verifisere at etablerte sikkerhetstiltak fungerer etter hensikten

Revisjonens samlede konklusjon er at Rakkestad kommune i hovedsak har etablert et styringssystem for informasjonssikkerhet og et bredt sett av organisatoriske, tekniske og menneskelige tiltak for å ivareta informasjonssikkerheten. De viktigste forbedringsområdene gjelder forankring av sikkerhetsarbeidet blant ansatte, dokumentasjon og oppfølging av risikoreduserende tiltak, uavhengig evaluering av sikkerhetsarbeid, opplæring og bevisstgjøring, og regelmessige gjennomføring av inntrengningstester.

Revisjonens anbefalinger

Basert på våre vurderinger og konklusjoner anbefaler vi at Rakkestad kommune bør:

a) styrke forankringen av informasjonssikkerhetsarbeidet blant ansatte
b) sikre bedre dokumentasjon og oppfølging av risikoreduserende tiltak gjennom tydelig ansvar, frister, status og gjennomføring
c) vurdere tiltak for å styrke den uavhengige evalueringen av informasjonssikkerhetsarbeidet.
d) styrke opplæring, bevisstgjøring og praktisk etterlevelse blant ansatte, ved å sikre regelmessig opplæring økt kjennskap til sikkerhetsrutiner og styrke etterlevelsen av rutiner for melding av informasjonssikkerhetshendelser og avvik
e) gjennomføre regelmessige inntrengingstester

2 MANDAT FOR FORVALTNINGSREVISJONEN

Revisjonen skal i henhold til kommunelovens § 24-2 (1) utføre forvaltningsrevisjon. Etter loven innebærer forvaltningsrevisjon å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Østre Viken kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med god kommunal revisjonsskikk, som vil si å følge *Standard for forvaltningsrevisjon* (RSK 001) (NKRF[1], 2020). Dette innebærer blant annet at rapporten skal skille klart mellom innsamlede data (fakta) og revisjonens vurderinger. Det skal være en tydelig sammenheng mellom problemstillinger, faktaopplysninger[2], vurderinger, konklusjoner og eventuelle anbefalinger. Etter kommuneloven skal revisor rapportere resultatene av sin revisjon til kontrollutvalget.

Forvaltningsrevisjonen er gjennomført på bakgrunn av plan for forvaltningsrevisjon juli 2024 – juli 2028, vedtatt i kommunestyret i Rakkestad kommune i sak 54/2024 (31.10.2024)

Plan for gjennomføring av forvaltningsrevisjonen ble vedtatt i kontrollutvalget 25.11.2025.
Planen ble vedtatt i tråd med revisjonens forslag.

Forvaltningsrevisjonen er gjennomført etter vedtatt prosjektplan i tidsrommet november 2025 – oktober 2026. Vi har gjennomført et oppstartsmøte med kommuneadministrasjonen slik at også administrasjonens innspill er vurdert i planleggingsprosessen.

Vi har kvalitetssikret innsamlet data underveis, både gjennom verifisering av intervjuer og intern kvalitetssikring. I tillegg er faktaopplysningene i sin helhet verifisert av kommunen, slik at eventuelle feil eller misforståelser er rettet opp. Revisjonen avholdt avsluttende møte med administrasjonen 27.08.2026 hvor revisjonens vurderinger, konklusjoner og anbefalinger ble gjennomgått. I etterkant av møtet er rapporten sendt på høring til kommunedirektøren. Kommunedirektørens uttalelse fremgår av vedlegg 7.2.

Forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Inger Marie Baardsen. Casper Støten har deltatt som oppdragsansvarlig revisor. Revisorenes habilitet og uavhengighet er vurdert opp mot kommunen og den undersøkte virksomheten, og revisjonen finner de habile til å utføre forvaltningsrevisjonen.

Revisor vil takke kontaktpersonen og andre som har deltatt for et godt samarbeid i forbindelse med gjennomføringen av forvaltningsrevisjonen.

Østre Viken kommunerevisjon IKS
Rolvsøy, 8. september 2026

Casper Støten
oppdragsansvarlig revisor

Inger Marie Baardsen
utførende forvaltningsrevisor

[1] NKRF er en faglig interesseorganisasjon og et kompetanseorgan for kontroll og revisjon av kommunal/offentlig virksomhet.

[2] Fakta er en gjengivelse av informasjonen vi har fått tilgang til gjennom datainnsamlingen.

3 FREMGANGSMÅTE

3.1 Problemstillinger og avgrensninger

Rapporten besvarer følgende problemstillinger:

Problemstilling 1: Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?
Den første problemstillingen tar utgangspunkt i hva som kreves av styringssystemer for informasjonssikkerhet. Revisjonen har blant annet undersøkt om kommunen har vurdert hvilke trusler som finnes, og hvor sårbar kommunen er, gjennom bruk av risikoanalyser.

Problemstilling 2: Har kommunen tilfredsstillende organisatoriske, tekniske og menneskelige tiltak for å ivareta informasjonssikkerhet?
Denne problemstillingen omhandler de konkrete organisatoriske, tekniske, og menneskelige tiltak som er iverksatt for å ivareta informasjonssikkerheten. Her er NSM sine grunnprinsipper for IKT-sikkerhet en relevant kilde for revisjonskriterier. Noen av prinsippene omhandler å identifisere, kartlegge, beskytte og opprettholde sikkerheten hos kommunen. Med organisatoriske tiltak menes blant annet tydelige roller og ansvar, etablerte rutiner, internkontroll og ledelsesforankring. Tekniske tiltak kan være brannmurer, tilgangsstyring, sikkerhetskopiering, kryptering, overvåking og hendelseshåndtering. Menneskelige tiltak omfatter opplæring, kompetanseplaner, bevisstgjøringskampanjer og rutiner for håndtering av avvik. Revisjonen har vurdert om ansatte har fått nødvendig opplæring, om det finnes planer for kompetanseutvikling, og om det gjennomføres regelmessige bevisstgjøringstiltak. Revisjonen har også undersøkt om tiltakene er kjent og etterleves i praksis.

3.2 Om revisjonskriterier

I henhold til forskrift om kontrollutvalg og revisjon § 15 skal revisor fastsette revisjonskriterier for den enkelte forvaltningsrevisjon. Revisjonskriteriene er den objektive målestokk som setter revisor i stand til å gjøre vurderinger på de fleste områder uten å ha formell fagspesifikk kompetanse. Revisjonskriteriene og revisors kunnskap og erfaring innen forvaltningsrevisjonsmetodikk, gjør at revisor kan gjøre objektive og holdbare vurderinger.

Revisjonskriteriene etablerer den norm som de innsamlede dataene skal vurderes opp mot. I tillegg til dette skal revisjonskriteriene også gjøre det tydelig for den reviderte enhet hva de måles opp mot. Revisjonskriteriene klargjør også overfor folkevalgte, media og andre lesere av forvaltningsrevisjonen, hva revisors vurderinger bygger på. Dette vil gjøre det enklere å etterprøve revisors vurderinger. Revisjonskriteriene skal være relevante, konkrete og i samsvar med de kravene som gjelder for revidert enhet.

Revisjonskriterier fastsettes vanligvis med basis i en eller flere følgende kilder: lovverk, politiske vedtak og føringer, kommunens egne retningslinjer, anerkjent teori på området, eller andre sammenlignbare virksomheters løsninger og resultater.

3.3 Revisjonsmetoder

I henhold til god revisjonsskikk skal praksis eller tilstand innen det reviderte området beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner. I denne forvaltningsrevisjonen har vi benyttet data fra ulike kilder, og brukt ulike metoder for innsamling av data, for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet.

Utfordringer og begrensninger i rapportens faktagrunnlag beskrives nedenfor sammen med beskrivelsen av de ulike metodene som er benyttet. Vi tar også hensyn til metodens begrensninger i vurderingene.

I denne forvaltningsrevisjonen er informasjonen hentet inn gjennom bruk av følgende metoder:

- Dokumentanalyse
- Intervjuer
- Spørreundersøkelse

Dokumentanalyse

Vi har gjennomgått sentrale dokumenter på området. Blant annet er Informasjonssikkerhetshåndboka og risikovurderinger sentrale for revisjonens undersøkelse. I tillegg har revisjonen sett på rutiner, prosedyrer og tiltakskort som omhandler informasjonssikkerhet. Dokumentene er oversendt fra kommunen. Fullstendig oversikt over dokumentene fremgår av kildehenvisningene i kapittel 6.

Intervjuer

Det er totalt gjennomført 8 intervjuer:

- Fagleder dokumentforvaltning
- Systemadministrator på Helse og skole
- To IT-konsulenter
- Enhetsleder IKT
- Informasjons- og digitaliseringsleder
- Leder HR

Revisjonen har fått verifisert syv av åtte intervjuer. Det betyr at den som er intervjuet, har fått lese gjennom referatet for å bekrefte at referatet er i overenstemmelse med det som ble sagt under intervjuet, og rette opp eventuelle misforståelser. Referatet som ikke ble verifisert er ikke brukt videre i revisjonsarbeidet. Revisjonen vurderer allikevel at dataene er troverdige.

Spørreundersøkelse

Det er sendt ut spørreundersøkelse til alle ansatte i Rakkestad kommune. Undersøkelsen er gjennomført ved hjelp av det nettbaserte spørreundersøkelsesverktøyet Questback. Spørreundersøkelse tar for seg ansattes erfaringer og opplevelser knyttet til tematikken.

Spørreundersøkelsen ble sendt ut 19. mars med i overkant av to ukers svarfrist. Av de 1154 ansatte som mottok undersøkelsen var det 244 som svarte. Dette gir en svarprosent på 21. Revisjonen mener at utvalget som har besvart er tilstrekkelig til å bidra til å belyse problemstillingene i rapporten på en hensiktsmessig måte.

Respondentene fordeler seg på alle kommunalområder, med den største andelen respondenter fra Oppvekst og kultur (33 %). Betydelige bidrag kom også fra Helse og mestring (25 %) og Velferd og levekår (19 %), mens Staber og fellesfunksjoner og Areal og infrastruktur stod for ca. (10 %) hver. 3 % av svarene tilhørte kategorien «annet». Dette tyder på en bred representasjon av ansatte på tvers av organisasjonen.

De fleste respondentene hadde høy stillingsprosent. Nesten tre av fire jobbet 80-100 % (75,3 %), mens bare små grupper oppga lavere stillingsbrøk, 7 % i 1-40 % stilling, 6 % i 41–60 % og 11 % i 61 – 80 %

stilling. Nesten alle var fast ansatte (92 %). Kun 6 % oppga å være ansatt i midlertidige stillinger og 2 % i andre kategorier, hvor de har svart lærling og politiker. Ansienniteten blant deltakerne er gjennomgående høy, 69 % har jobbet over 6 år i kommunen, mens 14 % har jobbet 1-3 år, og 11 % 4-6 år. Bare 6 % er nyansatte og har jobbet under 1 år. I spørreundersøkelsen fikk respondentene spørsmål om de hadde lederansvar, og hva de hadde ansvar for, det var mulig å svare på flere alternativer. Av de som har svart på undersøkelsen svarte 31,6 % (77 personer) at de var ledere med ansvar for fag, mens 21,7 % oppga å ha personalansvar. 16 % oppga å ha ansvar for budsjett i egen virksomhet. 65,6 % (160 personer) oppgir å ikke ha noen form for lederansvar.

Samlet sett framstår utvalget som bredt sammensatt på tvers av enheter, men med en klar overvekt av erfarne, fast ansatte medarbeidere i fulle stillinger. Nyansatte og deltids-/midlertidig ansatte er underrepresentert, noe som trekkes inn i vurderingen av datagrunnlagets variasjon og troverdighet. 34,4 % av respondentene er ledere i organisasjonen, noe som innebærer en svak overrepresentasjon av ansatte i lederstillinger.

For å sikre et godt nok svargrunnlag ble det sendt ut e-post vedlagt et skriv med informasjon om undersøkelsen og en tilhørende QR-kode som ansatte kunne skanne for å gjennomføre undersøkelsen på sine mobile enheter/smarttelefoner. Det ble også sendt ut tre påminnelser på undersøkelsen per e-post fra revisjonen. I løpet av undersøkelsen har det også blitt sendt ut en påminnelse fra kommunen for å øke svarprosenten. Revisjonen har vært i kontakt med kontaktpersonen ved flere anledninger knyttet til å øke svarprosenten. I tillegg har svarfristen på spørreundersøkelsen blitt flyttet for å få svarprosenten opp over 20 %.

Vurdering av dataenes troverdighet

Ved dokumentanalyse vil det alltid være en viss grad av subjektive vurderinger. Revisjonen har imidlertid gjennomgått alle mottatte dokumenter på en mest mulig nøytral måte, uten å ekskludere noen. Vi har redegjort for det vi vurderer som mest relevant for rapportens problemstillinger.

Intervjuer gir dybdeinnsikt og nyanser som ofte er vanskelig å fange opp i kvantitative data. Utvalget er lite og strategisk valgt for å representere variasjon i roller og erfaringer, men resultatene kan ikke uten videre generaliseres. Derfor brukes begrepet «overførbarhet» fremfor «generaliserbarhet», altså om funnene kan være relevante i andre sammenhenger med lignende kontekst. For å redusere risikoen for skjevheter har vi kvalitetssikret gjennom flere stadier og hatt dialog med den reviderte enheten. Vi gjennomførte 8 intervjuer, og mot slutten opplevde vi datametning, noe som styrker inntrykket av at vi har fanget opp de mest sentrale perspektivene.

Spørreundersøkelsen gir et kvantitativt supplement som gjør det mulig å generalisere på enkelte områder. Samtidig har den en relativt lav svarprosent. Dette kan innebære systematisk frafall av enkelte grupper ansatte, noe som svekker representativiteten. Revisjonen har vurdert om dette påvirker troverdigheten. Selv om lav svarprosent gir usikkerhet, ser vi ikke klare indikasjoner på at frafallet er skjevt i en retning som endrer hovedbildet. Undersøkelsen gir derfor fortsatt verdifulle indikasjoner, men med forbehold om begrenset generaliserbarhet.

Samlet sett gir kombinasjonen av dokumentanalyse, intervjuer og spørreundersøkelse et bredt og nyansert grunnlag. Metodene har ulike styrker og svakheter, men vurdert opp mot rapportens problemstillinger mener vi at de samlet gir et godt og troverdig bilde.

Bruk av personopplysninger

I forbindelse med denne forvaltningsrevisjonen har vi behandlet personopplysninger som navn og epostadresse til ansatte i kommunen. Vårt rettslige grunnlag for å behandle personopplysninger er kommuneloven § 24-2 fjerde ledd. Lesere av denne rapporten kan ta kontakt med Østre Viken kommunerevisjon dersom de ønsker mer informasjon om hvordan vi behandler personopplysninger.

4 STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET

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

4.1 Revisjonskriterier

Kommunen skal kunne dokumentere en helhetlig og systematisk internkontroll for informasjonssikkerhet som oppfyller kravene i gjeldende lovverk. Flere sentrale kilder stiller krav og forventninger til et slikt styringssystem. Problemstillingen tar utgangspunkt i hva som kreves av et styringssystem for informasjonssikkerhet. Revisjonen har blant annet undersøkt om kommunen har vurdert trusler og sårbarheter gjennom risikoanalyser.

Kommunen skal ha et dokumentert styringssystem for informasjonssikkerhet som er forankret i ledelsen og integrert i kommunens styring. Systemet skal omfatte klare sikkerhetsmål og strategier, være tilpasset kommunens risikoer og sikre etterlevelse av alle relevante lover, herunder kommuneloven, personvernregelverket og eventuelt sikkerhetsloven. Det bør baseres på anerkjente rammeverk som ISO 27001 eller tilsvarende og inkludere mekanismer for kontinuerlig forbedring. Når revisjonen vurderer denne problemstillingen, vil det være sentralt å se etter dokumentasjon som viser at kommunen har fastsatt overordnede målsettinger for informasjonssikkerhet, utarbeidet en strategi basert på risikovurderinger, fordelt ansvar og myndighet tydelig i organisasjonen, etablert rutiner for risikovurderinger og dokumentert sikkerhetsarbeidet og resultatene i nødvendig omfang.

Fullstendig utledning av revisjonskriterier er redegjort for i kapittel 7.1. Nedenfor følger de oppsummerte revisjonskriteriene.

Kommunen skal:

- fastsette overordnede målsettinger for informasjonssikkerhet i kommunen.
- utarbeide en overordnet strategi for å nå målene på området, som er basert på risikovurderinger.
- tydelig fordele ansvar, myndighet og oppgaver for informasjonssikkerhet i organisasjonen
- ha etablert styringssystem for digital sikkerhet og rutiner for rapportering av sikkerhetshendelser til relevante myndigheter
- ha rutiner for risikovurderinger knyttet til informasjonssikkerhet
- dokumentere sikkerhetsarbeidet og resultater fra dette i nødvendig omfang.
- gjennomføre intern revisjon og ledelsens gjennomgang, for å sikre at sikkerhetsarbeidet fungerer over tid.

4.2 Datagrunnlag

4.2.1 Mål, strategi og ansvarsfordeling

Gjennom Informasjonssikkerhetshåndboka har Rakkestad kommune definert mål og en overordnet sikkerhetsstrategi for informasjonssikkerhet. Det overordnede sikkerhetsmålet er at all informasjonsbehandling skal tilfredsstille kravene til konfidensialitet, integritet og tilgjengelighet, samt gjeldende personvernlovgivning. For å oppnå dette vektlegger kommunen blant annet[3]:

- at ledere og ansatte har nødvendig kompetanse i informasjonssikkerhet og personvern, gjennom forankring og opplæringstiltak.
- at sikkerhetshendelser tas tak i, blant annet ved at det responderes for å unngå eskalering.
- å gjennomføre årlige risiko- og sårbarhetsanalyser for å avdekke og redusere sårbarheter
- å behandle avvik og jevnlig vurdere behov for risikoreduserende tiltak.
- å sikre at behandling av personopplysninger skjer i samsvar med lovkrav og at det foreligger gyldig behandlingsgrunnlag, samtykke eller lovhjemmel, før personopplysninger samles inn, brukes, lagres eller slettes.

Kommunen legger vekt på å forebygge uønskede hendelser og begrense konsekvenser, samt å ta lærdom av sikkerhetshendelser for å forbedre rutiner. Informasjonssikkerhetshåndboken presiserer at alle ansatte i kommunen har et felles ansvar for å ivareta informasjonssikkerhet og personvern; «Ansatte har ansvar for å forstå hvordan de kan bidra til å ivareta konfidensialitet, integritet og tilgjengelighet i de dataene de har tilgang til og hvilken risiko som er knyttet til denne tilgangen»[4]. Sikkerhetsarbeidet skal bidra til å opprettholde tillit til kommunen og dens omdømme som et kompetent forvaltningsorgan.

I informasjonssikkerhetshåndboken står en beskrivelse av roller og ansvar innen informasjonssikkerhet. Kommunedirektøren har delegert det daglige operative ansvaret på kommunenivå til stabsleder Informasjon og IKT. Dette ansvaret inkluderer det løpende arbeidet med informasjonssikkerhet og personvern. Enhetsleder IKT innehar rollen som sikkerhetsansvarlig. Håndboken presiserer også at seksjonssjef for hvert enkelt kommunalområde har ansvaret for at prosedyrer og rutiner etterleves.
Noen sentrale roller er[5]:

- Behandlingsansvarlig: Øverste ansvar for at lovverkets krav etterleves, herunder å etablere nødvendige organisatoriske og tekniske tiltak for å sikre kontinuerlig etterlevelse av regelverket. Behandlingsansvarlig står også ansvarlig overfor Datatilsynet, og kan holdes rettslig ansvarlig ved brudd på personvernreglene.
- Sikkerhetsansvarlig (enhetsleder IKT): Hovedansvarlig for kommunens informasjonssikkerhet. Enhetsleder IKT innehar denne rollen og skal bygge en god sikkerhetskultur, ha oversikt over kommunens trusselbilde, og arbeide proaktivt med forbedring av sikkerhetstiltak. Sikkerhetsansvarlig har også primæransvar for å forvalte *informasjonssikkerhetshåndboken* med tilhørende retningslinjer og prosedyrer, samt å gjennomføre egenkontroller og ledelsens gjennomgang av sikkerhetsarbeidet.
- Eier av informasjonssikkerhetshåndboken: Kommunedirektøren er formell eier av håndboken, med delegert signaturrett til stabsleder for informasjon og IKT. Eieren skal sørge for at håndboken alltid er oppdatert og gir føringer for hvordan kommunen skal ivareta informasjonssikkerhet og personvern.

[3] Oversendt dokument: Informasjonssikkerhetshåndboken_Rakkestad_2025

[4] Ibid

[5] Ibid

- Kommunens ledelse: Har ansvar for å holde seg oppdatert på innholdet i sikkerhetshåndboken og det aktuelle trusselbildet, og for å sikre at alle ansatte følger etablerte prosedyrer for informasjonssikkerhet og personvern. Toppledelsen skal også gjennomføre en årlig ledelsesgjennomgang av informasjonssikkerheten og personvernet, for å påse at ansvarsområder ivaretas og at sikkerhetsarbeidet er effektivt.
- Systemeiere (ansvarlige for kommunens IT-systemer): Hver systemeier har ansvar for årlig risikogjennomgang av sin systemportefølje, i samarbeid med sikkerhetsansvarlig. Systemeiere skal også sørge for at det inngås nødvendige databehandleravtaler med eksterne leverandører der dette er aktuelt. Den har også ansvaret for å definere hvilke brukere eller brukergrupper som skal ha tilgang til informasjon i systemet. Systemeier er ansvarlig for å rapportere avvik til Datatilsynet i henhold til retningslinjer.
- Personvernombud: Kommunen har utpekt et eget personvernombud som har en rådgivende og kontrollerende funksjon i saker som gjelder personvern. Personvernombudet skal bistå kommunen i å etterleve personvernregelverket og påse at personopplysninger behandles lovlig.

Gjennom intervjuene får revisjonen bekreftet at mål og strategi er godt forankret på ledelsesnivå. For eksempel uttalte kommunens informasjons- og digitaliseringsleder at han selv deltok i utarbeidelsen av sikkerhetshåndboken og at sikkerhetsmålene og strategien er forankret i ledelsen, med et overordnet mål om å drifte alle systemer i samsvar med lover og regler. I spørreundersøkelsen gjennomført blant ansatte oppgir 56,7 % at de kjenner til kommunens sikkerhetsmål, mens 43,3 % svarer at de ikke gjør det. Dette kan tyde på at ikke alle ansatte er kjent med kommunens overordnede mål for informasjonssikkerhet, til tross for at mål og strategi er definert i styringsdokumentene og formidlet gjennom organisasjonen. På spørsmål om ansatte kjenner til informasjonssikkerhetshåndboken svarer 64,6 % nei, mens 35,4 % ja. I spørreundersøkelsen fikk ansatte en rekke påstander de skulle ta stilling til. En av påstandene var at informasjonssikkerhet først og fremst er IT sitt ansvar, 60 % var helt uenig (24 %) eller uenige (36 %) i påstanden, kun 11 % svarte at de var enige i at dette kun var IT sitt ansvar.

4.2.2 Styringssystem for digital sikkerhet

Kommunen har etablert et styringssystem for informasjonssikkerhet som integreres i kommunens internkontroll og tar utgangspunkt i relevante lover, forskrifter og standarder, som personopplysningsloven, eForvaltningsforskriften og nasjonale anbefalinger fra NSM og DigDir. Kommunen har definert styringssystem som «en strukturert tilnærming for å håndtere sikkerheten til organisasjonens informasjonsverdier og får at kommunens skal oppfylle juridiske, regulatoriske og kontraktsmessige krav»[6]. Informasjonssikkerhetshåndboken presiserer at styringssystem for informasjonssikkerhet og personvern omfatter alle ansatte, samt vikarer og praksiselever, alle lokasjoner hvor kommunen har virksomhet, alle IT-systemer, teknisk og fysisk infrastruktur som eies eller leies av kommunen, og alle informasjonsverdier, også eventuelt manuelle registre. Styringssystemet omfatter ikke interkommunale selskaper eller aksjeselskaper som kommunen er medeier i.

Styringssystemet er bygd på etter standarden ISO 27001[7], og består av en hierarkisk dokumentstruktur med styrende, gjennomførende og kontrollerende dokumenter som til sammen dekker alle sentrale områder i informasjonssikkerhetsarbeidet. De styrende dokumentene omfatter kommunens overordnede retningslinjer og policyer for informasjonssikkerhet, mens gjennomførende dokumenter utgjøres av operative rutiner og prosedyrer, og kontrollerende dokumenter omfatter mekanismer for tilsyn og evaluering

[6] Oversendt dokument: Informasjonssikkerhetshåndboken_Rakkestad_2025

[7] Standard for styringssystem for informasjonssikkerhet ISMS

som ledelsens gjennomgang og egenkontroller. Systemet skal sikre en systematisk og helhetlig forvaltning av informasjonssikkerhet, med en kontinuerlig forbedring og opprettholdelse av et tilfredsstillende sikkerhetsnivå. Rutinen for varsling ved alvorlige hendelser supplerer dette ved å definere hvem som skal varsles og når ved ulike alvorlighetsgrader på hendelser. Rutinene presiserer blant annet at NSM alltid skal varsles ved alvorlige IKT-sikkerhetshendelser, og skisserer hvordan kommuneledelsen og eventuelt politi eller media skal involveres basert på hendelsens varighet og omfang[8].

Rakkestad kommune har utformet en helhetlig portefølje av styringsdokumenter for digital sikkerhet. Blant annet ligger Informasjonssikkerhetshåndbok der som et overordnet rammeverk, og en Overordnet IT-beredskapsplan for håndtering av alvorlige IKT-hendelser. Det er flere spesifikke rutinebeskrivelser, for eksempel for tilgangsstyring, sikkerhetskopiering, overvåking og hendelseshåndtering, samt tiltakskort for ulike krisescenarier som cyberangrep, strømbrudd osv. Alle disse dokumentene er underlagt tydelig versjonskontroll og beskyttelse mot uautoriserte endringer, slik at kun godkjente oppdateringer kan iverksettes. Sikkerhetsansvarlig (Enhetsleder IKT) har ansvar for å holde dokumentene oppdatert og sørge for at de er forankret hos relevante aktører i organisasjonen. Intervjuer revisjonen har gjennomført bekrefter at styringssystemet er godt kjent i ledelsen, men at implementeringen blant alle ansatte fortsatt pågår. Enhetsleder IKT påpeker at styringssystemet er relativt nytt og at det fremdeles arbeides med å gjøre innholdet kjent for alle ansatte. Dokumentene er tilgjengelig i kommunens kvalitetssystem (QM+) og Elements, som primært er kjent for ledere og nøkkelpersoner. Det jobbes med å utarbeide mer brukervennlige versjoner av dokumentene tilpasset øvrige ansatte, for å øke kjennskapen slik at hele organisasjonen blir involvert i sikkerhetsarbeidet. Samtidig viser spørreundersøkelsen blant ansatte at 86 % mener at retningslinjene for informasjonssikkerhet som brukes i det daglige arbeidet, for eksempel regler for passord og utstyr, er tydelige og enkle å forstå, mens 14 % er uenige i dette. Dette kan indikere at de aller fleste ansatte oppfatter kommunens sikkerhetsrutiner som tydelige i praksis.

Kommunen har etablert et system for daglig oppfølging av at sikkerhetskravene etterleves i den løpende driften, som innebærer at de aktivt følger med på systemet hver dag. Oppfølgingen skjer blant annet ved at avvik meldes i kvalitetssystemet dersom rutiner ikke følges, samt gjennom jevnlig internkontroll og rapportering til ledelsen.

4.2.3 Risikovurderinger

Kommunen legger opp til en systematisk tilnærming til risikovurdering som en del av styringssystemet. Et av de overordnede sikkerhetsmålene er at det skal gjennomføres årlige risiko- og sårbarhetsanalyser (ROS-analyser) for å identifisere trusler og sårbarheter, samt oppdatere sikkerhetstiltak der det er nødvendig[9]. Dokumentasjonen kommunen har oversendt viser at kommunen har utarbeidet konkrete risikovurderinger av IKT-sikkerheten, hvor trusler og sårbarheter kartlegges og vurderes i sannsynlighet og konsekvens, med tilhørende eksisterende og planlagte tiltak. Risikovurderingen identifiserer flere hoved risikoområder innen IT, fysiske hendelser som for eksempel innbrudd og tyveri, cybertrusler som hacking og dataangrep, menneskelige eller organisatoriske forhold feil eller ondsinnede handlinger fra ansatte. For hver risiko beskrives et potensielt hendelsesforløp, worst case-scenario og risikonivået vurderes ut fra sannsynlighet og konsekvens. Videre angir dokumentet eksisterende sikkerhetstiltak som er på plass og nye tiltak som foreslås for å forebygge eller redusere konsekvensene dersom en slik

[8] Oversendt dokument: R02-Varsling

[9] Oversendt dokument: Informasjonssikkerhetshåndboken_Rakkestad_2025

hendelse inntreffer[10]. Ansvarlige enheter for tiltak og planlagt oppfølging fremgår også av oversikten, men uten detaljer om frister eller status.

Tilsvarende er det utarbeidet en risikovurdering som spesielt omhandler innføring av flerfaktorautentisering (MFA). Denne analysen belyser trusler ved manglende MFA for ulike brukergrupper som for eksempel elever eller innenfor helse, beregner risiko og foreslår tiltak som sterkere passordrutiner, segmentering av nettverk og opplæringstiltak[11].

Kommunens risikovurderinger benytter risikomatriser og inkluderer tilhørende handlingsplaner der ansvarlige og tidsfrister for tiltak fremgår tydelig, noe som tyder på at risikoarbeidet er strukturert og knyttes opp mot konkrete oppfølgingstiltak. Intervjudata bekrefter dette bildet. En av informantene forteller at håndboken inneholder et eget kapittel om risikovurderinger med definerte terskelverdier og kriterier for sannsynlighet og konsekvens, og at risikovurderinger gjennomføres av systemeierne/fagansvarlige for de respektive fagsystemene. Leder for digitalisering oppgir at de alltid gjennomfører ROS-analyser og en vurdering av personvernkonsekvenser (GDPR kartlegging) på samtlige anskaffelser og nye systemer, men på eldre systemer kan det det vær etterslep. En annen informant opplyste i intervjuet at hun alltid blir involvert ved anskaffelse av nye IKT-løsninger, hvor løsningen gjennomgås med tanke på blant annet personvern (GDPR), bruk av tredjepartsleverandører, sikker arkivering og lignende før løsningen tas i bruk. Dette innebærer at kommunen, selv om det ikke finnes en egen skriftlig prosedyre for sikkerhet i anskaffelser, i praksis sørger for at sikkerhets- og personvernhensyn vurderes ved innføring av nye IT-systemer, inkludert krav om Data Protection Impact Assessments (DPIA), databehandleravtaler og innarbeiding av sikkerhetskrav i kravspesifikasjoner.

4.2.4 Dokumentasjon av sikkerhetsarbeidet og intern revisjon

Kommunen har omfattende dokumentasjon som synliggjør hvordan informasjonssikkerhet ivaretas i praksis. Dokumentasjonen omfatter både overordnede styringsdokumenter, operative rutiner/prosedyrer, beredskapsplaner, sjekklister for rapporter fra analyser. Dette gir revisjonen et bredt innsyn i kommunens sikkerhetsarbeid. For eksempel er det utarbeidet et klassifiseringsregime som gir oversikt over kommunens mest kritiske IKT-systemer og definerer krav til maksimal akseptabel nedetid (gjenopprettingstid) for hver av dem[12]. Kommunen har detaljerte rutiner for håndtering av brukertilganger som beskriver prosessen for opprettelse og avslutning av brukerkontoer og tilganger i et integrert HR- og AD-system, med automatiske daglige synkroniseringer, samt manuelle kontrollrutiner for fjerning av spesialtilganger ved fratredelser[13]. Tilsvarende er det etablert skriftlige rutiner for overvåking av nettverk og systemer, med bruk av dedikerte verktøy for logganalyse og alarmhåndtering[14]. Alle dokumentene skal gjennomgås og vedlikeholdes periodisk, for eksempel skal den overordnede IT-beredskapsplanen gjennomgås og oppdateres minst én gang årlig eller etter større hendelser[15]. Den overordnede IT-beredskapsplanen for Rakkestad kommune beskriver kommunens IKT-sikkerhetsarbeid og internkontroll knyttet til IT-beredskap, med vekt på forebyggende tiltak, organisering av beredskapen og håndtering av alvorlige IT-hendelser. Planen definerer klare roller og ansvar i kriseberedskapen, og stiller krav om jevnlige tester og beredskapsøvelser for å opprettholde et tilfredsstillende beredskapsnivå.

[10] Oversendt dokument: Risikovurdering med handlingsplan, trusler IT

[11] Oversendt dokument: Risikovurdering mfa

[12] Oversendt dokument: G01-Klassifiseringsregime

[13] Oversendt dokument: R22-Brukerhåndtering

[14] Oversendt dokument: R06-Overvåking

[15] Oversendt dokument: Overordnet IT beredskapsplan Rakkestad

Når det gjelder intern revisjon av sikkerhetsarbeidet, skjer dette i stor grad gjennom kommunens internkontrollprosesser. I praksis innebærer dette at sikkerhetsansvarlig utfører egenkontroller som intern oppfølging og årlig forbereder ledelsens gjennomgang hvor toppledelsen evaluerer status for informasjonssikkerhet og personvern[16]. Slik ivaretas en form for intern revisjon gjennom ledelsens systematiske evaluering og sikkerhetsansvarliges løpende kontroller. I løpet av intervjuene fremkommer det at kommunen har kjøpt tjenester av Atea. Ved to anledninger har de gjennomført en modenhetsanalyse. Rapporten fra Atea ble politisk behandlet. Gjennomgang av oversendte dokumenter avdekker imidlertid ingen eksplisitte rutiner på kjøp av uavhengig internrevisjon av informasjonssikkerheten.

Gjennom intervjuene får revisjonen bekreftet at sikkerhetsarbeidet følges opp i linjen. Enhetsleder IKT forteller i sitt intervju at han rapporterer jevnlig til kommunedirektørens ledergruppe om status, avvik og forbedringstiltak innen informasjonssikkerhet.

4.3 Vurderinger

4.3.1 Mål, strategi og ansvarsfordeling

Kommunens mål om å ivareta konfidensialitet, integritet og tilgjengelighet, samt etterlevelse av personvernlovgivningen, dekker sentrale hensyn som må ligge til grunn for et systematisk sikkerhetsarbeid. Revisjonen legger særlig vekt på at målsettingene ikke bare beskriver tekniske forhold, men også omfatter styring, kompetanse, avvikshåndtering og læring etter hendelser. Revisjonen vurderer videre at kriteriet om å utarbeide en overordnet strategi for å nå målene, basert på risikovurderinger, i hovedsak er oppfylt. Vi ser det som positivt at strategien knytter informasjonssikkerhetsarbeidet til risikovurderinger, avvikshåndtering, opplæring og ansvarsplassering, og legger til grunn at en strategi på dette området bør bidra til å omsette overordnede sikkerhetsmål til praktiske prioriteringer og ansvar i organisasjonen. Etter revisjonens vurdering gir kommunens mål og strategi et formelt og risikobasert grunnlag for styring av informasjonssikkerheten. Likevel har den praktiske forankringen i organisasjonen fortsatt har forbedringspotensial, som vi kommer tilbake til i neste avsnitt.

Når det gjelder fordeling av ansvar, myndighet og oppgaver, vurderer revisjonen at kriteriet er oppfylt. Kommunen har definert sentrale roller innen informasjonssikkerhet, herunder behandlingsansvarlig, sikkerhetsansvarlig, personvernombud og systemeiere. Rollefordelingen tydeliggjør overordnet og operativt ansvar, reduserer risikoen for uklar ansvarsplassering og gir et nødvendig grunnlag for internkontroll. Revisjonen vurderer samtidig at kommunen har et forbedringspotensial knyttet til forankringen av mål, strategi og ansvar blant ansatte. Selv om de formelle strukturene er etablert, tilsier datagrunnlaget at kjennskapen til sikkerhetsmålene og informasjonssikkerhetshåndboken ikke er tilstrekkelig utbredt i hele organisasjonen. Vi mener at dette har betydning fordi informasjonssikkerhet i stor grad avhenger av at ansatte kjenner til og etterlever kravene i sitt daglige arbeid. Manglende kjennskap til overordnede mål og styrende dokumenter kan dermed svekke den praktiske gjennomføringen av kommunens strategi, selv om de formelle kriteriene er oppfylt.

Samlet vurderer revisjonen at kommunen har oppfylt de formelle kravene til mål, risikobasert strategi og ansvarsfordeling. Det er likevel et klart forbedringsbehov knyttet til implementering og intern forankring, ettersom en betydelig andel ansatte ikke kjenner til sikkerhetsmålene eller informasjonssikkerhetshånsboken.

[16] Oversendt dokument: Informasjonssikkerhetshåndboken_Rakkestad_2025

4.3.2 Styringssystem for digital sikkerhet

Kommunens styringssystem fremstår som et dokumentert og samlet rammeverk for å planlegge, gjennomføre, kontrollere og forbedre arbeidet med informasjonssikkerhet. Systemet er integrert i kommunens internkontroll og bygget opp med styrende, gjennomførende og kontrollerende dokumenter, noe som gir et strukturert grunnlag for arbeider på tvers av organisatoriske, tekniske og menneskelige forhold. Det er en styrke at styringssystemet bygger på en anerkjent standard og omfatter sentrale elementer som risiko, ansvar, avvik, hendelser og forbedring over tid. Etter revisjonens vurdering viser dette at kommunen i hovedsak har etablert et systematisk grunnlag for å styre informasjonssikkerheten. Revisjonen vurderer også at kriteriet om rutiner for rapportering av sikkerhetshendelser til relevante myndigheter er oppfylt. Kommunens rutiner angir hvordan alvorlige IKT-hendelser skal håndteres og hvem som skal varsles, noe som reduserer risikoen for uklarhet og gir et mer forutsigbart grunnlag for håndtering og rapportering.

Samtidig har kommunen et forbedringspotensial knyttet til implementering og praktisk forankring blant ansatte. Selv om styringssystemet fremstår godt forankret på ledernivå, viser datagrunnlaget at arbeidet med å gjøre innholdet kjent og tilgjengelig for alle ansatte fortsatt pågår. Dette er viktig fordi styringssystemet først får full praktisk virkning når krav, rutiner og ansvar forstås og etterleves i den daglige tjenesteutøvelsen. Det endrer likevel ikke revisjonens vurdering av at styringssystemet som sådan er etablert. Revisjonen legger vekt på at kommunen har et dokumentert og helhetlig rammeverk, at systemet inngår i internkontrollen, og at det finnes rutiner for sentrale deler av sikkerhetsarbeidet. På denne bakgrunn vurderer revisjonen at kommunen oppfyller kriteriet om et etablert styringssystem for digital sikkerhet.

4.3.3 Risikovurderinger

Datagrunnlaget viser at kommunen arbeider risikobasert med informasjonssikkerhet, og at risikovurderinger inngår som en del av styringssystemet. Kommunen identifiserer trusler og sårbarheter, vurderer risiko ut fra sannsynlighet og konsekvens, og kobler risikoene til eksisterende og planlagte tiltak. Etter vår vurdering gir dette kommunen et godt grunnlag for å kartlegge, prioritere og rette innsatsen mot de områdene hvor behovet er størst. Vi legger særlig vekt på at kommunen har utarbeidet risikovurderinger for sentrale deler av IKT-sikkerheten, som viser at kommunen har etablert en struktur for å kartlegge og prioritere risiko på området. Våre funn taler dermed for at kommunen i det vesentlige har en risikobasert tilnærming til informasjonssikkerhet.

Likevel vurderer vi at oppfølgingen av risikoreduserende tiltak ikke er fullt ut etterprøvbar. Selv om risikovurderingene viser ansvarlige enheter og planlagt oppfølging, fremgår det ikke alltid tydelige frister, status eller dokumentasjon på gjennomføringen. Vår vurdering er at dette svekker muligheten for å kontrollere om tiltakene gjennomføres innen rimelig tid, og om risikoen reduseres slik det er forutsatt. Kommunen har derfor et forbedringsbehov knyttet til å dokumentere tiltaksoppfølgingen bedre.

Revisjonen vurderer at kriteriet om rutiner for risikovurderinger er delvis oppfylt. Kommunen har etablert en systematisk praksis for å identifisere og vurdere risikoer, og risikovurderingene knytter identifiserte risikoer til eksisterende og planlagte tiltak. Samtidig viser datagrunnlaget at dokumentasjonen av tiltaksoppfølgingen ikke er konsekvent, særlig når det gjelder frister, status og sporbar oppfølging. Revisjonen anbefaler derfor at oppfølgingen av tiltak dokumenteres med tydelige frister, status og gjennomføring.

4.3.4 Dokumentasjon av sikkerhetsarbeidet og intern revisjon

Etter revisjonens vurdering har kommunen et omfattende dokumentasjonsgrunnlag som viser hvordan informasjonssikkerheten skal ivaretas. Dokumentasjonen omfatter overordnede styringsdokumenter, rutiner, beredskapsplaner, klassifiseringsregime og kontrollerende aktiviteter. Dette er et tilstrekkelig grunnlag for å etterprøve sentrale deler av sikkerhetsarbeidet og se sammenhengen mellom krav, tiltak, ansvar og kontroll. Revisjonen legger vekt på at dokumentasjonen ikke bare beskriver mål og prinsipper, men også omfatter rutiner og kontrollaktiviteter som skal bidra til gjennomføring og oppfølging. Dokumentene gjennomgås og oppdateres, noe som bidrar til at dokumentasjonen kan holdes relevant over tid.

Når det gjelder kriteriet om internrevisjon og ledelsens gjennomgang, vurderer revisjonen at dette er delvis oppfylt. Kommunen gjennomfører egenkontroller og ledelsens gjennomgang, noe som gir mekanismer for intern oppfølging og kan bidra til at svakheter avdekkes og følges opp. Etter revisjonens vurdering ivaretar dette i stor grad formålet med regelmessig intern oppfølging. Revisjonen legger samtidig til grunn at uavhengig internrevisjon ikke nødvendigvis er et eksplisitt lovkrav, men at en mer selvstendig evaluering kan styrke objektiviteten i vurderingen av om sikkerhetsarbeidet fungerer etter hensikten. Kommunen har kjøpt tjenester fra ekstern leverandør, revisjonen har ikke gjennomgått dokumentasjon fra leverandøren, og kan heller ikke se at det er formalisert i rutiner. Siden kommunen i hovedsak baserer seg på egenkontroller og ledelsens gjennomgang, vurderer revisjonen at formålet med intern oppfølging i stor grad ivaretas, men at kriteriet om regelmessig internrevisjon ikke er fullt ut oppfylt.

Samlet vurderer revisjonen at kriteriet om dokumentasjon av sikkerhetsarbeidet er oppfylt. Kriteriet om internrevisjon og ledelsens gjennomgang vurderes som delvis oppfylt, fordi kommunen har etablert egenkontroller og ledelsens gjennomgang, men ikke en mer separat eller uavhengig internrevisjon av informasjonssikkerhetsarbeidet. Etter revisjonens vurdering vil en tydeligere og mer uavhengig evaluering kunne styrke kommunens grunnlag for å vurdere om sikkerhetsarbeidet fungerer etter hensikten over tid.

4.4 Konklusjon og anbefalinger

Rakkestad kommune har i det vesentlige etablert et styringsgrunnlag for informasjonssikkerhet som svarer på sentrale krav i regelverket. Kommunen har fastsatt mål, etablert en sikkerhetsstrategi, fordelt ansvar, etablert et dokumentert styringssystem og utviklet et omfattende dokumentasjonsgrunnlag som gjør det mulig å etterprøve sentrale deler av sikkerhetsarbeidet. Revisjonen har samtidig identifisert enkelte forbedringsområder knyttet til forankring, oppfølging av risikoreduserende tiltak og evaluering av sikkerhetsarbeidet.

Datagrunnlaget viser at kjennskapen til sikkerhetsmål, strategi og styrende dokumenter ikke er tilstrekkelig utbredt blant alle ansatte. Dette kan svekke den praktiske gjennomføringen av sikkerhetsarbeidet, selv om de formelle strukturene er på plass. Revisjonen vurderer også at dokumentasjonen av oppfølgingen av risikoreduserende tiltak kan styrkes. Manglende tydelighet om frister, status og gjennomføring gjør det vanskeligere å etterprøve om identifiserte risikoer håndteres på en systematisk måte. Videre vurderer revisjonen at kommunen ikke fullt ut oppfyller kriteriet om intern revisjon av informasjonssikkerhetsarbeidet. Selv om egenkontroller og ledelsens gjennomgang i stor grad ivaretar formålet med intern oppfølging, mangler kommunen en mer uavhengig evaluering av om sikkerhetsarbeidet fungerer etter hensikten over tid.

Basert på våre vurderinger og konklusjon anbefaler vi at kommunen bør

- styrke forankringen av informasjonssikkerhetsarbeidet blant ansatte
- sikre bedre dokumentasjon og oppfølging av risikoreduserende tiltak gjennom tydelig ansvar, frister, status og gjennomføring
- vurdere tiltak for å styrke den uavhengige evalueringen av informasjonssikkerhetsarbeidet.

5 ORGANISATORISKE, TEKNISKE OG MENNESKELIGE TILTAK

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

5.1 Revisjonskriterier

Problemstillingen[17] omhandler de organisatoriske, tekniske og menneskelige tiltak som er iverksatt for å ivareta informasjonssikkerheten. NSM sine grunnprinsipper for IKT-sikkerhet er en relevant kilde for revisjonskriterier, og disse prinsippene omfatter identifisering, kartlegging, beskyttelse og opprettholdelse av sikkerheten i kommunen.

Organisatoriske tiltak innebærer tydelige roller og ansvar, styringsdokumenter, policyer, beredskapsplaner, etablerte rutiner, internkontroll og ledelsesforankring. Tekniske tiltak omfatter blant annet tilgangsstyring, kryptering, sikkerhetskopiering, brannmurer, overvåking og hendelseshåndtering. Menneskelige tiltak dreier seg om opplæring, kompetanseutvikling, bevisstgjøringskampanjer og rutiner for avvikshåndtering.

Revisjonen har vurdert om ansatte har fått nødvendig opplæring, om det finnes kompetanseplaner, og om det gjennomføres regelmessige bevisstgjøringstiltak. Det er også undersøkt om tiltakene er kjent og etterleves i praksis. Teknologi alene er ikke tilstrekkelig, menneskelige faktorer utgjør ofte den største risikoen, men samtidig den viktigste forsvarslinjen. Kommunen må derfor kunne dokumentere at et bredt sett av tiltak er satt i verk for å oppnå et tilfredsstillende sikkerhetsnivå i tråd med lovkrav og anbefalinger.

Fullstendig utledning av revisjonskriterier er redegjort for i kapittel 7.1. Nedenfor følger de oppsummerte revisjonskriteriene.

Kommunen skal:

- gjennomføre kompetansetiltak som bidrar til at medarbeidere som bruker kommunens informasjonssystemer, har tilstrekkelig kompetanse til å ivareta kommunens sikkerhetsbehov, og til å ivareta gjeldende krav og føringer for informasjonssikkerhet
- ha en oversikt over enheter i IKT-systemet
- ha en oversikt over programvare
- ha et system for styring av tilganger
- ivareta sikkerhet i anskaffelse- og utviklingsprosesser
- etablere og dokumentere en sikker IKT-arkitektur
- ha en plan for sikkerhetskopiering, og ta sikkerhetskopier
- ha et system for å overvåke sikkerheten og analysere data fra overvåkningen
- gjennomføre inntrengingstester
- ha en plan for hendelseshåndtering
- ha en plan for gjenoppretting

[17] Deler av revisjonskriteriene til problemstilling to er basert på Revisjon Midt-Norge sin forvaltningsrevisjon om Beredskap og Informasjonssikkerhet fra 2025

5.2 Datagrunnlag

5.2.1 Opplæring og kompetansetiltak

Rakkestad kommune har iverksatt en rekke opplærings- og kompetansetiltak for å styrke de ansattes evne til å ivareta informasjonssikkerheten. Informasjonssikkerhetshåndboken fastsetter at det skal gjennomføres årlige opplæringstiltak for alle ledere og medarbeidere, herunder e-læringskurs om relevante rutiner og sikker bruk av kommunens systemer[18]. Kommunen markerer den nasjonale sikkerhetsmåneden i oktober med bevisstgjøringstiltak for alle ansatte, ledere og folkevalgte. Nasjonal sikkerhetsmåned er en årlig kampanje i regi av Nasjonal sikkerhetsmyndighet for å styrke kunnskap og bevissthet om digital sikkerhet. I denne perioden gjennomføres det aktiviteter og eventuelt tester eller simuleringer for å måle kunnskapsnivået og identifisere behov for videre opplæring.[19] Videre inneholder håndboken et eget kapittel om kompetanseplaner, som skal sikre at medarbeiderne har tilstrekkelig kompetanse og forståelse til å bidra i det løpende sikkerhetsarbeidet. Tiltakene omfatter blant annet introduksjon for nyansatte, inkludert gjennomgang av informasjonssikkerhetshåndboken, rutiner for logging av aktivitet i informasjonssystemer og taushetserklæringer. Det gis også opplæring i relevante lover og forskrifter, trusler og risikoer, samt håndtering og registrering av avvik og sikkerhetsbrudd. For nye ledere er det etablert egne opplæringstiltak, som blant annet omfatter innføring i brudd på personopplysningssikkerheten, behandling av personopplysninger, lederansvar og krav til sporbarhet. Når det kommer til øvelser, fremgår det av informasjonssikkerhetshåndboken at kommunen skal gjennomføre Phishing-tester minimum en gang i året[20].

Kommunens overordnede IT-beredskapsplan fungerer som et overordnet styrings-, opplærings- og oversiktsdokument. Dokumentet beskriver blant annet ansvarsfordeling, forebyggende tiltak, beredskapsøvelser og krav til regelmessig øvelse av medarbeidere for å opprettholde kompetansenivået[21]. Kommunen har utarbeidet rutiner for læreprosesser etter hendelser for å trekke lærdom av faktiske hendelser. Etter hver alvorlig hendelse gjennomfører IT-avdelingen en evaluering med involverte parter for å identifisere forbedringsområder og dokumenterer erfaringer i en rapport[22].

HR-leder forteller i sitt intervju at kommunen har et strukturert opplæringsprogram for nyansatte som også omfatter IT-sikkerhet. Videre opplyser han at kommunen nylig har anskaffet et opplæringsprogram basert på Nanolearning i datasikkerhet som kan benyttes for både informasjonssikkerhet og personvernformål, for å øke de ansattes kompetanse på en effektiv måte. Han forteller at ved gjennomføring av phishing-tester er det enkelte ansatte som gjentatte ganger ikke består disse testene. I intervju med digitaliseringsleder opplyser vedkommende at kommunen foreløpig ikke har fastsatt et krav om at alle ansatte skal gjennomføre Nanolearning. Han forteller videre at er lagt opp til en tillitsbasert tilnærming i en innledende fase, hvor måloppnåelsen vil bli vurdert etter en periode, før eventuelle krav tydeliggjøres. Det fremgår videre av intervjuet at kommunen deltar i den nasjonale sikkerhetsmåneden hver oktober. Gjennom innsamlet data fremkommer det også at ansatte etterspør ytterligere kompetansetiltak. For eksempel fortalte en av informantene at han ikke kan huske å ha fått noen særskilt opplæring i informasjonssikkerhet de senere årene, utover generelle e-poster, og at han forstår det slik at ledere skal få opplæring først, deretter øvrige ansatte i løpet av våren 2026. En slik plan for opplæring bekreftes av dokumentasjonen, blant annet gjennom sikkerhetsmål om at ledere og ansatte skal ha nødvendig kompetanse, jf. målsettinger i sikkerhetshåndboken.

[18] Oversendt dokument: Informasjonssikkerhetshåndboken_Rakkestad_2025

[19] Ibid

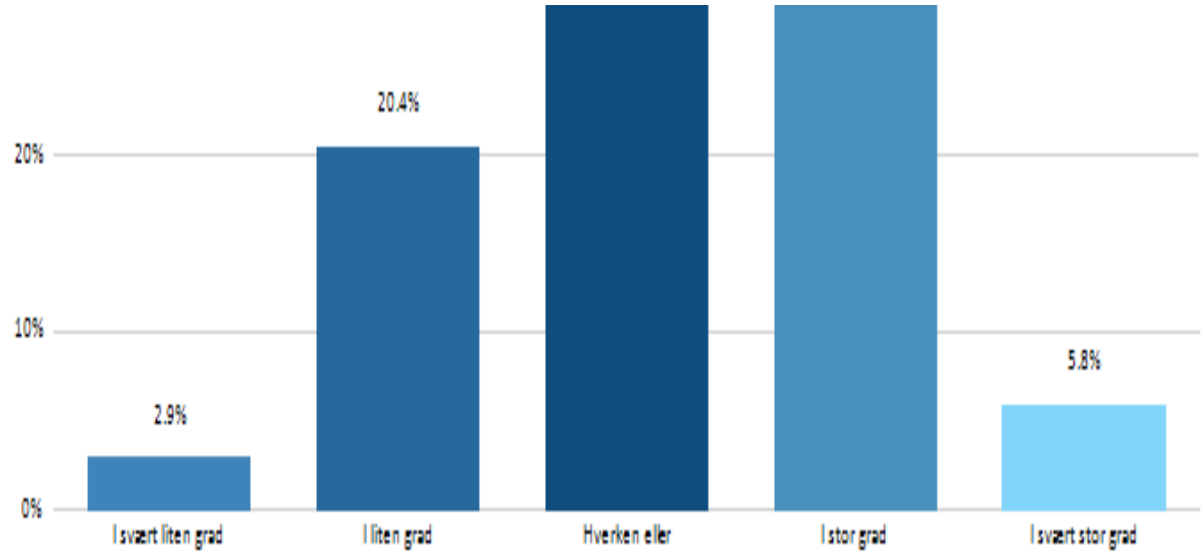
[20] Ibid

[21] Oversendt dokument: Overordnet IT beredskapsplan Rakkestad

[22] Oversendt dokument: R05-Læreprosesser

I spørreundersøkelsen gjennomført blant ansatte kommer det frem at 31,9 % av respondentene har deltatt på kommunens nyansattopplæring, mens 68,1 % ikke har deltatt (N=47[23]). Blant dem som har deltatt, svarer 71,4 % at opplæringen inneholdt tema om informasjonssikkerhet**.** Samtidig oppgir 28,6 % i denne gruppen at informasjonssikkerhet ikke var et tema i opplæringen. Selv om de fleste nyansatte altså fikk sikkerhetsopplæring, tyder dette på at enkelte nytilsatte kan ha deltatt på introduksjonskurs uten at informasjonssikkerhet ble vektlagt. Av 84 ledere som svarte på undersøkelsen, er det 51 som svarer at de ofte eller noen ganger har informasjonssikkerhet som tema i samhandling med sine ansatte. 19 ledere svarer «sjeldent», en svarer at det ikke har blitt prioritert og 10 respondenter svarer at det ikke er deres ansvarsområde.

I spørreundersøkelsen ble ansatte spurt i hvilken grad de har fått tilstrekkelig opplæring i informasjonssikkerhet, slik at de kan utføre jobben på en trygg måte. Der svarte 39 % at de i stor grad eller svært stor grad har fått opplæring. 23 % svarte i svært liten eller i liten grad hadde fått nok opplæring, mens 38 % svarte «hverken eller».



Figur 1 : Tilstrekkelig opplæring i informasjonssikkerhet. N= 240

Spørreundersøkelsen viser gjennomgående at de fleste respondentene oppgir at de i liten grad utfører handlinger som innebærer åpenbare brudd på grunnleggende krav til informasjonssikkerhet. Et klart flertall oppgir blant annet at de ikke deler brukernavn eller passord med kollegaer (90,1 %), at de ikke bruker samme passord på jobb og privat (90,1 %), og at de ikke svarer på e-poster som ber om informasjon uten å kontrollere henvendelsen nærmere (90,5 %). Tilsvarende oppgir 81,8 % at de aldri videresender e-poster med personopplysninger uten først å vurdere om mottaker har behov for opplysningene, og 73,2 % sier at de ikke åpner e-postvedlegg uten å være sikre på hvem avsenderen er.

Samtidig viser undersøkelsen at det fortsatt finnes flere risikoområder. Ett av de tydeligste funnene er at 20,6 % oppgir at de lar PC-en stå ulåst når de forlater kontoret i korte perioder. Videre oppgir 16,3 % at de har lagret dokumenter med personopplysninger lokalt på PC-en, og 10,5 % at de noen ganger arbeider med kommunale dokumenter på privat PC eller mobil. Selv om flertallet svarer at de ikke gjør dette, viser resultatene at det finnes en ikke ubetydelig andel ansatte som oppgir praksis som kan være

[23] Ansatte som har vært ansatt i under ett år, eller mellom 1-3 år har svart på dette spørsmålet.

i strid med krav til sikker behandling av informasjon. Undersøkelsen viser også enkelte tegn til usikkerhet og varierende forståelse av hva som kreves i konkrete arbeidssituasjoner. For eksempel svarer 11,7 % at de noen ganger klikker på lenker i e-post uten å kontrollere avsender nøye, mens 12,5 % oppgir at de har skrevet ned passordet sitt på papir eller lagret det lett tilgjengelig. I tillegg er det 21,5 % som svarer «hverken eller» på spørsmålet om de er usikre på hvordan de melder avvik knyttet til informasjonssikkerhet, og ytterligere 19,1 % som sier seg enige i at de er usikre. På enkelte områder fremstår svarene som mer positive, men også her er det grunn til nyansering. For eksempel oppgir 59,1 % at de aldri bruker åpne eller usikrede trådløse nettverk når de jobber. Samtidig innebærer dette at rundt fire av ti enten er uenige, nøytrale eller ikke tydelig bekrefter sikker praksis. Det samme mønsteret finnes i spørsmål om fysisk skjerming ved hjemmearbeid og låsing av PC. Selv om flertallet svarer i tråd med ønsket praksis, viser svarfordelingen at det fortsatt er en gruppe ansatte som enten har en risikofylt praksis eller som ikke fremstår som tilstrekkelig sikre på hva som forventes.

Til slutt i spørreundersøkelsen fikk ansatte muligheten til å legge inn egne kommentarer om temaet. Kommentarene fra respondentene tegner et relativt tydelig bilde av hvordan personvern og informasjonssikkerhet oppleves i praksis. Det mest gjennomgående inntrykket er at informasjonssikkerhet oppleves som et område med for lite systematisk opplæring og oppfølging, og at dette påvirker etterlevelsen i organisasjonen. Flere kommentarer peker på manglende eller utilstrekkelig opplæring både ved nyansettelser og i form av løpende oppdateringer. Det fremheves særlig behov for kortere, hyppigere og mer praktisk rettet opplæringstiltak, fremfor omfattende og lite tilgjengelige styringsdokumenter. Et annet tydelig funn er at ansvaret for informasjonsarbeidet i stor grad oppleves å være delegert til ledere uten tilstrekkelig støtte. Enkelte beskriver at enhetslederne allerede har et stort personalansvar og begrensede forutsetninger for å sikre god oppfølging av alle ansatte, særlig i tjenester med mange deltidsansatte og vikarer. Flere kommentarer knytter også dette til manglende tilrettelegging fra organisasjonen sentralt, blant annet i form av lite brukervennlige systemer og utdaterte dokumenter. Videre går det igjen i kommentarene at eksisterende styringsdokumenter i liten grad oppleves som relevante eller tilgjengelige i praksis. Samtidig uttrykkes det at mengden dokumentasjon kan gjøre det vanskelig å orientere seg. Dette understøtter et gjennomgående ønske om enklere og mer konkrete tiltak, som korte kurs, faste påminnelser og visuelle hjelpemidler, for eksempel plakater med sentrale sikkerhetsregler. Kommentarene peker også på manglende bevissthet og kompetanse i deler av organisasjonen, særlig knyttet til håndtering av taushetsbelagte opplysninger og bruk av riktige løsninger. Det trekkes frem eksempler på at sensitiv informasjon deles mellom kollegaer, og at enkelte ansatte har begrenset kunnskap om anonymisering og taushetsplikt. Flere respondenter etterlyser også tydeligere kommunikasjon og bedre informasjon om hva som forventes av den enkelte ansatte, herunder hva som er tillatt praksis og hvordan avvik skal håndteres.

5.2.2 Oversikt over kommunens IKT-systemer, programvare og tilgangsstyring

Rakkestad kommune har som nevnt tidligere etablert dokumentasjon som gir oversikt over kritiske IKT-systemer og en rutine for å holde oversikten oppdatert. Klassifiseringsregimet inneholder en tabellarisk oversikt over de viktigste programmene/systemene, med angivelse av hvor raskt hver av dem må være operasjonelle igjen ved avbrudd, det vil si krav til akseptabel nedetid. Oversikten oppdateres fortløpende etter hvert som kommunens enheter gjennomfører ROS-analyser av sine fagsystemer. Dette er et ledd i å kartlegge kritiske systemer og deres betydning for tjenestene[24]. Gjennom dokumentene fremkommer

[24] Oversendt dokument: G01-Klassifiseringsregime

det en egen liste over alle IKT-enheter og programvarer i kommunen, det er en fullstendig, kontinuerlig oppdatert aktiva-oversikt over alle IKT-komponenter. Listen administreres i KS DigiOrden[25].

Når det gjelder tilgangsstyring viser dokumentene at kommunen har rutiner for å opprette og deaktivere brukere og tilganger. Rutinen for brukerhåndtering beskriver hvordan nye brukerkontoer etableres og avsluttes i et integrert system med HRM. Når en ny ansatt registreres i personalsystemet (Visma HRM), synkroniseres dette automatisk med kommunens AD-system daglig, slik at brukerkontoer opprettes i god tid før ansettelsesstart. Tilsvarende blir brukere deaktivert automatisk ved sluttdato registrert i HR-systemet, selv om selve slettingen først utføres manuelt et par ganger i året for å bevare mulighet til reaktivering ved nyansettelse[26]. Rakkestad kommune har et overvåkingssystem (Checkmk). Alle på IT skal sjekke denne om morgenen, og ved telefoner som kan tyde på problemer ved en av deres servere. Ved røde varsler i overvåkingen skal disse vurderes og eventuelt håndteres. Ifølge rutinen kan det settes opp SMS-varsling fra systemet ved hendelser. På revisjonstidspunktet er det ikke gjort, da kommunen ikke har IT-vakt[27]. I verifiseringen av faktautkastet får revisjonen opplyst at det er satt opp i løpet av våren. Kommunen har hatt en IT-vakt siden julen 2025.

Informasjon fra intervjuene tilsier at tilganger styres strengt. Kun et begrenset antall personer har myndighet til å tildele nye brukertilganger, og i enkelte systemer må ansatte fullføre opplæring før de får tilgang, eksempelvis er tilganger i sak- og arkivsystemet Elements betinget av at man gjennomfører kurs, ifølge intervjuet med fagleder for dokumentforvalting. I intervjuet får revisjonen høre at kommunen har et omfattende system for loggkontroll, fagleder for dokumentforvaltning forteller at kommunen har god oversikt over loggdata og gjennomfører jevnlig utvidede loggkontroller som en del av virksomhetens internkontroll, uten at det er avdekket uautoriserte tilganger så langt. Flere av informantene forteller at tilgangsstyringen hovedsakelig baserer seg på HR-systemet. Hvilke tilganger man har, utgår fra hvilken stilling man har. Alle andre tilganger man skal ha som går utover rollen, må meldes inn til IT-avdelingen. Informantene fra IT-avdelingen har beskrevet kommunens overvåkningsløsninger, som kan konfigureres til å sende alarmer ved uregelmessigheter, og at systemforvaltere mottar varsel ved endringer i rolletilganger og gjør nødvendige justeringer fortløpende. Når det kommer til andre fagsystemer som for eksempel Gerica, kan det være veldig sårbart med få personer som kan gi tilganger. I tillegg er det mange forskjellige typer roller som gir forskjellige tilganger i systemet.

I spørreundersøkelsen revisjonen sendte ut spurte vi om ansatte har tilgang til informasjon de sjeldent eller aldri har bruk for. 15 % var enig eller helt enig i den påstanden, mens 70 % var helt uenig eller uenig i at de hadde tilgang til informasjon de ikke hadde behov for.

5.2.3 Sikkerhetskopiering, IKT- arkitektur, overvåking og anskaffelser

Rakkestad kommune har rutine for sikkerhetskopiering av data. I «Rutine 04 – Backup» fremgår det at det tas daglig sikkerhetskopi av alle servere hver kveld, og at det kopieres en ekstra backup til en server på en annen lokasjon. Denne eksterne kopien er utformet slik at den ikke kan endres på 10 dager, for å forhindre manipulasjon eller sletting av backupen ved et angrep. I tillegg praktiseres månedlig offline-backup som lagres utenfor kommunens ordinære driftsmiljø. IT-avdelingen mottar daglig e-post med logg fra backup-kjøring og skal kontrollere at backupen har blitt utført som planlagt. Ved hver planlagt månedlig driftsstans gjennomføres test av gjenoppretting av utvalgte data for å verifisere at backupene

[25] Oversendt dokument: Applikasjoner

[26] Oversendt dokument: R22-Brukerhåndtering

[27] Oversendt dokument: R06-Overvåking

faktisk fungerer[28]. Dette sikrer at man til enhver tid har fungerende sikkerhetskopier som kan tas i bruk dersom en hendelse inntreffer. I Informasjonssikkerhetshåndboken er det beskrevet retningslinjer for sikkerhetskopiering og gjenoppretting. Retningslinjene definerer krav for informasjon og data fra kommunens informasjonssystemer, og skal sikre forsvarlig gjennomføring av sikkerhetskopiering og gjenopprettingen. Målsettingen er å sikre tjenlighet og tjenestekontinuitet ved å kunne gjenopprette systemer og data, og redusere risiko for tap av informasjon. Kommunen skal ta sikkerhetskopi av alle systemer, både lokalt og i sky, og sikre at også databehandlere oppfyller kravene gjennom avtaler. Sikkerhetskopier skal beskyttes og lagres med offline/offsite-løsninger. Omfang og hyppighet av backup skal baseres på systemenes kritikalitet, herunder krav til gjenopprettingstid og akseptabel datatapstid. Videre skal det finnes dokumenterte prosedyrer både for sikkerhetskopiering og gjenoppretting, som beskriver hvilke systemer som omfattes og hvordan arbeidet gjennomføres. Gjenoppretting skal testes jevnlig, minimum årlig, og prosedyrene skal angi prioritering av systemer ved gjenoppretting[29].

Når det gjelder IKT-arkitektur og tekniske sikringstiltak, har Rakkestad kommune innarbeidet en rekke retningslinjer i informasjonssikkerhetshåndboken. Dette inkluderer blant annet retningslinje for nettverkssikkerhet, kryptografi og informasjonsoverføring, samt retningslinje for fysisk sikkerhet for å beskytte infrastruktur og utstyr. Retningslinjene utgjør et samlet rammeverk for hvordan kommunen skal sikre informasjon gjennom tekniske, organisatoriske og fysiske tiltak. Retningslinje for nettverkssikkerhet har som formål å beskytte informasjon som flyter i kommunens nettverk ved å redusere risikoen for sikkerhetsbrudd på nettverksnivå. Denne gjelder for alle lokale nettverk og nettverkskomponenter og stiller krav til dokumentasjon av nettverksutstyr, kryptering av nettverkstrafikk, sikker konfigurasjon av nettverksenheter, løpende oppdatering og overvåking, samt segmentering av nettverket i adskilte soner som klienter, servere, backup og gjestenett. All tilgang og trafikk skal begrenses, logges og overvåkes, og trafikk mot internett skal filtreres for å hindre skadevare og uautorisert tilgang. Sikkerhetsansvarlig har overordnet ansvar for retningslinjen. Retningslinje for kryptografi skal sikre at informasjon i kommunens produksjonssystemer oppnår tilstrekkelig konfidensialitet, integritet og autentisitet. Retningslinjen gjelder for alle produksjonssystemer og fastsetter at informasjon som lagres eller overføres skal krypteres. Det stilles krav til etablering av prosedyrer for håndtering av kryptografiske kontroller, inkludert sertifikater og kryptonøkler. Brukerutstyr skal ha kryptert lagring, og informasjon som overføres internt og eksternt skal sikres gjennom sertifikater, krypterte protokoller, VPN-løsninger og kryptert e-post. Passord skal lagres som sikre hasher[30] i tråd med beste praksis. Sikkerhetsansvarlig er ansvarlig for innholdet, og alle som anskaffer, forvalter eller drifter systemer og nettverk plikter å følge retningslinjen. Retningslinje for informasjonsoverføring regulerer hvordan informasjon skal overføres internt i kommunen og mellom kommunen og eksterne parter. Formålet er å beskytte personopplysninger og annen informasjon under overføring, og retningslinjen gjelder for alle systemer og prosesser som omfattes av styringssystemet for informasjonssikkerhet. All ekstern informasjonsoverføring skal alltid være kryptert, og interne dataforbindelser skal krypteres der det er mulig. Eksponerte tjenester skal benytte sertifikater, e-post skal sikres med etablerte mekanismer, og gamle eller usikre autentiseringsprotokoller skal ikke benyttes. Retningslinjen stiller også krav til forsiktighet ved verbal informasjonsutveksling og til bruk av databehandleravtaler og taushetsavtaler der dette er nødvendig. Sikkerhetsansvarlig, systemeiere, enhetsleder IKT og alle ansatte har ansvar for etterlevelse innenfor sine roller[31].

Retningslinje for fysisk sikkerhet fastsetter krav til hvordan informasjonssikkerheten skal ivaretas i kommunale bygg og lokaler. Den gjelder for all informasjonsbehandling i kommunens lokaler og har som

[28] Oversendt dokument: R04-Backup

[29] Oversendt dokument: Informasjonssikkerhetshåndboken_Rakkestad_2025

[30] passord ikke lagres i lesbar form, men omgjøres til en kryptert verdi (en hash) ved hjelp av en matematisk funksjon.

[31] Oversendt dokument: Informasjonssikkerhetshåndboken_Rakkestad_2025

mål å forhindre uautorisert adgang, skade og forstyrrelser av lokaler, IT-systemer og informasjon. Bygg og lokaler skal deles inn i soner basert på informasjonens klassifiseringsnivå, med tilpassede sikkerhetstiltak som adgangskontroll, logging, alarmer og fysiske barrierer. Sikre områder skal beskyttes mot både uautorisert tilgang og ytre miljøtrusler som brann og oversvømmelse. Retningslinjen stiller også krav til ryddig arbeidsplass, låsing av IT-utstyr ved fravær og forsvarlig bruk av kameraovervåking i tråd med personvernregelverket. Sikkerhetsansvarlig har ansvar for innholdet i retningslinjen, mens systemeiere, byggansvarlige og alle ansatte har ansvar for å følge kravene i praksis[32]. Kommunens informasjonssikkerhetssystem er for øvrig basert på anerkjente standarder (ISO 27001), integrert i kommunens internkontroll, og fokuserer på å forebygge uønskede hendelser gjennom dokumenterte rutiner og løpende forbedringer.

Når det gjelder sikkerhet i anskaffelses- og utviklingsprosesser, er dette omtalt i et eget kapittel i sikkerhetshåndboken. Retningslinjen for anskaffelse og forvaltning av programvarelisenser fastsetter rammer for kommunens bruk av lisensiert programvare, slik at bruken skjer lovlig og i samsvar med kontraktsmessige krav. Den gjelder for all anskaffelse og bruk av lisensiert programvare i kommunen, med mål om å sikre etterlevelse av relevante lover og lisensvilkår. For anskaffelse av programvarelisenser kreves det at behovet er reelt og at en budsjettansvarlig leder har godkjent kjøpet på forhånd, rollen som systemeier skal være avklart, og Enhetsleder IKT skal rådføres for å unngå unødvendige innkjøp av programvare kommunen allerede har. Det er videre forbudt å laste ned gratis programvare fra internett uten avklaring, og kun ansatte med behov i jobben skal få tilgang til lisensiert programvare. Alle anskaffede lisenser skal registreres i kommunens lisensoversikt og rapporteres til Enhetsleder IKT, samt skal lisensavtalene arkiveres i kommunens arkivsystem. For forvaltning av programvarelisenser skal kommunen til enhver tid ha full oversikt over alle lisensierte programmer og sørge for at bruken skjer i henhold til lisensavtalene. Alle nye lisensanskaffelser skal rapporteres til Enhetsleder IKT da det er ikke er tillatt å bruke, dele eller kopiere programvare i strid med lisensbetingelsene[33].

5.2.4 Inntrengingstester, hendelseshåndtering og gjenoppretting

Gjennom dokumentgjennomgangen og intervjuene fremkommer det at Rakkestad kommune ikke har dokumenterte phishing-tester på revisjonstidspunktet. I verifiseringen av faktautkastet får revisjonen opplyst at en phishing-test ble gjennomført juni 2026. Resultatene viste at kun 2 av 1000 mottakere feilet testen. Revisjonskriteriet om regelmessig gjennomføring av slike tester belyses ikke i det fremlagte datagrunnlaget. Det fremkommer videre gjennom intervjuer at kommunen samarbeider med KommuneCert/HelseCert, som gjennomfører regelmessige inntrengingstester i form av portskanninger. Disse testene har til hensikt å avdekke åpne porter og andre svakheter som kan unyttes av uvedkommende. Det er imidlertid ikke dokumentert at kommunen har gjennomført penetrasjonstesting. Innhold i informasjonssikkerhetshåndboken og informasjon fra våre informanter tyder på at arbeidet med å starte opp slike tester er høyt prioritert. I intervjuet med en ansatt ved IT-avdelingen får vi opplyst at kommunen har påbegynt arbeidet med å sende ut enkle phishing-tester, men at brannmurene til kommunen er så sterke at det blir stoppet før det når ut til ansatte. Kommuneledelsen har imidlertid gjennomført beredskapsøvelser som en del av oppfølgingen av IT-beredskapsplanen. Rutine for testing og øving beskriver at IKT-beredskapsplanen og tilhørende rutiner jevnlig skal testes for å opprettholde et tilfredsstillende beredskapsnivå, og involvere nødvendige underleverandører der det er relevant[34].

[32] Oversendt dokument: Informasjonssikkerhetshåndboken_Rakkestad_2025

[33] Ibid

[34] Oversendt dokument: R03-Testing og øving

Kommunen har utarbeidet et relativt omfattende system for håndtering av sikkerhetshendelser som beskriver hvordan alvorlige IKT-hendelser skal håndteres ved å følge en systematisk prosess i faser, i tråd med Nasjonal sikkerhetsmyndighets (NSM) anbefalte modell. Prosessen inkluderer forberedelse, deteksjon og analyse, isolering/begrensning, fjerning av trussel, gjenoppretting og læring i etterkant[35]. Kommunen har fokus på dokumentasjon av hendelsesforløp, og rutinen for hendelsesregistrering beskriver hvordan en logg skal føres under en alvorlig hendelse, der alle tiltak, tidspunkter og tekniske detaljer registreres fortløpende av det involverte personellet. Loggen føres typisk i en dedikert Teams-kanal eller et felles dokument, og sikrer at viktig informasjon ikke går tapt under krisehåndteringen[36].

Når det kommer til gjenoppretting, har kommunen på plass planer for å kunne gjenopprette data og tjenester etter alvorlige hendelser. Som nevnt tidligere i rapporten tas det regelmessige backups med test av gjenoppretting, hvilket er en forutsetning for rask restitusjon. I scenario-dokumenter og tiltakskort vises det til at kommunen er forberedt på å benytte alternative løsninger ved katastrofale hendelser; i tiltakskort «serverrom utilgjengelig» beskrives det at hvis kommunens primære serverrom blir satt ut av drift, vil man måtte overføre data til sky-løsninger eller anskaffe nytt utstyr i samarbeid med eksterne leverandører. Her er forventet nedetid beregnet til noen dager før normal drift kan gjenopprettes[37].

Gjennom våre informanter får revisjonen bekreftet at hendelseshåndteringen er etablert i praksis. Fagleder for dokumentforvaltning opplyser at hendelseshåndtering er godt beskrevet i beredskapsplanen for IT, og at kvalitetssystemet Qm+ angir tydelig hva man skal gjøre og vurdere ved hendelser. Det fremgår også at kommunen har kjørt interne øvelser relatert til informasjonssikkerhet, som for eksempel simulerte phishing-eposter, selv om slike øvelser ligger flere år tilbake i tid. 11 % av respondentene bekrefter at de har opplevd en informasjonssikkerhetshendelse uten å melde fra i avvikssystemet. 64 % av respondentene føler seg trygge på hva de skal gjøre hvis de mistenker et sikkerhetsbrudd.

5.3 Vurderinger

5.3.1 Opplæring og kompetansetiltak

Kommunen har etablert flere kompetanse- og opplæringstiltak som samlet bidrar til å styrke de ansattes kompetanse innen informasjonssikkerhet. Dette omfatter blant annet opplæring gjennom e-læringskurs, bevisstgjøringstiltak og introduksjon av informasjonssikkerhet i nyansattopplæringen. Revisjonen vurderer det også som positivt at kommunen har tatt i bruk nye opplæringsformer gjennom anskaffelsen av et nanolæringsprogram, som kan bidra til mer kontinuerlig og tilgjengelig opplæring på et område hvor trusselbildet er i stadig endring. Tiltakene viser at kommunen anerkjenner betydningen av menneskelige faktorer i sikkerhetsarbeidet og har etablert strukturer som kan styrke sikkerhetskulturen over tid.

Samtidig viser datagrunnlaget at opplæringstiltakene ikke har nådd alle ansatte i tilstrekkelig grad. Både intervjudata og resultater fra spørreundersøkelsen indikerer at flere ansatte opplever å ha fått begrenset opplæring eller etterlyser mer kompetanseheving på området. Dette er vesentlig fordi informasjonssikkerhet forutsetter at ansatte har nødvendig kunnskap til å identifisere risikoer og handle riktig i konkrete situasjoner. Manglende opplæring i deler av organisasjonen kan derfor svekke effekten av de etablerte tiltakene.

[35] Oversendt dokument: R01-Hendelseshåndtering

[36] Oversendt dokument: R10-Hendelsesregistrering

[37] Oversendt dokument: t06it-utigjengelig_serverrom

På denne bakgrunn vurderer revisjonen at kriteriet om kompetanse- og opplæringstiltak er delvis oppfylt. Kommunen bør arbeide videre med å sikre at opplæringen når alle ansatte i tilstrekkelig omfang og med nødvendig regelmessighet.

5.3.2 Oversikt over kommunens IKT-systemer, programvare og tilgangsstyring

Revisjonen legger til grunn at oversikt over digitale ressurser er en grunnleggende forutsetning for å kunne identifisere sårbarheter, prioritere sikkerhetstiltak og opprettholde kontroll over IKT-porteføljen. Datagrunnlaget viser at kommunen har etablert systemer og rutiner som gir en oppdatert oversikt over IKT-miljøet. Oversikten holdes løpende oppdatert gjennom risikovurderinger og forvaltning av systemporteføljen, noe som bidrar til å redusere risikoen for at systemer eller programvare faller utenfor kommunens sikkerhetsstyring. På denne bakgrunnen vurderes kriteriet om oversikt over IKT-systemer og programvare som oppfylt.

Når det gjelder tilgangsstyring, vurderer revisjonen at kommunen har etablert tilfredsstillende mekanismer for tildeling og avvikling av tilganger. Tilgangsstyringen fremstår systematisk og er integrert i kommunens administrative prosesser. Kommunens praksis er i tråd med sentrale prinsipper for identitets- og tilgangsstyring, der tilgang gis ut fra tjenstlig behov og begrenses til det som er nødvendige. Dette bidrar til å redusere risikoen for uautorisert tilgang til informasjon og systemer.

Samlet vurderer revisjonen at kommunen har etablert tilfredsstillende kontroll med IKT-ressurser og tilgangsstyring. Kriteriene knyttet til oversikt over IKT-systemer, programvare og styring av tilganger vurderes som oppfylt.

5.3.3 Sikkerhetskopiering, IKT-arkitektur, overvåking og anskaffelser

Datagrunnlaget viser at kommunen har etablert flere sentrale tiltak for å beskytte og opprettholde informasjonssikkerheten. Revisjonen legger særlig vekt på arbeidet med sikkerhetskopiering, IKT-arkitektur, overvåking og sikkerhet i anskaffelser. Samlet sett vurderes tiltakene som tilfredsstillende, selv om enkelte områder fortsatt har forbedringspotensial.

Når det gjelder sikkerhetskopiering, vurderer revisjonen at kommunen har etablert løsninger som i stor grad reduserer risikoen for tap av data og langvarige driftsavbrudd. Det legges særlig vekt på at sikkerhetskopieringen omfatter både lagring av data og testing av gjenoppretting, noe som gir et reelt beredskapsgrunnlag ved alvorlige hendelser. Kriteriet om sikkerhetskopiering og gjenoppretting vurderes derfor som oppfylt.

Revisjonen vurderer videre at kommunen i det vesentlige oppfyller kriteriet om en sikker og dokumentert IKT-arkitektur. Kommunen har etablert styrende prinsipper og sikkerhetstiltak som gir et tilfredsstillende grunnlag for å beskytte informasjon mot interne og eksterne trusler.

Når det gjelder overvåking, vurderer revisjonen at kommunen har etablert mekanismer for å oppdage avvik og sikkerhetshendelser. Datagrunnlaget viser blant annet at kommunen har iverksatt tiltak som IT-vakt og varslingsløsninger, og at overvåkingen samlet sett gir et tilfredsstillende grunnlag for å identifisere og håndtere sikkerhetsrelaterte hendelser. Kriteriet om overvåking vurderes som oppfylt.

For anskaffelses- og utviklingsprosesser vurderer revisjonen at kommunen i praksis ivaretar sikkerhets- og personvernhensyn på en tilfredsstillende måte. Sikkerhetsvurderinger inngår som den del av kommunens praksis, og revisjonen vurderer at dette gir et tilfredsstillende grunnlag for å ivareta informasjonssikkerhet ved anskaffelse og utvikling av nye løsninger.

Samlet vurderer revisjonen at kriteriet knyttet til sikkerhetskopiering, IKT-arkitektur, overvåkning og sikkerhet i anskaffelser er oppfylt. Kommunen har etablert tiltak og rutiner som samlet fir et tilfredsstillende grunnlag for å beskytte informasjon og opprettholde sikker drift av IKT-systemene.

5.3.4 Inntrengingstester, hendelseshåndtering og gjenoppretting

Etter revisjonens vurdering er regelmessig testing av teknisk sårbarhet et viktig virkemiddel for å identifisere svakheter før de kan utnyttes av uvedkommende. Datagrunnlaget viser at kommunen har etablert enkelte tiltak for å avdekke og håndtere sårbarheter, blant annet gjennom samarbeid med KommuneCert/HelseCert, som gjennomfører regelmessige portskanninger og kontroller av eksponerte tjenester. Samtidig viser datagrunnlaget at kommunen i begrenset grad har dokumentert gjennomføring av mer omfattende sikkerhetstesting, som penetrasjonsteser eller tilsvarende tester av interne systemer. Manglende dokumentasjon på et bredere spekter av sikkerhetstester reduserer kommunens mulighet for å bekrefte at etablerte sikkerhetstiltak fungerer som forutsatt.

Når det gjelder hendelseshåndtering, vurderer revisjonen at kommunen har etablert et strukturert rammeverk for å håndtere sikkerhetshendelser. Revisjonen legger vekt på at det foreligger rutiner for varsling, håndtering, dokumentasjon og læring etter hendelser, noe som gir et godt grunnlag for systematisk oppfølging og forbedring. Kriteriet om hendelseshåndtering vurderes derfor som oppfylt. Revisjonen vurderer samtidig at det finnes et forbedringspotensial knyttet til etterlevelsen av rutinene. Datagrunnlaget viser at ikke alle ansatte melder sikkerhetshendelser gjennom avvikssystemet. Dette kan svekke kommunens evne til å fange opp og analysere hendelser på en systematisk måte, og peker mot et behov for videre arbeid med sikkerhetskultur og bevisstgjøring.

Når det gjelder gjenoppretting, vurderer revisjonen at kommunen har etablert tiltak som gir gode forutsetninger for å gjenopprette data og tjenester etter alvorlige hendelser. Gjenopprettingsarbeidet er understøttet av sikkerhetskopiering, testing og beredskapsplanverk, noe som styrker kommunens evne til å opprettholde kritiske tjenester ved alvorlige hendelser. Kriteriet om gjenoppretting vurderes derfor som oppfylt.

Samlet vurderer revisjonen at kriteriet om regelmessig gjennomføring av inntrengingstester ikke er oppfylt, mens kriteriene knyttet til hendelseshåndtering og gjenoppretting i hovedsak er oppfylt. Mangelen på systematiske og regelmessige inntrengingstester utgjør et vesentlig forbedringsområde.

5.4 Konklusjon og anbefalinger

Rakkestad kommune har i hovedsak etablert tilfredsstillende organisatoriske, tekniske og menneskelige tiltak for å ivareta informasjonssikkerheten. Kommunen har etablert flere kompetanse- og bevistgjøringstiltak, tilfredsstillende kontroll med IKT-ressurser og tilgangsstyring, dokumenterte løsninger for sikkerhetskopiering og gjennomretting, samt et strukturert rammeverk for håndtering av sikkerhetshendelser.

Samtidig viser datagrunnlaget at opplæringen ikke i tilstrekkelig grad har nådd alle ansatte, og at kjennskapen til sikkerhetsmål, styrende dokumenter og etablerte rutiner varierer i organisasjonen. Dette innebærer et forbedringsbehov knyttet til forankring, kompetanse og praktisk etterlevelse av sikkerhetskravene. Videre vurderes overvåkingen av sikkerhetshendelser som delvis oppfylt, fordi datagrunnlaget ikke fullt ut dokumenterer en helhetlig og kontinuerlig overvåking gjennom hele revisjonsperioden. Revisjonen vurderer også at arbeidet med sikkerhet i anskaffelser blir ivaretatt på en tilfredsstillende måte.

Det mest sentrale forbedringsområdet gjelder manglende systematisk og regelmessig gjennomføring av inntrengingstester. Etter revisjonens vurdering reduserer dette kommunens mulighet til å avdekke tekniske sårbarheter og verifisere at etablerte sikkerhetstiltak fungerer etter hensikten.

Basert på våre vurderinger og konklusjon anbefaler vi at kommunen bør:

- styrke opplæring, bevisstgjøring og praktisk etterlevelse blant ansatte, ved å sikre regelmessig opplæring, økt kjennskap til sikkerhetsrutiner og styrke etterlevelsen av rutiner for melding av informasjonssikkerhetshendelser og avvik
- gjennomføre regelmessige inntrengingstester

6 KILDER

Dokumenter oversendt fra kommunen

- G01-Klassifiseringsregime.docx
- Informasjonssikkerhetshåndboken_Rakkestad_2025.docx
- Overordnet_IT_beredskapsplan_Rakkestad.docx
- P04-Backup.docx
- P05-Helpdesk.docx
- P06-Overvåking.docx
- P10-Hendelsesregistrering.docx
- P13-LMP-telefoner.docx
- P14-Oppsett av nye pcer.docx
- P16-pureservice.docx
- P17-Bestillinger.docx
- P18-Ferie.docx
- P20-Reinstallering av gamle pcer.docx
- P21-Månedlig nedetid.docx
- P22-Brukerhåndtering.docx
- P23-Kommune-tv.docx
- P24-Oppretting av servere.docx
- P25-Sletting av servere.docx
- R01-Etablering_av_kommunenes_kriseorganisasjon.docx
- R01-Hendelseshåndtering.docx
- R02-Varsling.docx
- R03-Testing og øving.docx
- R04-Backup.docx
- R05-Helpdesk.docx
- R05-Læreprosesser.docx
- R06-Overvåking.docx
- R07-Mediehaandtering1.docx
- R08-Cyberangrep.docx
- R09-Lokale forhold.docx
- R10-Hendelsesregistrering.docx
- R11-Sjekkliste hendelser.docx
- R13-LMP-telefoner.docx
- R14-Oppsett av nye pcer.docx
- R15-Checkmk.docx
- R16-pureservice.docx
- R17 Bestillinger.docx
- R18-Ferie.docx
- R19-Varsling om nedetid.docx
- R20-Reinstallasjon av gamle pcer.docx
- R21-Månedlig nedetid.docx
- R22-Brukerhåndtering.docx
- R23-kommune-tv.docx
- R24-Oppretting av servere.docx
- R25-Sletting av servere - Kopi.docx
- R26-Oppsett av telefoner.docx

- Risikovurdering_med_handlingsplan,trusler_IT.docx
- Risikovurdering_mfa.docx
- t01-svikt i strømforsyning.docx
- t01it-svikt i strømforsyning.docx
- t02it-innbrudd_tyveri.docx
- t03it-cyberangrep.docx
- t04it-ansatte_sletter.docx
- t05it-nettverksbrudd.docx
- t06it-utilgjengelig_serverrom.docx
- t07it-mobilnett_nede.docx
- t08it-sykdom_it.docx

7 VEDLEGG

7.1 Utledning av revisjonskriterier

Utledning av revisjonskriterier for

Informasjonssikkerhet – Rakkestad kommune

Revisjonskriterier, også kalt «foretrukket praksis», er samlebetegnelser for de krav eller forventninger som brukes som grunnlag for å vurdere kommunens virksomhet.
Revisjonskriteriene er utledet med bakgrunn i lov og forskrift samt anbefalinger og veiledere.

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

Kommunen skal kunne dokumentere en helhetlig og systematisk internkontroll for informasjonssikkerhet som oppfyller kravene i gjeldende lovverk. Flere sentrale kilder stiller krav og forventninger til et slikt styringssystem. Problemstillingen tar utgangspunkt i hva som kreves av et styringssystem for informasjonssikkerhet. Revisjonen vil blant annet undersøke om kommunen har vurdert trusler og sårbarheter gjennom risikoanalyser.

Kommuneloven
Kommuneloven § 25-1 stiller krav om at kommunen skal ha internkontroll som sikrer at lover og forskrifter følges. Informasjonssikkerhet er en integrert del av internkontrollen, fordi manglende styring kan medføre brudd på personvern, økonomiske tap og svekket tillit. Internkontrollen skal være dokumentert, systematisk og tilpasset risiko og vesentlighet. Dette innebærer at kommunen må ha et rammeverk av retningslinjer, prosedyrer og kontrollaktiviteter som sikrer at informasjonssikkerhet ivaretas i praksis. Det skal foreligge skriftlige sikkerhetspolicyer og rutiner for sentrale områder som tilgangsstyring, håndtering av avvik, klassifisering av informasjon og bruk av utstyr. Videre må roller og ansvar være tydelig definert og dokumentert, og ledelsen skal ha utpekt hvem som har ansvar for ulike deler av sikkerhetsarbeidet. Kommuneloven forutsetter også at det finnes mekanismer for internkontroll, som intern revisjon og ledelsens gjennomgang, for å sikre at sikkerhetsarbeidet fungerer over tid.

eForvaltningsforskriften
For statlige og kommunale forvaltningsorganer er eForvaltningsforskriften § 15 den mest konkrete føringen. Den krever at forvaltningsorganer som bruker elektronisk kommunikasjon, skal ha definerte sikkerhetsmål og en sikkerhetsstrategi for informasjonssikkerhet. Disse skal danne grunnlaget for internkontrollen og være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør integreres i virksomhetens helhetlige styringssystem. Forskriften presiserer at sikkerhetsmål, strategi og tiltak skal inkludere relevante krav fra annet regelverk, som personvernregelverket og sikkerhetsloven.

Sikkerhetsloven og Digitalsikkerhetsloven
Disse lovene gjelder for virksomheter med samfunnskritiske funksjoner. Kommunen kan omfattes dersom den leverer kritiske tjenester som vannforsyning, helse eller beredskap. Loven krever styringssystem for digital sikkerhet, risikostyring og rapportering av hendelser. Kommunen skal ha vurdert om den

omfattes av lovene, etablert styringssystem for digital sikkerhet og rutiner for rapportering av sikkerhetshendelser til relevante myndigheter

Nasjonale retningslinjer og standarder
I tillegg til lovkrav gir nasjonale anbefalinger føringer for beste praksis. Nasjonal sikkerhetsmyndighet (NSM) og Digitaliseringsdirektoratet (DigDir) fremhever at informasjonssikkerhetsarbeidet bør være helhetlig og risikoorientert. DigDir anbefaler ISO 27001[38], som innebærer at styringssystemet inneholder elementer som ledelsesforankring, risikostyring, policyer, opplæring, hendelseshåndtering og kontinuerlig forbedring. NSM har utviklet grunnprinsipper for sikkerhetsstyring, som vektlegger identifisering av verdier og risiko, beskyttelse og opprettholdelse av nødvendig sikkerhetsnivå, samt effektiv håndtering av hendelser. Selv om NSMs anbefalinger ikke er lovfestede, kan de benyttes som revisjonskriterier fordi de reflekterer anerkjent beste praksis i offentlig sektor.

Kommunen skal ha et dokumentert styringssystem for informasjonssikkerhet som er forankret i ledelsen og integrert i kommunens styring. Systemet skal omfatte klare sikkerhetsmål og strategier, være tilpasset kommunens risikoer og sikre etterlevelse av alle relevante lover, herunder kommuneloven, personvernregelverket og eventuelt sikkerhetsloven. Det bør baseres på anerkjente rammeverk som ISO 27001 eller tilsvarende og inkludere mekanismer for kontinuerlig forbedring. Når revisjonen vurderer denne problemstillingen, vil det være sentralt å se etter dokumentasjon som viser at kommunen har fastsatt overordnede målsettinger for informasjonssikkerhet, utarbeidet en strategi basert på risikovurderinger, fordelt ansvar og myndighet tydelig i organisasjonen, etablert rutiner for risikovurderinger og dokumentert sikkerhetsarbeidet og resultatene i nødvendig omfang.

Punktvis oppsummering av kriteriene:
Kommunen skal:

- **fastsette overordnede målsettinger for informasjonssikkerhet i kommunen.**
- **utarbeide en overordnet strategi for å nå målene på området, som er basert på risikovurderinger.**
- **tydelig fordele ansvar, myndighet og oppgaver** for informasjonssikkerhet i organisasjonen
- ha etablert styringssystem for digital sikkerhet og rutiner for rapportering av sikkerhetshendelser til relevante myndigheter
- **ha rutiner for risikovurderinger knyttet til informasjonssikkerhet**
- **dokumentere sikkerhetsarbeidet** og resultater fra dette i nødvendig omfang.
- gjennomføre intern revisjon og ledelsens gjennomgang, for å sikre at sikkerhetsarbeidet fungerer over tid.

Problemstilling 2 – Har kommunen iverksatt tilfredsstillende organisatoriske, tekniske og menneskelige tiltak for å ivareta informasjonssikkerhet?

Problemstillingen[39] omhandler de organisatoriske, tekniske og menneskelige tiltak som er iverksatt for å ivareta informasjonssikkerheten. NSM sine grunnprinsipper for IKT-sikkerhet er en relevant kilde for revisjonskriterier, og disse prinsippene omfatter identifisering, kartlegging, beskyttelse og opprettholdelse av sikkerheten i kommunen.

[38] Verdensledende standard for informasjonssikkerhet som for et rammeverk for sikkerhetsarbeidet tilpasset viskomheten

[39] Deler av revisjonskriteriene til problemstilling to er basert på Revisjon Midt-Norge sin forvaltningsrevisjon om Beredskap og Informasjonssikkerhet fra 2025

Organisatoriske tiltak innebærer tydelige roller og ansvar, styringsdokumenter, policyer, beredskapsplaner, etablerte rutiner, internkontroll og ledelsesforankring. Tekniske tiltak omfatter blant annet tilgangsstyring, kryptering, sikkerhetskopiering, brannmurer, overvåking og hendelseshåndtering. Menneskelige tiltak dreier seg om opplæring, kompetanseutvikling, bevisstgjøringskampanjer og rutiner for avviks-håndtering.

Revisjonen skal vurdere om ansatte har fått nødvendig opplæring, om det finnes kompetanseplaner, og om det gjennomføres regelmessige bevisstgjøringstiltak. Det undersøkes også om tiltakene er kjent og etterleves i praksis. Teknologi alene er ikke tilstrekkelig – menneskelige faktorer utgjør ofte den største risikoen, men samtidig den viktigste forsvarslinjen. Kommunen må derfor kunne dokumentere at et bredt sett av tiltak er satt i verk for å oppnå et tilfredsstillende sikkerhetsnivå i tråd med lovkrav og anbefalinger.

Kommuneloven
Kommuneloven § 25-1 pålegger alle kommuner, som nevnt under første problemstilling, å ha internkontroll som sikrer at lover og forskrifter overholdes. Dette innebærer at kommunen skal drive **systematisk styring og kontroll** med sine aktiviteter, tilpasset risiko og omfang. Internkontrollen skal bl.a. omfatte nødvendige rutiner/prosedyrer, avdekke og følge opp avvik, dokumenteres i nødvendig omfang, og jevnlig evalueres og forbedres. Anvendt på informasjonssikkerhet betyr dette at kommunen skal ha et styringssystem som kontinuerlig sikrer etterlevelse av sikkerhetskravene og tilpasses kommunens egenart og risikoforhold.

eForvaltningsforskriften
Forskriften krever at offentlige virksomheter har styring og kontroll med informasjonssikkerhet. Kommunen skal ha rutiner for hendelseshåndtering, beredskap og kontinuitet, og sikre at elektronisk kommunikasjon og lagring skjer på en sikker måte. Dette innebærer at kommunen må gjennomføre regelmessige risikovurderinger og tilpasse sikkerhetstiltakene til endringer i trusselbildet.

Nasjonale veiledere og anbefalinger
NSMs «Grunnprinsipper for IKT-sikkerhet» og Digitaliseringsdirektoratets veiledere gir beste praksis for styring og kontroll. Selv om de ikke er lovpålagte, er de anerkjente standarder som forventes fulgt for å redusere risiko. Kommunen skal gjennomføre risikovurderinger minst årlig, ha kompetanseplaner og opplæringstiltak for ansatte, og etablere rutiner for bevisstgjøring og håndtering av menneskelige feil. Disse veilederne understreker viktigheten av å identifisere, beskytte, oppdage og håndtere sikkerhetshendelser. NSM sine grunnprinsipper er delt inn i fire kategorier:

1. Identifisere og kartlegge	2. Beskytte og opprettholde
Kartlegge styringsstrukturer, leveranser og understøttende systemer Kartlegge enheter og programvare Kartlegge brukere og behov for tilgang	Ivareta sikkerhet i anskaffelses- og utviklingsprosesser Etablere en sikker IKT-arkitektur, ivareta en sikker konfigurasjon Beskytte virksomhetens nettverk, kontroller dataflyt Ha kontroll på identiteter og tilganger

	Beskytt data i ro og i transitt, beskytt e-post og nettleser Etabler evne til gjenoppretting av data, integrer sikkerhet i prosess for endringshåndtering
3. Oppdage	4. Håndtere og gjenopprette
Oppdage og fjerne kjente sårbarheter og trusler Etablere sikkerhetsovervåkning Analysere data fra sikkerhetsovervåkning Gjennomføre inntrengingstester	Forberede virksomheten på håndtering av hendelser Vurdere og klassifisere hendelser Kontrollere og håndtere hendelser Evaluere og lære av hendelser

Tabell 2: NSM sine grunnprinsipper

Identifisere og kartlegge
Kommunen bør ha full oversikt over sine IKT-ressurser. NSM anbefaler å kartlegge alle enheter og programvarer i kommunen for å vite hva som finnes i nettverket, og hvilke sårbarheter som er til stede. Dette gir et nødvendig grunnlag for å sikre systemene før eventuelle angripere utnytter ukjente svakheter. Kommunen må også ha oversikt over brukere, roller og tilganger. Mange ansatte kan ha tilganger de ikke trenger, noe som øker risikoen ved et angrep eller intern misbruk. I tråd med god praksis bør kommunen følge prinsippet om å tildele brukere kun de tilgangene som er nødvendige for å utføre deres arbeidsoppgave. Risikobildet må vurderes når behovet for sikkerhet veies mot tjenesteleveranser. I praksis kan kommunen komme til å akseptere enkelte enheter med lavere sikkerhetsnivå av hensyn til kritiske funksjoner, men da må dette være et bevisst valg basert på vurdering av risiko versus nytte.

Tiltak i denne kategorien innebærer at kommunen har en oppdatert oversikt over alle IKT-enheter og programvarer i bruk, samt et system for tilgangsstyring der brukeres rettigheter er kjente og kontrollerte.

Beskytte og opprette
Denne kategorien omhandler å etablere forsvarstiltak og sikre robuste løsninger. NSM legger vekt på at sikkerhet skal ivaretas i anskaffelses- og utviklingsprosesser. Kommunen bør stille sikkerhetskrav ved innkjøp av nye IKT-systemer og under utvikling av nye løsninger, for å minimere risikoen for at disse innfører konfigurasjons- eller arkitektursvakheter. Videre bør kommunen etablere en sikker IKT-arkitektur, IKT-systemet består gjerne av mange komponenter fra ulike produsenter som må fungere sikkert sammen. En helhetlig og dokumentert arkitektur med klart definerte sikkerhetssoner bidrar til å begrense sårbarheter. For eksempel bør nettverket segmenteres (deles opp) i soner basert på tillitsnivå for å hindre at et angrep sprer seg ukontrollert mellom systemer med ulik sensitivitet. Konfigurasjonsstyring bør også skje sentralt og standardiseres per enhetstype, dersom hver enhet konfigureres ulikt, øker risikoen for menneskelige feil, dobbeltarbeid og oversette sårbarheter.

Under prinsippet om sikker konfigurasjon anbefaler NSM å ha et sentralt regime for sikkerhetsoppdateringer. Kommunen bør installere sikkerhetsoppdateringer så raskt som mulig når de foreligger, for å tette kjente sårbarheter før de utnyttes. Det bør finnes en prioritert plan for oppdateringer, slik at de mest kritiske oppdateringene tas først, og det må være klare rutiner for hvor ofte oppdateringer gjennomføres. Det bør også være tydelig definert hvem som er ansvarlig for oppfølging dersom en oppdatering ikke kan utføres umiddelbart eller må utsettes.

Et annet sentralt element er sikkerhetskopiering og gjenoppretting. NSM påpeker at kommunen må ha en metode for sikkerhetskopiering av kritiske data for å unngå tap av informasjon. Det anbefales å utarbeide en plan for jevnlig sikkerhetskopiering av alle viktige virksomhetsdata samt prosedyrer for rask gjenoppretting. Regelmessige backup-rutiner sikrer at kommunen kan rekonstruere data og gjenopprette tjenester dersom systemer skulle svikte eller data går tapt som følge av en hendelse.

Oppsummert skal kommunen i denne kategorien ivareta sikkerheten i alle nye anskaffelser og utviklingsprosjekter, ha en helhetlig sikkerhetsarkitektur og sentral styring av konfigurasjon og oppdateringer, samt sikre jevnlig sikkerhetskopiering av data.

Oppdage

Tiltak i denne kategorien skal gjøre kommunen i stand til å avdekke sikkerhetshendelser tidlig. NSM anbefaler å etablere sikkerhetsovervåking, det vil si kontinuerlig overvåking av nettverk, systemer og logger for å samle inn relevante data som kan indikere uønskede aktiviteter. Målet er å oppdage innbrudd eller avvik så tidlig som mulig, slik at man kan begrense skadeomfang eller forhindre at en sikkerhetshendelse utvikler seg. For at dette skal lykkes må kommunen ha tilgang til tilstrekkelige og riktige data, det kan være avgjørende å ha logget det som trengs for senere å kunne analysere hendelsen, gjenopprette normaltilstand og hindre gjentakelse. Derfor bør kommunen ikke bare overvåke, men også analysere data fra sikkerhetsovervåkningen. Systematisk bearbeiding og korrelering av logger og andre sikkerhetsdata øker sannsynligheten for å avdekke skjulte angrep eller mistenkelig aktivitet som ellers ville passert ubemerket.

Et annet prinsipp under «Oppdage» er å gjennomføre inntrengingstester (penetrasjonstester). Kommunen bør jevnlig teste sin egen forsvarsevne ved å simulere angrep mot egne systemer. Slik testing verifiserer at eksisterende sikkerhetstiltak fungerer etter hensikten, og avdekker eventuelle svakheter i systemer, konfigurasjoner eller rutiner. Resultatene fra inntrengingstester gir grunnlag for å forbedre beredskapen. Ofte utnytter angripere kjente svakheter i rutiner eller systemer, så funnene bør brukes til å stramme opp praksis der det trengs.

I praksis betyr dette at kommunen skal ha et system for aktiv sikkerhetsovervåkning og logganalyse, og at den bør gjennomføre periodiske tester av sine sikkerhetstiltak gjennom simulerte angrep.

Beskytte og opprette

Selv med gode forebyggende tiltak vil risikoen for sikkerhetshendelser aldri være null. Derfor må kommunen være forberedt på å håndtere hendelser og gjenopprette normal drift dersom noe skjer. NSM anbefaler at kommunen etablerer et planverk for hendelseshåndtering. Uten en klar plan og prosedyrer på forhånd kan det bli vanskelig å reagere effektivt når en alvorlig hendelse inntreffer. En hendelseshåndteringsplan skal definere hva som utgjør en sikkerhetshendelse, hvem som har ansvar for å gjøre hva når alarmen går, og hvordan hendelser skal eskaleres og rapporteres. Målet er å håndtere situasjonen riktig og med riktige ressurser slik at skadevirkningene minimeres og man så raskt som mulig gjenoppretter normal drift.

En nært tilknyttet oppgave er gjenoppretting (restaurering av systemer og data) etter en hendelse. Kommunen må ha en plan for hvordan man kommer tilbake til normal tilstand underveis i eller i etterkant av en alvorlig hendelse. Dette inkluderer for eksempel å ha alternative løsninger for kritiske tjenester (beredskapsløsninger) og å vite hvilke sikkerhetskopier som skal benyttes for å rekonstruere tapt informasjon. Uten en slik gjenopprettingsplan vil det være krevende å begrense skadeomfanget og få tjenestene opp igjen innen rimelig tid f.eks. etter et dataangrep. Beredskapsplanverket må derfor omfatte klare rutiner for både umiddelbar respons og for kontinuitet og reetablering av normale tjenester.

Det siste prinsippet innebærer at kommunen utarbeider konkrete planer for hvordan sikkerhetshendelser skal håndteres og hvordan kritiske data og tjenester skal gjenopprettes etter et avbrudd.

Menneskelige tiltak
På tvers av alle de fire kategoriene over, er det avgjørende at kommunen har de riktige organisatoriske rammer og kompetansetiltak. Organisatoriske tiltak vil si at det er tydelige roller og ansvar knyttet til informasjonssikkerhet, at det finnes oppdaterte styringsdokumenter, sikkerhetspolicyer, beredskapsplaner og interne rutiner, og at ledelsen er engasjert og fører internkontroll med at disse etterleves i praksis. Teknologiske sikringstiltak alene er ikke tilstrekkelig, og ofte er det menneskelige faktorer som utgjør den største risikoen, men samtidig er det ansattes kunnskap og årvåkenhet som er det viktigste forsvarsverket. Derfor må kommunen satse på opplæring og bevisstgjøring. Ansatte bør få jevnlig kompetanseutvikling innen informasjonssikkerhet, kjenne til gjeldende rutiner for sikker bruk av systemene og være bevisste på hvordan de skal rapportere og håndtere eventuelle avvik eller sikkerhetstrusler. Kommunen bør dokumentere at et bredt sett av tiltak er iverksatt, organisatoriske, tekniske og menneskelige, for å oppnå et tilfredsstillende sikkerhetsnivå i tråd med lovkrav og anbefalinger.

Nedenfor oppsummeres revisjonskriteriene punktvis. Disse kriteriene representerer det sett av krav og anbefalinger (fra lovverk og anerkjent standard) som kommunen forventes å oppfylle for god informasjonssikkerhet:

Punktvis oppsummering av kriteriene

- Kommunen må gjennomføre kompetansetiltak som bidrar til at medarbeidere som bruker kommunens informasjonssystemer, har tilstrekkelig kompetanse til å ivareta kommunens sikkerhetsbehov, og til å ivareta gjeldende krav og føringer for informasjonssikkerhet
- Kommunen bør ha en oversikt over enheter i IKT-systemet
- Kommunen bør ha en oversikt over programvare
- Kommunen bør ha et system for styring av tilganger
- Kommunen bør ivareta sikkerhet i anskaffelse- og utviklingsprosesser
- Kommunen bør etablere og dokumentere en sikker IKT-arkitektur
- Kommunen må ha en plan for sikkerhetskopiering, og ta sikkerhetskopier
- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen
- Kommunen bør gjennomføre inntrengingstester
- Kommunen bør ha en plan for hendelseshåndtering
- Kommunen må ha en plan for gjenoppretting

7.2 Kommunedirektørens uttalelse

Revisjonen mottok per e-post datert 7. september 2026 følgende uttalelse fra kommunedirektøren i Rakkestad kommune:

> Rakkestad kommune har ingen ytterligere kommentarer til forvaltningsrevisjonsrapporten om informasjonssikkerhet.