FORVALTNINGSREVISJONS-
RAPPORT 9 - 2025

DIGITAL SIKKERHET

UTARBEIDET FOR
KONTROLLUTVALGET I
ØYER KOMMUNE

INNLANDET REVISJON IKS

1. september 2025
2025-923/GSL

FORORD

Denne rapporten er et resultat av forvaltningsrevisjonsprosjektet IKT-sikkerhet i Lillehammerregionen som er gjennomført på oppdrag av kontrollutvalgene i Gausdal, Lillehammer og Øyer kommuner.

Forvaltningsrevisjon er en lovpålagt oppgave som innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak (Kommunelovens § 23-3.).

Prosjektarbeidet er gjennomført i perioden januar til august 2025. Problemstilling én er utarbeidet av forvaltningsrevisor Guro Selfors Lund, mens problemstilling to er utarbeidet av forvaltningsrevisor Astrid Gerdts. Guro Selfors Lund har vært oppdragsansvarlig for prosjektet, og rapporten er kvalitetssikret av leder for forvaltningsrevisjon og eierskapskontroll Ole I. Gjerald. I arbeidet med prosjektet har revisjonen leid inn ekstern kompetanse knyttet til informasjonssikkerhetsmiljøet på Gjøvik, gjennom bedriften Diri AS.

Utkast til rapport er sendt kommunedirektøren til uttalelse. Svaret fra kommunedirektøren er vedlagt rapporten.

Vi vil takke alle som har bidratt med informasjon i prosjektet. Når rapporten er ferdig behandlet i kontrollutvalget og kommunestyret, vil den bli lagt ut på Irev.no og i forvaltningsrevisjonsregisteret.

Lillehammer, 1. september 2025

Guro Selfors Lund
Oppdragsansvarlig revisor

Astrid Gerdts
Prosjektansvarlig revisor

INNHOLDSFORTEGNELSE

SAMMENDRAG

Rapporten undersøker om kommunene Lillehammer, Gausdal og Øyer har etablert tilfredsstillende sikkerhetstiltak mot digitale angrep og en digital sikkerhetskultur blant ansatte.

Undersøkelsen bygger på dokumentanalyse, intervjuer, spørreundersøkelse og sårbarhetsskanning av utvalgte IKT-systemer. Bakgrunnen er et skjerpet nasjonalt trusselbilde, der kommunene håndterer store mengder sensitiv og samfunnskritisk informasjon. Selv om det ikke er indikert forhøyet risiko i regionen, kan konsekvensene av digitale angrep være alvorlige for tjenesteleveransen, økonomien og omdømmet.

Det er utarbeidet revisjonskriterier for begge problemstillingene, basert på relevante krav og forventninger til kommunenes arbeid med digital sikkerhet.

Det er utarbeidet informasjonssikkerhetspolicy og -håndbok i fellesskap mellom Lillehammer, Gausdal og Øyer kommune som del av 3:1-samarbeidet. Informasjonssikkerhetspolicyen fastsetter kommunenes overordnede mål og prinsipper for sikker informasjonsbehandling. Informasjonssikkerhetshåndboken beskriver roller, ansvar og praktiske tiltak for å sikre etterlevelse av krav til informasjonssikkerhet. Den omfatter både tekniske og organisatoriske tiltak, og danner grunnlaget for internkontroll og årlig gjennomgang av sikkerhetsarbeidet.
Det ble formulert to problemstillinger for prosjektet. Nedenfor gjengis revisjonens konklusjoner og anbefalinger for hver problemstilling.

Problemstilling 1, Har kommunen etablert tilfredsstillende sikkerhetstiltak mot digitale angrep i utvalgte IKT-systemer?

Visma Flyt Sikker Sak
Konklusjon:
Revisjonen mener at informasjonssikkerheten i Visma Flyt Sikker i stor grad er ivaretatt. VFSS behandler informasjonsverdier som krever høy beskyttelse av konfidensialitet og integritet. Dette betyr at informasjon på avveie kan medføre alvorlige konsekvenser.

KK2
Konklusjon:
Øyer kommune ivaretar i høy grad informasjonssikkerheten i KK2. Systemet håndterer informasjonsverdier som stiller krav om høy integritet, og det er avgjørende at informasjonen er korrekt og ikke endres utilsiktet eller urettmessig.

Begrunnelse for konklusjonene:
Kommunen har utarbeidet en informasjonssikkerhetshåndbok som gir føringer og veiledning innen flere sentrale områder av informasjonssikkerhetsarbeidet. Revisjonen ser det som positivt at Øyer kommune har vedtatt en oppdatert versjon av informasjonssikkehetshåndboken. Håndboken beskriver blant annet prinsipper for tilgangsstyring, krav til risikovurderinger, logging, sikkerhetsoppdateringer og håndtering av sikkerhetshendelser.

Dette gir et viktig rammeverk for kommunens arbeid med å sikre sine systemer og data, og bidrar til å etablere en felles forståelse av ansvar og praksis på tvers av organisasjonen.

I våre undersøkelser har vi tatt utgangspunkt i et sett revisjonskriterier som bygger på NSMs grunnprinsipper. For hvert system har vi vurdert om kriteriene er oppfylt, delvis oppfylt eller ikke oppfylt, basert på dokumentasjon, intervjuer og tekniske funn. For begge disse systemene ser vi at de fleste kriteriene er oppfylt.

Selv om flere kriterier er vurdert som oppfylt, er det viktig å understreke at oppfyllelse kan romme et bredt spekter av praksis og modenhet. I noen tilfeller har kommunene fremlagt omfattende dokumentasjon, tydelige rutiner og opplysninger om systematisk oppfølging som underbygger vurderingen. I andre tilfeller er det færre skriftlige rutiner og mindre dokumentasjon, men praksis og intervjuer viser likevel at kriteriet er ivaretatt i tilstrekkelig grad. Dette viser at det kan være ulik modenhet og ulik grad av systematikk i hvordan kriteriene oppfylles. Et system kan ha etablert tiltak som teknisk sett oppfyller kravene, men mangler strukturert dokumentasjon og forankring. Andre systemer kan ha høy grad av formalisering og krav til seg, som gjør det mindre aktuelt å ha lokal forankring.

De to systemene som er undersøkt i Øyer, VFSS og KK2, leveres som skytjenester og begge behandler personopplysninger som må følge krav etter GDPR. Kommunen må uansett alltid være sitt ansvar bevisst, da det er den som sitter med konsekvensene av uønskede hendelser, uavhengig av hvilken leverandør de bruker.

Når det gjelder gjennomføring av ROS-analyser, har revisjonen avdekket svakheter ved dette arbeidet i begge systemene. Det er særlig svakheter knyttet til kommunenes arbeid med å identifisere og kartlegge risikoer og verdier knyttet til digitale sikkerhetstrusler som er aktuelle for det enkelte system. På bakgrunn av dette mener revisjonen det kan være behov for å styrke de ansattes kompetanse når det gjelder betydningen av digital sikkerhet i kommunens risikoarbeid.

Problemstilling 2, I hvilken grad har kommunen etablert en digital sikkerhetskultur blant ansatte i organisasjonen?

Revisjonen viser at kommunens arbeid med å etablere en sikkerhetskultur er påbegynt, men fortsatt i en tidlig fase.

Ledelsen har ansvaret for at sikkerhetsarbeidet er godt integrert i arbeidshverdagen, og det forventes at ledere prioriterer sikkerhet både strategisk og i det daglige arbeidet. Ansatte skal på sin side bidra til å etterleve krav til sikkerhetsatferd, rapportere avvik og delta i opplæring og kompetanseutvikling. Ansattes bidrag er avgjørende for å oppnå en robust sikkerhetskultur i virksomheten.

Revisjonen viser at kommunen har etablert enkelte strukturer og tiltak som skal fremme en sikkerhetskultur, herunder retningslinjer, opplæringstiltak og et system for avvikshåndtering. Det synes å være økt bevissthet om digital sikkerhet i virksomheten, og noen tiltak er iverksatt for å styrke de ansattes kunnskap og praksis. Opplæringen skjer imidlertid i begrenset grad, og lav registrering av avvik reduserer muligheten for læring og forbedring. Det er også variasjon i hvordan rutiner følges opp i tjenestene.

En systematisk og målrettet opplæringsstrategi vil ikke bare bidra til økt etterlevelse av rutiner og sikkerhetstiltak, men også styrke organisasjonens felles forståelse av hva IKT-sikkerhet og digital

sikkerhetskultur faktisk innebærer i praksis. En slik bevisstgjøring er særlig viktig i en tid med økende digital kompleksitet og trusselbilde, og bør forankres både på strategisk og operativt nivå.

Samlet sett tyder revisjonens funn på at innsatsen med å etablere en digital sikkerhetskultur foreløpig er lite systematisk og svakt forankret i kommunen. Det vurderes å være behov for en mer helhetlig, systematisk og lokalt forankret tilnærming for å bygge og styrke sikkerhetskulturen i organisasjonen.

På bakgrunn av revisjonens samlede vurderinger og konklusjoner presenteres følgende anbefalinger for forbedring. Kommunen bør:

- påse at kravene til informasjonssikkerhet i systemene de bruker er ivaretatt.
- ha en strategi og plan for opplæring innenfor digital sikkerhet. Planen bør sikre at ansatte og ledere får den opplæringen og kompetanseutviklingen de trenger for å ivareta sin rolle innen informasjonssikkerhet.
- påse at ansatte med ansvar for risikobasert arbeid har nødvendig kompetanse i risikostyringsmetodikk, og at de har tilstrekkelig kunnskap om hvilke verdier som skal beskyttes.
- påse at ansatte og ledere har tilstrekkelig kompetanse til å identifisere, registrere og følge opp avvik innen digital sikkerhet.

1. INNLEDNING

1.1 OM BESTILLINGEN

Innlandet Revisjon IKS utarbeidet i 2022 en foranalyse om IKT-sikkerhet for kontrollutvalgene i Lillehammer, Gausdal og Øyer kommuner. Foranalysen ble behandlet i et felles kontrollutvalgsmøte 24. januar 2023.

Arbeidet med foranalysen viste at kommunene hadde kommet godt i gang med å få på plass overordnede dokumenter i et styringssystem for informasjonssikkerhet. Felles i prosjektplanene for de tre kommunene er at revisjonen anbefalte at «(…) en eventuell forvaltningsrevisjon burde fokusere på den faktiske sikkerheten i IKT-systemene og ansattes kjennskap til retningslinjer og rutiner innenfor IKT-sikkerhet».

Kontrollutvalget i Gausdal behandlet sin prosjektplan allerede 18. april 2023, og fikk en statusoppdatering fra revisjonen 15. februar 2024. Kontrollutvalgene i Øyer og Lillehammer behandlet prosjektplanene i to omganger, og den reviderte planen ble vedtatt av Øyer kommune 29. mai 2024 og av Lillehammer kommune 12. februar 2024. I et felles KU-møte 12. februar 2025 ble det gitt en statusorientering, og det ble avklart at rapportene legges fram i et felles KU-møte 10. september 2025.

Digital sikkerhet[1] handler om organisatoriske, tekniske, fysiske og menneskelige faktorer. Med dette som utgangspunkt vedtok kontrollutvalgene å bestille en forvaltningsrevisjon som undersøkte problemstillingene:

1. Har kommunen etablert tilfredsstillende sikkerhetstiltak mot cyberangrep i utvalgte IKT-systemer?
2. I hvilken grad har de ansatte i kommunen tilstrekkelig kjennskap til retningslinjer og rutiner for informasjonssikkerhet?

Ved gjennomføring av prosjektet har vi sett behov for å justere noe på ordlyden i problemstillingene. I den første problemstillingen er begrepet «digitale angrep» valgt fremfor «cyberangrep» for å bruke et mer forståelig og allment språk, uten at dette endrer innholdet i problemstillingen. I den andre problemstillingen ønsket vi i større grad å synliggjøre at det er kommunen som er ansvarlig og som revideres, og ikke de ansatte. Vi ønsket også å tydeliggjøre at digital sikkerhet handler om mer enn kjennskap til rutiner, da det handler om både bevissthet, kunnskap og faktiske ferdigheter. Vi mener derfor at «digital sikkerhetskultur» er et mer dekkende og treffende begrep for undersøkelsene som gjøres i denne problemstillingen.

Justeringen i ordlyden på problemstillingene innebærer ikke en endring i formålet med problemstillingen eller metodene som er valgt for å gjennomføre undersøkelsen.

[1] «Digital sikkerhet» brukes her fordi det favner både tekniske, organisatoriske og menneskelige tiltak for å beskytte digitale verdier. «IKT-sikkerhet» viser primært til sikring av informasjons- og kommunikasjonsteknologi (systemer, nettverk og data).

1.2 FORMÅL OG PROBLEMSTILLINGER

Formålet med revisjonen er å undersøke om kommunene i Lillehammerregionen har etablert tilfredsstillende tiltak for digital sikkerhet. Prosjektet har to problemstillinger:

1. Har kommunen etablert tilfredsstillende sikkerhetstiltak mot digitale angrep i utvalgte IKT-systemer?
2. I hvilken grad har kommunen etablert en digital sikkerhetskultur blant ansatte i organisasjonen?

1.3 RAPPORTENS OPPBYGGING

Videre i dette innledningskapitlet følger i punkt 1.4 en omtale av metodisk tilnærming, 1.5 en bakgrunnsbeskrivelse av temaet, 1.6 en presentasjon av kommunens organisering, 1.7 en redegjørelse for informasjonssikkerhet i 3:1-samarbeidet, 1.8 personvernsikkerhet og 1.9 informasjon om helhetlig ROS-analyse fra Lillehammer, Øyer og Gausdal. Kapittel nr. to gir en innføring i de krav og forpliktelser som kommunene må forholde seg til.

Kapittel tre og fire handler om prosjektets to problemstillinger. Disse kapitlene innledes med en utfyllende beskrivelse av temaet og utledning av revisjonskriterier. Deretter presenteres revisjonens funn og vurderinger.

I kapittel fem finnes konklusjoner og revisors anbefalinger til kommunen.

1.4 METODISK TILNÆRMING

Foranalysen viste at kommunene er godt i gang med å etablere et styringssystem for informasjonssikkerhet. Revisjonsprosjektet er derfor innrettet mot den faktiske sikkerheten i IKT-systemene og sikkerhetskulturen i kommunene.

Datainnsamlingen ble gjennomført fra mars til august 2025. Undersøkelsen kombinerer dokumentanalyse, intervjuer og en spørreundersøkelse. Det er også gjennomført sårbarhetsanalyse av tre utvalgte IKT-system.

Den første problemstillingen er belyst gjennom intervjuer med fagpersoner i de tre samarbeidende kommunene som har ansvar for, eller særskilt kunnskap om, forvaltning og drift av de aktuelle IKT-systemene. Formålet med intervjuene har vært å innhente informasjon fra personer med inngående kjennskap til systemenes funksjon, bruk og tilhørende sikkerhetstiltak.

I tillegg er det gjennomført en dokumentgjennomgang av kommunenes overordnede styringsdokumenter for informasjonssikkerhet, samt av tekniske og organisatoriske tiltak knyttet til de to utvalgte systemene:

- **Visma Flyt Sikker Sak** (i det videre omtales Visma Flyt Sikker Sak som VFSS) er et digitalt saksbehandlingssystem i skyen som lar ansatte i skole, barnehage og andre offentlige virksomheter håndtere og arkivere sensitive personopplysninger på en sikker, enkel og trygg måte. Systemet brukes spesielt til saker som involverer barn og unge.

- **KK2 – innfordringsverktøy fra KapitalKontroll AS** innebærer at en virksomhet følger opp utestående krav for å sikre betaling fra skyldnere, i tråd med gjeldende lover og regler. Prosessen omfatter varsling, purring, avtaleinngåelse, betalingsoppfølging og ev. rettslige skritt. Dette innfordringsverktøyet er det digitale systemet som brukes til å administrere innfordringsprosessen.

Dokumenter mottatt fra kommunen er inkludert i analysen og framgår av dokumentoversikten i vedlegg 2. Nettsider som er brukt som kilder, er dokumentert fortløpende i fotnoter i teksten.

Når det gjelder VFSS, har Gausdal, Lillehammer og Øyer kommune et tett samarbeid. Systemet ble anskaffet i fellesskap, og systemansvarlige i de tre kommunene har løpende kontakt og samordning. I presentasjonen av funnene for VFSS oppgis felles data for alle tre kommunene. Eventuelle forskjeller mellom kommunene fremgår særskilt. Når ikke annet er angitt, gjelder beskrivelsene alle tre kommunene. VFSS leveres av en stor leverandør som blant annet har en ISO 27001-sertifisering[2].

Det er også gjennomført en sårbarhetsskanning[3] som en del av undersøkelsen. Denne er foretatt på de tre systemene som er kommunespesifikke, altså for KK2 for Øyer kommune.

Den andre problemstillingen er belyst gjennom intervjuer med ledere innen fagområdene helse, skole/barnehage og teknisk. Holdninger og praksis er kartlagt via en elektronisk spørreundersøkelse sendt til alle ansatte i kommunen.

Det tas forbehold om at det kan finnes relevant informasjon eller praksis i kommunen som ikke har kommet frem gjennom dokumentgjennomgangen eller intervjuene.

Prosjektet er gjennomført i tråd med RSK 001-standarden for forvaltningsrevisjon[4]; ekstern kvalitetssikring av revisjonskriterier og vurderinger er utført av Diri AS. Alle informanter har godkjent intervjureferater, og kommunedirektøren har fått rapportutkast til uttalelse.[5] Utfyllende metodeinformasjon fremgår av vedlegg 2.

1.5 BAKGRUNN OM TEMA

Innenfor alle virksomheter i kommunen behandles store mengder informasjon. Kvaliteten på informasjonsbehandlingen er avgjørende for å ivareta grunnleggende sikkerhet og personvern, og for at kommunen skal nå sine mål.

[2] ISO 27001 er en internasjonal standard for styringssystemer for informasjonssikkerhet, som setter krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av informasjonssikkerhet i virksomheter.

[3] Sårbarhetsskanning/rekognosering er en simulering av hvordan en målrettet angriper kan angripe kommunens systemer og organisasjon. En rekognosering har som mål å identifisere eventuelle datalekkasjer og andre forhold som kan utgjøre en risiko for at uvedkommende kan komme seg inn i kommunens systemer. Dette kan gi et godt bilde av hvilken risiko som eksisterer i organisasjonen.

[4] RSK 001 Standard for forvaltningsrevisjon. Fastsatt av NKRFs styre 12.08.2020.

[5] Vedlegg 1: Kommunedirektørens uttalelse

Kommuner håndterer lovregulerte opplysninger, som for eksempel personsensitive opplysninger. De håndterere også konkurransesensitiv informasjon fra private og kommunale selskaper, samt opplysninger som omhandler kritiske samfunnsfunksjoner og nasjonal sikkerhet.

Nasjonal Sikkerhetsmyndighet[6] (NSM) har observert en økning i digitale angrep mot offentlig forvaltning. Angrepene blir stadig mer avanserte og utnytter både teknologiske og menneskelige sårbarheter. NSM advarer om at det er et økende gap mellom sikkerhetstruslene og forebyggende tiltak, og mener at motstandskraften må styrkes gjennom tiltak på teknisk, menneskelig og organisatorisk nivå.[7]

Den nasjonale strategien for digital sikkerhet omfatter en delstrategi for digital sikkerhetskompetanse. Blant de prioriterte områdene er sikrere digitalisering og styrket sikkerhetskompetanse. Strategien inkluderer flere anbefalte tiltak for offentlig og privat sektor, blant annet om ledelse, risikostyring, sikkerhetskultur og tilgangskontroll. Tiltakene skal styrke virksomheters evne til å beskytte seg mot og håndtere digitale angrep.[8] Ikke all informasjon har samme behov for, eller krav til, beskyttelse. Nivået på informasjonssikkerhet må derfor følge av en konkret vurdering av krav og risiko. Styring av informasjonssikkerhet dreier seg om å ha kontroll på risiko knyttet til informasjon og informasjonsbehandling.[9]

Foranalysen avdekket ikke holdepunkter for at risikoen for digitale angrep er større i Lillehammerregionen enn andre steder. Likevel, sett i lys av risikobildet som tegnes av norske sikkerhetsmyndigheter, er det sannsynlig at også kommunene i Lillehammerregionen kan bli utsatt for angrep. Konsekvensen av et angrep, dersom det er vellykket, kan få store følger både for kommunenes mulighet til å levere tjenester til innbyggerne, men også for kommunenes økonomi og omdømme.

[6] NSM opplyser på sin nettside at de, sammen med Etterretningstjenesten og Politiets sikkerhetstjeneste (PST), utgjør Norges tre etterretnings-, overvåknings- og sikkerhetstjenester. NSM sin hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Kilde: https://nsm.no/om-oss/dette-er-nsm/

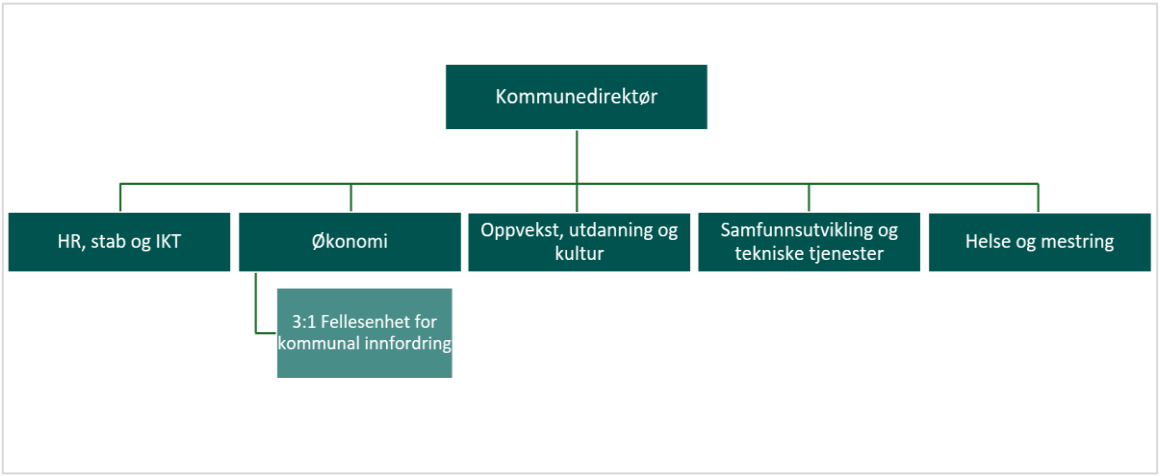
[7] Nasjonal sikkerhetsmyndighet (NSM, 2023), Nasjonalt digitalt risikobilde 2023

[8] Nasjonal strategi for digital sikkerhet - regjeringen.no. Tiltaksoversikt til nasjonal strategi for digital sikkerhet (regjeringen.no)

[9] Oslo kommunerevisjon «Overordnet styring av informasjonssikkerheten» 06/2018.

1.6 ØYER KOMMUNES ORGANISERING

Øyer kommune ledes av kommunedirektøren som har det øverste administrative ansvaret. Under kommunedirektøren er kommunen organisert i fem sektorer eller tjenesteområder med ansvar for blant annet oppvekst, utdanning og kultur, helse og omsorg, samfunnsutvikling og tekniske tjenester, samt felles stabs-, støtte- og utviklingsfunksjoner. Den administrative organiseringen fremgår av kommunens organisasjonskart, som tydelig viser linjeledelse og støttefunksjoner.[10] Vi kommer bl.a. tilbake til organisering og ledelsesforankring i avsnittene der vi ser nærmere på ulike fagsystemer.



Figur 1: Overordnet administrativ organisasjonsstruktur i Øyer kommune. Organisasjonskartet er forenklet og bearbeidet av revisor.

IKT- og digitaliseringsfunksjonen er organisert som en del av kommunens sentrale støttefunksjoner. Det administrative ansvaret for IKT-området omfatter drift, forvaltning og utvikling av kommunens digitale løsninger, brukerstøtte, anskaffelser, lisenshåndtering og tilgangsstyring. Kommunen har også ansvar for å følge opp sikkerhetstiltak og krav til universell utforming i digitale løsninger.

1.7 INFORMASJONSSIKKERHET I 3:1-SAMARBEIDET, GAUSDAL

Kommunene i Lillehammerregionen har opprettet flere interkommunale samarbeid og de har inngått ulike former for samarbeid for å løse felles oppgaver og utfordringer. Grunnlaget for dette «3:1-samarbeidet» ble lagt i 2001, under mottoet: «Hva har vi tre av som vi kan klare oss med en av?». I 2003 opprettet kommunene et felles IKT -selskap, Ikomm[11]. De besluttet at kommunene, så langt det var mulig, skulle ha felles dataprogrammer innenfor alle fagområdene. Øyer kommune deltar i 3:1-samarbeidet med Lillehammer og Gausdal. Ifølge kvalitet- og sikkerhetssjefen i Lillehammer, har de tre kommunene, som eierkommuner i Ikomm,

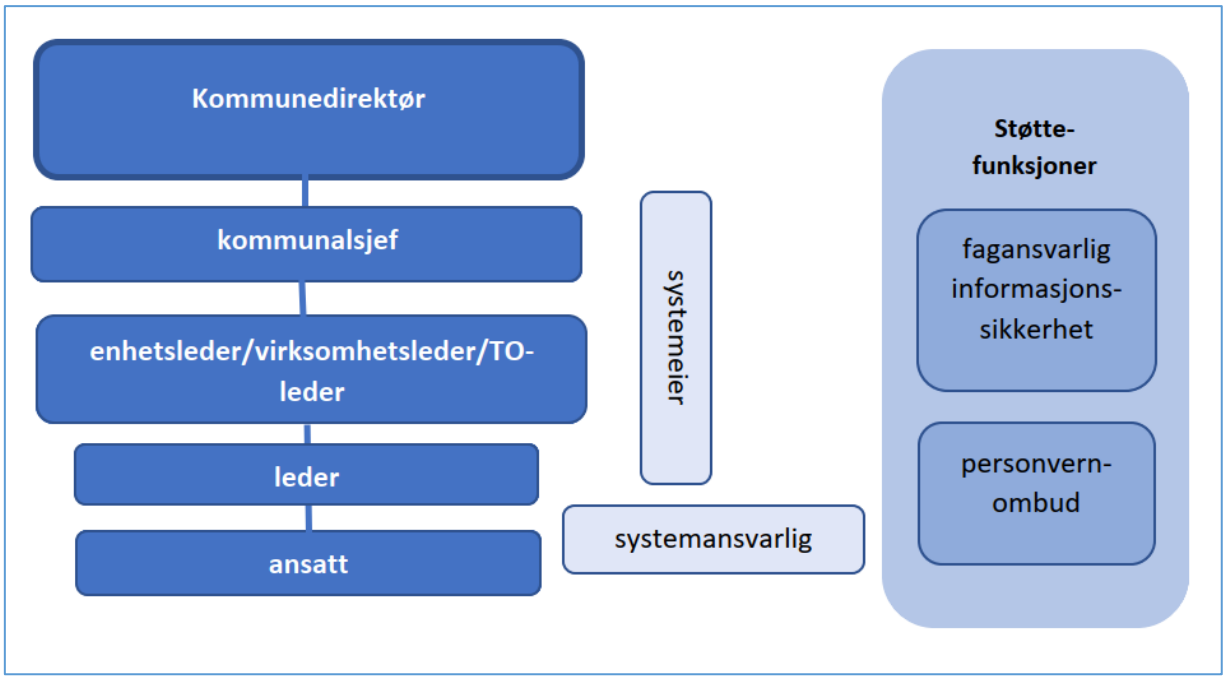
[10] https://oyer.kommune.no/om-kommunen/organisasjon/organisasjonskart/?utm_source=chatgpt.com

[11] Ikomm AS er et interkommunalt samarbeid mellom kommunene Lillehammer, Øyer og Gausdal. Kommunene har overført ansvaret for IT-drift og digital infrastruktur til Ikomm. Dette innebærer at Ikomm fungerer som en felles IT-avdeling for kommunene, med ansvar for drift og vedlikehold av datasentre, skytjenester og hybridløsninger, brukerstøtte, samt utvikling og implementering av digitale løsninger i samarbeid med kommunene. Ikomm omfattes ikke av revisjonen

et felles informasjonssikkerhetsforum for erfaringsutveksling og kompetansedeling. Forumet har ikke hatt møte siden høsten 2024, men anses fortsatt som aktivt. De tre IT-ansvarlige i Lillehammer, Gausdal og Øyer opplyser at de har et tett og løpende samarbeid.

IKT-driften i i de tre kommunene Øyer, Lillehammer og Gausdal er satt bort til Ikomm og systemleverandører, mens kommunen selv har ansvar for oppfølging av driftsavtaler, videreutvikling av systemer og ivaretakelse av sikkerhet og personvern. Tjenesteområdene er systemeiere for egne fagsystemer, mens administrasjonen har ansvar for fellesløsninger som Microsoft 365, nasjonale tjenester, og samhandling med Ikomm.

Det er utarbeidet en felles informasjonssikkerhetshåndbok i 3:1 samarbeidet. Her presiseres det at linjeledelsen har ansvar for at håndboken, samt tilhørende retningslinjer og prosedyrer, etterleves. Det innebærer at det utøvende ansvaret for informasjonssikkerhet kan delegeres fra kommunedirektøren til enhetsledere. Figuren under er hentet fra håndboken.



1.8 PERSONVERNSIKKERHET

I forbindelse med kartleggingen av kommunenes arbeid med informasjonssikkerhet, har revisjonen gjennomført en samtale med personvernombudet i de tre kommunene for å få innsikt i hans rolle og vurderinger knyttet til dette arbeidet.

Etter ny personvernlov fra 2018 må alle offentlige virksomheter ha et personvernombud. Kommunene Gausdal, Øyer, Ringebu og Lillehammer har ett felles personvernombud. Oppgaven til personvernombudet er å jobbe for

å unngå krenkelse av personvernet både overfor ansatte og innbyggere. Virksomheten skal rette eller slette opplysninger om deg når de er feilaktige, mangelfulle eller unødvendige.[12]

Personvernombudet i de tre kommunene har en rådgivende rolle i arbeidet med informasjonssikkerhet, og deltar blant annet i den årlige gjennomgangen av systemoversikten og risikovurderinger i samarbeid med fagansvarlig for informasjonssikkerhet. Personvernombudet har også deltatt i arbeidet med oppdatering av informasjonssikkerhetshåndboken i forbindelse med tilsyn fra Datatilsynet i Øyer.

Personvernombudet påpeker at det er viktig å bli involvert tidlig i kommunens prosesser som omfatter behandling av personopplysninger. Det oppleves imidlertid at dette ikke alltid skjer – for eksempel ved utlysning av kravspesifikasjoner der personopplysninger inngår.

Personvernombudet forteller at han bistår kommunene ved behov i arbeidet med risiko- og sårbarhetsanalyser (ROS), men deltar ikke systematisk. Ombudet har en veiledende funksjon, men er ikke involvert i opplæring knyttet til ROS-tematikken.

1.9 HELHETLIG RISIKO OG SÅRBARHETSANALYSE 2023-2026

Lillehammer, Øyer og Gausdal har utarbeidet en felles helhetlig ROS-analyse for perioden 2023–2026. ROS-analysen identifiserer digitale trusler som et område med vesentlig sårbarhet. Kommunenes drift er i stor grad avhengig av stabile IKT-systemer, og analysen viser at både bortfall og tilsiktede angrep kan ha omfattende konsekvenser. Det trekkes fram eksempler som hacking, ondsinnet programvare, samt sårbarhet knyttet til strømforsyning og elektronisk kommunikasjon. Videre fremheves behovet for robuste beredskapsløsninger, samarbeid med nasjonale sikkerhetsmyndigheter og tiltak for å styrke kompetanse og sikkerhetskultur. I analysen plasseres IKT-sikkerhet i kategorien høy risiko, og området løftes fram som et felt hvor forebygging og beredskap må gis særlig oppmerksomhet i kommunenes videre arbeid.

[12] https://oyer.kommune.no/personvern/

2. KOMMUNENS ANSVAR OG FORPLIKTELSER

Kommunens ansvar for digital sikkerhet er omfattende. Kommunedirektøren som øverste leder vil alltid være ansvarlig for personvern og informasjonssikkerhet i virksomheten.[13] Det gjelder også i tilfeller der andre enn kommunen selv har ansvaret for å utføre tjenestene, for eksempel gjennom interkommunale samarbeid.

Kommunen må forholde seg til en rekke lovkrav og føringer i sitt arbeid. Følgende kilder ligger til grunn for revisjonskriteriene i denne forvaltningsrevisjonen:

- Kommunelovens kapittel 25 om internkontroll
- eForvaltningsforskriften (forskrift til forvaltningsloven)
- Personopplysningsloven med personvernforordningen
- Sikkerhetsloven
- Standard for ledelsessystem for informasjonssikkerhet (ISO/IEC 27001:2023)
- Nasjonal sikkerhetsmyndighets grunnprinsipper for sikkerhetsstyring
- Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet
- Nasjonal sikkerhetsmyndighets grunnprinsipper for personellsikkerhet
- KS – «Verktøykasse for personvern og informasjonssikkerhet»
- KS – veileder «Orden i eget hus. Kommunedirektørens internkontroll»
- Digitaliseringsdirektoratets veileder om kompetanse og roller

Hva er revisjonskriterier?
I en forvaltningsrevisjon skal revisor utlede revisjonskriterier som kommunens virksomhet skal måles opp mot.

Kriteriene skal være en «objektiv målestokk» og de er grunnlaget for revisjonens vurderinger.

Revisjonskriterier kan utledes fra lover, forskrifter, retningslinjer, kommunale vedtak, og aksepterte faglige standarder.

Veileder i forvaltningsrevisjon og eierskapskontroll (NKRF, 2023)

De konkrete revisjonskriteriene vil utledes under hver av problemstillingene i kapittel tre og fire.

2.1 SENTRALE LOVKRAV

2.1.1 KOMMUNELOVEN

Kommuneloven § 25-1 konkretiserer minstekravene til kommunens internkontroll. Loven omtaler ikke IKT-sikkerhet direkte, men hvordan kommunene skal sørge for internkontroll. Internkontrollen innebærer:

- En beskrivelse av virksomhetens hovedoppgaver, mål og organisering.
- Nødvendige rutiner og prosedyrer.
- Avdekke og følge opp avvik og risiko for avvik.

[13] Kommunedirektøren har det øverste ansvaret for å følge opp kravene i personopplysningsloven, sikkerhetsloven og eForvaltningsforskriften.

- Dokumentasjon av internkontrollen i den form og det omfang som er nødvendig.
- Evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

2.1.2 SIKKERHETSLOVEN

Sikkerhetsloven gjelder for alle kommuner og skal blant annet bidra til å forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Sikkerhetsloven § 4-1 stiller krav om sikkerhetsstyring og slår fast at det er virksomhetens øverste leder som har ansvaret for det forebyggende sikkerhetsarbeidet.

Sikkerhetslovens krav om sikkerhetsstyring gjelder uavhengig av om kommunen har skjermingsverdige verdier. Alle kommuner må derfor sikre at forebyggende sikkerhetsarbeid inngår som en del av styringssystemet, og dersom kommunen har skjermingsverdige verdier som faller inn under loven, skal det iverksettes tiltak for å sikre disse verdiene.

2.1.3 EFORVALTNINGSFORSKRIFTEN

eForvaltningsforskriften er en forskrift til forvaltningsloven som stiller krav til hvordan offentlige virksomheter skal behandle elektronisk informasjon og tilrettelegge for digital forvaltning. Formålet er å «legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen». § 15 i forskriften fastsetter spesifikt at virksomhetene skal etablere, dokumentere og følge opp tiltak for styring og kontroll med informasjonssikkerheten (internkontroll). Det fastsettes også i §15 at Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet.

Dette innebærer blant annet å gjennomføre risikovurderinger, iverksette sikkerhetstiltak og kontrollere at tiltakene virker som de skal, slik at konfidensialitet, integritet og tilgjengelighet ivaretas. For å oppfylle disse kravene brukes ofte NSMs grunnprinsipper og ISO 27001, som forklares nærmere nedenfor, som normgivende rammeverk og anerkjente standarder.

2.1.4 PERSONOPPLYSNINGSLOVEN MED PERSONVERNFORORDNINGEN

Personopplysningsloven består av nasjonale regler og EUs personvernforordning (GDPR - General Data Protection Regulation). Personvernforordningen er et sett med regler som gjelder for alle EU/EØS-land.

Formålet med personvernforordningen er å sikre enkeltmenneskers rett til vern av personopplysninger. Forordningen pålegger alle virksomheter som behandler personopplysninger en rekke plikter. Norske kommuner behandler personopplysninger om innbyggere, politikere og ansatte og skal derfor følge regelverket som gjelder for behandling av personopplysninger. [14]

[14] Personvernforordningen definerer «behandling» som; enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring (artikkel 4, nr. 2).

Det går frem av artikkel 24 i personvernforordningen at den behandlingsansvarlige har ansvar for å gjennomføre «*egnede tekniske og organisatoriske tiltak*» som skal «*sikre*» og «*påvise*» at behandlingen av personopplysninger utføres i samsvar med forordningens krav. Krav til gjennomføring av risiko- og sårbarhetsanalyser (ROS-analyser) er forankret i personvernforordningens artikkel 24 og artikkel 32.

2.2 NASJONALE FØRINGER

2.2.1 STANDARD FOR LEDELESSSYSTEM FOR INFORMASJONSSIKKERHET (ISO/IEC 27001:2023)

ISO/IEC 27001:2023, ofte omtalt som *ISO-standarden* for ledelsessystemer for informasjonssikkerhet, er en internasjonalt anerkjent standard. Den er utformet slik at den er relevant for alle typer virksomheter, og anbefales av Digitaliseringsdirektoratet for offentlige virksomheter.

Standarden gir tydelige føringer for hvordan arbeidet med informasjonssikkerhet bør organiseres og følges opp. Den vektlegger ledelsesforankring, systematikk og kontinuerlig forbedring. Følgende områder er sentrale i standarden:[15]

- Mål, strategi og plan for arbeidet
- Organisering og ansvar
- Risikovurdering og risikohåndtering
- Evaluering og kontroll

2.2.2 GRUNNPRINSIPPER FRA NASJONALE MYNDIGHETER

Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet et sett med *grunnprinsipper for sikkerhetsstyring*[16]. Disse prinsippene og anbefalte tiltak skal hjelpe virksomheter med å oppnå og opprettholde et akseptabelt sikkerhetsnivå, og bidra til en helhetlig tilnærming til sikkerhetsarbeidet.

Sikkerhetsstyring omfatter alle tiltak som er nødvendige for å beskytte og styrke virksomhetens verdier. NSM legger særlig vekt på følgende overordnede premisser:

- Lederen har ansvaret for sikkerheten.
- Sikkerhetsstyring skal være en integrert del av virksomheten.
- Hele virksomheten skal ha god forståelse for risiko og sikkerhet.
- Det forebyggende sikkerhetsarbeidet skal være helhetlig.

Grunnprinsippene for sikkerhetsstyring gir et overordnet rammeverk, og er videre konkretisert gjennom egne prinsipper for fysisk sikkerhet, IKT-sikkerhet og personellsikkerhet.

Grunnprinsippene for IKT-sikkerhet[17] inneholder anbefalte tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade og misbruk. De er utviklet i samarbeid med virksomheter som forvalter kritiske samfunnsfunksjoner og infrastruktur, og gjelder både for virksomheter som er underlagt sikkerhetsloven og de

[15] Se vedlegg 3 for ytterligere omtale.

[16] https://nsm.no/getfile.php/134493-1605693992/NSM/Filer/Dokumenter/Grunnprinsipper%20for%20sikkerhetsstyring.pdf

[17] NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.1 De fire kategoriene og rammeverket er definert av Nasjonal sikkerhetsmyndighet, og har forankring i kravene til internkontroll i eForvaltningsforskriften § 15, som gjelder for kommunene. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/ta-i-bruk-grunnprinsippene/

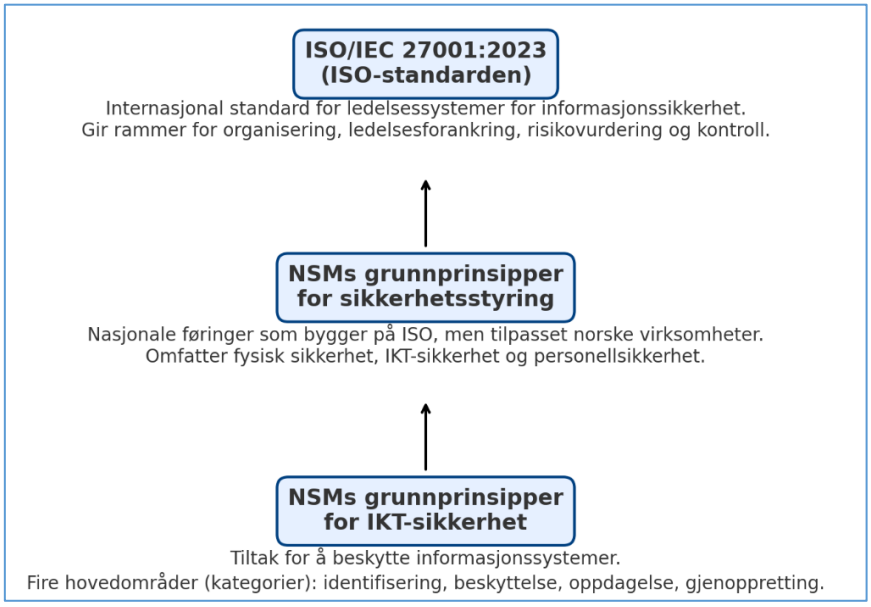
som ikke er det. Tiltakene omfatter både teknologiske og organisatoriske sider, de supplerer eksisterende regelverk og rammeverk, og fremhever sentrale sikringstiltak fra ISO-standarden.

Tiltakene er strukturert rundt fire hovedområder, også omtalt som kategorier: identifisering, beskyttelse, oppdagelse og gjenoppretting. Disse danner grunnlaget for kriteriene i den første problemstillingen i prosjektet og forklares nærmere innledningsvis i kapittel 3.

Grunnprinsipper for personellsikkerhet[18] gir anbefalinger om hvordan virksomheter kan etablere et helhetlig system for å sikre ansatte og andre med tilgang til verdier. NSM peker på at samfunnsutviklingen har ført til at stadig flere får tilgang til virksomheters verdier, noe som gjør personellsikkerhet til en sentral del av det forebyggende sikkerhetsarbeidet. Ledere har et overordnet ansvar for å sikre tilstrekkelig kompetanse og ressurser, og for å bygge en sterk sikkerhetskultur. Gjennom bevisstgjøring og gode rutiner kan virksomheten opprettholde og styrke personellsikkerheten. Disse prinsippene er særlig relevante for prosjektets andre problemstilling.

Kravene i ISO-standarden og NSMs grunnprinsipper har mange berøringspunkter. Begge rammeverkene legger vekt på ledelsesforankring, systematikk og kontinuerlig forbedring av sikkerhetsarbeidet, og grunnprinsippene for IKT-sikkerhet konkretiserer flere av tiltakene fra ISO-standarden.

Figuren nedenfor viser hvordan ISO/IEC 27001:2023, NSMs grunnprinsipper for sikkerhetsstyring og grunnprinsipper for IKT-sikkerhet henger sammen, og hvordan de danner grunnlaget for revisjonskriteriene i den første problemstillingen.



Figur 2.1: Sammenhengen mellom ISO/IEC 27001:2023, NSMs grunnprinsipper for sikkerhetsstyring og grunnprinsipper for IKT-sikkerhet. Kilde: ISO/IEC 27001:2023 og NSM (tilpasset av revisor).

[18] https://nsm.no/getfile.php/134159-1598879548/NSM/Filer/Dokumenter/Grunnprinsipper%20for%20personellsikkerhet%20.pdf

3. SIKKERHETSTILTAK MOT DIGITALE ANGREP

Dette kapittelet handler om problemstilling 1:

> Har kommunen etablert tilfredsstillende sikkerhetstiltak mot digitale angrep i utvalgte IKT-systemer?

I dette kapittelet gir vi først en oversikt over revisjonskriteriene vi vurderer kommunens praksis opp mot. Deretter presenterer vi relevant dokumentasjon som beskriver styringssystemet for informasjonssikkerhet i Lillehammerregionen. Videre gir vi en kort beskrivelse av de to IKT-systemene som undersøkes nærmere – det oppvekstadministrative systemet *Visma Flyt Sikker Sak* og innfordringsverktøyet KK2. Deretter presenteres innhentet informasjon før revisjonen avslutter med en vurdering knyttet til de ulike systemene.

3.1 REVISJONSKRITERIER – PROBLEMSTILLING 1

Se omtalen av ISO-standarden NSMs grunnprinsipper i kapittel 2.2.

For å sikre en solid og helhetlig tilnærming til informasjonssikkerhet, bør virksomheten etablere tiltak og prosesser innen fire hovedkategorier. Disse kategoriene dekker hele livssyklusen for sikkerhetsarbeidet – fra å forstå hva som skal beskyttes, til å forebygge, oppdage og håndtere hendelser som kan true sikkerheten.

Kategori 1: Identifisere og kartlegge

Denne kategorien utgjør fundamentet for virksomhetens arbeid med informasjonssikkerhet. Den handler om å etablere oversikt over hvilke informasjonsverdier[19] som skal beskyttes, hvilke trusler og sårbarheter som finnes, og hvilke rammebetingelser som gjelder – herunder relevante lover, forskrifter og bransjenormer.

Et sentralt element i denne fasen er å identifisere og klassifisere informasjonsverdier, det vil si å vurdere hvilken betydning ulike typer informasjon har for virksomheten, og hvor sensitive de er. Dette omtales ofte som verdisetting, og danner grunnlaget for videre risikovurdering. Verdsettingen skal bidra til å prioritere hvilke verdier (altså hvilken informasjon) som krever særlig beskyttelse, og hvilke konsekvenser det kan få dersom akkurat denne informasjonen blir utilgjengelig, endret eller kommer på avveie.

[19] «Informasjonsverdier» omfatter den informasjonen virksomheten behandler, lagrer eller formidler, og som har verdi for virksomheten eller samfunnet, som for eksempel personopplysninger, finansielle data, teknisk eller operativ informasjon og tjeneste- eller systemdata.

Virksomheten skal benytte en risikovurderingsprosess som er definert for virksomheten, jf. ISO/IEC 27001 punkt 6.1.2. Risikovurderinger skal gjennomføres i planlagte intervaller og ved vesentlige endringer, jf. ISO/IEC 27001 punkt 8.2. Basert på vurderingene skal virksomheten velge hensiktsmessige tiltak ut fra fastsatte risikokriterier, og utarbeide en plan for håndtering av risikoene, inkludert ansvar og tidsfrister, jf. ISO/IEC 27001 punkt 6.1.3.

I tillegg skal virksomheten dokumentere både prosessene for risikovurdering og -håndtering, og resultatene av disse. Dette innebærer å lagre informasjon om hvilke vurderinger som er gjort, hvilke beslutninger som er tatt, og hvilke tiltak som er iverksatt, jf. ISO/IEC 27001 punkt 6.1.2, 6.1.3, 8.2 og 8.3.

Kategori 2: Beskytte og opprettholde (forebygge)

Her ligger tiltakene som skal sikre at systemene er trygge i drift og forblir det over tid. Det inkluderer sikker konfigurasjon[20], tilgangsstyring, opplæring av ansatte, og krav til leverandører. Informasjon skal beskyttes både under bruk, overføring og lagring. Det skal også etableres evne til å gjenopprette data og systemer ved tap eller angrep, blant annet gjennom sikkerhetskopiering og testing av disse. Informasjonssikkerheten skal ivaretas i hele systemets levetid, fra anskaffelse til systemet tas ut av bruk.

Et grunnleggende tiltak for å ivareta informasjonssikkerheten er å sikre at ansatte og kontraktører er klar over og oppfyller sitt ansvar for informasjonssikkerhet. Dette innebærer at alle ansatte må få hensiktsmessig opplæring, samt regelmessig oppdatering på relevante rutiner og prosedyrer (ISO 7.2). Denne anbefalingen er også relevant i behandlingen av problemstilling to, som dreier seg om sikkerhetskultur.

NSM Grunnprinsipp 2.1 er *å ivareta sikkerhet i anskaffelses- og utviklingsprosesser*. Dette innebærer blant annet å minimere risiko for at nye IKT-produkter og tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter. Dette betyr at man må passe på at nye dataprogrammer og digitale løsninger ikke kommer med innstillinger eller tekniske oppsett som gjør systemet lettere å angripe eller utnytte. Det understrekes at virksomhetens ansvar for sikkerheten gjelder uavhengig av om tjenesten er satt ut til leverandør (skytjenester). Virksomheten bør f.eks. sette krav til leverandørens eget system for informasjonssikkerhet.

IKT-systemet er under kontinuerlig endring når løsninger først er satt i drift. Eksempler er oppgradering av enheter og programvare, tilgang til data og tjenester basert på nye brukerbehov, endringer i trusselbildet, nyoppdagede sårbarheter m.m. Det er derfor viktig at konfigurasjonen oppdateres og verifiseres med jevne mellomrom og at avvik registreres, rapporteres og håndteres på en effektiv måte.

Informasjonssikkerhet handler om å beskytte informasjonsverdier. Virksomheten må beskytte informasjonen både ved bruk, overføring (dataflyt) og oppbevaring, slik at den ikke på noe tidspunkt er tilgjengelig for uvedkommende, eller at den er uleselig dersom den kommer på avveie.

[20] Konfigurasjon handler om hvilke innstillinger som er valgt i et datasystem – som hvem som har tilgang, hvilke funksjoner som er aktivert, og hvordan systemet håndterer hendelser. En sikker konfigurasjon innebærer at disse valgene er gjort for å redusere risiko og hindre uautorisert bruk, på samme måte som man låser dører og bestemmer hvem som får nøkkel.

Grunnprinsipp 2.6 handler om å *ha kontroll på identiteter og tilganger*. Målet med prinsippet er at virksomheten har oversikt over identiteter og kontoer i informasjonssystemene og styrer tilgang til ressurser effektivt og i henhold til virksomhetens retningslinjer. Ansatte som har flere rettigheter enn de trenger er et problem i mange virksomheter. Hvis alle brukere har rettigheter til «alt» vil kompromittering av én bruker kunne kompromittere hele IKT-systemet. Kommunen bør derfor ha etablert en formell prosess for å tildele, følge opp og deaktivere administratorkontoer (NSM 2.6.2). Videre bør kommunen bruke multifaktorautentisering for kontoer med tilgang til kritiske systemer eller data (NSM 2.6.7).

Virksomheten bør etablere en evne til å gjenopprette tapte eller endrede data og systemkonfigurasjoner. Dataangrep kan medføre at kritiske konfigurasjoner, programvare eller informasjon endres eller gjøres utilgjengelig, som igjen kan påvirke virksomhetskritiske prosesser. NSM grunnprinsipp 2.9 *Etabler evne til gjenoppretting av data*, har som mål å etablere en metode for sikkerhetskopiering og gjenoppretting av kritiske data. Det er også viktig å teste sikkerhetskopier regelmessig, for å sjekke at sikkerhetskopiene fungerer.

Kategori 3: Oppdage

Denne kategorien handler om å kontrollere sikkerhetstilstanden for å oppdage og fjerne sårbarheter eller forhold av sikkerhetstruende karakter.

NSM grunnprinsipp 3.2 sier at virksomheten skal *etablere en sikkerhetsovervåking*. Å etablere en sikkerhetsovervåking av IKT-systemene er viktig for å oppdage hendelser og legge et grunnlag for å analysere hendelsen. Innsamling og analyse av sikkerhetsrelevant data kan bidra til å oppdage sikkerhetshendelser tidlig, vurdere skadeomfang og hendelsens karakter og forstå hendelsesforløpet. Mangelfull sikkerhetsovervåkning kan innebære at angripere kan skjule tilstedeværelse, handlinger og aktiviteter i virksomhetens informasjonssystemer.

Å registrere hendelser og fremskaffe bevis er et sikringsmål i ISO 27001 (A.8.15, A.8.20). Foreslåtte sikringstiltak inkluderer produksjon, oppbevaring, gjennomgang og beskyttelse av hendelseslogger som dokumenterer brukeraktiviteter, avvik, feil og sikkerhetshendelser. For å sikre sporbarhet skal systemadministratorers og systemoperatørers aktiviteter loggføres særskilt. Hva som anses som "tilstrekkelig sikret" må tolkes i lys av kravene til integritet, tilgjengelighet og gjenopprettbarhet. Det innebærer at loggene må ha høy integritet – altså være beskyttet mot uautorisert endring – være tilgjengelige ved hendelser eller revisjon, og ha sikkerhetskopier. Et konkret eksempel på betydningen av dette er angrepet mot Østre Toten kommune, der angripere slettet logger for å hindre sporbarhet og gjøre etterforskning vanskeligere.

Virksomheten bør også jevnlig teste egen forsvarsevne gjennom å gjennomføre inntrengningstester (penetrasjonstest), slik at mangler og svakheter i den tekniske infrastrukturen kan identifiseres og tettes, samt mangler og svakheter i rutiner, jf. NSM grunnprinsipp 3.4 *Gjennomfør inntrengningstester*.

Kategori 4: Håndtere og gjenopprette (respons)

Hensikten med anbefalingene i denne kategorien er å få på plass aktiviteter for å håndtere hendelser. Dette innebærer å forberede seg på, vurdere, kontrollere og håndtere hendelser, gjenopprette normaltilstand, samt forbedre sikkerheten basert på erfaringer fra hendelseshåndteringen.

Når hendelsen inntreffer er det for sent å utarbeide gode prosedyrer, rapporteringsrutiner, datainnsamling, ledelsesansvar og kommunikasjonsstrategier. Disse må utarbeides og øves jevnlig for å gjøre virksomheten i stand til å forstå, håndtere og gjenopprette normaltilstanden.

Det skal være utarbeidet en hendelseshåndteringsplan for systemet, jf. NSM grunnprinsipp 4.1.1. Planen skal ivareta behovet for kontinuitet ved uønskede hendelser og krise. ISO A.5.26 sier at virksomheten skal reagere på informasjonssikkerhetsbrudd i samsvar med dokumenterte prosedyrer. Videre skal systemene være utformet slik at tilgjengelighet er sikret, jf. ISO A.8.14, dvs. at systemet skal ha tilstrekkelig redundans[21].

Av dette har vi utledet følgende konkrete revisjonskriterier for problemstilling 1.

Identifisere og kartlegge

- Kommunen skal ha gjennomført risikovurdering av systemet.
- Foreslåtte tiltak knyttet til risikovurderingen bør ha blitt gjennomført i henhold til en fastsatt plan, med fastsatt tiltakseier og tidsfrist.
- Kommunen bør oppdatere risikovurderingen i faste intervaller og ved betydelige endringer.

Beskytte og opprettholde

- Det bør være etablert et regime for sikkerhetsoppdatering av systemet.
- Kommunen bør ha kontroll på identiteter og tilganger.
- Kommunen bør bruke multifaktorautentisering for kontoer med tilgang til kritiske systemer eller data.
- Kommunen bør beskytte data i systemet i samsvar med gjennomført klassifisering av systemets informasjonsverdier.
- Kommunen bør ha sikret muligheten til å gjenopprette systemets data.

Oppdage

- Det bør være etablert sikkerhetsovervåking av systemet gjennom at
    - Kommunen sikrer at systemet har logger over systemaktiviteter
    - Systemets logger bør være tilstrekkelig sikret.
- Det bør være gjennomført penetrasjonstest av systemet.

Håndtere og gjenopprette:

- Kommunen bør sørge for at det er utarbeidet en hendelseshåndteringsplan for systemet.
- Kommunens systemer bør ha redundansmuligheter som sikrer tilgjengelighetskrav.

[21] Redundans innebærer at systemet er utstyrt med reservekomponenter eller parallelle løsninger som automatisk overtar funksjonen dersom en del svikter. Dette bidrar til å opprettholde tilgjengelighet og kontinuitet i tjenesten, selv ved tekniske feil eller avbrudd.

3.2 OVERORDNEDE STYRINGSDOKUMENTER FOR INFORMASJONSSIKKERHET

Som en del av kommunens arbeid med å etablere og opprettholde et systematisk arbeid med informasjonssikkerhet, er det utarbeidet sentrale styringsdokumenter. Disse tar blant annet utgangspunkt i kravene i eForvaltningsforskriften. Dokumentene viser også til anbefalinger fra rådgivende aktører som Nasjonal sikkerhetsmyndighet (NSM) og Kommune-CSIRT[22], og bygger dermed i praksis på anerkjente standarder og prinsipper, som ISO/IEC 27001 og NSMs grunnprinsipper for IKT-sikkerhet.

Øverst i denne strukturen står informasjonssikkerhetspolicyen, som fastsetter kommunens overordnede mål, prinsipper og forpliktelser innen informasjonssikkerhet, og som forankrer arbeidet i ledelsen.

For å sette policyen ut i praksis er det også utarbeidet en informasjonssikkerhetshåndbok som beskriver hvordan kommunens sikkerhetsarbeid skal gjennomføres. Håndboken redegjør blant annet for roller, rutiner og tiltak. Sammen danner disse dokumentene et hierarkisk styringssystem der policyen gir retning og forpliktelse, mens håndboken skal sikre praktisk etterlevelse i tråd med kravene til dokumentert informasjon i ISO 27001 og de operative rådene i NSMs prinsipper.[23]

Informasjonssikkerhetspolicy og -håndbok er utarbeidet i fellesskap mellom de tre kommunene i Lillehammerregionen. Øyer kommune hadde i slutten av 2024 tilsyn fra Datatilsynet, og gjorde en revidering av håndboka som følge av tilsynet.[24] Oppdateringene ble diskutert av de tre IT-ansvarlige i Lillehammer, Gausdal og Øyer.

I en e-post til revisjonen opplyses det at den nyeste revisjonen foreløpig ikke er godkjent av kommunedirektørene i Lillehammer og Gausdal. Det er orientert om at felles arbeid med en ny versjon skal starte rett over sommeren 2025. Inntil den reviderte versjonen er godkjent i alle tre kommunene, gjelder versjon 1.1 (vedtatt i januar 2023) for Gausdal og Lillehammer, og versjon 1.2 (vedtatt i desember 2024) for Øyer).[25]

3.2.1 INFORMASJONSSIKKERHETSPOLICY

Informasjonssikkerhetspolicyen for 3:1-kommunene gjelder all behandling av informasjon – både internt og eksternt – og omfatter alt fra muntlig og skriftlig kommunikasjon til digital lagring og bruk av IKT-verktøy. Målet med policyen er å sikre at informasjonsbehandlingen støtter kommunenes tjenester og mål på en lovlig, effektiv og pålitelig måte.

---

[22] Kommune-CSIRT IKS var tidligere sektor-CSIRT for kommunene, men ansvaret for sikkerhetshendelser i kommunesektoren er nå overført til Norsk helsenett SF.CERT.

[23] Dokumentene «Informasjonssikkerhetspolicy-3-1» versjon 1.2 og «Informasjonssikkerhetshåndbok-3-1» versjon 1.2 er mottatt i forbindelse med revisjonen.

[24] https://prod01.elementscloud.no/publikum/Documents/ShowDocument/1e19ac68-b074-44df-9273-d74cf116eb4e/1229689/2063906

[25] Forskjeller mellom ny og tidligere versjon av informasjonssikkerhetspolicy og -håndbok omtales eksplisitt i teksten. Der det ikke er forskjeller, refereres det til dokumentene uten versjonsangivelse.

I policyen presiseres det som et sikkerhetsmål at kommunenes informasjon skal behandles i tråd med lovpålagte og interne krav, og sikres gjennom fysiske, tekniske og organisatoriske tiltak. Det legges særlig vekt på konfidensialitet, integritet, tilgjengelighet og robusthet. Dette innebærer blant annet at informasjon kun skal være tilgjengelig for autoriserte brukere, at den ikke skal endres utilsiktet, og at systemene skal tåle uønskede hendelser og raskt kunne gjenopprettes. For å nå disse målene, beskriver policyen en sikkerhetsstrategi som skal være forankret i linjeledelsen, gjennomføres systematisk og være risikobasert.

Policyen beskriver også konkrete sikkerhetstiltak. Formålet med tekniske, organisatoriske og fysiske sikkerhetstiltak er å beskytte systemer og informasjon ut fra deres behov for konfidensialitet, integritet, tilgjengelighet og robusthet. Tekniske tiltak inkluderer tilgangsstyring, sikkerhetslogging, antivirus, sikkerhetskopiering og segmentering av systemer. Organisatoriske tiltak omfatter rutiner for passord, mobile enheter, fysisk sikring og etterlevelse av personvernlovgivning. Fysiske tiltak handler blant annet om sikring mot innbrudd og brann, kryptering av bærbare enheter og sikker destruksjon av sensitiv informasjon.

Alle ansatte har en viktig rolle i dette arbeidet. De skal kjenne til sikkerhetsmålene, forstå hvilke krav som gjelder for deres informasjonsbehandling, og følge relevante rutiner og retningslinjer. Dette handler om den menneskelige faktoren i sikkerhetsarbeidet og omtales nærmere i revisjonens omtale av problemstilling to.

Tilgangsstyring omtales i den tidligere informasjonssikkerhetspolicyen, men er utdypet som et sentralt prinsipp i den oppdaterte versjonen, som foreløpig kun er vedtatt i Øyer kommune. I denne oppdaterte policyen fremgår det at tilgang til informasjon skal være autorisert, nødvendig og proporsjonal med informasjonsverdien. All systemaktivitet skal loggføres for å sikre sporbarhet og dokumentasjon, i tråd med kravene i GDPR og nasjonalt regelverk. Bruk av databehandlere og leverandører skal reguleres gjennom kontrakter som oppfyller kravene i GDPR artikkel 28 og 29. Eksterne skal kun gis tilgang til kommunens systemer dersom det foreligger en godkjent avtale. Det understrekes også at gradert informasjon skal håndteres i samsvar med gjeldende lovverk for det aktuelle fagområdet.

3.2.2 INFORMASJONSSIKKERHETSHÅNDBOK FOR LILLEHAMMER, GAUSDAL OG ØYER

Informasjonssikkerhetshåndboken beskriver gjeldende retningslinjer og krav til behandling av informasjon i kommunene. Dokumentet gjelder for alle ansatte og samarbeidspartnere som har tilgang til kommunenes informasjonssystemer, og omfatter både digital og fysisk informasjon.

I likhet med informasjonssikkerhetspolicyen, har håndboken som formål å sikre at informasjon behandles i samsvar med gjeldende lovverk og interne krav, og at konfidensialitet, integritet, tilgjengelighet og robusthet ivaretas. Den omfatter både generelle prinsipper og konkrete tiltak for å beskytte informasjon mot uautorisert tilgang, endring og tap.

Håndboken beskriver roller og ansvar innen informasjonssikkerhet og behandling av personopplysninger i kommunen. Det presiseres at «*Alle ansatte i kommunen skal overholde informasjonssikkerhetsreglementet, og beskytte verdien som ligger av informasjon i fagsystemer, elektroniske enheter og infrastruktur*». Videre beskrives ledelsens ansvar: kommunedirektøren har det overordnede ansvaret for informasjonssikkerheten, mens linjeledelsen har ansvar for den praktiske oppfølgingen. Det framkommer ikke ytterligere av håndboken hva «praktisk oppfølging» innebærer. Systemeiere og systemansvarlige har ansvar for sikkerheten i de enkelte

IT-systemene. I tillegg skal fagansvarlig for informasjonssikkerhet og personvernombudet skal bistå med rådgivning og kontroll. Dette vil vi også komme tilbake til under problemstilling nr. 2 senere i rapporten.

Håndboken beskriver en rekke tekniske og organisatoriske tiltak. Dette inkluderer tilgangsstyring basert på tjenstlig behov, bruk av to-faktorautentisering, logging og sporbarhet, samt rutiner for sikker sletting og avhending av utstyr. Det er også etablert retningslinjer for bruk av mobile enheter, e-post og skylagring.

Internkontrollen er forankret i håndboken og skal støttes av underliggende prosedyrer og verktøy som skal være tilgjengelige i kommunenes kvalitetssystemer, TQM. Det vises blant annet til behandlingsprotokoller, risikovurderinger, personvernkonsekvensvurderinger (DPIA[26]), databehandleravtaler og rutiner for tilgangsstyring og logging. Det står også at det skal gjennomføres årlig ledelsesgjennomgang og revisjon av sikkerhetsarbeidet.[27]

Det generelle rammeverket som er beskrevet i håndboken, danner et viktig bakteppe for den videre gjennomgangen. I de påfølgende delkapitlene presenteres en nærmere gjennomgang av hvordan dette er fulgt opp i praksis, basert på tilgjengelige data.

3.3 INFORMASJONSSIKKERHET I VISMA FLYT SIKKER SAK

Vi starter med å presentere innhentet informasjon, deretter vurderer vi funnene opp mot de konkrete revisjonskriteriene. Opplysningene baserer seg på mottatt dokumentasjon, intervju med systemansvarlige i kommunen som har ansvar for Visma Flyt Sikker Sak og svar på skriftlige henvendelser til oppnevnt kontaktperson i kommunen.

3.3.1 OM VISMA FLYT SIKKER SAK

Visma Flyt Sikker Sak er et digitalt saksbehandlingssystem i skyen som lar ansatte i skole, barnehage og andre offentlige virksomheter håndtere og arkivere sensitive personopplysninger på en sikker, enkel og trygg måte. Systemet brukes spesielt til saker som involverer barn og unge.

I 2018 inngikk de tre kommunene databehandleravtaler med Visma Enterprise AS; løsningen ble satt i drift ved skolestart høsten 2019. Avtalen omfatter et skybasert oppvekstadministrativt system som håndterer et stort volum personopplysninger om både ansatte og tjenestemottakere med familie. Anskaffelsen ble gjort i fellesskap av Øyer, Lillehammer og Gausdal. Det er mange applikasjoner innenfor Visma. Visma Flyt Sikker Sak, som undersøkes nærmere her, er en spesialisert applikasjon for sikker elektronisk saksbehandling, særlig rettet mot håndtering av sensitive saker.

[26] DPIA (Data Protection Impact Assessment): En vurdering av personvernkonsekvenser som gjennomføres for å identifisere og redusere risiko ved behandling av personopplysninger, i tråd med kravene i personvernforordningen (GDPR) artikkel 35.

[27] Revisjonen har ikke gjennomgått rutiner og dokumentasjon som er lagret i TQM-systemet, utover den dokumentasjonen som er etterspurt og mottatt i tilknytning til de IKT-systemene som inngår i undersøkelsen.

I bestillingsgrunnlaget uttrykte de tre kommunene at målsettingen var å få «en fremtidsrettet og brukervennlig løsning for administrativt arbeid innenfor oppvekstområdet» med sikker innlogging og rollestyring, slik at brukerne kan nå alle funksjoner uavhengig av hvor de jobber eller hvilken enhet de bruker.

Leverandøren beskriver selv tjenesten som «en helhetlig sammensetning av skytjenester for administrasjon av oppvekstsektoren, fullt integrert med Visma Community». All drift, oppgradering og overvåking håndteres av Visma. I Lillehammer kommune omfatter systemet om lag 13.000 registrerte brukere.

Tabellen under viser ansvarsfordeling for informasjonssikkerhet, slik det framkommer av databehandleravtalen med Visma:

Aktør	
Lillehammer Kommune (behandlingsansvarlig)	• Sikre at eget nettverk, klienter og tredjepartsløsninger fungerer • Etterleve avtalens krav, herunder intern opplæring og korrekt bruk • Følge opp integrasjoner med tredjeparter som leverandøren ikke eksplisitt drifter
Visma Enterprise AS Databehandler	• Drift, overvåking og support av Saas-tjenestene[28] • Gjennomføre organisatoriske, tekniske og fysiske tiltak som oppfyller GDPR art. 32
Ikomm (single Point of Contact)	• En samlet kontaktflate mellom kommune og leverandør • Mottar feilmeldinger fra kommune og videreformidler dem til Visma • Bekrefter retting og lukking overfor kommunen.

3.3.2 IDENTIFISERE OG KARTLEGGE

Vi så i kapittel 2.2.2 at denne kategorien innen NSMs grunnprinsipper handler om å forstå virksomhetens verdier, risikoer og rammebetingelser.

Informasjonssikkerhetshåndboka legger føringer for at det skal utarbeides ROS-analyser ved innfyring av nye systemer. Denne skal utarbeides før man tar systemet i bruk, ved tekniske endringer eller utvidelser av eksisterende systemer. ROS-analysen beskrive formålet med systemet og vurdere om datainnhenting omfattes av relevant lovverk. Det presiseres at leverandørens ROS-analyse bør etterspørres og brukes som grunnlag, men den kan ikke erstatte kommunens egen ROS. Hensikten er å identifisere risiko og iverksette tiltak, og dersom det fortsatt gjenstår høy restrisiko, skal kommunedirektøren ta stilling til videre bruk av systemet.

Videre presiserer håndboka på s 19 at det skal gjøres en vurdering av om det skal utarbeides DPIA, altså en vurdering av personvernet til de registrerte i et datasystem ivaretas:

[28] En skybasert SaaS-løsning (Software as a Service) er en programvare som leveres over internett, der leverandøren har ansvar for drift, vedlikehold og sikkerhet. Brukerne får tilgang til tjenesten via nettleser, uten å installere programvaren lokalt.

5.4 Personkonsekvensvurdering (DPIA)

Dersom det er sannsynlig at en type behandling av personopplysninger vil medføre høy risiko for folks rettigheter og friheter, skal den behandlingsansvarlige vurdere hvilke konsekvenser den planlagte behandlingen vil ha for personvernet. En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de registrerte (f.eks. innbygger, ansatte, elever, pasienter) i valgt datasystemet ivaretas.
Artikkel 35 i personvernforordningen (GDPR) definerer når det er påkrevd å gjøre en personvernkonsekvensanalyse, hva den skal inneholde og hvem som skal gjennomføre den. Personvernombudet skal godkjenne DPIA, samt delta i utarbeidelsen av dokumentet. Mal for personvernkonsekvensvurdering finnes i TQM. Dokumentet skal lagres i DigiOrden eller lignende system.

Når det gjelder roller og overordnet ansvarlig, framkommer det av informasjonssikkerhetshåndboken at;

- Systemeier er ansvarlig for å ivareta informasjonssikkerheten i fagsystemene/IT-systemene. Systemeier har også ansvar for å utarbeide risikoanalyse og registrere personopplysninger fra fagsystemene i behandlingsprotokollen, i tillegg til å vurdere om det skal utarbeides DPIA. Systemeier utpeker systemansvarlig.
- Systemansvarlig er ansvarlig for daglig å forvalte systemet. Rollen som systemansvarlig omfatter tilgangsstyring, brukerstøtte og å initiere og gjennomføre ROS-arbeid sammen med systemeier.

System for risikovurderinger

Det er opplyst at de tre kommunene bruker en felles mal for utarbeidelse av ROS-analyser. Det finnes ingen skriftlig, detaljert prosedyre, men ved behov gis veiledning i gjennomføringen, og rådgivere deltar som regel i prosessen.[29]

Revisjonen har mottatt felles ROS-analyse og DPIA for VFSS fra de tre kommunene, datert 2023. ROS-analysen benytter fargeklassifisering (rød, gul, grønn) med tilhørende tallskala for å angi alvorlighetsgrad. Her forklares risiko slik:

		Ubetydelig konsekvens	Liten konsekvens	Moderat konsekvens	Alvorlig konsekvens	Katastrofal konsekvens
		1	2	3	4	5
Svært høy sannsynlighet	5	Moderat (5)	Moderat (10)	Høy (15)	Katastrofal (20)	Katastrofal (25)
Høy sannsynlighet	4	Lav (4)	Moderat (8)	Høy (12)	Høy (16)	Katastrofal (20)
Moderat sannsynlighet	3	Lav (3)	Moderat (6)	Moderat (9)	Høy (12)	Høy (15)
Liten sannsynlighet	2	Lav (2)	Lav (4)	Moderat (6)	Moderat (8)	Moderat (10)
Svært liten sannsynlighet	1	Lav (1)	Lav (2)	Lav (3)	Lav (4)	Moderat (5)

Mørk rødt:
Strakstiltak. (Meget kritisk = fare for liv og helse)
Rødt:
Tiltak må iverksettes – utarbeid tiltaksplan
Gult:
Det må vurderes om tiltak skal iverksettes
Grønt:
Ikke nødvendig å iverksette tiltak

[29] Ref. felles e-post fra de tre IT-ansvarlige i 3-1-samarbeidet, 13.06.2025.

I intervju er det opplyst at risikoer klassifisert som røde (samlet verdi 10 eller høyere) skal følges opp med tiltak og beskrivelse. For risikoer vurdert som gule eller grønne viser ROS-analysen til eksisterende tiltak, men angir ikke ytterligere anbefalte tiltak, ansvarlig for oppfølging eller frist. Revisjonen observerer at dette ikke er i tråd med hva som fremgår i forklaringen av tabellen i ROS-analysen vi har mottatt, der det står at det på nivå gult skal vurderes om tiltak skal iverksettes.

Alle tre kommunene har opplyst at det er gjennomført en ROS-analyse i 2024, men at denne ikke er loggført.

Gjennomgangen av ROS-analysen viser at ingen av de vurderte risikomomentene er gitt en samlet risikoverdi høyere enn 9 i risikomatrisen. Dette innebærer at alle identifiserte risikoer er plassert innenfor det som i matrisen defineres som lav til moderat risiko.

Vurderingene omfatter blant annet behandling av store mengder sensitiv informasjon og komplekse dataflyter. Revisjonen har observert konkrete eksempler på tilsynelatende likeartede hendelser som er vurdert ulikt i analysen. Det fremgår ikke av dokumentasjonen hvordan slike forskjeller er begrunnet.

For eksempel: konsekvensen av at sensitiv informasjon kommer på avveie på grunn av feil i tilgangsstyring er vurdert som «svært alvorlig» i risikoanalysen. Konsekvensen av at samme type informasjon kommer på avveie på grunn av feil utsending av e-post, er imidlertid vurdert som «mindre alvorlig». I begge tilfeller er resultatet det samme – at sensitiv informasjon kan komme på avveie – men konsekvensen er vurdert ulikt.

I ROS-analysen er hendelsen «opplysninger om personer med hemmelig adresse blir tilgjengelig for uvedkommende» vurdert i flere ulike scenarier. I ett scenario er konsekvensen angitt som lav, mens den i et annet scenario er angitt som høy. Det fremgår ikke av analysen hvorfor konsekvensen er vurdert ulikt mellom scenariene.

DPIAen følger en standard mal og vurderer først personopplysningene som behandles av systemet, som for eksempel om de inneholder særlige kategorier av personopplysninger, om det gjennomføres i stor skala eller om de omfatter sårbare grupper. Videre er det blant annet foretatt en beskrivelse av behandlingen som redegjør for formål, behandlingsgrunnlag, behandlingens art, behandlingens omfang, konteksten behandlingen utføres i, og hvilke tekniske og organisatoriske tiltak som er gjort for å ivareta personvernkrav. Her vises det blant annet til ROS-vurderingen, i tillegg til at det nevnes tiltak som pålogging via tofaktor og ID-porter, at systemene er tilgang- og rollestyrt, og at foresatte kun kan se opplysninger om egne barn og elever kun om seg selv. Flere av de samme tiltakene som nevnes i DPIAen står også som eksisterende tiltak i ROS-analysen.

Oppfølging av identifiserte tiltak

Ifølge opplysninger fra intervjuene er tidligere identifiserte røde risikoer fulgt opp med tiltak. Disse risikoområdene er derfor ikke lenger synlige i den siste ROS-analysen. Ved siste vurdering (i 2024) ble det opplyst at det ikke ble identifisert nye forhold som krevde oppfølging.

Den mest fremtredende risikoen i den felles ROS-analysen fra 2023 skal ifølge informantene ha vært at brukere forlater skjermer uten å låse dem. Dette er dokumentert i ROS-analysen med samlet risikoverdi 9 i risikomatrisen. Det ble forklart at det er iverksatt tiltak for å redusere denne risikoen, blant annet gjennom en intern

informasjonskampanje og automatisk skjermlås etter inaktivitet. I og med at risikoen er vurdert til verdi 9, framkommer det ikke tekniske eller organisatoriske tiltak for oppfølging i ROS-analysen.

Periodisk oppdatering av ROS-analyser
Ifølge opplysninger fra de tre systemansvarlige i kommunene gjennomføres det en felles risikovurdering én gang i året, vanligvis i oktober eller november. I tillegg forteller de at vurderingene skal oppdateres dersom det skjer vesentlige endringer i systemene. Sist oppdaterte dokumentasjon av ROS-analyse er fra 2023. Det ble i intervjuene opplyst at de gjennomførte en ny ROS-analyse i 2024. Systemansvarlige i alle tre kommunene opplyste at det ved denne gjennomgangen ikke ble identifisert nye risikoer eller endringer. Det er derfor ikke er loggført en ny ROS-analyse for 2024.

3.3.3 BESKYTTE OG OPPRETTHOLDE

Sikkerhetsopplæring
I sikkerhetshåndboken er det definert at systemansvarlig har hovedansvar for å gi opplæring til brukerne av hvert enkelt fagsystem og for å følge opp at informasjonen forvaltes forsvarlig, mens enhetsleder – som del av linjeansvaret – skal sikre at opplæring faktisk blir gjennomført og dokumentert:

«Systemansvarlig (…) har hovedansvar for å gi opplæring til ansatte av fagsystemene/IT-systemene om forsvarlig forvaltning av informasjonen» (s. 14). «Virksomhetsleder må sørge for å etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid. Virksomhetsleder må kunne dokumentere at den opptrer i samsvar med reglene» (s. 13).

Da systemet var nytt i 2019, ble det gjennomført en felles oppstarts- og opplæringsrunde. Det opplyses i intervju at opplæring av nye brukere i systemet gjennomføres av den enkelte skole i Gausdal. Rektor og inspektør, som har skoleadministrasjonsrollen, har ansvar for å gi nødvendig opplæring til nyansatte slik at de kan bruke systemet. Prinsippet har vært at de ansatte lærer systemet mens de jobber med konkrete saker.

Det fremgår at opplæringen gis ved behov, og Øyer og Lillehammer beskriver en tilsvarende praksis. Det er ikke fremkommet informasjon om at det finnes nedskrevne rutiner for opplæring og dokumentasjon av denne i tilknytning til bruk av fagsystemet.

Ansattes vurderinger av opplæringen innen digital sikkerhet er omtalt under problemstilling 2. Det samme gjelder ledernes oppfatning av sitt ansvar og hvilke forutsetninger de har for å ivareta dette ansvaret.

Regime for sikkerhetsoppdatering av systemet
Når det gjelder sikkerhetsoppdatering av systemet, beskriver Informasjonssikkerhetshåndboken ansvar og arenaer for å holde kommunenes fagsystemer oppdaterte.

Ansvaret for den tekniske gjennomføringen legges på IT-driftsleverandøren, som skal sørge for at informasjonssikkerheten «ivaretas i infrastruktur, maskinvare og sikkerhetssystemer», og krever at dette forankres i driftsavtaler og følges opp gjennom revisjon og kontroll. (s. 14)

Systemeier pålegges i hht. sikkerhetshåndboken å invitere IT-drift og informasjonssikkerhetsansvarlig til en årlig informasjonssikkerhetsgjennomgang. Formålet er å oppdatere risikovurderingen og identifisere tiltak, noe som også kan omfatte behov for tekniske oppdateringer. (s. 16)

I databehandleravtalen mellom kommunen og Visma fremgår det på s. 3 at «Databehandler skal sørge for et høyt sikkerhetsnivå i sine produkter og tjenester. Dette skal skje ved organisatoriske, tekniske og fysiske sikkerhetstiltak, i henhold til kravene til informasjonssikkerhet som fremgår av GDPR artikkel 32».

Opplysninger om hvor ansvaret for oppdateringer av systemet ligger, bekreftes av kvalitet- og-sikkerhetssjef i Lillehammer kommune som uttalte at systemet er en skybasert tjeneste, der leverandør jevnlig oppdaterer dette.

Tilgangsstyring
Informasjonssikkerhetshåndboken beskriver prinsipper for tilgangsstyring. Lederen er ansvarlig for at ansattes gis tilgang til systemer og programmer og at tilgangene til enhver tid er begrenset til kun det de har behov for i jobben.

Intervjuene med systemansvarlige i de tre kommunene viser at multifaktorautentisering er etablert som standard for tilgang til Visma Flyt Skole (VFSS). Det opplyses at innlogging skjer via BankID eller tilsvarende løsninger som oppfyller kravene til autentiseringsnivå 4, i tråd med nasjonale sikkerhetskrav.30.

Revisjonen har mottatt rutiner for tilgangsstyring i Visma Flyt Skole (VFSS) fra Lillehammer, Øyer og Gausdal. Gjennomgangen viser at alle tre kommuner har etablert rutiner med lik oppbygging og innhold, og at tilgangsstyring er en del av den løpende driftsoppfølgingen. Rutinene beskriver hvordan roller tildeles og justeres ved skolestart og gjennom året, og det fremgår at tilgangene gjennomgås systematisk ved oppstart av nytt skoleår, basert på informasjon fra skolene. Endringer og behov for å aktivere eller fjerne tilganger håndteres fortløpende. Enhetsleder Barnehage og skole i Lillehammer forteller at de har oversikt over hvem som har tilgang ved at administrator kan gå inn på den enkelte rolle i VFSS og se antall brukere og hvem de er.

Følgende fremgår eksplisitt i alle tre rutiner: Administrator skal ved skolestart og gjennom året aktivere eller deaktivere tilganger basert på informasjon og behov fra skolene (VFS, VFSS, VFT).
Det er likevel enkelte forskjeller mellom kommunene. Rutinene for Lillehammer og Øyer inneholder en mer detaljert beskrivelse av roller enn rutinen for Gausdal. I tillegg fremgår det kun i rutinene for Lillehammer og Øyer at:

- Tilgang til Sikker Sak avsluttes automatisk når en stilling avsluttes.
- Ved skolebytte mister ansatte automatisk tilgang til tidligere skole(r) i Sikker Sak.

Opplysningene om hvordan tilgangene håndteres i praksis er bekreftet gjennom intervjuene med systemansvarlige i de tre kommunene. Informantene beskriver en felles forståelse og praksis, der tilgangene

[30] Autentiseringsnivå 4 er det høyeste nivået i det norske rammeverket for elektronisk identitet og autentisering, og brukes der det stilles strenge krav til sikkerhet – for eksempel ved tilgang til sensitive personopplysninger eller kritiske systemer. Ref. Digdir.no

gjennomgås ved skolestart og justeres løpende gjennom året, i tråd med informasjon fra skolene. Dette gjelder selv om innholdet i de skriftlige rutinene varierer noe mellom kommunene.

Tilgangsstyringen er i stor grad automatisert og knyttet til ansettelsesforhold. Når en ansatt registreres i personalsystemet (Agresso), synkroniseres informasjonen automatisk med Visma-systemene. Dette gir tilgang til relevante systemer og roller uten manuell behandling. Ved avsluttet arbeidsforhold deaktiveres tilganger automatisk. Systemansvarlig forteller at når ansatte bytter skole, hender det at det må gjøres manuelle justeringer. Rutiner for slik manuell håndtering er ikke dokumentert.

Revisjonen har ikke mottatt dokumentasjon som beskriver hvordan administratorrettigheter forvaltes. Det fremgår imidlertid av intervjuene med systemansvarlige at det kun er et fåtall personer som har slike rettigheter, og at de ansvarlige har oversikt over hvem dette gjelder. Det er heller ikke etablert en fast prosess som sikrer at rettighetene er avgrenset, tidsbegrenset og gjenstand for jevnlig kontroll.

Klassifisering av systemets informasjonsverdier

I informasjonssikkerhetshåndboken for kommunene fremgår det at informasjonens innhold og hvilken sammenheng den behandles i, skal ligge til grunn for vurdering av sikkerhetsbehov. Det vises til prinsippene om konfidensialitet, integritet og tilgjengelighet, og det understrekes at sensitive og virksomhetskritiske data skal behandles i egnede fagsystemer. I den oppdaterte håndboka til Øyer kommune (s.22), fremgår det i tillegg at systemene skal ha «systemeiere som klassifiserer informasjonen i systemene og definerer korrekte tilgangsnivåer».

Håndboka legger også føringer for at alle systemenes behandling for informasjonssikkerhetsgjennomgang skal utgjøre grunnlaget for systemoversikten som skal dokumenteres i DigiOrden eller regneark. Det er også føringer for bruk av behandlingsprotokoll.

I intervjuer får revisjonen opplyst at IT-ansvarlige i kommunene har oversikt over systemer og personopplysninger, basert på behandlingsprotokoller, ROS-analyser og DPIAer for de fleste fagsystemer. Protokollene inneholder informasjon om hvilke personopplysninger som behandles, formål med behandlingen og hvilke systemer som benyttes. På spørsmål fra revisjonen om kommunene har gjennomført en klassifisering av informasjonsverdiene i ikt-system på et overordnet, var svaret at de hittil ikke har «gjort noe systematisk arbeid for å kartlegge og kategorisere alle [sine] informasjonsverdier». Det er heller ikke «gjennomført noen klassifisering på overordnet nivå».

I intervjuene med ansatte som arbeider med systemet, beskrives Visma Flyt Skole som et system med høy verdi for kommunens virksomhet. Det opplyses at systemet inneholder personsensitiv informasjon. For VFSS er det gjennomført både risikovurdering og personvernkonsekvensvurdering (DPIA), noe som fremgår av dokumentasjon mottatt i revisjonen. Revisjonen har mottatt et vedlegg til avtalen mellom Visma og kommunene som gir oversikt over hvilke personopplysninger som behandles i VFSS. Dette dokumentet danner grunnlag for klassifisering av systemets informasjonsverdier. Systemet behandler opplysninger om ansatte, tjenestemottakere, pårørende og andre kontaktpersoner, inkludert både vanlige personopplysninger og jobbrelatert informasjon.

Gjenopprettelse av data/ test av sikkerhetskopi
VFSS er en skytjeneste, og avtalen mellom kommunene og leverandøren beskriver hvordan sikkerhetskopiering skal håndteres.

I avtalen mellom kommunen og Visma framkommer det at Visma, som leverandør, er ansvarlig for sikkerhetskopiering og gjenoppretting av data i løsningen. Det fremgår av avtalen at det tas flere sikkerhetskopier daglig, som lagres geografisk atskilt fra driftsmiljøet. Data lagres i datasentre i Europa i samsvar med europeiske personvernregler. Gjenoppretting av data er mulig for inntil én måned tilbake i tid. Tjenesten benytter minst to uavhengige internettforbindelser, med automatisk overføring ved avbrudd for å sikre tilgjengelighet.[31]

Avtalen beskriver at hver kommune har sin egen database i Visma Flyt Skole, (som VFSS er en del av). Sikkerhetskopier (backup) lagres i inntil ett år før de automatisk overskrives. Dersom behov oppstår, kan data gjenopprettes helt ned til det eksakte minuttet – innen én uke etter hendelsen – ved forespørsel fra kommunen. I tillegg finnes det en tilsvarende historikk for endringer i sentrale databasetabeller. Dette gjør det mulig å gjenopprette deler av databasen, dersom kommunen som behandlingsansvarlig ber om det.

Backupene er kryptert og lagres på flere lokasjoner hos Visma IT i Oslo. Avtalen bekrefter også at alle datasentre følger anerkjente industristandarder for fysisk sikkerhet og driftssikkerhet, inkludert ISO-standarden.[32]

3.3.4 OPPDAGE

Sikkerhetsovervåking - logg som viser systemaktiviteter /Hendelseslogg
Informasjonssikkerhetshåndboken slår fast at alle kommunale fagsystemer skal føre aktivitets- og hendelseslogger som gjør det mulig å spore uønskede hendelser når det er nødvendig. Konkret kreves det at alle søk, endringer og slettinger i systemer som behandler personopplysninger registreres, og at systemeier eller leder kan gjennomgå loggene ved behov.[33]

Systemansvarlige i de tre kommunene forteller at de er kjent med at all aktivitet logges i VFSS. Det opplyses at hendelseslogg ikke gjennomgås regelmessig, men at de gjennomgår denne ved behov – for eksempel dersom det oppstår en konkret hendelse.

Systemansvarlige i de tre kommunene opplyser at de ikke kjenner til hvordan logger i VFSS beskyttes. Flere har imidlertid erfart at det har vært mulig å hente ut historikk ved behov, for eksempel i forbindelse med hendelseshåndtering.

Penetrasjonstest

[31] Ref. dokument «Bilag 1-8 SSA-L LØG» s. 13
[32] Ibid s. 14
[33] I den oppdaterte informasjonssikkerhetshåndboken for Øyer kommune er kravene til logging utvidet og omtalt i et eget kapittel

Visma er ISO/IEC 27001-sertifisert. Denne standarden stiller krav til systematisk arbeid med informasjonssikkerhet, herunder håndtering av sårbarheter og gjennomføring av sikkerhetstesting.[34] I intervjuene med systemansvarlige i kommunene opplyses det at de ikke er kjent med om det er gjennomført penetrasjonstesting av Visma Flyt-systemene.

3.3.5 HÅNDTERE OG GJENOPPRETTE

Hendelseshåndteringsplan

De overordna styringsdokumentene til kommunen fremhever betydningen av at systemene de benytter må ha beredskapstiltak som bidrar til å begrense skade og at kommunen raskt kommer tilbake til normal drift.

Det fremgår i avtalen mellom kommunen og Visma at leverandøren er «ansvarlig for gjenopprettingsplaner og beredskapsplaner knyttet til løsningen» (s. 13). Videre beskriver avtalen responstid fra leverandøren knyttet til ulike feilsituasjoner ut fra alvorsgrad. Avtalen fastslår også følgende (s. 16): «Leverandøren [skal] etablere en hendelsesrapport, som inkluderer beskrivelse,
bakenforliggende årsak, samt tiltak som er truffet eller planlagt for å hindre at en slik
hendelse skjer igjen. Rapporten blir tilgjengeliggjort for Kunden.»

Redundansmulighet

Redundans innebærer at systemet er utstyrt med reservekomponenter eller parallelle løsninger som automatisk overtar funksjonen dersom en del svikter. Dette bidrar til å opprettholde tilgjengelighet og kontinuitet i tjenesten, selv ved tekniske feil eller avbrudd.

I avtalen mellom kommunen og Visma fremgår det blant annet at deres skytjenester benytter minst to uavhengige internettforbindelser til datasenteret. Ved avbrudd skjer automatisk overføring til en fungerende forbindelse, vanligvis uten at tjenesten påvirkes.

3.3.6 REVISJONENS VURDERING – VISMA FLYT SIKKER SAK

Revisjonskriterier:

Identifisere og kartlegge

- **Kommunen skal ha gjennomført risikovurdering av systemet.**
- **Foreslåtte tiltak knyttet til risikovurderingen bør ha blitt gjennomført i henhold til en fastsatt plan, med fastsatt tiltakseier og tidsfrist.**
- **Kommunen bør oppdatere risikovurderingen i faste intervaller og ved betydelige endringer.**

Samlet vurderes kriteriene knyttet til kommunens arbeid med ROS-analyser innenfor VFSS som oppfylt.

Informasjonssikkerhetshåndboken legger føringer for at kommunene skal gjennomføre risikovurderinger og DPIAer på systemer som behandler personopplysninger.

[34] https://www.visma.com/trust-centre/vismaclouddelivery

Våre undersøkelser viser at kommunene har utarbeidet DPIA og en felles ROS-analyse for systemet, og av loggen fremgår det at ny analyse gjennomført i 2023 erstattet den tidligere for perioden 2019–2023. Det er også opplyst i intervju at en ny gjennomgang ble gjort i 2024, uten at denne er loggført.

Metodikken som brukes gir en risikoklassifisering med farge- og tallskala etter alvorlighetsgrad. For risikoer vurdert til «rød» eller «gul», skal det vurderes tiltak, mens på risikoer som er kategorisert som «grønne» er det ikke krav om at det skal iverksettes tiltak. Malen legger videre opp til at det da skal foreslås anbefalte tiltak, ansvarlig for oppfølging og frist for gjennomføring. I ROS-analysen revisjonen har sett på er det ingen risikoer som er klassifisert som røde, og risikoene klassifiserte som «gule» har ikke beskrevet noen tiltak. Etter revisjonens forståelse samstemmer ikke veiledningen i ROS-analysen med informantenes forståelse av hvilke risikoer som krever at man beskriver tiltak i ROS-vurderingen. I ROS-vurderingen vi har sett på, er det ikke oppført noen tiltak på risikoer som er markert som «gule» selv om det i henhold til veiledningen skal være iverksatt tiltak her.

Revisjonen stiller spørsmål ved at kommunen ikke har identifisert risikoer og sårbarheter i systemet som vurderes til høyeste alvorlighetsnivå. VFSS behandler store mengder sensitive personopplysninger og omfatter barn og unge. Sikkerhetshendelser innenfor dette systemet kan få alvorlige konsekvenser for sårbare grupper. Våre undersøkelser indikerer også at det er noe inkonsekvens i vurderingene av likeartede hendelser.

Samlet sett viser revisjonens undersøkelser av kommunenes arbeid med ROS-analyser innen VFSS at det kan være behov for å styrke kompetansen hos dem som gjennomfører ROS-analysene om hvordan en jobber risikobasert innen dette feltet.

Beskytte og opprettholde

- **Det bør være etablert et regime for sikkerhetsoppdatering av systemet.**

Revisjonen vurderer at kriteriet er oppfylt.

Informasjonssikkerhet er omtalt i kommunens informasjonssikkerhetshåndbok, og det fremgår at IT-driftsleverandøren skal sørge for at informasjonssikkerheten ivaretas i systemet, og at dette skal forankres i driftsavtalen mellom kommunen og leverandøren.

Det fremgår av databehandleravtalen med Visma at det er etablert et regime for sikkerhetsoppdatering.

- **Kommunen bør ha kontroll på identiteter og tilganger.**
- **Kommunen bør bruke multifaktorautentisering for kontoer med tilgang til kritiske systemer eller data.**

Revisjonen vurderer at kommunene har kontroll på identiteter og tilganger.

Kommunens informasjonssikkerhetshåndbok beskriver prinsipper for tilgangsstyring, blant annet at brukere skal ha lavest mulig rettighetsnivå og at tilgangene skal være styrt av roller. Hver av kommunene har i tillegg rutiner for tilgangsstyring, som revisjonen har mottatt.

Intervjuer viser at kommunene har etablert flere gode og risikoreduserende praksiser for tilgangsstyring. Automatiseringen av tilganger basert på ansettelsesforhold, kombinert med bruk av multifaktorautentisering og en etablert rutine for tilgangsstyring, gir et solid grunnlag for sikker tilgangskontroll. Det er også positivt at det er få personer med administratorrettigheter, og at disse er kjent med sitt ansvar for å tildele og justere tilganger for andre brukere.

Bruken av multifaktorautentisering i alle tre kommuner vurderes som en godt etablert sikkerhetsmekanisme for tilgang til VFSS. At innlogging skjer via BankID eller tilsvarende løsninger som tilfredsstiller autentiseringsnivå 4, innebærer at kommunene har valgt en løsning som gir høy grad av beskyttelse for kontoer med tilgang til sensitive og kritiske data. Dette er i tråd med anbefalte krav til sikker autentisering.

- **Kommunen bør beskytte data i systemet i samsvar med gjennomført klassifisering av systemets informasjonsverdier.**

Revisjonen vurderer at kommunene har etablert flere viktige tiltak for å sikre dataene som behandles i VFSS, men mangler en klassifisering av informasjonen som sikrer at sikkerhetstiltakene er tilpasset informasjonsverdienes betydning.

Kommunene Lillehammer, Øyer og Gausdal har etablert flere sentrale tiltak som bidrar til å ivareta personvern og informasjonssikkerhet i VFSS. Dette omfatter blant annet risikovurdering, personvernkonsekvensvurdering (DPIA) og oversikt over behandlingsaktiviteter basert på behandlingsprotokoller. Protokollene gir informasjon om hvilke personopplysninger som behandles, formål med behandlingen og hvilke systemer som benyttes. Dokumentasjonen fra leverandøren gir i tillegg oversikt over hvilke typer personopplysninger som behandles i VFSS, som omfatter både vanlige og sensitive opplysninger knyttet til ansatte, tjenestemottakere, pårørende og andre kontaktpersoner.

Det fremgår imidlertid av intervjuer at det ikke er foretatt en klassifisering av informasjon utover dette.[35]

Med den dokumentasjonen og oversikten som allerede foreligger, har kommunene et godt utgangspunkt for å klassifisere informasjonsverdiene de behandler. Et slikt arbeid ville gitt et tydelig grunnlag for å tilpasse og prioritere sikkerhetstiltak i tråd med informasjonsverdienes betydning, og styrket dokumentasjonen for at data beskyttes i samsvar med gjennomført klassifisering. Dette er et helt sentralt grunnlag for kommunens risikobaserte arbeid.

- **Kommunen bør ha sikret muligheten til å gjenopprette systemets data.**

[35] Når det gjelder Øyer, ble det i oppstartmøte informert om at kommunen har flyttet samtlige av kommunens fagsystemer over i sky, og at de samtidig gjennomførte en overordnet IKT-ROS (risiko- og sårbarhetsanalyse) for å få oversikt over prioriterte risikoområder. Kartleggingen identifiserte omtrent 150 systemer som krever innlogging og kan utgjøre en sikkerhetsrisiko.

Revisjonen vurderer at kommunene har sikret muligheten til å gjenopprette systemets data.

VFSS er en skytjeneste, og avtalen mellom kommunene og leverandøren beskriver hvordan sikkerhetskopiering skal håndteres.

Oppdage

- **Det bør være etablert sikkerhetsovervåking av systemet gjennom at**
    - **Kommunen sikrer at systemet har logger over systemaktiviteter**
    - **Systemets logger bør være tilstrekkelig sikret.**

Revisjonen vurderer at kommunen har oppfylt kriteriene.

Det fremgår av informasjonssikkerhetshåndboken at kommunens fagsystemer skal føre aktivitets- og hendelseslogger som gjør det mulig å spore uønskede hendelser når det er nødvendig. I avtalen mellom kommunen og Visma fremgår det at all aktivitet i systemet logges og at loggene kan gjennomgås ved behov. Dette bekreftes også av systemansvarlige.

Systemets logger vurderes å være tilstrekkelig sikret ut fra hva revisjonen kan lese ut av dokumentasjon fra Visma om systemets tekniske sikkerhetsløsninger.

- **Det bør være gjennomført penetrasjonstest av systemet.**

Visma er ISO/IEC 27001-sertifisert, noe som innebærer krav til systematisk arbeid med informasjonssikkerhet, inkludert håndtering av sårbarheter og sikkerhetstesting. ISO-sertifiseringen gir en viss trygghet for at leverandøren har etablert rutiner for penetrasjonstesting, og på denne bakgrunn vurderer revisjonen at penetrasjonstesting mest sannsynlig er gjennomført for det aktuelle systemet.

Det fremgår imidlertid ikke av avtalen mellom kommunen og Visma noe krav om at leverandøren gjennomfører penetrasjonstester. Intervjuene viser at informantene fra kommen ikke er kjent med om Visma gjennomfører slik testing.

Revisjonen vil mener kommunen bør ha kjennskap til om det gjennomføres penetrasjonstesting, da dette er sentralt for å kunne vurdere sikkerheten i systemet og følge opp leverandørens ansvar.

Håndtere og gjenopprette:

- **Kommunen bør sørge for at det er utarbeidet en hendelseshåndteringsplan for systemet.**

Revisjonen vurderer kriteriet som oppfylt.

Avtalen mellom kommunen og Visma stiller krav til leverandøren om å utarbeide gjenopprettingsplaner og beredskapsplaner knyttet til løsningen. Avtalen beskriver også hvordan leverandøren skal respondere på ulike

feilsituasjoner, prioritert etter alvorlighetsgrad av konsekvenser for kunden, for å gjenopprette normalsituasjonen.

- **Kommunens systemer bør ha redundansmuligheter som sikrer tilgjengelighetskrav.**

Revisjonen vurderer kravet som oppfylt.

Redundansmuligheter innebærer at tilgjengeligheten til systemet ivaretas gjennom alternative løsninger dersom uforutsette hendelser oppstår.

I avtalen mellom kommunen og Visma fremgår det at produksjonsdata lagres i primært datasenter, med kopi til sekundært datasenter. Ved avbrudd skjer automatisk overføring til en fungerende forbindelse, vanligvis uten at tjenesten påvirkes. Dette beskriver en form for nettverksredundans, som bidrar til å sikre tilgjengelighet ved nettverksfeil.

3.4 INFORMASJONSSIKKERHET KAPITALKONTROLL KK2

Vi starter med å presentere innhentet informasjon, deretter vurderer vi informasjonen opp mot de konkrete revisjonskriteriene. Informasjonen baserer seg i hovedsak på intervju med aktuelle personer i kommunen som har ansvar for KK2 og svar på skriftlige henvendelser, i tillegg til aktuelle styringsdokumenter revisjonen har innhentet. Dokumentene som er mottatt er listet opp i oversikten i vedlegg 2.

Om bruk av KK2 i Øyer kommune
I 2022 inngikk Øyer kommune en databehandleravtale med KapitalKontroll AS. Grunnlaget for databehandleravtalen var at Øyer kommune bruker innfordringsverktøyet KK2 fra KapitalKontroll AS til innfordring[36] av kommunale krav. Systemet inneholder personopplysninger som kan knyttes til enkeltpersoner. Avtalen regulerer hvordan databehandler skal behandle personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse. Eksempler på opplysninger som behandles er skyldneres navn, fødselsdato, kontaktopplysninger, betalingshistorikk og innfordringstiltak.

Ifølge databehandleravtalen er Øyer kommune behandlingsansvarlig, mens KapitalKontroll AS er databehandler. Kommunen har ansvar for at opplysningene som registreres i KK2 er korrekte, relevante og nødvendige, og plikter å rette eventuelle feil. Avtalen stiller også krav om at kommunen skal ha et styringssystem for informasjonssikkerhet i tråd med gjeldende regelverk, og at det kun skal benyttes systemer med innebygd personvern (jf. GDPR art. 25).

Øyer kommune har foretatt en vurdering av personvernkonsekvenser (DPIA) i hht. artikkel 35 i personvernforordningen (GDPR). Det framkommer i DPIAen at GDPR artikkel 6(1) bokstav e) gir lovlig grunnlag for behandling av personopplysninger når det er «*nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt*». Hjemmel for å utøve tjenesten er «*Vedtak om felleskontor for skatteinnkreving og innfordring for Gausdal, Lillehammer og Øyer kommuner, datert 28.3.2011*».

KapitalKontroll AS er forpliktet til å gjennomføre tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysninger skjer i samsvar med personopplysningsloven og ivaretar den registrertes rettigheter. KK2 er et skybasert system bygget på Microsoft Azure og benyttes av nær halvparten av norske kommuner.[37] Systemet er integrert med en rekke økonomi- og regnskapssystemer, inkludert Agresso, som benyttes av Øyer kommune.

[36] Innfordring innebærer at en virksomhet følger opp utestående krav for å sikre betaling fra skyldnere, i tråd med gjeldende lover og regler. Prosessen omfatter varsling, purring, avtaleinngåelse, betalingsoppfølging og ev. rettslige skritt. Innfordringsverktøy er det digitale systemet som brukes til å administrere innfordringsprosessen. Verktøyet gir støtte for registrering, oppfølging, dokumentasjon og rapportering av krav, og bidrar til å sikre struktur, sporbarhet og etterlevelse av regelverk.
[37] https://www.kapitalkontroll.no/

Systemet er nettbasert, etter tidligere å ha vært driftet lokalt hos Ikomm. Kommunikasjonen mellom KK2 og økonomisystemet i kommunen skjer via en programvareagent. Tekniske problemer håndteres i samarbeid mellom KK2 og Ikomm.

3.4.1 IDENTIFISERE OG KARTLEGGE

System for risikovurderinger

Revisjonen har mottatt en ROS-analyse, DPIA og en ny personvernerklæring for avdelingen. Det er opplyst at ROS-analysen og personvernerklæringen er gjennomgått og oppdatert forbindelse med revisjonsprosjektet. De mottatte dokumentene er ikke datert. I intervju beskriver innfordringsleder at arbeidet med risikovurderinger er godt integrert i den daglige driften, og at tiltak vurderes og iverksettes etter behov.

Gjennomgangen av ROS-analysen ved innfordringskontoret viser at analysen i hovedsak er hendelsesbasert og tar utgangspunkt i konkrete situasjoner som kan oppstå i møte med publikum eller ved manuell behandling av informasjon. De uønskede hendelsene som er identifisert omhandler blant annet at innringer får utlevert informasjon uten å være pårørende, at skyldnere møter fysisk på kontoret og nekter å forlate det. I tillegg er det vurdert risiko knyttet til ekstern videresending av interne e-poster og feil i skriftlig kommunikasjon. Det fremgår ikke av analysen at det er gjennomført vurderinger av IKT-relaterte risikoer. Det opplyses i intervju at innfordringskontoret har etablert en praksis for gjennomføring av risikovurderinger.

KapitalKontroll AS, som leverer systemet KK2, har utarbeidet «Retningslinjer for håndtering av personopplysninger i KK» og de har oversendt et notat til kunder av KapitalKontroll (kommunen) om risiko som de «bør være oppmerksom på i egne rutiner» (notatet er ikke datert). Det framkommer også av de ulike policyene som er mottatt fra KapitalKontroll at de skal arbeide ut fra en risikobasert tilnærming. Det framkommer at KK2 i sine risikovurderinger skiller mellom intern og ekstern sikkerhet. Ekstern sikkerhet gjelder forsøk på tilgang fra personer uten gyldig brukerkonto, mens intern sikkerhet omfatter risiko knyttet til brukere med gyldige tilgangsrettigheter, for eksempel ved at brukeridentiteter kommer på avveie eller at ansatte får for høy tilgang.

KapitalKontroll vurderer den største risikoen å være at saksbehandlere beholder tilgang etter at de har avsluttet arbeidsforholdet. Det gjennomføres derfor kvartalsvise rapporter for å identifisere inaktive brukere. Det er opplyst at KK2 i Øyer per i dag har tre brukere, og at disse har vært de samme siden oppstart. Endringer i brukertilgang har dermed ikke vært nødvendig.

DPIAen som er utarbeidet følger en standard mal. I DPIAen vurderes behandlingsgrunnlag og hvilken type personopplysninger som behandles av systemet, for eksempel at de ikke inneholder særlige kategorier av personopplysninger. Det vurderes også om datainnsamling gjennomføres i stor skala. Videre er det blant annet foretatt en beskrivelse av behandlingen som redegjør for formål, behandlingsgrunnlag, behandlingens art, behandlingens omfang, konteksten behandlingen utføres i, og hvilke tekniske og organisatoriske tiltak som er gjort for å ivareta personvernkrav. Her er det blant annet krysset av «ja» for at det er gjennomført «prosess-ROS og teknisk », i tillegg til at det nevnes tiltak som to-trinns pålogging, adgangskontroll styrt av leder og rollebasert tilgangsstyring.

Tidsplan/Oppfølging av tiltak

I DPIAen står det at risiko- og sårbarhetsanalysen som er gjennomført skiller mellom «prosess-ROS» og «teknisk ROS». Dette ble bekreftes i intervju. Innfordringsleder fortalte at risikoer som gjelder prosesser håndteres av den aktuelle avdelingen, mens tekniske forhold kan kreve oppfølging fra systemleverandører. Som eksempel ble det vist til feiloverføring av informasjon mellom systemer, der innfordringskontoret retter den konkrete feilen, mens systemeier har ansvar for å sikre at feilen ikke gjentar seg.

ROS-analysen angir forslag til nye tiltak for hver hendelse, men det fremgår ikke av dokumentet at det er fastsatt tiltakseier eller tidsfrister for gjennomføring. Dette samsvarer med opplysningene fra intervjuene, der det ble opplyst at vurderinger skjer løpende og ved behov, uten en fastsatt plan for oppdatering.

3.4.2 BESKYTTE OG OPPRETTHOLDE

Regime for sikkerhetsoppdatering av systemet.

KapitalKontroll AS er ansvarlig for drift, vedlikehold og oppdatering av det skybaserte systemet KK2. Det fremgår av leveransebeskrivelsen at alle funksjonalitetsforbedringer og nye løsninger gjøres fortløpende tilgjengelig for alle brukere uten ekstra kostnad. Det står videre i beskrivelsen at det ikke er behov for lokal installasjon, og kommunen belastes ikke med teknisk drift. Det opplyses også at systemet kontinuerlig utvikles og vedlikeholdes av KapitalKontroll.

I notatet om risiko fra KK2 fremgår det at sikkerhet er et kontinuerlig fokusområde for leverandøren. Mottatte policyer fra KK2, beskriver leverandørens generelle sikkerhetskrav, inkludert at de nyeste sikkerhetspatcher og programvareversjoner skal installeres så snart det er praktisk mulig.

Leverandøren har opplyst til kommunen at det foreligger prosesser for regelmessig testing, vurdering og evaluering av effektiviteten av tekniske og organisatoriske tiltak.[38]

Det opplyses fra innfordringsleder at informasjon om tekniske sårbarheter formidles jevnlig fra leverandøren, både gjennom webinarer og varsler direkte i systemet.

Han forteller videre at for et par år siden opplevde leverandøren en alvorlig hendelse der systemet kollapset som følge av et angrep. Sikkerhetssystemet fungerte som det skulle, og leverandøren stengte ned systemet for å forhindre videre skade. Leverandøren informerte i etterkant om at tiltakene hadde fungert etter planen, og at systemet hadde blitt midlertidig koblet ned nettopp for å hindre at situasjonen utviklet seg. Innfordringsleder forteller at denne hendelsen bidro til å styrke tilliten til sikkerheten i systemet, spesielt med tanke på de sensitive opplysningene som behandles.

Tilgangsstyring

Informasjonssikkerhetshåndboken beskriver prinsipper for tilgangsstyring. Tilganger skal gis ut fra faktiske behov. Brukere skal ha lavest mulig rettighetsnivå. Tilgangene skal være styrt av roller. Systemansvarlig skal

[38] I forbindelse med revisjonen har leder for innfordring sendt en e-post til KK2 med forespørsel om utfyllende informasjon. Ett av dokumentene som ble oversendt, var spørsmål fra en kommune til og svar fra KK2 som mulig leverandør av informasjonssikkerhetssystem.

jevnlig gå gjennom tilgangene. For administratorkontoer står det at de ikke skal ha høyere rettigheter enn nødvendig.[39] I den oppdaterte Informasjonssikkerhetshåndboken, som foreløpig kun gjelder for Øyer er det også lagt til flere prinsipper som skal følges for alle brukerkontorer. Det er også et nytt avsnitt som omhandler privilegerte kontoer (administratorkontoer). Privilegerte brukerkontoer skal ha minst mulig tilgang, ikke brukes på egne enheter, sikres med multifaktorautentisering – helst passordløs – og bruken av slike kontoer bør helst være tidsavgrenset. Alle informasjonssystemer skal ha systemeiere som klassifiserer informasjonen i systemene og definerer korrekte tilgangsnivåer.

Leder for innfordringsavdelingen har administratorrettigheter i KK2 og kan opprette og slette brukere i systemet. Det er også opplyst at leverandøren, KapitalKontroll AS, har rettigheter til å deaktivere hovedadministratoren. Det er opplyst at KK2 i Øyer per i dag har tre brukere, og at disse har vært de samme siden oppstart. Alle tre ansatte i avdelingen har samme tilgangsnivå, ettersom de utfører likeartede oppgaver i systemet. Dersom det blir aktuelt å gi tilgang til nye ansatte eller vikarer, er det hovedadministratoren som håndterer dette. Innfordringsleder fortalte at de ikke har en egen prosedyre for tilgangsstyring når det gjelder KK2. I og med at alle de tre brukerne har vært med siden oppstart av systemet har endringer i brukertilgang ikke vært nødvendig.

I KK2 sine «Retningslinjer for håndtering av personopplysninger i KK2» står det at tilgangskontroll og sikkerhet KK2 er sikret fysisk ved at servere er plassert i eget avkjølt og avlåst datarom hos et norsk datasenter. Bygningen er sikret ved elektronisk adgangskontroll. Datarommet er sikret ved elektronisk adgangskontroll. Serverne er sikret med brannmurer som hindrer uautorisert tilgang til system og opplysninger lagret i systemet. Det kommer også fram av KapitalKontroll sine risikovurderinger at manglende kontroll på tilganger vurderes som en stor risiko. KK2 følger opp dette ved å utarbeide kvartalsvise rapporter for å identifisere inaktive brukere.

Det benyttes multifaktorautentisering ved innlogging. Dette innebærer at brukerne, i tillegg til brukernavn og passord, må oppgi en unik kode som genereres for hver pålogging. Dette tiltaket er etablert som en del av sikkerhetsrutinene for å beskytte mot uautorisert tilgang.

Klassifisering av systemets informasjonsverdier.
IT-ansvarlige i kommunene opplyser at de har oversikt over systemer og personopplysninger, basert på behandlingsprotokoller. Protokollene inneholder informasjon om hvilke personopplysninger som behandles, formål med behandlingen og hvilke systemer som benyttes. I oppstartmøtet med Øyer kommune, ble det opplyst at de har flyttet samtlige av kommunens fagsystemer over i sky, og at de samtidig gjennomførte en overordnet IKT-ROS (risiko- og sårbarhetsanalyse) for å få oversikt over prioriterte risikoområder. Kartleggingen identifiserte omtrent 150 systemer som krever innlogging og kan utgjøre en sikkerhetsrisiko.[40]

Databehandleravtalen fra september 2022 presiserer krav til behandling og sikring av data. Innfordringsavdelingen har utarbeidet en ny personvernerklæring og det foreligger en

[39] Når det gjelder tilgangsstyring, er dette oppdatert i informasjonssikkerhetshåndboken for Øyer kommune, men endringen er foreløpig ikke vedtatt i de to andre kommunene.
[40] Opplysningen er gitt i oppstartmøtet 10.01.2025. Revisjonen fikk innsyn i oppsettet på oppstartmøtet, men har ikke etterspurt ytterligere dokumentasjon som viser oversikten.

personvernkonsekvensvurdering (DPIA) for KK2, som beskriver og vurderer risikoer knyttet til behandling av personopplysninger.

Gjenopprettelse av data og test av sikkerhetskopi
Av avtalen mellom kommunen og KK2 framkommer det at KapitalKontroll, som leverandør av KK2 er ansvarlig for sikkerhetskopiering og gjenoppretting av data i løsningen:

> *«KapitalKontroll har en tredelt backup-løsning: en lokal kopi, en ekstern harddisk på kontoret og en sikker kopi lagret et annet sted. Hvis systemet svikter, følger Business Continuity Team (BCT) faste rutiner for å hente tilbake data. De finner riktig backup og bruker loggfiler for å redusere tap av informasjon. Det tar vanligvis rundt 20 minutter å gjenopprette data fra lokal backup».*

Det står videre at før systemet startes opp igjen, sjekkes alt nøye. Hvis det oppdages feil, starter en prosess for vedlikehold og backup. Da testes backupen for å sikre at den fungerer som den skal. Systemet overvåkes hele tiden, og backup er en viktig del av hvordan man håndterer slike hendelser.

3.4.3 OPPDAGE

Sikkerhetsovervåking - logg som viser systemaktiviteter/ Hendelseslogg
Den oppdaterte informasjonssikkerhetshåndboka for Øyer har utvidet kravene til logging. De nye og oppdaterte retningslinjene gjelder alle informasjonssystemer – både papirbaserte og digitale – som innebærer oppslag, endring, retting og sletting. Dette omfatter systemer som kommunen selv drifter, samt systemer driftet av eksterne leverandører. Det fremgår at formålet med logging er å sikre dokumentasjon av system- og brukeraktiviteter, og å kunne avdekke uautorisert bruk. Videre presiseres det at alle systemlogger skal gjennomgås som en del av kommunens årshjul. Hendelser som logges inkluderer blant annet pålogging og avlogging, endringer i systeminnstillinger og forsøk på uautorisert tilgang, og det står at dette ofte benevnes som aktivitets- og hendelseslogger.

Det framgår av databehandleravtalen mellom kommunen og leverandøren at leverandøren «*…vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne Avtalen oppfyller kravene i personopplysningsloven og vern av den registrertes rettigheter, herunder innfrir alle krav etter artikkel 32 i personvernforordningen*»

Leder for innfordring har i forbindelse med revisjonen innhentet opplysninger om logging og sikkerhetskopiering fra KK2. Leverandøren opplyser i sitt svar at det meste logges, inkludert innlogginger, endringer på saker og produserte tiltak. En del av loggene vises direkte i systemet under notater, mens andre er tilgjengelige for supportpersonell. Det opplyses at det meste fjernes, og at loggene oppbevares i henhold til GDPR-rutiner, med noe rullering. Det framkommer videre i den mottatte dokumentasjonen "Applications Security Policy" at *alle sikkerhetsrelaterte hendelser på kritiske eller sensitive systemer skal logges*. Dette viser at det er etablert en praksis for logging av systemaktiviteter

I intervju ble det opplyst om at KK2 har tilgang til opplysningene som behandles av innfordringskontoret, og at de i enkelte tilfeller går inn i systemet for å undersøke feil.

Penetrasjonstest

I forbindelse med revisjonen har leder for innfordring sendt en e-post til KK2 med forespørsel om utfyllende informasjon. Leverandøren har i den forbindelse opplyst at selskapet har egne ressurser innen cybersikkerhet, og at det jevnlig gjennomfører testing for sårbarheter i systemene. Det ble videre opplyst at systemene revideres av ekstern revisor (EY). Rapportene fra testene er i utgangspunktet ment for intern bruk, men kan gjøres tilgjengelig for kunden i egnet format ved forespørsel.

Når det gjelder gjennomføring av en penetrasjonstest gjennomføres slike gjerne i etterkant av en sårbarhetsskanning, og den innebærer at man forsøker å utnytte de identifiserte sårbarhetene i praksis – altså simulerer et reelt angrep – for å teste hvor langt en angriper faktisk kan komme. En sårbarhetsskanning er en systematisk gjennomgang av et IT-system for å identifisere kjente svakheter og feilkonfigurasjoner som kan utnyttes. Skanningen gir et oversiktsbilde over mulige inngangspunkter for angrep.

Som del av denne revisjonen har vi gjennomført en kontrollert sårbarhetsskanning. Resultatet viste følgende:

> *Konklusjonen fra sårbarhetsskanningen viste at systemet har en godt kontrollert angrepsflate med lav eksponering med kun moderate og lave sårbarheter. Det som er funnet, relaterer seg i hovedsak til modenhet i sikkerhetskonfigurasjon snarere enn direkte sårbarheter. Det anbefales å følge opp forbedringspunktene som del av kontinuerlig herding og sikkerhetsvedlikehold.*

3.4.4 HÅNDTERE OG GJENOPPRETTE

Hendelsehåndteringsplan

De overordna styringsdokumentene til kommunen fremhever betydningen av at systemene de benytter må ha beredskapstiltak som bidrar til å begrense skade og at kommunen raskt kommer tilbake til normal drift.

Av dokumentasjonen mottatt fra KK2 er det beskrevet hvordan leverandøren skal agere når ulike hendelser oppstår. Det framkommer blant annet at i avtalen med KK2 at leverandøren forplikter seg til å følge opp mislighold/avvik som skyldes Skytjenesten. Videre framkommer det opplysninger om KK2 sin «kontinuerlige prosess for å overvåke, revidere og oppdatere de tiltakene som er innført for å sikre at behandlingen av personopplysningene er i samsvar med personvernregelverket og de registrertes forventninger».[41]

Det er opplyst i intervju at det per i dag ikke foreligger en egen hendelseshåndteringsplan for KK2 ved innfordringskontoret. Det uttrykkes samtidig et behov for å få på plass en slik plan, og at de vil ta kontakt med leverandøren, KapitalKontroll AS, for å få informasjon om hvordan slike hendelser håndteres hos dem.

Redundansmuligheter

Redundans innebærer at systemet er utstyrt med reservekomponenter eller parallelle løsninger som automatisk overtar funksjonen dersom en del svikter. Dette bidrar til å opprettholde tilgjengelighet og kontinuitet i tjenesten, selv ved tekniske feil eller avbrudd.

[41] Dette framkommer av retningslinje for håndtering av personopplysninger i KK2 og i Vurdering av KK2 opp mot personvernforordningen artikkel 15.

I forbindelse med revisjonen har leder for innfordring mottatt utfyllende informasjon fra KK2. Den mottatte dokumentasjonen viser at det er etablerte rutiner for hendelser knyttet til programvare og maskinvare. Systemet har tre nivåer av sikkerhetskopiering: lokal backup, ekstern disk og offsite-lagring, som gir både lokal og geografisk dataredundans. Ved maskinvarefeil kan data flyttes til alternative servere, og trafikk omdirigeres midlertidig. Gjenoppretting fra lokal backup tar ca. 20 minutter, og prosesser skal starte innen fem minutter i arbeidstid.

Som del av denne revisjonen har vi gjennomført en automatisert sårbarhetsskanning. Den gjennomførte sårbarhetsskanningen vister følgende:

> *«Risikonivået anses som lavt, og det er ingen umiddelbar indikasjon på eksponering for alvorlige angrep. Funnene bør likevel følges opp som del av normal sikkerhetsherding og modenhetsutvikling – spesielt med tanke på best practices for applikasjonssikkerhet og TLS-konfigurasjon.*
> *Konklusjon:*
> *Systemet har en godt kontrollert angrepsflate med lav eksponering med kun moderate og lave sårbarheter. Det som er funnet, relaterer seg i hovedsak til modenhet i sikkerhetskonfigurasjon snarere enn direkte sårbarheter. Det anbefales å følge opp forbedringspunktene som del av kontinuerlig herding og sikkerhetsvedlikehold».*

3.4.5 REVISJONENS VURDERING – KK2

Identifisere og kartlegge

- **Kommunen skal ha gjennomført risikovurdering av systemet.**
- **Foreslåtte tiltak knyttet til risikovurderingen bør ha blitt gjennomført i henhold til en fastsatt plan, med fastsatt tiltakseier og tidsfrist.**
- **Kommunen bør oppdatere risikovurderingen i faste intervaller og ved betydelige endringer**.

Revisjonen vurderer kriteriet som ikke oppfylt.

Revisjonens undersøkelser viser at innfordringskontoret har gjennomført en DPIA for personopplysninger som behandles i KK2, og de har utarbeidet en risikovurdering for avdelingen.

Revisjonens gjennomgang viser imidlertid at den mottatte ROS-analysen kun beskriver konkrete uønskede hendelser som kan oppstå ved avdelingen. Etter vår vurdering inneholder den gjennomførte ROS-analysen ikke vurderinger av risikoer knyttet til KK2-systemet, og kan dermed ikke anses som en risikovurdering av systemet.

Revisjonen stiller uansett spørsmål ved at det ikke er identifisert andre typer digitale risikoer i ROS-analysen vi har mottatt, som for eksempel datainnbrudd eller utilsiktet deling av sensitiv informasjon via digitale kanaler.

Det er positivt at systemleverandøren gjennom dokumentasjon viser at de har gjort omfattende vurderinger av hvilke risikoer som finnes i systemet. Denne kan brukes som grunnlag, men den kan imidlertid ikke, som det framgår av informasjonssikkerhetshåndboken, erstatte kommunens egen ROS.

Vi har videre observert at ROS-analysen vi har mottatt ikke er datert, og det fremgår ikke at de foreslåtte tiltakene skal følges opp gjennom en fastsatt plan med tiltakseier og tidsfrister. Kommunen opplyser at risikovurderinger gjennomføres ved behov, og ikke etter faste intervaller eller ved betydelige endringer.

Samlet sett viser revisjonens undersøkelser av kommunenes arbeid med ROS-analyser at det kan være behov for å styrke kompetansen hos dem som gjennomfører ROS-analysene om hvordan en jobber risikobasert innen dette feltet.

Beskytte og opprettholde:

- **Det bør være etablert et regime for sikkerhetsoppdatering av systemet.**

Revisjonen vurderer at kriteriet er oppfylt.

Informasjonssikkerhet er omtalt i kommunens informasjonssikkerhetshåndbok, og det fremgår at IT-driftsleverandøren skal sørge for at informasjonssikkerheten ivaretas i systemet, og at dette skal forankres i driftsavtalen mellom kommunen og leverandøren.

Avtalen mellom kommunen og KK2 viser at det er etablert et tydelig ansvarsforhold som gir leverandøren ansvar for informasjonssikkerhet. KK2 har dokumentert i sine policyer og leveransebeskrivelse hvordan oppdateringer gjennomføres og loggføres i henhold til fastsatte prosedyrer, og kommunen mottar jevnlig informasjon om tekniske sårbarheter.

- **Kommunen bør ha kontroll på identiteter og tilganger.**
- **Kommunen bør bruke multifaktorautentisering for kontoer med tilgang til kritiske eller data.**

Revisjonen vurderer kriteriene som oppfylt.

Det er i dag tre brukere av systemet og alle har samme rolle. Likt tilgangsnivå er vurdert som nødvendig, da alle har likeartede oppgaver i systemet. Avdelingsleder har administratorrettigheter og håndterer opprettelse og sletting av brukere. Revisjonen ser at de oppdaterte rutinene for tilgangsstyring som er lagt inn i informasjonssikkerhetshåndboken i Øyer langt på veg er ivaretatt med den praksisen som beskrives av kommunen i dag.

Det benyttes multifaktorautentisering ved innlogging, der brukerne må oppgi en unik kode i tillegg til brukernavn og passord. Dette er i tråd med anbefalte krav til sikker autentisering.

Det er opplyst i intervju med kommunen og i dokumentasjon fra KK2 at leverandøren, gjennom sine rutiner, følger opp og identifiserer eventuelle inaktive brukere i systemet.

- **Kommunen bør beskytte data i systemet i samsvar med gjennomført klassifisering av systemets informasjonsverdier.**

Revisjonen vurderer at kommunene har etablert flere viktige tiltak for å sikre dataene som behandles i KK2, og at de har kommet langt i arbeidet med systematisk klassifisering av informasjon som sikrer at sikkerhetstiltakene er tilpasset informasjonsverdienes betydning.

Kommunene har etablert flere sentrale tiltak som bidrar til å ivareta personvern og informasjonssikkerhet i KK2. Dette omfatter blant annet personvernkonsekvensvurdering (DPIA) og oversikt over behandlingsaktiviteter basert på behandlingsprotokoller. Protokollene gir informasjon om hvilke personopplysninger som behandles, formål med behandlingen og hvilke systemer som benyttes. Kommunen oppgir også at de har kartlagt og identifiserte omtrent 150 systemer for å skaffe seg en oversikt over prioriterte risikoområder.

Revisjonen vurderer at kommunene har etablert flere viktige tiltak for å identifisere systemets informasjonsverdier og for å beskytte dataene som behandles i KK2. Med den mengden dokumentasjon og analyser som allerede foreligger, virker kommunen å ha kommet langt i arbeidet med å etablere en helhetlig klassifiseringsprosess.

Arbeidet klassifisere informasjonsverdiene de behandler vil kunne gi et tydelig grunnlag for å tilpasse og prioritere sikkerhetstiltak i tråd med informasjonsverdienes betydning, og styrket dokumentasjonen for at data beskyttes i samsvar med gjennomført klassifisering. Dette er et helt sentralt grunnlag for kommunens risikobaserte arbeid.

- **Kommunen bør ha sikret muligheten til å gjenopprette systemets data.**

Revisjonen vurderer at kriteriet er oppfylt.

KK2 er en skytjeneste, og avtalen mellom kommunen og leverandøren beskriver hvordan sikkerhetskopiering skal håndteres. Det vises blant annet til at systemet overvåkes kontinuerlig, og det er synliggjort rutiner for vedlikehold og backup.

Oppdage:

- **Det bør være etablert sikkerhetsovervåking av systemet gjennom at**
    - **Kommunen sikrer at systemet har logger over systemaktiviteter**
    - **Systemets logger bør være tilstrekkelig sikret.**

Revisjonen vurderer at kriteriene er oppfylt.

Det fremgår av informasjonssikkerhetshåndboken at kommunens fagsystemer skal føre aktivitets- og hendelseslogger som gjør det mulig å spore uønskede hendelser når det er nødvendig.

Avtalen mellom kommunen og leverandøren bekrefter at all databehandling i avtalen skal sikres med egnede tekniske og organisatoriske tiltak henhold til 32 i personvernforordningen. Dette innebærer at leverandøren må etabler loggføring og sikkerhetsovervåking – fordi dette er nødvendig for å møte lovens krav.

Dette underbygges av tilleggsinformasjon fra KK2, der det fremgår at all aktivitet i systemet logges og at loggene kan gjennomgås ved behov. Dette bekreftes også av systemansvarlige.

- **Det bør være gjennomført penetrasjonstest av systemet.**

Revisjonen vurderer kriteriet som oppfylt.

Avtalen mellom kommunen og KK2 stiller ikke eksplisitte krav om gjennomføring av penetrasjonstester.

Det er i forbindelse med revisjonen innhentet opplysninger fra leverandøren, og her opplyses det at det jevnlig gjennomføres penetrasjonstesting og at systemene revideres av ekstern revisor (EY). Tester utføres av interne cybersikkerhetsressurser, og rapporter kan gjøres tilgjengelig ved forespørsel. På bakgrunn av dette, legger revisjonen til grunn at penetrasjonstesting gjennomføres.

Håndtere og gjenopprette:

- **Kommunen bør sørge for at det er utarbeidet en hendelseshåndteringsplan for systemet.**

Revisjonen vurderer kriteriet som delvis oppfylt.

Avtalen mellom kommunen og KK2 stiller ikke eksplisitte krav om at leverandøren pliktes å ha beredskasplanverk/hendelseshåndteringsplan/gjenopprettelsesplaner. Den synliggjør imidlertid krav til leverandøren om hvordan de skal respondere på ulike hendelser som kan oppstå. Det er også lagt fram et notat fra systemleverandøren som viser vurderinger av hvilke risikoer som finnes i systemet og det er lagt fram tiltak for å møte slik risiko.

- **Kommunen bør ha vurdert redundansmuligheter som sikrer tilgjengelighetskrav.**

Vi vurderer kriteriet som oppfylt.

Dokumentasjon fra leverandøren viser at det er etablert redundansmuligheter som sikrer systemets tilgjengelighet og kontinuitet i tjenesten ved feil eller driftsavbrudd.

4. ARBEID MED SIKKERHETSKULTUR

Dette kapittelet besvarer problemstilling 2:

> I hvilken grad arbeider kommunen systematisk med å etablere en sikkerhetskultur i virksomheten?

I kapittel 4.1 og 4.2 gis en beskrivelse av temaet *sikkerhetskultur*, før de konkrete revisjonskriteriene for problemstillingen presenteres i kapittel 4.3. Deretter gjør vi rede for faktagrunnlaget i kapittel 4.4, og til slutt kommer revisjonens vurderinger i kapittel 4.5.

4.1 RISIKO FOR MENNESKELIG SVIKT

God informasjonssikkerhet og personvern er avhengig av menneskene i organisasjonen. I tillegg til virksomhetens teknologiske infrastruktur og internkontroll, må alle ansatte bidra gjennom en sikker praksis. Det være seg å beskytte informasjon, etterleve rutiner og retningslinjer, samt å melde avvik.

Ny teknologi, økt bruk av hjemmekontor og flere mobile enheter utfordrer informasjonssikkerheten ved at skillet mellom arbeid og privat blir mindre, i tillegg til at virksomheten har mindre kontroll enn tidligere. Det samme gjelder i tilfeller der kommunen løser sine oppgaver ved hjelp av eksterne aktører.

Systemene kan ødelegges fra innsiden, gjennom innsidere, dersom ikke sikkerheten ivaretas av den enkelte. NSM skiller mellom den ubevisste og den bevisste innsideren. Den bevisste innsideren utnytter sin kunnskap om eller tilgang på informasjon i virksomheten. Den ubevisste innsideren tar sikkerhetsrisiko uten å være oppmerksom på det, for eksempel ved å åpne e-post med skadevare eller ikke gjennomføre nødvendige sikkerhetsoppdateringer. Årsaken kan være manglende kompetanse og/eller bevissthet.

Skadelig programvare aktiveres ofte ved å manipulere brukere til å foreta en handling, for eksempel trykke på en lenke eller åpne et vedlegg. NSM presiserer derfor at opplæring er spesielt viktig.

Sårbarhetene NSM oftest finner i sine kartlegginger er:

- Dårlige passord, for eksempel standardpassord, og lett tilgjengelige passordhuskelister.
- Slurv med tilganger, for eksempel kontoer som ikke er deaktivert og kontoer med høyere rettigheter enn nødvendig.
- Utdaterte systemer, for eksempel versjoner som ikke produserer sikkerhetsoppdateringer.

4.2 HVA ER «SIKKERHETSKULTUR» - OG HVORDAN OPPNÅ DET?

Begrepet «sikkerhetskultur» handler om hvordan mennesker forholder seg til informasjonssikkerhet. Ifølge Norsk senter for informasjonssikring (NorSIS)[42] innebærer en sterk sikkerhetskultur at ansatte forstår viktigheten av å beskytte data mot uautorisert tilgang (konfidensialitet), sikre at informasjon forblir nøyaktig og pålitelig (integritet), og sørge for at informasjon og systemer er tilgjengelige når det trengs (tilgjengelighet). [43]

> «Organisasjonens sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale ivaretagelse av informasjonssikkerhet og personvern.»
>
> KS (2022)

Gjennom bevisstgjøring, opplæring og gode rutiner kan kommunens ansatte bidra til å styrke disse prinsippene i det daglige arbeidet, noe som reduserer risikoen for brudd på sikkerheten og styrker kommunens samlede motstandskraft mot digitale trusler.

Digitaliseringsdirektoratet minner om at virksomhetens digitale sikkerhetskultur er en del av organisasjonskulturen som helhet, og at kompetanse- og kulturutvikling en kontinuerlig prosess.[44]

4.3 REVISJONSKRITERIER – PROBLEMSTILLING 2

Revisjonskriteriene for denne problemstillingen er utledet fra kildene som er nevnt i kapittel 2. Her trekker vi frem de momentene som er særlig aktuelle for sikkerhetskultur.

4.3.1 OVERORDNETE VEILDERE FOR INTERNKONTROLL

«Verktøykasse for personvern og informasjonssikkerhet» [45] er en veileder for internkontroll etter kommuneloven § 25-1 som er omtalt i kapittel 2. Veilederen er rettet mot informasjonssikkerhet og personvern, og det står:

[42] Norsk senter for informasjonssikring (NorSIS) er en del av Nasjonal sikkerhetmyndighets arbeid for å sikre grunnleggende nasjonale funksjoner. https://norsis.no/om-norsis/

[43] "The Norwegian Cybersecurity Culture" (NorSIS, 2016)

[44] Digitaliseringsdirektoratet, Veileder i kompetanse- og kulturutvikling innen digital sikkerhet

[45] Kommunenes sentralforbund (KS, 2022) Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

> *«God informasjonssikkerhet og personvern er til syvende og sist avhengig av menneskene i organisasjonen. Teknologi, etterlevelse, virksomhetsstyring, risikovurderinger og kontinuitet er alle avhengige av menneskenes ferdigheter og kunnskaper.»*
>
> KS (2022, s.10)

For at ansatte skal praktisere en trygg sikkerhetskultur er det avgjørende at de har forståelse for hva det innebærer. KS understreker at det er ledelsens ansvar at digital sikkerhet ivaretas. Det innebærer blant annet å sørge for at ansatte har tilstrekkelig kunnskap på området.

KS peker på avviksmeldinger og avvikshåndtering som et godt grunnlag for erfaring og læring, og anbefaler kommunene å ha rutiner for dette arbeidet. Avvikskultur er særlig omtalt i KS sin veileder *«Orden i eget hus. Kommunedirektørens internkontroll».* Veilederen viser til at avvik gjerne oppstår som følge av beslutninger og/eller handlinger gjort av ansatte. Det er også hver enkelt ansatt som må vurdere om en hendelse skal rapporteres som et avvik. Derfor anser KS det som viktig at virksomheten har klare definisjoner på hva et avvik er.

I den samme veilederen anbefaler KS at det innføres avviksrapportering helt fra virksomhets-/ tjenestenivå til strategisk og folkevalgt ledelse. De viser til at god avvikshåndtering med fokus på forbedring, øker sannsynligheten for at medarbeidere melder avvik. [46]

4.3.2 FOREBYGGENDE SIKKERHETSARBEID OG PERSONVERNFORORDNINGEN

Det vises til omtalen av sikkerhetsloven og personvernforordningen i kapittel 2.

Kommunens øverste leder har ansvaret for det forebyggende sikkerhetsarbeidet. Kravene til dette arbeidet ligger i lovens kapittel 4. Det handler blant annet om å sikre at sikkerhet er en integrert del av virksomhetens ledelse og risikostyring, samt at risiko vurderes kontinuerlig. Virksomheten skal sørge for at ansatte har tilstrekkelig risiko- og sikkerhetsforståelse, og ifølge loven skal virksomheten *«gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå»* (§4-3).

Personvernforordningen stiller krav til at det gjennomføres nødvendige tekniske og organisatoriske tiltak for å ivareta sikkerheten.[47] Eksempler på organisatoriske tiltak er retningslinjer og rutiner, tydelige ansvarsforhold og kompetansehevende tiltak for dem som behandler personopplysningene.

[46] Kommunedirektorens-internkontroll-veileder-08092020.pdf (ks.no)

[47] https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr#gdpr

Forebyggende sikkerhetstiltak kan oppsummeres som alt som beskytter virksomhetens informasjonsverdier, reduserer sårbarhet og gjør virksomheten i stand til å oppdage og håndtere trusler.

4.3.3 ISO-STANDARD OG NSM GRUNNPRINSIPPER

I den første problemstillingen ble ISO-standarden og NSMs grunnprinsipper gjennomgått med vekt på tekniske, organisatoriske og styringsmessige tiltak for å sikre informasjonssystemene. I den andre problemstillingen er disse rammeverkene fortsatt et viktig grunnlag for revisjonskriteriene, men fokuset er her rettet mot den menneskelige faktoren – sikkerhetskultur og de ansattes rolle i å ivareta informasjonssikkerheten.[48]

ISO-standarden gir et systematisk rammeverk til hjelp for kommunene i arbeidet med å bygge en kultur der informasjonssikkerhet er en integrert del av virksomheten. Følgende krav og prinsipper i standarden støtter opp under elementer som er sentrale i en sterk sikkerhetskultur:

- Forankring i ledelsen
- Tydelige mål og forståelig retning
- Klare roller med ansvar og myndighet
- Risikoforståelse
- Kontinuerlig læring og forbedring

I *grunnprinsippene for sikkerhetsstyring* peker NSM på at alle ansatte har et ansvar for å ivareta sikkerheten for virksomhetens verdier. Som mulige sårbarheter i virksomheten, nevner grunnprinsippene blant annet:

- Manglende system for avviks- og hendelseshåndtering
- Svak forståelse blant medarbeiderne om hvorfor sikkerhet er viktig for virksomheten
- Manglende kunnskap på hvordan den enkelte kan bidra til god sikkerhet

Svakheter i sikkerhetsstyringen kan blant annet føre til at personellmessige sårbarheter ikke blir håndtert. Grunnprinsippene fastslår at det overordnede ansvaret ligger hos ledelsen, men peker på at også de ansatte har ansvar, siden alle på en eller annen måte har kontakt med virksomhetens verdier.

For å sikre et godt sikkerhetsarbeid er det derfor nødvendig å gjennomføre aktiviteter som støtter opp om dette. Slike aktiviteter kan for eksempel handle om opplæring, tydelig fordeling av roller og ansvar, og håndtering av hendelser.

Grunnprinsipper for personellsikkerhet fastslår at virksomheter først vil kunne oppnå et akseptabelt sikkerhetsnivå når den har tiltak som både ivaretar det organisatoriske, teknologiske, fysiske og menneskelige aspektet.

[48] Det vises til omtalen av ISO-standarden og NSMs grunnprinsipper for sikkerhetsstyring i kapittel 2. Grunnprinsippene er også nærmere omtalt i kapittel 3.1.

Alle medarbeidere påvirker virksomhetens kultur og holdninger. Hvordan de forholder seg til sikkerhet, har betydning for risikoen virksomheten står overfor. Virksomheten bør derfor motivere ansatte og gjøre sikkerhet til en del av det daglige arbeidet, slik at de blir gode barrierer mot trusler både utenfra og innenfra. Blant tiltakene som anbefales er:

- Skriftliggjorte rutiner og retningslinjer
- Opplæring og bevisstgjøring
- Tydelige forventninger
- System for å fange opp, rapportere og følge opp avvik og hendelser

4.3.4 KOMPETANSE OG ROLLER

Digitaliseringsdirektoratet har utarbeidet en veileder som omhandler kompetanse- og kulturutvikling innen digital sikkerhet[49]. I tillegg til å etablere et planverk som sikrer informasjonssikkerheten, legger direktoratet vekt på å ha kontinuerlige aktiviteter som skaper en kultur for å ivareta sikkerheten. De har utarbeidet en modell som viser hvordan organisasjonens kultur påvirkes av den enkeltes kunnskap, bevissthet og ferdigheter.

Kunnskap viser til hva den enkelte kan, bevisstgjøring innebærer at man forstår hvorfor og ferdigheter innebærer at man vet hvordan. Kilde: Digitaliseringsdirektoratet

De ansatte trenger kunnskap om hvilken betydning informasjonssikkerhet har i de arbeidsoppgavene de utfører, og hvordan de kan gjennomføre arbeidet på en måte som ivaretar informasjonssikkerheten.

Det handler blant annet om å ha en tilfredsstillende forståelse av trusler og risiko, og videre om å forstå hvordan uønskede hendelser kan hindre dem i å få gjort jobben sin, samt hvordan dette kan få konsekvenser for andre parter.

Digitaliseringsdirektoratet anbefaler at opplæringstiltak iverksettes på bakgrunn av behov, og sees i sammenheng med øvrig aktivitet. Det er viktig at ansatte kjenner til kommunens interne rutiner for varsling av informasjonssikkerhetshendelser/ melde avvik.

Av dette har vi utledet følgende konkrete revisjonskriterier for problemstilling 2:

- Kommunen må sørge for at ansatte er orientert om rutiner og retningslinjer for den digitale sikkerheten
- Kommunen må sørge for relevant opplæring til ansatte innen digital sikkerhet
- Kommunen må sørge for at ansatte kjenner til hvordan avvik og uønskete hendelser innen digital sikkerhet skal rapporteres, og jevnlig følge opp og etterspørre slike avviksmeldinger

[49] Veileder i kompetanse- og kulturutvikling innen digital sikkerhet | Digdir

4.4 DATAGRUNNLAG

Som nevnt innledningsvis har revisjonen lagt til grunn at overordnete rutiner og retningslinjer for digital sikkerhet finnes i kommunen. Informasjonssikkerhetspolicyen og informasjonshåndboken for 3:1 samarbeidet omtales i kapittel 3.2. Vi har ikke innhentet rutiner og retningslinjer på tjenestenivå.

Problemstilling to belyses hovedsakelig fra ansattes perspektiv. Informasjonssikkerhetshåndboken gjelder for alle ansatte og det vises til denne. Dokumentet «*Retningslinjer for sikker informasjonshåndtering»* ligger også til grunn for beskrivelsen i dette kapittelet.

Utover dette baserer dette avsnittet seg på informasjon fra intervjuer med tre tjenesteledere innenfor fagområdene helse, utdanning og teknisk, samt spørreundersøkelsen som er besvart av kommunens ansatte.

Der ikke annet er spesifisert, viser begrepet «ansatte» til alle ansatte, både ledere på ulike nivå og øvrige medarbeidere.

4.4.1 KUNNSKAP

Kjennskap til rutiner og retningslinjer

Informasjonssikkerhetshåndboken understreker betydningen av at rutiner og retningslinjer for behandling av informasjon er godt forankret i organisasjonen. Det kommer frem at det skal utarbeides og tas i bruk rutinebeskrivelser for behandling av informasjon, og det stilles krav til at ansatte følger gjeldende rutiner og retningslinjer.

Ifølge håndboken, har alle ansatte et selvstendig ansvar for å kjenne til og etterleve innholdet i håndboken, samt øvrige relevante rutiner og retningslinjer. Det er ledernes ansvar å sikre at medarbeiderne har nødvendig kunnskap om og tilgang til gjeldende rutiner og retningslinjer. Dette inkluderer å sørge for at alle ansatte har lest og forstått informasjonssikkerhetshåndboken.

I intervju viser tjenestelederne til at nytilsatte får en første innføring i kommunens rutiner for digital sikkerhet gjennom arbeidskontrakten, i vedlegget *«Retningslinjer for sikker informasjonshåndtering»*. Når man signerer arbeidskontrakten som nytilsatt, signerer man også vedlegget. Retningslinjen inneholder punkter om blant annet passord, lagring, bruk av e-post og mobile enheter.

Utover dette varierer tjenesteledernes beskrivelser av rutiner og retningslinjer for ivaretakelse av digital sikkerhet i kommunen. En av lederne beskriver at de har et stort og nylig oppdatert dokument med rutiner for tjenesten, men vedkommende er usikker på om de ansatte er bevisst dette dokumentet. Lederen forteller at det har vært viktig å beskrive all ønsket sikkerhetspraksis i rutiner og retningslinjer på grunn av utskiftinger i personalgruppen. De andre tjenestelederne opplyser at de ikke har rutiner for digital sikkerhet på tjenesten, og at dette temaet ikke er inkludert i internkontrollen på tjenestenivå. En av lederne vi intervjuet er ikke kjent med hvorvidt kommunen har overordnete rutiner for digital sikkerhet.

I spørreundersøkelsen bekrefter nesten alle tjenestelederne at kommunen har regler for digital sikkerhet. Et tydelig flertall oppgir også at det finnes rutiner eller retningslinjer spesielt for eget fagfelt eller tjeneste. På spørsmålet om hvorvidt rutiner for digital sikkerhet er gjennomgått med personalet i tjenesten i løpet av 2024, fordeler tjenestelederne seg på svarkategoriene «ja», «nei» og «vet ikke».

Når det gjelder ansattgruppen som helhet oppgir nesten 85 prosent at kommunen har overordnete rutiner og retningslinjer for digital sikkerhet. 65 prosent svarer at det finnes regler for digital sikkerhet i egen tjeneste, mens én av fire er usikre på dette. Blant de som bekrefter at slike regler finnes, oppgir nesten 70 prosent at de vet hvor de kan finne dem.

De ansatte er delt når det gjelder hvorvidt rutiner for digital sikkerhet er gjennomgått med personalet i sin tjeneste. Mens dette bekreftes av 55 prosent, svarer mer enn én av fire henholdsvis «nei» eller «vet ikke». Disse respondentene fordeler seg på sektorene i kommunen. Spørreundersøkelsen gir ikke svar på om det er overordnete eller tjenestespesifikke rutiner som er tatt opp med personalet.

Kompetanse og opplæring

Det står i informasjonssikkerhetshåndboken at det skal gis opplæring og informasjon til alle ansatte som bruker kommunens datasystemer. Det stilles krav om at opplæring og bevisstgjøring skal være systematisk, og at innholdet skal være tilpasset den enkeltes rolle og oppgaver. Opplæringen skal gjentas ved behov, for å sikre at kunnskapen holdes ved like.

Ifølge håndboken har den enkelte ansatte ansvar for å delta i nødvendig opplæring. Dette innebærer også å forstå hvilke krav som gjelder for seg. Ledere har ansvar for å sørge for at opplæring blir gjennomført, både å tilrettelegge for opplæring og å følge opp at ansatte har tilstrekkelig kompetanse.

Gjennom intervjuene kommer det frem at tjenesteledere oppfatter kompetansenivået blant ansatte som variabelt. En av dem peker på at det er en utfordring å sikre at alle får tilstrekkelig opplæring. Vedkommende forklarer at de har en generell opplæring i tjenesten, men handler mest om vern av personopplysninger. En annen beskriver at de ansatte får sin opplæring gjennom kampanjer som er felles for hele kommunen, og mener at dette er dekkende for behovet i tjenesten. Den samme lederen gir uttrykk for at det er større fokus i kommunen på kompetanseheving på området nå enn tidligere.

I intervju forteller tjenesteledere at de ikke har rutiner for opplæring i digital sikkerhet på tjenestene, foruten at det finnes tilknyttet noen av de store fagsystemene. I denne sammenheng nevnes Gerica og Visma Sikker Sak spesielt. Én av lederne beskriver at digital sikkerhet skal være en del av opplæringspakken, og bemerket at de ved et nylig tilsyn har fått påpekt manglende rutiner når det gjelder opplæring.[50] Det har ifølge lederen vært litt tilfeldig hvilken opplæring ansatte har fått ved oppstart.

I perioden for revisjonen, gjennomfører kommunen en informasjonskampanje utarbeidet av KS.[51] Dette er et e-læringstilbud som går ut til alle ansatte. Tjenesteledere nevnte kampanjen som et eksempel på opplæringstiltak

[50] Referanse til Informasjonssikkerhetshåndboken/datatilsynet

[51] Kampanjen består av ti temaer som presenteres fordelt på ti måneder. Målet med kampanjen er å sikre at de ansatte endrer vaner, for eksempel når det gjelder låsing av enheter, passord, bruk av e-post, lagring og sikkerhet på reise. Se mer informasjon her: https://www.ks.no/fagomrader/digitalisering/digital-kompetanse/informasjonssikkerhet-og-personvern/veiviser-for-a-styrke-robusthet/slik-bruker-kommunen-kampanjen/

innen digital sikkerhet, og la til at kommunen har hatt lignende kampanjer tidligere. Utover dette har ikke kommunen tilbud om opplæring i digital sikkerhet, ifølge lederne.

Spørreundersøkelsen viser at et tydelig flertall, oppunder 80 % av respondentene, ikke kjenner til at kommunen har tilbudt opplæring utover kampanjen fra KS. I overkant av én av fem har imidlertid fått slik tilbud og av disse har om lag halvparten tatt imot ytterligere opplæring.

Nesten 70 prosent av de ansatte som har besvart undersøkelsen oppgir at de har deltatt i KS-kampanjen, enten hver gang eller noen ganger. Av deltakerne oppgir 80 prosent at kampanjen har vært nyttig.[52]

Rundt 70 opplyser at de ønsker mer kunnskap om digital sikkerhet, mens én av ti ikke gjør det. På spørsmål om hvilke områder de ansatte ønsker kunnskap om, trekker de frem «digitale trusler» og «sikkerbruk av KI».

Eksempler på opplæring knyttet til konkrete fagsystem, Visma Flyt Sikker Sak og VA800-X, kan leses under problemstilling en.

4.4.2 FERDIGHETER

Sikkerhetsatferd

Informasjonssikkerhetshåndboken legger stor vekt på sikkerhetsatferd som en integrert del av arbeidshverdagen. Alle ansatte har et ansvar for å opptre sikkerhetsbevisst, for eksempel ved å beskytte informasjon gjennom forsvarlig bruk av e-post, internett, mobile enheter, passord og fysisk tilgang. De skal sikre at uvedkommende ikke får tilgang til informasjon eller IKT-systemer. Håndboken presiserer at leder har ansvar for å tilrettelegge for god sikkerhetsatferd, samt å selv være en tydelig rollemodell.

Retningslinjene for sikker informasjonshåndtering, som følger arbeidskontrakten, inneholder en rekke sikkerhetstiltak til bruk i arbeidshverdagen. I intervju beskriver tjenesteledere ulike tiltak, som for eksempel at de snakker om betydningen av å låse av PCen, systemer med tilgangsstyring og tofaktor-autorisering og smartkort for å komme inn på sikker sone, samt forbud mot TikTok på tjenestetelefoner og privattelefoner dersom man også har jobb-epost og turnusprogram.

Én av tjenesteledere peker på den daglige sikkerhetsatferden som en utfordring, særlig behovet for å integrere sikkerhet som en naturlig del av arbeidshverdagen. Vedkommende antar at de eksisterende rutinene er enkle å følge, men mener det er behov for jevnlige påminnelser for å opprettholde bevisstheten.

I spørreundersøkelsen oppgir 65 prosent at de «alltid» eller «som regel» undersøker om en nettside er sikker før de bruker den. 85 prosent oppgir at de låser skjermen når de forlater datamaskinen sin. Ytterligere noen flere bekrefter at de undersøker om lenker og vedlegg i e-post er sikre før de åpner dem.

Avvik og avvikshåndtering

[52] I «ganske stor» og «svært stor» grad.

Informasjonssikkerhetshåndboken beskriver etablerte rutiner og prosesser for å håndtere uønskede hendelser knyttet til informasjonssikkerhet. Det framgår at avvik skal rapporteres i kvalitetssystemet TQM. Å melde avvik er en viktig del av det å sikre kontinuerlig forbedring og registrerte avvik skal inngå i grunnlaget for ledelsens årlige gjennomgang.

Det kommer frem i håndboken at alle ansatte har et ansvar for å melde fra når de observerer brudd på rutiner eller regler, og for å bidra til en kultur der det er forventet å rapportere uønskede hendelser. Leders ansvar er å sørge for at alle ansatte kjenner til hvordan avvik skal registreres, og for å følge opp at avvik meldes og håndteres i tråd med rutinene. Det innebærer også å bruke kunnskapen fra avvikshåndteringen aktivt i forbedringsarbeid og risikostyring.

Det kommer frem i intervjuene med tjenestelederne at det sjelden registreres avvik innen digital sikkerhet. Et par av dem beskriver at de har hatt gjennomgang av rutiner og/eller oppmerksomhet rettet mot avvik, og dette gjenspeiles i at de ansatte registrerer avvik. Den tredje lederen opplyser at det sjelden meldes avvik i tjenesten. Det forekommer likevel avvik, og lederen antar at de ansatte kjenner til hvordan avvik skal meldes.

Felles for de tre tjenestene er at det ikke kommer inn avvik på IKT-hendelser. Informantene har ikke oppfattet at det er underrapportering på området.

Én av lederne forteller at de arbeider med å oppdatere internkontrollsystemet i tjenesten. I den forbindelse diskuterer de også grenseoppgangen mellom avvik og uønskede hendelser. Det påpekes at det kan være ulik forståelse av hva som regnes som et avvik, og dette er noe de nå arbeider med å tydeliggjøre.

Informasjon fra intervjuene tilser at avvik først lukkes av nærmeste leder, det vil si enten avdelingsleder eller tjenesteleder. Deretter godkjennes avviket av ledernivået over, henholdsvis tjenesteleder eller kommunalsjef. Ifølge de lederne vi har intervjuet, er det tjenestelederne som har ansvar for å rutinemessig rapportere på avvik. Lederne er samstemte i at informasjon og/eller avvik om digital sikkerhet ikke etterspørres, men en av dem opplyser at overordnet ledelse følger med på avvikene generelt sett.

Det kommer frem i spørreundersøkelsen at nesten 80 prosent kjenner til at det finnes rutiner for hvordan man skal melde avvik i kommunen. Én av fem er imidlertid usikre på dette. Over 65 prosent oppgir at de helt eller delvis vet hvordan de skal melde avvik, og én av ti oppgir selv å ha meldt et avvik vedørende digital sikkerhet. I overkant av 30 prosent er usikre på hva som skal meldes som avvik, og 60 prosent er helt eller delvis uenige i at deres leder etterspør avvik innenfor digital sikkerhet.

I gruppen tjenesteledere oppgir nesten alle å kjenne til hva de skal melde som avvik og hvordan de skal gjøre det. Over halvparten oppgir imidlertid å være helt eller delvis uenige i at deres leder etterspør slike avvik.

4.4.3 HOLDNINGER OG BEVISSTHET

Risikoforståelse

Risikoforståelse handler om å ha innsikt i hva som kan gå galt, hva konsekvensene kan bli, og hvilke sårbarheter og trusler som finnes.

Tjenesteledernе er delt i sin oppfatning av hvorvidt ansatte er opptatt av digital sikkerhet. I intervjuene kommer det frem at én av dem mener ansatte er bevisste og forsiktige, og at det ikke er motstand mot sikkerhetstiltakene i kommunen. En annen har inntrykk av at de ansatte verken er opptatt av digital sikkerhet eller er spesielt bekymret for at noe kan gå galt. Denne lederen får sjelden spørsmål om temaet, utover praktiske ting. Vedkommende fikk negative bemerkninger da det ble innført 16-tegnspassord, og tror mange tenker at sikkerhet er tilstrekkelig ivaretatt gjennom påloggings-tiltakene. Også den tredje tjenestelederen vi har intervjuet, beskriver lite bekymring for uautorisert tilgang. Vedkommende mener likevel det er en bevissthet i personalgruppen på å sikre informasjon. Sikkerhetsbruddet i Østre Toten kommune i 2021 var en påminning om hva som kan skje, og hendelsen førte til innstramminger i egen tjenesten, ifølge lederen.

Spørreundersøkelsen viser at de ansatte oppfatter risiko ulikt. På påstanden *«å bruke internett på arbeid er generelt forbundet med høy risiko for sikkerhetsbrudd»* fordeler respondentene seg tilnærmet jevnt i grupper helt/delvis uenig, delvis enig eller helt enig. Undersøkelsen viser også at 85 prosent mener de i stor grad er i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett.[53] Det er imidlertid stor variasjon i hvordan de vurderer risiko knyttet til aktiviteter som bruk av e-post, sosiale medier, kunstig intelligens, flyttbare lagringsenheter og sky-tjenester. I overkant av én av ti vurderer at det er ingen eller liten risiko ved å dele passord med andre.

Lederrollen og ledelsens prioritering

Informasjonssikkerhetshåndboken slår fast at arbeidet med informasjonssikkerhet skal være en integrert del av lederansvaret. Det skal til enhver tid være tydelig hvilke oppgaver og hvilket ansvar som ligger til den enkelte leder. Både ansvars- og myndighetsforhold skal være klart definert.

I intervju kommer det frem at tjenestelederne mener det er viktig at de er opptatt av digital sikkerhet.
En av dem erkjenner likevel at temaet «drukner» litt i hverdagen, og for tjenester som behandler personopplysninger, er det gjerne slik at vern om disse får størst oppmerksomhet.

Tjenestelederne fremstår samstemte i intervjuene i at de har ansvar for det faglige arbeidet i tjenesten og det dette innebærer. En av informantene forklarer at leder har ansvar for at de ansatte følger reglementet, og de to andre fremhever ansvaret for fagsystemene. Tjenestelederne har ikke oppfattet å ha ansvar for digital sikkerhet utover dette. Ifølge en av lederne, finnes ansvaret ikke beskrevet i stillingsbeskrivelse eller rutine.

Det kommer frem i intervjuene at tjenestelederne kontakter IKT-ansatte dersom det skulle være noe. En av lederne beskriver dem som tilgjengelige og som en god støtte. Når det gjelder tekniske problemer er det Ikomm som kontaktes.

Tjenestelederne oppfatter ikke at kommuneledelsen har en særlig oppmerksomhet rettet mot digital sikkerhet. Én av dem beskriver at teamet tas opp i lederforum, noe som bekreftes av en annen leder som sier det har vært et viktig tema.[54] Vedkommende har ikke hatt dialog om digital sikkerhet i sin kontakt med kommunalsjef, men

[53] I «ganske stor» eller i «svært stor» grad

[54] Lederforum er et møtepunkt for kommunalsjefer og tjenesteledere som ledes av kommunedirektør.

opplyser å ha støtte fra overordnet ledelse. Ifølge en av informantene bygger kommunen nå opp sin HR-avdeling med kapasitet på IKT, og vedkommende erkjenner at det kan ha vært jobbet mye med digital sikkerhet uten at det har nådd ut til hele organisasjonen.

Det kommer frem av spørreundersøkelsene at nesten alle tjenestelederne oppfatter at arbeid med digital sikkerhet er en del av deres arbeidshverdag og at de er kjent med sitt ansvar for å gi ansatte opplæring og veiledning. Når det gjelder hvorvidt de har den kompetansen de trenger for å ivareta dette ansvaret, er det flere som er uenige. Mer enn halvparten av respondentene i gruppen opplever ikke å ha tilstrekkelig tid og rom i arbeidshverdagen til å følge opp de ansatte på området.

Nesten alle tjenestelederne opplyser at de får hjelp og støtte fra kommunens IKT-avdeling når de trenger det, og omtrent like mange oppgir at de får hjelp og støtte fra kommunens øverste ledelse på området.

Som helhet fordeler respondentene i spørreundersøkelsen seg på de ulike svaralternativene på spørsmålet om hvorvidt ledelsen har kommunisert tydelige forventninger til dem når det gjelder digital sikkerhet. I overkant av 30 prosent svarer «ikke i det hele tatt», «i svært liten grad» eller «i ganske liten grad». I overkant av 60 prosent svarer «i ganske stor grad» eller «i svært stor grad».

4.5 VURDERINGER

På bakgrunn av innsamlet informasjon skal revisor vurdere om kommunens praksis er i tråd med revisjonskriteriene.

Revisjonskriteriene for denne problemstillingen er utledet i kapittel 5.3. De baserer seg blant annet på Digitaliseringsdirektoratets forståelse av hva som utgjør en sikkerhetskultur; kunnskap, ferdigheter og bevisstgjøring.

4.5.1 KOMMUNEN MÅ SØRGE FOR AT ANSATTE ER ORIENTERT OM RUTINER OG RETNINGSLINJER FOR DEN DIGITALE SIKKERHETEN

Vi vil nå vurdere problemstilling 2:
I hvilken grad arbeider kommunen systematisk med å etablere en sikkerhetskultur i virksomheten?

Kommunen har etablert rutiner og retningslinjer for digital sikkerhet, og det gis informasjon til nytilsatte ved ansettelse. Informasjonssikkerhetshåndboken pålegger både ansatte og ledere ansvar for at reglene følges og er kjent. Spørreundersøkelsen viser at mange ansatte kjenner til at det finnes slike rutiner, og en stor andel vet hvor de finner dem.

Samtidig er det variasjon i hvordan dette følges opp i praksis. Flere tjenesteledere er usikre på om ansatte kjenner rutinene, og temaet synes i liten grad å være integrert i internkontrollen på tjenestenivå. I spørreundersøkelsen oppgir mange ansatte og ledere at rutiner ikke er gjennomgått med personalet, eller at de ikke vet om det har skjedd.

På bakgrunn av foreliggende informasjon vurderes det at kommunen har kommet i gang med arbeidet, men at det fortsatt finnes et klart forbedringspotensial. Kommunen har etablert rutiner og retningslinjer og gir en grunnleggende orientering til ansatte. Oppfølgingen synes imidlertid ikke å være systematisk. Det er variasjon i praksis og usikkerhet blant både ledere og ansatte trekker ned helhetsbildet. Det er behov for mer strukturert oppfølging og tydeligere forankring i internkontrollen.

4.5.2 KOMMUNEN MÅ SØRGE FOR RELEVANT OPPLÆRING TIL ANSATTE INNEN DIGITAL SIKKERHET

Kommunen har iverksatt enkelte tiltak for å gi ansatte opplæring innen digital sikkerhet. Det mest sentrale tiltaket på tidspunktet for revisjonen er en informasjonskampanje i regi av KS, som gjennomføres blant ansatte. Et flertall av respondentene i spørreundersøkelsen har deltatt, og mange oppgir at kampanjen har vært nyttig. I tillegg er det også noe opplæring knyttet til bruk av spesifikke fagsystemer.

Undersøkelsene våre tyder på at opplæringen i hovedsak er begrenset til enkeltstående tiltak, og ikke skjer systematisk og tilpasset behov. Til tross for at ansvaret er formelt definert, fremstår opplæringen noe tilfeldig og praksis synes å variere mellom tjenestene. Tjenestelederne påpeker at det mangler rutiner for opplæring på tjenestenivå. Kun et mindretall av ansatte har fått tilbud om opplæring utover kampanjen fra KS.
Ansattes ønske om ytterligere opplæring kommer tydelig frem i spørreundersøkelsen, og dette understøtter at dagens tilbud ikke er tilstrekkelig dekkende for behovene i organisasjonen.

Oppsummert fremstår kommunens arbeid også på dette området som delvis etablert, og med behov for videreutvikling. Særlig gjelder dette systematisk gjennomføring, tilpasning og forankring i tjenestene.

4.5.3 KOMMUNEN MÅ SØRGE FOR AT ANSATTE KJENNER TIL HVORDAN AVVIK OG UØNSKETE HENDELSER INNEN DIGITAL SIKKERHET SKAL RAPPORTERES, OG JEVNLIG FØLGE OPP OG ETTERSPØRRE SLIKE AVVIKSMELDINGER

Kommunen har et system for avvikshåndtering (TQM), og det fremgår av informasjonssikkerhetshåndboken at avvik skal meldes, følges opp og brukes i forbedringsarbeid. Rundt 80 prosent av de ansatte oppgir i spørreundersøkelsen at det finnes rutiner for avvikshåndtering, og over halvparten vet hvordan de skal melde slike avvik. Tjenesteledere bekrefter i intervju at de har ansvar for å rapportere avvik, og at det finnes en form for oppfølging.

Samtidig viser både intervjuer og spørreundersøkelse at dette ikke er godt implementert i praksis. Mange ansatte er usikre på hva som skal meldes som avvik, og én av fem kjenner ikke til rutinene ifølge spørreundersøkelsen. Det meldes få eller ingen digitale avvik i tjenestene, og tjenestelederne opplyser i intervju at slike avvik ikke

etterspørres fra overordnet nivå. Også i spørreundersøkelsen svarer et flertall at deres leder ikke etterspør avvik innen digital sikkerhet.

Revisjonens vurdering er at kommunen har etablert grunnleggende strukturer, men det er behov for bedre implementering i praksis. Kommunen har et kvalitetssystem og formelle rutiner, men disse er ikke godt kjent eller i aktiv bruk. Oppfølging og etterspørsel fremstår som lite systematisk.

5. KONKLUSJONER OG ANBEFALINGER

Formålet med revisjonen har vært å undersøke om Øyer kommune har etablert tilfredsstillende tiltak for IKT-sikkerhet. På bakgrunn av vurderingene skal revisor konkludere i forhold til problemstillingene. Dersom revisor finner vesentlige avvik, skal dette komme tydelig til uttrykk i forvaltningsrevisjonsrapporten.

5.1 KONKLUSJONER

5.1.1 HAR KOMMUNEN ETABLERT TILFREDSSTILLENDE SIKKERHETSTILTAK MOT DIGITALE ANGREP I UTVALGTE IKT-SYSTEMER?

Visma Flyt Sikker Sak
Konklusjon:
Revisjonen mener at informasjonssikkerheten i Visma Flyt Sikker i stor grad er ivaretatt. VFSS behandler informasjonsverdier som krever høy beskyttelse av konfidensialitet og integritet. Dette betyr at informasjon på avveie kan medføre alvorlige konsekvenser.

KK2
Konklusjon:
Øyer kommune ivaretar i høy grad informasjonssikkerheten i KK2. Systemet håndterer informasjonsverdier som stiller krav om høy integritet, og det er avgjørende at informasjonen er korrekt og ikke endres utilsiktet eller urettmessig.

Begrunnelse for konklusjonene:
Kommunen har utarbeidet en informasjonssikkerhetshåndbok som gir føringer og veiledning innen flere sentrale områder av informasjonssikkerhetsarbeidet. Revisjonen ser det som positivt at Øyer kommune har vedtatt en oppdatert versjon av informasjonssikkehetshåndboken. Håndboken beskriver blant annet prinsipper for tilgangsstyring, krav til risikovurderinger, logging, sikkerhetsoppdateringer og håndtering av sikkerhetshendelser. Dette gir et viktig rammeverk for kommunens arbeid med å sikre sine systemer og data, og bidrar til å etablere en felles forståelse av ansvar og praksis på tvers av organisasjonen.

I våre undersøkelser har vi tatt utgangspunkt i et sett revisjonskriterier som bygger på NSMs grunnprinsipper. For hvert system har vi vurdert om kriteriene er oppfylt, delvis oppfylt eller ikke oppfylt, basert på dokumentasjon, intervjuer og tekniske funn. For begge disse systemene ser vi at de fleste kriteriene er oppfylt.

Selv om flere kriterier er vurdert som oppfylt, er det viktig å understreke at oppfyllelse kan romme et bredt spekter av praksis og modenhet. I noen tilfeller har kommunene fremlagt omfattende dokumentasjon, tydelige rutiner og opplysninger om systematisk oppfølging som underbygger vurderingen. I andre tilfeller er det færre skriftlige rutiner og mindre dokumentasjon, men praksis og intervjuer viser likevel at kriteriet er ivaretatt i tilstrekkelig grad. Dette viser at det kan være ulik modenhet og ulik grad av systematikk i hvordan kriteriene oppfylles.

Et system kan ha etablert tiltak som teknisk sett oppfyller kravene, men mangler strukturert dokumentasjon og forankring. Andre systemer kan ha høy grad av formalisering og krav til seg, som gjør det mindre aktuelt å ha lokal forankring.

De to systemene som er undersøkt i Øyer, VFSS og KK2, leveres som skytjenester og begge behandler personopplysninger som må følge krav etter GDPR. Kommunen må uansett alltid være sitt ansvar bevisst, da det er den som sitter med konsekvensene av uønskede hendelser, uavhengig av hvilken leverandør de bruker.

Når det gjelder gjennomføring av ROS-analyser, har revisjonen avdekket svakheter ved dette arbeidet i begge systemene. Det er særlig svakheter knyttet til kommunenes arbeid med å identifisere og kartlegge risikoer og verdier knyttet til digitale sikkerhetstrusler som er aktuelle for det enkelte system. På bakgrunn av dette mener revisjonen det kan være behov for å styrke de ansattes kompetanse når det gjelder betydningen av digital sikkerhet i kommunens risikoarbeid.

5.1.2 I HVILKEN GRAD ARBEIDER KOMMUNEN SYSTEMATISK MED Å ETABLERE EN SIKKERHETSKULTUR I VIRKSOMHETEN?

Revisjonen viser at kommunens arbeid med å etablere en sikkerhetskultur er påbegynt, men fortsatt i en tidlig fase.

Ledelsen har ansvaret for at sikkerhetsarbeidet er godt integrert i arbeidshverdagen, og det forventes at ledere prioriterer sikkerhet både strategisk og i det daglige arbeidet. Ansatte skal på sin side bidra til å etterleve krav til sikkerhetsatferd, rapportere avvik og delta i opplæring og kompetanseutvikling. Ansattes bidrag er avgjørende for å oppnå en robust sikkerhetskultur i virksomheten.

Revisjonen viser at kommunen har etablert enkelte strukturer og tiltak som skal fremme en sikkerhetskultur, herunder retningslinjer, opplæringstiltak og et system for avvikshåndtering. Det synes å være økt bevissthet om digital sikkerhet i virksomheten, og noen tiltak er iverksatt for å styrke de ansattes kunnskap og praksis. Opplæringen skjer imidlertid i begrenset grad, og lav registrering av avvik reduserer muligheten for læring og forbedring. Det er også variasjon i hvordan rutiner følges opp i tjenestene.

En systematisk og målrettet opplæringsstrategi vil ikke bare bidra til økt etterlevelse av rutiner og sikkerhetstiltak, men også styrke organisasjonens felles forståelse av hva IKT-sikkerhet og digital sikkerhetskultur faktisk innebærer i praksis. En slik bevisstgjøring er særlig viktig i en tid med økende digital kompleksitet og trusselbilde, og bør forankres både på strategisk og operativt nivå.

Samlet sett tyder revisjonens funn på at innsatsen med å etablere en digital sikkerhetskultur foreløpig er lite systematisk og svakt forankret i kommunen. Det vurderes å være behov for en mer helhetlig, systematisk og lokalt forankret tilnærming for å bygge og styrke sikkerhetskulturen i organisasjonen.

5.2 ANBEFALINGER

På bakgrunn av revisjonens samlede vurderinger og konklusjoner presenteres følgende anbefalinger for forbedring. Kommunen bør:

- påse at kravene til informasjonssikkerhet i systemene de bruker er ivaretatt.
- ha en strategi og plan for opplæring innenfor digital sikkerhet. Planen bør sikre at ansatte og ledere får den opplæringen og kompetanseutviklingen de trenger for å ivareta sin rolle innen informasjonssikkerhet.
- påse at ansatte med ansvar for risikobasert arbeid har nødvendig kompetanse i risikostyringsmetodikk, og at de har tilstrekkelig kunnskap om hvilke verdier som skal beskyttes.
- påse at ansatte og ledere har tilstrekkelig kompetanse til å identifisere, registrere og følge opp avvik innen digital sikkerhet.

SENTRALE DOKUMENTER OG LITTERATUR

Digitaliseringsdirektoratet. *Veileder i kompetanse- og kulturutvikling innen digital sikkerhet*. Hentet fra https://www.digdir.no

Digitaliseringsdirektoratet. *Veileder for kartlegging av digital sikkerhetskultur*., hentet fra: https://www.digdir.no

ISO. (2017). ISO/IEC 27001:2017 *Information technology — Security techniques — Information security management systems — Requirements.* International Organization for Standardization.

Kommunenes sentralforbund (KS). (2022). *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet.*

Nasjonal sikkerhetsmyndighet (NSM). (2021). *Grunnprinsipper for IKT-sikkerhet* (Versjon 2.1).

Nasjonal sikkerhetsmyndighet (NSM). (2023). *Nasjonalt digitalt risikobilde 2023.*

NorSIS. (2016). *The Norwegian Cybersecurity Culture*.

Oslo kommunerevisjon. (2018). *Overordnet styring av informasjonssikkerheten* (Rapport 06/2018).

Regjeringen. (2019). *Nasjonal strategi for digital sikkerhet*.

Regjeringen. (2019). *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*.

Personvernforordningen (GDPR). (2016). *Europaparlaments- og rådsforordning* (EU) 2016/679, artikkel 4, nr. 2.

VEDLEGG 1: KOMMUNEDIREKTØRENS UTTALELSE

ØYER KOMMUNE

INNLANDET REVISJON IKS
Att.Guro Selfors Lund
Kirkegata 72
2609 LILLEHAMMER

Offl. § 13, jf. Fvl. § 13 1. ledd

Deres ref	Vår ref	Saksbehandler	Dato
	2024/2720-12	Irene Hagen	29.08.2025

Svar - Høringsbrev vedr. forvaltningsrevisjon IKT-sikkerhet - Samlet vurdering

Det vises til høringsbrev sendt Øyer kommune, den 20.08.2025.

Her inviteres kommunedirektøren til å komme med uttalelse på utkast av forvaltningsrevisjonsrapporten.

Her er en samlet vurdering fra kommunedirektøren:

Som kommunedirektør takker jeg for revisjonens grundige arbeid med å kartlegge og vurdere kommunens rutiner og praksis knyttet til datasikkerhet. Rapporten gir viktige innspill til hvordan vi som kommune kan styrke vår digitale beredskap og sikre innbyggernes personopplysninger på en trygg og forsvarlig måte.

Revisjonen peker på flere områder hvor kommunen har forbedringspotensial, blant annet knyttet til opplæring av ansatte og dokumentasjon av sikkerhetsrutiner. Administrasjonen vil følge opp anbefalingene med konkrete tiltak i tråd med rapportens konklusjoner. Det er samtidig positivt at revisjonen også fremhever områder hvor kommunen allerede har etablert gode rutiner og systemer. Dette gir et godt utgangspunkt for videre arbeid.

Datasikkerhet er et kontinuerlig arbeid som krever både teknisk kompetanse og organisatorisk bevissthet. Dette området må prioriteres i vår videre utvikling, og sikre at kommunen har robuste systemer og rutiner som ivaretar både lovkrav og innbyggernes tillit.

Øyer kommune
Kongsvegen 325
2637 Øyer

Telefon: 61 26 81 00
E-post:postmottak@oyer.kommune.no |
oyer.kommune.no
Org.nr.:

Kommunedirektøren vil sørge for oppfølging av rapporten og at tiltak blir iverksatt i tråd med kommunens ansvar og målsettinger.

Med hilsen

Trond Henning Klausen

Fungerende kommunedirektør

VEDLEGG 2: UTFYLLENDE INFORMASJON OM METODE

Ved å hente informasjon fra flere kilder og benytte ulike metoder for datainnsamling, øker sannsynligheten for at revisjonen gjør riktige funn. Samtidig er det viktig å være oppmerksom på at opplysningene i rapporten er et utvalg av fakta.

DOKUMENTANALYSE

Følgende overordnete dokumenter er gjennomgått:

- Informasjonssikkerhetshåndbok for Lillehammer og Gausdal, versjon 1.1. Vedtatt 25.01.2023
- Informasjonssikkerhetshåndbok for Øyer, versjon 1.2. Vedtatt 02.12.2024
- Informasjonssikkerhetspolicy 3-1 Mål og strategier, versjon 1.1. Vedtatt 06.01.2022 (Lillehammer og Gausdal)
- Informasjonssikkerhetspolicy 3-1 Mål og strategier, versjon 1.2. Vedtatt 04.12.2024 (Øyer)
- Helhetlig risiko og sårbarhetsanalyse 2023-2026 for kommunene Gausdal – Lillehammer og Øyer. Vedtatt 22.06.2023 (Gausdal)

Visma Flyt Sikker Sak, følgende dokumenter er gjennomgått:

- Generell Databehandleravtale -signert av behandlingsansvarlig, 06.06.2018
- Bilag 1-8 til SSA-L LØG (002) Versjon 2017. (Avtale om løpende tjenestekjøp)
- Veiledende bilag til SSA-L – Avtale om løpende tjenestekjøp
- Behandlingsprotokoller skole – (ikke datert)
- Visma Fagsystemer - Appendix A+B (opplysninger om kategorier av registrerte og personopplysninger/ oversikt underleverandører)
- DPIA Visma Flyt applikasjoner
- Rutine tilganger Visma Flyt Sikker Sak (ikke datert)

Egeninkassosystem KK2, KapitalKontroll AS (Øyer), følgende dokumenter er gjennomgått:

- Leveransebeskrivelse Øyer, Lillehammer og Gausdal, 16.09.2022
- Vedlegg til avtale, Notat om risiko, fra KapitalKontroll AS
- Vedlegg til avtale, teknisk, fra KapitalKontroll AS
- Avtale om tilgang til skytjenester, 16.11.2022
- Databehandleravtale, 16.11.2022
- DPIA inkludert ROS, ikke datert
- ROS analyse, ikke datert. (Ifølge informasjonsskriv om oversendt dokumentasjon, er ROS-analysen nylig utarbeidet)
- Personvernerklæring Innfordringskontoret, ikke datert (Ifølge informasjon om oversendt dokumentasjon er denne nylig utarbeidet)
- Retningslinjer for håndtering av personopplysninger i KK2
- Vurdering av KK2 opp mot personvernforordningen artikkel 15

INTERVJUER

Når det gjelder den første problemstillingen, er utgangspunktet kommunenes informasjonssikkerhetshåndbok, hvor det framgår at systemansvarlige har det daglige ansvaret for oppfølging av oppgaver knyttet til de ulike fagsystemene. På bakgrunn av dette har revisjonen valgt å gjennomføre intervjuer med et utvalg systemansvarlige, med formål om å belyse hvordan informasjonssikkerhet og systemforvaltning ivaretas i praksis. For å sikre et bredere datagrunnlag, er denne informasjonen supplert med innspill fra andre relevante personer i organisasjonen, der dette har vært nødvendig for å utdype eller avklare forhold av betydning for revisjonen. Vi har blant annet hatt dialog med IT-ansvarlige i de tre kommunene.

Når det gjelder den andre problemstillingen, ønsket vi gjennom intervjuene å få en dypere forståelse av sikkerhetskulturen i kommunen og hvordan organiseringen av sikkerhetsarbeidet fungerer i praksis. Særlig ønsket vi innblikk i hvordan tjenestelederne vurderer sikkerhetskulturen innenfor eget ansvarsområde.

Det ble benyttet en intervjuguide i samtalene. Informantene fikk referat fra intervjuene til godkjenning.

Informasjonen fra intervjuene er sortert i nøkkeltema knyttet til digital sikkerhetskultur. Vi har sett etter mønstre i det informantene har fortalt, men også variasjon. Videre har vi sett etter hvorvidt informasjon fra informantene støttes av andre kilder som for eksempel funn i spørreundersøkelsen.

SPØRREUNDERSØKELSE

For å undersøke sikkerhetskulturen har vi gjennomført en spørreundersøkelse blant de ansatte i kommunen.

Spørreundersøkelser gir mulighet til å innhente informasjon fra et stort antall personer. Denne undersøkelsen er basert på Norsk senter for informasjonssikring (NorSIS) sin metode for å måle sikkerhetskulturen i befolkningen. Sammen med Digitaliseringsdirektoratet har NorSIS tilpasset denne til bruk for å undersøke digital sikkerhetskultur i en virksomhet. [55]

Vi har tatt utgangspunkt i dette spørsmålssettet[56] ved utformingen av undersøkelsen, og konferert med Digitaliseringsdirektoratet og DIRI. Metoden er nærmere omtalt i Digitaliseringsdirektoratet sin *«Veileder for kartlegging av digital sikkerhetskultur»*.[57]

Spørsmålene fordeler seg på følgende områder:

- Holdninger til digitalisering og digital sikkerhet
- Oppfattelse av risiko
- Synet på styring og kontroll

[55] Metoden er tilpasset av NorSIS med støtte fra Digitaliseringsdirektoratet, Statens Kartverk, OsloMet - Storbyuniversitetet, Fylkesmannen i Oslo og Viken og Rælingen kommune.

[56] I rapporten «The Norwegian Cybersecurity Culture» gjør NorSIS rede for bakgrunnen for temaene i undersøkelsen.

[57] Veileder for kartlegging av digital sikkerhetskultur: https://www.digdir.no/informasjonssikkerhet/veileder-kartlegging-av-digital-sikkerhetskultur/2142

- Sikkerhetsatferd
- Kunnskap, læring og interesse

Tjenesteledere har i tillegg fått spørsmål knyttet til egen lederrolle.

Det ligger ikke offentlig tilgjengelig resultater til bruk for sammenligning. Hensikten er at virksomheten selv kan gjenta kartleggingen for å sammenligne egne tall og følge med på utviklingen.

Gjennomføring
Innlandet revisjon bruker systemet SurveyXact til spørreundersøkelser. Før undersøkelsen sendte kommunen selv ut informasjon til ansatte. Kommunen hadde også ansvar for å tilrettelegge for at så mange som mulig fikk anledning til å besvare undersøkelsen innenfor arbeidstiden i løpet av de to ukene undersøkelsen skulle være tilgjengelig.

Innlandet Revisjon sendte ut en lenke med tilgang til spørreskjemaet til alle ansatte med kommunal e-postadresse. I Øyer kommune ble lenken sendt til 668 e-postadresser.

Gjennom systemet ble det sendt ut en påminning før svarfristen gikk ut, samt en purring en stund etterpå.

Svarprosent
Av de 668 e-postadressene som fikk tilsendt undersøkelsen gav 62 returmelding (feilmelding og ulike varianter av fraværsmeldinger). Totalt 479 personer åpnet lenken til spørreundersøkelsen. Det var 189 som besvarte spørsmålene, og av disse har SurveyXact klassifisert 16 besvarelser som «noen svar», altså delvis besvart spørreskjemaet.

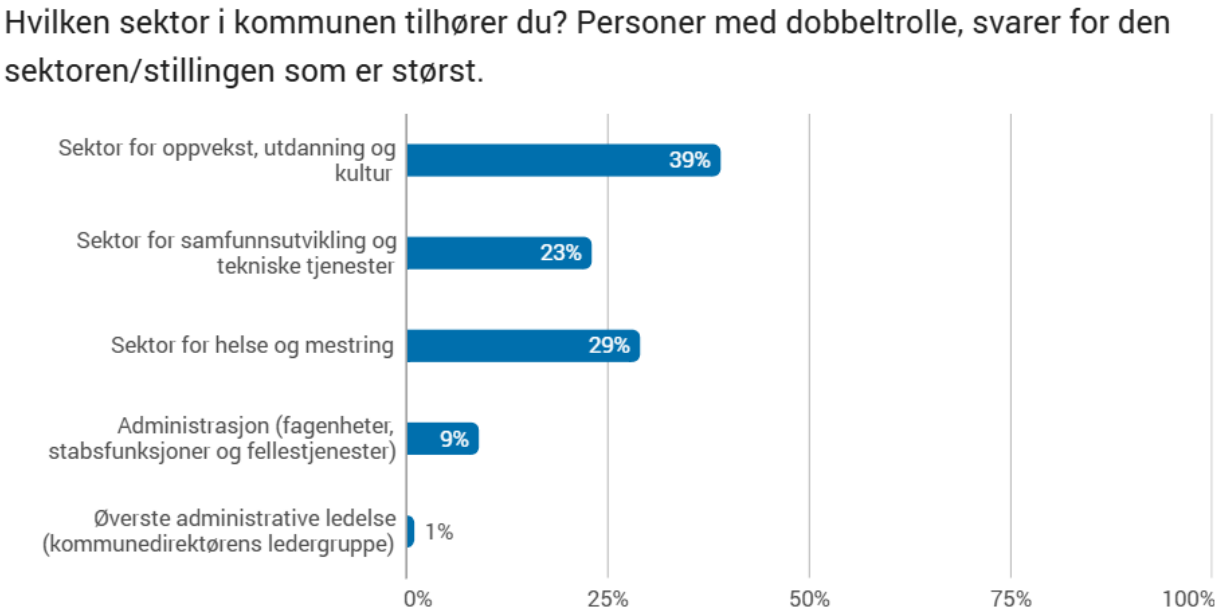
I SurveyXact kategoriseres besvarelser som «noen svar» når en respondent har svart på ett eller flere spørsmål, men ikke har trykket «send» for å fullføre undersøkelsen. Disse besvarelsene regnes dermed ikke som fullførte og vises som delvis gjennomførte i systemet.

Vi har foretatt en konkret vurdering av samtlige delvise besvarelser med tanke på relevans og informasjonsverdi. Blant disse 24 besvarelsene var det noen som kun inneholdt svar på de innledende spørsmålene, mens andre var tilnærmet fulle besvarelser. Vår vurdering er at besvarelsene i denne kategorien samlet sett ikke hadde tilstrekkelig kvalitet til å inngå i analysen, og de ble derfor utelatt fra det endelige datagrunnlaget.

Med dette som utgangspunkt kan vi anslå at i overkant av 28 prosent har besvart spørreundersøkelsen i Øyer kommune. Det finnes ingen klar standard for svarprosent, og *«Veileder i forvaltningsrevisjon og eierskapskontroll»*[58] gir ikke en generell veiledning for hva som er forsvarlig svarprosent.

[58] Veileder i forvaltningsrevisjon og eierskapskontroll, NKRF 2023, https://www.nkrf.no/filarkiv/File/Publikasjoner/Veileder_forvaltningsrevisjon_og_eierskapskontroll_10_2023_FERDIG.pdf

De inkluderte besvarelsene fordeler seg på kommunens tjenester slik det fremgår av figuren nedenfor. Personer med dobbeltrolle har svart for den sektoren/ stillingen som er størst.



Andel respondenter fordelt på sektorer og kategoriserte enheter. Totalt 173 besvarelser er inkludert i analysen.

Ledere

Av de 173 besvarelsene som er inkludert i analysen, oppgir 36 respondenter å ha en lederrolle i Øyer kommune. 14 personer oppgir å være tjenesteledere.[59]

Revisjonen får opplyst at kommunen har 17 tjenesteledere, og vi kan legge til grunn en svarprosent på 80 prosent i dette lederleddet.

Bortfallsanalyse

I utgangspunktet vil et systematisk bortfall svekke verdien av en undersøkelse. Det er likevel slik at undersøkelsen kan gi verdifull informasjon dersom man er oppmerksom på, og tar hensyn til, det bortfallet som finnes.

Revisjonen får opplyst at det er 819 ansatte i kommunen. Det betyr at noen adresser ikke var oppført på e-postlisten som ble benyttet, eller at det finnes ansatte uten kommunal e-postadresse. Det kan være timesvikarer eller ansatte med operative oppgaver som ikke trenger e-post. Ansatte i denne gruppen vil likevel

[59] Spørsmålene hadde to alternativer: 1) Tjenesteleder (inkl. fag-, personal- og økonomiansvar), 2) Annen lederrolle

kunne ha kommunal pålogging med tilgang til kommunens domene og eventuelle fagsystemer i virksomheten de er tilknyttet.

Respondentene valgte selv om de ville svare på undersøkelsen de fikk tilsendt. Dette kan medføre skjevheter for eksempel knyttet til arbeidssituasjon, kunnskap om temaet, personlige interesser og/eller egenskaper.

Analysen viser at av de 173 personene som har fullført undersøkelsen, har 80 prosent en fast arbeidsstasjon. Flertallet av disse oppgir også at de utfører mesteparten av jobben fra arbeidsstasjonen. Over 85 prosent av besvarelsene kommer fra ansatte i over 80 prosent stilling, og under 15 prosent kommer fra ansatte i 60 prosent stilling eller lavere, inkludert vikarer.

Konkret innebærer dette at det er lav deltakelse blant ansatte i deltidsstillinger og vikarer, samt dem som bruker delt arbeidsstasjon eller kun mobile tjenesteer.

Spørreundersøkelsen gir ikke mulighet for å se hvordan respondentene fordeler seg på for eksempel kjønn, alder, fartstid i kommunal sektor og/ eller personlig interesse for data og IKT-sikkerhet.

Analyse

Hensikten med spørreundersøkelsen var å samle informasjon om hvorvidt kommunen jobber systematisk for å etablere og/eller opprettholde en sikkerhetskultur i organisasjonen.

Undersøkelsen antyder i hvilken grad en slik kultur er representert, og gir informasjon om hvordan arbeidet følges opp i praksis. Spørreundersøkelsen gir likevel ikke ett konkret svar på problemstillingen. Flere forhold ligger til grunn for dette:

- I en stor organisasjon som en kommune, er det ikke gitt at det finnes *èn* sikkerhetskultur. Tvert imot vil det utvikle seg flere kulturer, også innenfor områder der det kan være ønskelig for øverste ledelse å ha en felles organisasjonskultur.
- Spørreundersøkelsen er besvart av anslagsvis 39 prosent av kommunens ansatte. Det innebærer at et flertall *ikke* har besvart spørsmålene. Det var frivillig å besvare spørreskjemaet, og det er ikke sikret representativitet i utvalget.
- Det er krevende å kategorisere subjektive oppfatninger. Når det gjelder sikkerhetskultur, kan man stille seg spørsmål om når det er godt nok, og om det noen gang egentlig blir godt nok på et område som er i stadig utvikling.

Undersøkelsen gir nyttig informasjon om hvordan respondentene vurderer forholdene i virksomheten de er en del av og kommunen som helhet. Samlet sett gir et tall på nesten 300 respondenter mulighet for å si noe om sikkerhetskulturen i kommunen som helhet. Til tross for at de fleste tjenestelederne ser ut til å ha besvart undersøkelsen, er det for få respondenter i gruppen «tjenesteledere» til å utføre analyse utover at vi kan se om det finnes variasjon eller om lederne er samstemte.

Når det gjelder revisjonens vurderinger av kommunens arbeid med sikkerhetskultur er det summen av besvarelsene i spørreundersøkelsen, samt hvordan de sammenfaller med informasjon fra datainnsamlingen for øvrig, som er interessant.

VEDLEGG 3: STANDARD FOR LEDELESSSYSTEM FOR INFORMASJONS-SIKKERHET (ISO/IEC 27001:2023)

NS-ISO/IEC 27001:2023 er en anerkjent standard for ledelsessystemer for informasjonssikkerhet. Kravene i standarden er generelle og er ment å være anvendelige for alle virksomheter, uavhengige av type, størrelse eller art.

Mål, strategi og plan for arbeidet
Ifølge standarden skal den øverste ledelsen etablere en informasjonssikkerhetspolicy som egner seg for organisasjonens formål og inneholder en forpliktelse til å etterleve aktuelle krav til informasjonssikkerhet. Policyen bør inneholde sikkerhetsmål som tar hensyn til gjeldende krav til informasjonssikkerhet og resultater fra risikovurdering.

Ledelsen skal sikre tilstrekkelige ressurser til arbeidet og sikre at kravene i ledelsessystemet for informasjonssikkerhet integreres i organisasjonens prosesser.

Organisering og avklaring av roller og ansvar
I tråd med standarden bør ledelsen sikre at de nødvendige ressursene for ledelsessystemet for informasjonssikkerhet er tilgjengelige, og at ansvar og myndighet for roller som er relevante for informasjonssikkerheten, er tildelt og kommunisert.

Risikovurdering og håndtering
Ifølge standarden bør virksomheten utarbeide prosesser for risikovurdering på informasjonssikkerhetsområdet, gjennomføre risikovurderinger i tråd med prosedyrene, utarbeide planer for håndtering av informasjonssikkerhetsrisikoene og dokumentere resultatene fra håndteringen.

Virksomheten bør fastsette alle sikkerhetstiltak som er nødvendige for å håndtere risikoene.

Evaluering og kontroll
Ifølge standarden bør virksomheten evaluere informasjonssikkerheten og virkningen av ledelsessystemet gjennom systematisk måling, og det bør gjennomføres interne revisjoner med planlagte intervaller. Virksomheten skal overvåke informasjonssikkerheten. Det skal defineres hva som skal overvåkes, når og hvilke metoder som skal tas i bruk, hvem som skal overvåke, når resultatene skal analyseres og evalueres og hvem som skal gjøre denne evalueringen.

Den øverste ledelsen bør gjennomgå ledelsessystemet for informasjonssikkerhet med planlagte mellomrom. I ledelsens gjennomgang bør det blant annet vurderes status for tiltak fra tidligere gjennomganger, endringer i relevante eksterne og interne forhold, samt informasjon som gjør det mulig å vurdere oppnåelse av sikkerhetsmålene (som avvik og korrigerende tiltak, overvåkings- og måleresultater, resultater fra revisjoner, resultater fra risikovurderinger).