FORVALTNINGSREVISJONS-
RAPPORT NR. 17-2021

INFORMASJONSSIKKERHET I IKT-SYSTEMER

UTARBEIDET FOR
KONTROLLUTVALGET I
INNLANDET FYLKESKOMMUNE

INNLANDET REVISJON IKS

25.2.2022
2022- 240/IS

FORORD

Denne rapporten er et resultat av forvaltningsrevisjonsprosjektet *«Informasjonssikkerhet i IKT-systemer»* som er gjennomført på oppdrag av kontrollutvalget i Innlandet fylkeskommune.

Forvaltningsrevisjon er en lovpålagt oppgave som innebærer at det føres kontroll med at den kommunale forvaltningen foregår i samsvar med gjeldende lover, regler og vedtak, og har en effektiv ressursbruk i forhold til vedtatte mål. Det er kontrollutvalget som har ansvaret for å se til at det gjennomføres forvaltningsrevisjon, jf. Kommuneloven § 23 nr. 2.

Prosjektarbeidet er i hovedsak utført våren og høsten 2021 av forvaltningsrevisorene Birgitte Ulimoen Bue og Ingvild Selfors. Birgitte Ulimoen Bue var prosjektansvarlig fram til hun sluttet i Innlandet Revisjon i september 2021. Ingvild Selfors er oppdragsansvarlig revisor og Reidun Grefsrud har kvalitetssikret rapporten. I arbeidet med prosjektet har revisjonen leid inn ekstern kompetanse knyttet til informasjonssikkerhetsmiljøet på Gjøvik, gjennom bedriften Diri AS.

Revisjonen har vurdert sin uavhengighet overfor fylkeskommunen, jf. kommuneloven § 24 nr. 4 og forskrift om kontrollutvalg og revisjon, kapittel 3. Vi kjenner ikke til forhold som er egnet til å svekke vår uavhengighet og objektivitet.

Utkast til rapport (høringsutkast) ble opprinnelig sendt fylkeskommunedirektøren for uttalelse den 26.11.2021. Høringsutkastet er et utkast til endelig rapport som baserer seg på mottatt informasjon i prosjektperioden. Revisjonen fikk tilbakemelding på høringsutkastet den 16.12.2021, som innebar en del ny informasjon og kommentarer til rapporten. Revisjonen redigerte rapporten iht relevante kommentarer knyttet til fakta. Informasjon om nye dokumenter og rutiner som kom på plass senhøsten 2021 ble ikke vurdert, men dette er opplyst i noter der hvor det er aktuelt.

Nytt høringsutkast (andre versjon) ble oversendt fylkeskommunen den 3.1.2022. Etter ønske fra fylkeskommunen ble det gjennomført et møte den 14.1.2022 der fylkeskommunen la fram synspunkter knyttet til det nye høringsukastet. Revisjonen har etter dette foretatt noen justeringer i rapporten og nytt og endelig høringsutkast (tredje versjon) ble oversendt fylkeskommunen den 16.1.2022.

Fylkeskommunedirketørens uttalelse til rapporten følger som vedlegg 2.

Vi takker for godt samarbeid med ansatte i fylkeskommunen som vi har hatt kontakt med i prosjektarbeidet.

Lillehammer, 25. februar 2022.

Ingvild Selfors

Ingvild Selfors
Oppdragsansvarlig revisor

INNHOLD

SAMMENDRAG

Digitale løsninger har endret hverdagen vår og gjennomsyrer i dag store deler av våre liv. Koronaperioden har også medført økt behov for gode digitale tjenester, og ifølge SSB, har digitaliseringstakten økt i fire av fem statlige virksomheter og kommuner i denne perioden[1]. Denne utviklingen har også gjort oss mer sårbare. Behovet for forsvarlig IKT-sikkerhet har økt i takt med digitaliseringen.

Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. Formålet med denne forvaltningsrevisjonen er å sette fokus på informasjonssikkerhetsarbeidet i Innlandet fylkeskommune. Prosjektet er todelt. Den første problemstillingen dreier seg om det overordnede informasjonssikkerhetsarbeidet i fylkeskommunen og om fylkeskommunen har etablert en tilfredsstillende internkontroll på informasjonssikkerhetsområdet. I den andre problemstillingen undersøker vi i hvilken grad informasjonssikkerhet er ivaretatt på sentrale områder i utvalgte IKT-systemer.

Revisjonen har gjennomført forvaltningsrevisjonen i tråd med RSK 001 Standard for forvaltningsrevisjon, som innebærer at våre vurderinger er gjort med grunnlag i utarbeidde revisjonskriterier. Vi har brukt en kombinasjon av dokumentanalyse og intervjuer i datainnsamlingen.

Revisjonen har i dialog med fylkeskommunen valgt ut to IKT-systemer for nærmere vurdering i prosjektet. Disse er Skyssweb og Elements Cloud. Det er satt som krav at systemene skal behandle sensitive personopplysninger[2]. Skyssweb er et IT-system som brukes til saksbehandling av søknader om skoleskyss i Innlandstrafikk, mens Elements er fylkeskommunens sak- og arkivsystem.

Det ble formulert to problemstillinger for prosjektet. Nedenfor gjengis revisjonens konklusjoner og anbefalinger for hver problemstilling.

Problemstilling 1:

Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i Innlandet fylkeskommune?

Konklusjon:
Innlandet fylkeskommune har ikke etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet.

Innlandet fylkeskommune er en relativt ny organisasjon og det jobbes med å få på plass et fullverdig styringssystem for personvern og informasjonssikkerhet (internkontrollsystem for informasjonssikkerhet). Det er godkjent flere styrende dokumenter underveis i perioden revisjonsprosjektet har pågått. Revisjonen finner likevel at det er mangler ved styringssystemet ved revisjonsprosjektets slutt. En av utfordringene synes å være manglende kapasitet til å utvikle styringssystemet.

[1] SSB: «Økt digitalisering i offentlig sektor som følge av koronapandemien», 6.5.2021. Artikkel som en del av serien «Bruk av IKT i offentlig sektor».
[2] Definert som «særlige kategorier av personopplysninger» i personvernlovgivningen.

Begrunnelse:
Revisjonen har vurdert om fylkeskommunen har på plass en rekke sentrale krav til et styringssystem (internkontrollsystem) for informasjonssikkerhet.

Fylkeskommunen har etablert en intern organisering av arbeidet med informasjonssikkerhet. Det er definert og tildelt roller og ansvar. Revisjonen mener at rollene sikkerhets- og beredskapssjef og avdelingsleder har fått tildelt svært omfattende ansvarsområder, og at dette kan framstå som noe sårbart. Sikkerhets- og beredskapssjefen har en sentral rolle i å bygge opp styringssystemet, og samtidig det faglige ansvaret for fylkeskommunens sikkerhet på personvern- og informasjonssikkerhetsområdet. Dette arbeidet utføres i praksis av noen få personer, og revisjonen mener at kapasitetsproblemer er en utfordring for framdriften i fylkeskommunens arbeid med å utvikle styringssystemet for personvern og informasjonssikkerhet. I henhold til ISO 27001 skal ledelsen sikre at de nødvendige ressursene for internkontrollsystemet er tilgjengelig og at den interne organisasjonen er hensiktsmessig.

Et viktig element i styringssystemet er en policy eller en strategi for informasjonssikkerhet som skal vise ledelsens mål for arbeidet med informasjonssikkerhet og hvordan målene er tenkt oppnådd. En slik policy/strategi skal danne grunnlaget for virksomhetens internkontroll på informasjonssikkerhetsområdet. Fylkeskommunen har utarbeidet dokumentet *Styringsdokument for personvern og informasjonssikkerhet* som utgjør deres overordnede styringsdokument for arbeidet med personvern og informasjonssikkerhet.

Revisjonen vurderer at målene gitt i styringsdokumentet er lite spesifikke og ikke basert på fylkeskommunens risiko og behov på informasjonssikkerhetsområdet. Det gis ingen plan for hvordan det enkelte mål skal oppnås. Revisjonen mener også at styringsdokumentet i for stor grad har et personvernperspektiv.

Når det gjelder andre styrende rutinedokumenter som skal være en del av internkontrollsystemet finner revisjonen at fylkeskommunen ikke har på plass godkjente rutiner for kompetanse og opplæring, sikkerhet i leverandørforhold, samt kontinuitet og beredskap/hendelseshåndtering. Overordnet retningslinje for risikostyring, samt sikkerhetsinstruks og opplæringspakke for personvern og informasjonssikkerhet er under arbeid[3]. Revisjonen mener at risikostyring er grunnleggende i arbeidet med informasjonssikkerhet og at det er viktig at rutiner for metodikk og kriterier for risikoaksept kommer på plass.

Ifølge ISO 27001 skal virksomheten kontinuerlig evaluere og forbedre internkontrollsystemet for informasjonssikkerhet. Revisjonen mener at arbeidet med kontinuerlig evaluering og forbedring av fylkeskommunens styringssystem for personvern og informasjonssikkerhet ikke er systematisert i tilstrekkelig grad. Når det gjelder rapportering av status for informasjonssikkerhetsarbeidet til ledelsen er det ikke etablert en endelig modell for hvordan denne skal foregå[4].

[3] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst (16.12.21) at dokumentet «*Overordnet sikkerhetskrav for risikostyring av personvern og informasjonssikkerhet*» ble godkjent den 16.11.21 og at fylkeskommunens risikostyringsmetodikk ble godkjent den 5.12.21. Revisjonen har ikke sett disse dokumentene.
[4] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst (16.12.21) at modell for rapportering ble godkjent 19.11.21. Revisjonen har ikke sett denne modellen.

Problemstilling 2:

I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?

Revisjonen har svart på denne problemstillingen gjennom å kontrollere informasjonssikkerheten i to utvalgte IKT-system.

Elements Cloud:

Konklusjon:
Innlandet fylkeskommune ivaretar i høy grad informasjonssikkerheten i sak- og arkivsystemet Elements Cloud.

Begrunnelse:
Elements behandler informasjonsverdier som krever høy beskyttelse av konfidensialitet og integritet. Dette betyr at informasjon på avveie kan medføre alvorlige konsekvenser. Elements er et skybasert system som innebærer en fordeling av sikkerhetsansvaret mellom fylkeskommunen og leverandøren. Revisjonen mener at fylkeskommunen i stor grad har sikret at informasjonen i systemet er beskyttet i samsvar med risikovurderingen av informasjonsverdiene.

Revisjonen vil peke på at det er noen sårbarheter knyttet til ivaretagelsen av informasjonssikkerheten. Det er ikke utarbeidet en hendelseshåndteringsplan, hverken for informasjonssikkerhetshendelser generelt, eller for Elements spesielt.
Det er viktig at organisasjonen har tenkt igjennom ulike scenarioer for hva som kan skje og er forberedt dersom en større hendelse skulle oppstå. Revisjonen mener også at det er en svakhet at det ikke er gjennomført en penetrasjonstest av systemet. Dette er viktig for å teste egen forsvarsevne og avdekke systemets sårbarheter.

Når det gjelder risikovurdering mener revisjonen at det bør utarbeides en rutine for revidering av risikovurderingen med faste mellomrom, og at tiltak iverksettes i henhold til en fastlagt plan som konkretiserer tiltakseier og tidsfrist.

Skyssweb:

Konklusjon:
Basert på den informasjonen som foreligger konkluderer revisjonen med at Innlandet fylkeskommune ikke i tilstrekkelig grad ivaretar informasjonssikkerheten i skoleskyss-systemet Skyssweb. Revisjonen finner flere mangler ved informasjonssikkerheten.

Begrunnelse:
Skyssweb behandler informasjonsverdier som krever høy beskyttelse av konfidensialitet. Systemet driftes av fylkeskommunen og informasjonssikkerheten ivaretas gjennom fylkeskommunens sikkerhetsrutiner. Revisjonen finner ikke at organisatoriske og tekniske tiltak er basert på risikovurderinger.

Når det gjelder organisatoriske tiltak finner revisjonen at det mangler rutine for tilgangsstyring. Det er sårbarheter knyttet til for høye tilgangsrettigheter. Fylkeskommunen sier at dette skal bli bedre når ny versjon av

Skyssweb er implementert. Det er ikke kjent hvordan tilgang til brukere med utvidede rettigheter vil bli sikret etter oppgraderingen, eller når den nye versjonen blir implementert.

Når det gjelder tekniske tiltak påpeker revisjonen følgende:

- Rutine for sikkerhetsoppdateringer medfører risiko for at kritiske sårbarheter forblir i systemet over tid.
- Den tekniske sikringen av data under oppbevaring og i transitt (dataflyt) er vanskelig å vurdere basert på den informasjonen som foreligger. Data under oppbevaring og intern datatrafikk er ikke kryptert, men det foreligger ingen vurdering som sier at dette er i samsvar med risiko. Dersom den fysiske sikringen av serverne har sårbarheter, vil dette kunne medføre at inntrengere kan få tilgang til ukrypterte data.
- Det er etablert evne til å gjenopprette data. Det oppbevares to separate sikkerhetskopier, men det er ikke etablert offline back-up. Dersom det ikke foreligger sikkerhetskopier utenfor det interne nettverket, vil eventuelle inntrengere kunne kryptere/låse all back-up.
- Det er opprettet en hendelseslogg for systemet, men revisjonen stiller spørsmålstegn ved om loggene er tilstrekkelig sikret. Det er uheldig at det finnes muligheter til å endre logger og at loggene slettes etter relativt kort tid.
- Det er ikke etablert en tilfredsstillende sikkerhetsovervåking av systemet. Dette kan medføre risiko for at hendelser ikke oppdages i tide.
- Det er ikke utarbeidet en hendelseshåndteringsplan/beredskapsplan, hverken for systemet eller for informasjonssikkerhetsområdet generelt. Dette kan medføre at organisasjonen ikke er forberedt på hvilke hendelser som kan oppstå, og hvordan de kan håndteres.

<u>Revisjonen har følgende anbefalinger:</u>

Problemstilling 1:

- Fylkeskommunen bør sikre nødvendige ressurser til informasjonssikkerhetsarbeidet. Dagens arbeidsfordeling gir et omfattende ansvar til enkeltpersoner.
- Fylkeskommunen bør sikre at alle ansatte har fått nødvendig opplæring i informasjonssikkerhet som samsvarer med sine roller.
- Fylkeskommunen bør etablere en rutine for systematisk forbedringsarbeid på informasonssikkerhetsområdet.
- Fylkeskommunen bør utarbeide en beredskapsplan/hendelseshåndteringsplan for informasjonssikkerhetsområdet.
- Fylkeskommunen bør utarbeide en policy for informasjonssikkerhet i leverandørforhold.
- Fylkeskommunen bør redigere *Styringsdokument for personvern og informasjonssikkerhet* slik at det blir bedre balanse mellom personvern og informasjonssikkerhet.
- Fylkeskommunen bør redigere *Styringsdokument for personvern og informasjonssikkerhet* slik at fylkeskommunens overordnede mål for informasjonssikkerhet blir bedre tilpasset fylkeskommunens risiko og behov på informasjonssikkerhetsområdet. Det bør videre beskrives en plan/strategi for hvordan målene skal oppnås.

Problemstilling 2:

- Fylkeskommunen bør utarbeide en rutine for å gjennomføre og revidere risikovurderinger av informasjonssystemene i faste intervaller.
- Risikovurderinger av systemer som driftes lokalt bør også inkludere teknisk drift og vedlikehold.
- Fylkeskommunen bør utarbeide en rutine for iverksetting av risikoreduserende tiltak knyttet til risikovurderinger, slik at ansvaret for iverksetting er tildelt og gitt en frist.
- Fylkeskommunen bør sikre en tilfredsstillende sikkerhetsopplæring av brukere av informasjonssystemer.
- Fylkeskommunen bør gjennomføre penetrasjonstester for å teste egen forsvarsevne.
- Fylkeskommunen bør gjennomgå interne rutiner for sikring av IKT-systemer som driftes lokalt. Hvert system skal ha en tilpasset sikring som står i forhold til verdien av informasjonen som behandles. Viktige element i sikringen er:
    - Regelmessige sikkerhetsoppdateringer
    - Rutiner for tilgangsstyring og passord-policy
    - Standardpassord for standardbruker bør byttes
    - Tilstrekkelig sikring av data under oppbevaring og i transitt (dataflyt)
    - Tilstrekkelig sikring av back-up
    - Tilstrekkelig sikring av logger
    - Rutine for sikkerhetsovervåking
    - Tilstrekkelig fysisk sikring av serverpark

1. INNLEDNING

1.1 KONTROLLUTVALGETS BESTILLING

Kontrollutvalget i Innlandet fylkeskommune vedtok i møtet den 4.6.2020, sak 25/2020, å bestille en foranalyse om anskaffelsesprosessen av nye IKT-systemer knyttet til fylkessammenslåingen. Stikkord for bestillingen var ivaretagelse av sikkerhetskrav i anskaffelsene av de ulike IKT-systemene. Foranalysen ble behandlet i kontrollutvalget den 3.9.2020, sak 34/2020.

Informasjonssikkerhet er et stort tema og revisjonen anbefalte i foranalysen at en forvaltningsrevisjon burde avgrenses tematisk for at prosjektet ikke skulle bli for omfangsrikt. Med utgangspunkt i vurderingene i foranalysen ble informasjonssikkerhet i IKT-systemer foreslått som ett av to områder som revisjonen anbefalte å gå videre med. Selve anskaffelsesprosessen ble således ikke en del av prosjektene i denne omgang.

Kontrollutvalget fattet følgende vedtak i behandlingen av foranalysen:

1. Kontrollutvalget bestiller to forvaltningsrevisjoner basert på den fremlagte foranalysen «IKT-anskaffelser og sikkerhet» med følgende tema:
    - Ivaretagelse av informasjonssikkerheten i sentrale IKT-systemer hvor formålet skal være å bidra til å sette fokus på informasjonssikkerheten i sentrale IKT-systemer i fylkeskommunen.
    - Elevdokumentasjon og tilgangskontroller hvor formålet skal være å sette fokus på tilgangsstyring i sentrale IKT-systemer i de videregående skolene.

2. Kontrollutvalget ønsker at prosjektplaner for begge temaene legges fram på neste møte den 15.10.2020.

Denne rapporten omhandler ivaretagelse av informasjonssikkerhet i sentrale IKT-systemer. Det ble lagt fram en prosjektplan for prosjektet i kontrollutvalgets møte den 15.10.2020.

1.2 FORMÅL OG PROBLEMSTILLINGER

Formålet med revisjonsprosjektet er å sette fokus på informasjonssikkerhetsarbeidet i fylkeskommunen og hvordan fylkeskommunen sikrer informasjon i utvalgte IKT-systemer.

Det er formulert følgende problemstillinger for prosjektet:

1. Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i Innlandet fylkeskommune?
2. I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?

I prosjektplanen var det foreslått én problemstilling. Revisjonen har i samarbeid med kontrollutvalget lagt til en problemstilling om internkontroll for informasjonssikkerhet.

I den første problemstillingen undersøker vi det overordnede informasjonssikkerhetsarbeidet i fylkeskommunen. Vi ser på om fylkeskommunen har en tilfredsstillende internkontroll i samsvar med krav som stilles i kommuneloven, personvernlovgivningen og krav som følger av eforvaltningsforskriften.

I den andre problemstillingen undersøker vi i hvilken grad informasjonssikkerhet er ivaretatt på sentrale områder i utvalgte IKT-systemer som behandler sensitiv informasjon. Vi vurderer hvilke tiltak som er iverksatt for å identifisere risikoområder, forebygge uønskede hendelser, oppdage og avdekke uønskede hendelser, samt håndtere uønskede hendelser.

Revisjonen har i dialog med fylkeskommunen valgt ut to IKT-systemer for nærmere vurdering i prosjektet. Disse er Skyssweb og Elements Cloud. Det er satt som krav at systemene skal behandle sensitive personopplysninger[5].

Skyssweb er et IT-system som brukes til saksbehandling av søknader om skoleskyss i Innlandstrafikk, mens Elements er fylkeskommunens sak- og arkivsystem. Systemene blir beskrevet nærmere nedenfor.

1.3 AVGRENSNING

Temaet *tilgangsstyring* behandles ikke særskilt i dette revisjonsprosjektet, siden Innlandet Revisjon gjennomfører et eget prosjekt om tilgangsstyring i Innlandet fylkeskommune sine IKT-systemer som behandler elevdokumentasjon. Fagsystemer i de videregående skolene er derfor ikke vurdert som aktuelle IKT-systemer i dette prosjektet. Tilgangsstyring er et viktig tiltak i informasjonssikkerhetsarbeidet, og det er valgt å behandle dette emnet i en egen forvaltningsrevisjon. Begge revisjonsprosjektene er utført samtidig.

Personopplysningslovens krav til den registrertes rettigheter, slik som retting og sletting, er heller ikke en del av dette prosjektet.

1.4 DEFINISJONER AV BEGREPER

Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. Begrepet IKT-sikkerhet brukes ofte synonymt med informasjonssikkerhet, men informasjonssikkerhet dreier seg om beskyttelse av alle informasjonsverdier, også de som ikke behandles digitalt. I dette prosjektet har vi valgt å bruke begrepet informasjonssikkerhet med fokus på informasjonsverdier som er lagret i IKT-systemer. Vi mener dette er i tråd med bestillingen fra kontrollutvalget.

Informasjonssikkerhet omfatter beskyttelse av:

- Konfidensialitet – at informasjonen ikke blir kjent for uvedkommende.
- Integritet – at informasjonen ikke blir endret utilsiktet eller av uvedkommende.
- Tilgjengelighet – at informasjonen er tilgjengelig for autoriserte brukere ved behov.

[5] Definert som «særlige kategorier av personopplysninger» i personvernlovgivningen.

Personvern er en menneskerettighet forankret i Den europeiske menneskerettighetskonvensjonen (EMK) og i Grunnloven (§ 102). Personvernbegrepet refererer til vern av privatlivets fred og den enkeltes personlige integritet, samt vern av den enkeltes rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv. Vi skal i størst mulig grad kunne være med å bestemme over egne personopplysninger. Med de nye personvernreglene som er innført i hele EU/EØS fra 2018, har disse rettighetene blitt ytterligere styrket.

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson[6]. Typiske personopplysninger er navn, adresse, telefonnummer, e-post og fødselsnummer, men andre eksempler kan være et bilde, et lydopptak, fingeravtrykk, personlige kjennetegn, etc.

Sensitive personopplysninger (kalles særlige kategorier i personvernforordningen) er opplysninger som f.eks. rasemessig/etnisk opprinnelse, politisk oppfatning, religion eller medlemskap i fagforening. Det er et strengere regelverk knyttet til behandling av sensitive personopplysninger.

1.5 OM TEMAET

Digitale løsninger har endret hverdagen vår og gjennomsyrer i dag store deler av våre liv. Koronaperioden har også medført økt behov for gode digitale tjenester, og ifølge SSB, har digitaliseringstakten økt i fire av fem statlige virksomheter og kommuner i denne perioden[7]. Denne utviklingen har også gjort oss mer sårbare. Behovet for forsvarlig IKT-sikkerhet har økt i takt med digitaliseringen. God IKT-sikkerhet, evne til å ivareta personvern og håndtere uønskede digitale hendelser er en forutsetning for at privatpersoner og virksomheter skal ha tillit til den offentlige tjenesteytingen.

I stortingsmeldingen *IKT-sikkerhet. Et felles ansvar* (Meld. St. 38 2016-2017) vises det til trusselvurderinger som viser at fremmede stater er villige til å bruke ulike virkemidler for å få tilgang til sensitiv og skjermingsverdig informasjon og påvirke politiske, økonomiske og forvaltningsmessige beslutninger. De samme virkemidlene benyttes også av kriminelle aktører. Svikt eller sikkerhetsbrudd i digitale tjenester kan inntreffe i en kombinasjon av flere forhold, både tilsiktede handlinger og forsøk på misbruk, så vel som menneskelig svikt, feil i utstyr eller uklar organisering. I PSTs nasjonale trusselvurdering for 2021 vurderes den digitale trusselen fra statlige aktører som alvorlig og økende, og at den største trusselen er fra Russland og Kina.

I SSB[8] sin statistikk om bruk av IKT i offentlig sektor fra 2020 oppgir 4,6 % av norske kommuner at de har vært utsatt for virusangrep e.l. som har ført til vesentlig tap av data eller arbeidstid i løpet av det siste året. Videre oppgir 10,2 % av kommunene at de har opplevd uautorisert tilgang til systemer eller data, og hele 52,9 % av kommunene har opplevd forsøk på identitetstyveri. Østre Toten kommune ble i januar 2021 utsatt for et stort dataangrep, som var et såkalt løsepengeangrep. Angrepet innebar at fremmede aktører brøt seg inn i datasystemene, krypterte data og slettet alle sikkerhetskopier. De fleste av kommunens IKT-systemer ble derfor utilgjengelige for bruk.

[6] Personopplysninger er definert i personvernforordningens artikkel 4.
[7] SSB: «Økt digitalisering i offentlig sektor som følge av koronapandemien», 6.5.2021. Artikkel som en del av serien «Bruk av IKT i offentlig sektor».
[8] SSB: Statistikk hentet fra serien «Bruk av IKT i offentlig sektor». Tabell; IKT-sikkerhetsproblemer i løpet av det siste året 2019-2020.

Den 31. mars fikk kommunen bekreftet at dokumenter med personopplysninger som ble stjålet i dataangrepet var lagt ut på det «mørke nettet»[9]. Dette innebærer at personopplysninger om kommunens innbyggere kan bli misbrukt av kriminelle. Datatilsynet har i oktober 2021 varslet Østre Toten kommune om et overtredelsesgebyr på fire millioner kroner for mangler ved personopplysningssikkerheten og tilhørende internkontroll[10]. I begrunnelsen står det at kommunen blant annet ikke har brukt tofaktor-autentisering ved pålogging og at de har manglet tilfredsstillende back-up systemer og logging av viktige hendelser.

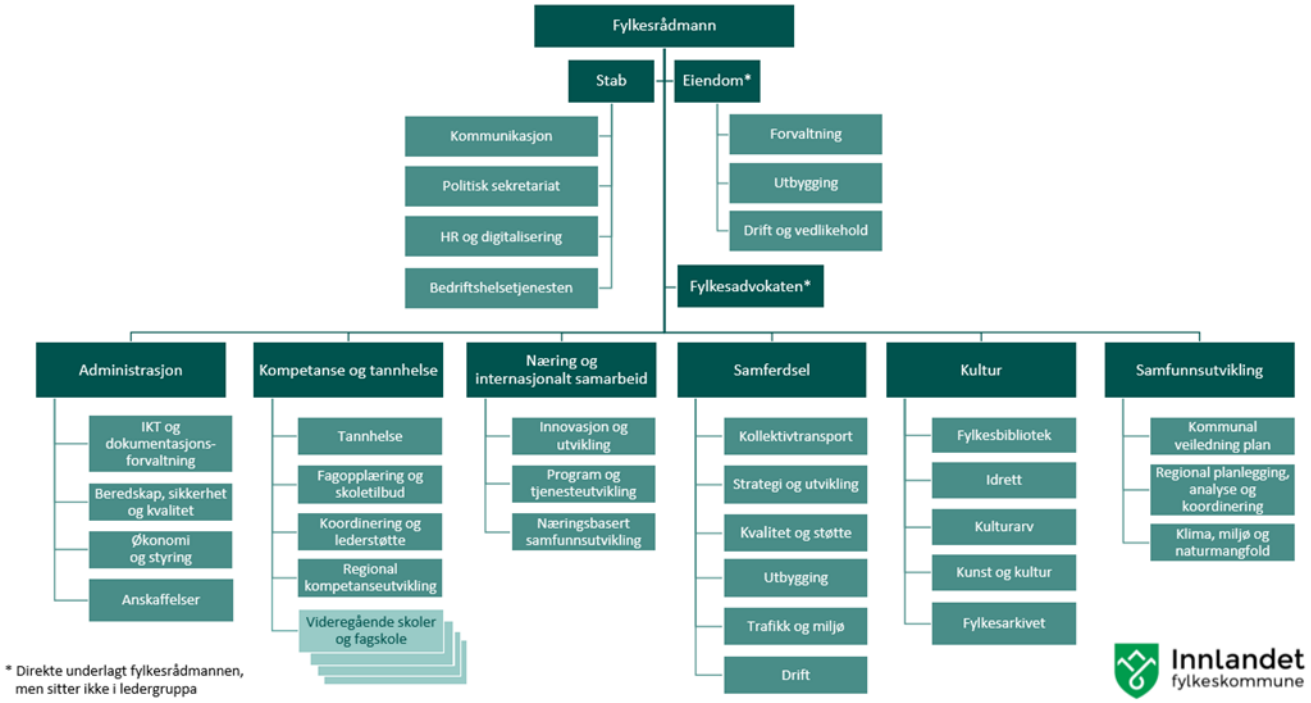
I rapporten som er utarbeidet av KPMG om angrepet i Østre Toten står det at undersøkelser blant norske kommuner, gjennomført av blant annet Digitaliseringsdirektoratet, viser generelt store forbedringsområder innen IKT-sikkerhet. Det er derfor grunn til å anta at tilstanden i sammenlignbare kommuner ligger på omtrent samme nivå som Østre Toten forut for hendelsen.

KS har i etterkant av angrepet i Østre Toten oppfordret alle kommuner om å være oppmerksomme på unormal aktivitet. De vurderer i likhet med nasjonale myndigheter at flere kommuner er utsatt for å kunne rammes av liknende angrep i tiden som kommer. Når en hendelse først inntreffer må kommunene på forhånd ha etablert nødvendige tiltak som sørger for at konsekvensene blir lavest mulig.

[9] KPMG, 26.8.2021: «IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021». Kartlegging og ekstern vurdering.
[10] www.Datatilsynet.no

2. KORT OM FYLKESKOMMUNEN OG IKT-SYSTEMENE

2.1 ORGANISERING



Hedmark og Oppland fylkeskommuner ble slått sammen til Innlandet fylkeskommune 1. januar 2020. Fylkeskommunedirektøren er fylkeskommunens øverste administrative leder. I tillegg til stabs- og eiendomsavdelingene er fylkeskommunen organisert i seks avdelinger: Administrasjonsavdeling, avdeling for Kompetanse og tannhelse, avdeling for Næring og internasjonalt samarbeid, avdeling for Samferdsel, avdeling for Kultur og avdeling for Samfunnsutvikling. Avdelingene består av flere seksjoner og underenheter.

Innlandet fylkeskommune har ca. 4000 ansatte. Fylkeskommunen eier og drifter 23 videregående skoler, Fagskolen Innlandet, 2 folkehøgskoler, karrieresentre, 41 tannklinikker, nesten 7000 km fylkesveger, og har ansvaret for kollektivtrafikken i fylket gjennom Innlandstrafikk.[11]

2.2 IKT-SYSTEMER

Revisjonen har fått oversendt en oversikt over de viktigste administrative IKT-systemene som var i bruk i Innlandet fylkeskommune pr. august 2020, og dette utgjorde ca. 20 systemer. Det er et langt større antall systemer/programvare som er i bruk i IFK totalt. I 2019 ble det gjennomført en kartlegging som viste ca. 400 ulike programvarer i bruk.

[11] Informasjon hentet fra www.innlandetfylke.no.

I dette revisjonsprosjektet har vi plukket ut to IKT-systemer som vi benytter som case for våre undersøkelser.

2.2.1 SKYSSWEB

Skyssweb (Trapeze Cert[12]) er et fagsystem for skoleskyss som brukes av Innlandstrafikk. Systemet ble anskaffet i 2009/2010 av Oppland fylkeskommune.

Formålet med systemet er å planlegge og fatte vedtak om skoleskyss eller skysstilskudd for elever som har rett til å få skoleskyss dekket etter reglene i opplæringsloven. Systemet brukes både for elever i grunnskolen og videregående skole. Vedtak om skoleskyss er et enkeltvedtak[13] og hver elev (eller foresatt) skal søke om skoleskyss for hvert skoleår. For elever i grunnskolen er det skyssansvarlig i skolene eller i kommunen som melder inn behovet for skyss. Elever i videregående skole søker selv gjennom portalen MinSkyss, som er et brukervennlig webgrensesnitt mot Skyssweb.

Elever som bor i en viss avstand fra skolen har rett til gratis skoleskyss[14]. Gratis skoleskyss kan også innvilges uavhengig av veilengden dersom skoleveien vurderes som særlig farlig eller vanskelig, eller dersom eleven har spesielle behov. Skyssweb kan derfor også behandle sensitive personopplysninger.

Fylkeskommunen opplyser at det var 23 364 elever som hadde godkjent skoleskyss i en eller annen form skoleåret 2020/2021. Videre var det 430 aktive brukere av Skyssweb, hvorav ca. 15 er ansatte i Innlandstrafikk. Øvrige brukere er skyssansvarlige i kommunene som legger inn søknader i systemet, samt ansatte i videregående skole som bruker systemet for å kunne hjelpe elever med søknader og bestilling av busskort. Andre brukere av systemet er transportørene (taxi) som trenger tilgang til opplysninger om elever de skal kjøre.

Leverandør og utvikler av systemet er Trapeze, som er et kanadisk firma[15]. På hjemmesiden til Trapeze står det at de utvikler innovativ teknologi til kollektivtrafikk.

2.2.2 ELEMENTS CLOUD

Sak- og arkivsystemet Elements er et stort system som er i bruk i hele fylkesforvaltningen og som behandler store mengder personopplysninger, både personopplysninger om ansatte og om «brukere» av en fylkeskommunal tjeneste. Systemet er nytt og ble implementert samtidig med fylkessammenslåingen. Elements Cloud er en skyløsning som driftes av leverandøren Sikri AS[16].

Elements benyttes til ulike tjenester og består av flere moduler. Disse er;

---

[12] Trapeze Cert er leverandørens navn på systemet.
[13] Definisjonen av enkeltvedtak følger av forvaltningsloven § 2 b: Et vedtak som gjelder rettigheter eller plikter til en eller flere bestemte personer.
[14] Skyssgrensen for gratis skyss varierer mellom skoletrinnene. For elever i 1. kl. er skyssgrensen 2 km, for 2. -10. kl. er grensen 4 km, og for elever i videregående er grensen 6 km. Elever har også rett til drosje til/fra bussholdeplass dersom avstanden til holdeplass er mer enn 3 km.
[15] Det er Europa-kontoret i Danmark som er fylkeskommunens leverandør.
[16] Opprinnelig Evry.

Elements digital post: Mottak/utsending av digital post via digitale kanaler knyttet opp mot Elements, som KS Fiks meldingsformidler, SvarUt og SvarInn.

Elements sak/arkiv: Saksbehandling og arkivering, saksframlegg til politisk behandling, administrative vedtak, m.m.

Elements publikum: Publisering av offentlig postliste og møtedokumenter, bestilling av innsyn via postliste, m.m.

Elements møte: For- og etterarbeid ved møter, avvikling av digitale møter, tilgang til elektroniske møtedokumenter.

Informasjonen som behandles i Elements kan systematiseres i hovedkategorier, avhengig av type saker. Informasjonen i systemet finnes i personalmapper, elevmapper, politiske saker, saker knyttet til anskaffelser, eller saker knyttet til generell saksbehandling. I tillegg vil det være informasjonsverdier i e-poster.

3. METODE

Prosjektet er gjennomført i henhold til RSK 001 Standard for forvaltningsrevisjon, som er gjeldende som god kommunal revisjonsskikk fastsatt av Norges kommunerevisorforening. Innlandet Revisjon IKS har et internt kvalitetssikringssystem som er i samsvar med RSK 001.

Det ble avholdt oppstartsmøte for prosjektet den 10. november 2020 på Teams. På møtet deltok fylkeskommunedirektør Tron Bamrud, administrasjonssjef Åge Solheim, daværende seksjonssjef for IKT og dokumentasjonsforvaltning Bjørn Rune Holmen, sikkerhets- og beredskapssjef Endre Hjelseth, enhetsleder for dokumentasjonsforvaltning Daiva Skoglund, leder drift og forvalting kollektiv Tor Haugstulen, rådgiver Per Solbakken (Skyssweb), og systemansvarlig for Elements Hanne Andersen Østvang. I møtet redegjorde revisjonen for den planlagte gjennomføringen av prosjektet, herunder problemstillinger, revisjonskriterier, og metode. Et referat fra oppstartmøtet ble sendt fylkeskommunen for verifisering.

Revisjonen har valgt å knytte til seg ekstern ekspertise for å kvalitetssikre revisjonskriterier og vurderinger. Dette ble formidlet i oppstartmøtet og er i samsvar med prosjektplanen. Det ble opprettet kontakt med selskapet Diri AS som leverer tjenester knyttet til informasjonssikkerhet, og som springer ut av informasjonssikkerhetsmiljøet ved NTNU i Gjøvik. Konsulenten som har vært benyttet er Gaute Wangen.

Prosjektet baserer seg i stor grad på dokumentanalyse i informasjonsinnhentingen, samt intervjuer med sentrale personer. Det er også innhentet informasjon via e-post. På grunn av koronapandemien har de fleste samtalene med personer i fylkeskommunen foregått via videosamtaler.

Datainnsamlingen gjelder i hovedsak fylkeskommunens praksis våren 2021. En beskrivelse av innsamlet informasjon (utkast til rapportens datakapitler) ble oversendt fylkeskommunen for gjennomgang i september 2021. Fylkeskommunens kommentarer til datakapitlene ble innarbeidet i rapporten. Revisjonen har også stilt oppfølgingsspørsmål ila høsten 2021. Fylkeskommunen har underveis i prosjektperioden oversendt nye rutinedokumenter etter hvert som de er blitt godkjent.

3.1 VALG AV IKT-SYSTEMER

I prosjektplanen ble det antydet at vi ville plukke ut to IKT-systemer i samarbeid med fylkeskommunen. IKT-systemer som benyttes i skolene er holdt utenfor i dette prosjektet for å avgrense mot revisjonsprosjektet som gjennomføres parallelt om tilgangsstyring. Kriteriene for utvelgelse av IKT-system var at de skulle behandle sensitive personopplysninger og at de ikke var system som behandlet elevdokumentasjon.

Sak- og arkivsystemet Elements Cloud er et nytt system med et stort antall brukere og som behandler store mengder personopplysninger, inkludert særlige kategorier (sensitive personopplysninger). Dette er et sentralt system for fylkeskommunen, og ble derfor valgt ut som ett av systemene vi skulle se nærmere på.

I samarbeid med fylkeskommunen ble saksbehandlingssystemet Skyssweb valgt som det andre systemet. Skyssweb benyttes i Innlandstrafikk og behandler søknader om skoleskyss. Systemet inneholder sensitive personopplysninger.

Det ble også vurdert om systemene som tannhelse bruker kunne være aktuelle. Hedmark Revisjon IKS gjennomførte i 2016 en forvaltningsrevisjon om IKT- sikkerhet, drift og utvikling i Hedmark fylkeskommune, hvor sikring av personopplysninger i tannhelsetjenesten var noe av det som ble vurdert. Revisjonen vurderte derfor at risikoen var lavere for disse systemene enn systemer som ikke tidligere hadde blitt gjenstand for kontroll.

Vi mener det potensielt vil kunne gi store konsekvenser for brukere hvis begge de valgte systemene skulle bli utsatt for sikkerhetsbrudd.

3.2 DOKUMENTANALYSE

3.2.1 PROBLEMSTILLING 1

Følgende dokumenter er gjennomgått:

- Styringsdokument for personvern og informasjonssikkerhet, godkjent av Åge Solheim 7.4.2021.
- Roller og ansvar for informasjonssikkerhet og personvern, godkjent av Åge Solheim 1.3.2021.
- Overordnede sikkerhetskrav for informasjonsklassifisering, godkjent av Åge Solheim 7.4.2021.
- Overordnede sikkerhetskrav til adressesperre for trusselutsatte personer, godkjent av Åge Solheim 4.6.2021.
- Bruk av «følsomhet», klassifisering av informasjon i Office 365. Ikke merket med godkjenning.
- Arkitekturprinsipper for Innlandet fylkeskommune. Versjon 2.0, godkjent av fylkesrådmannen 10.8.2020.
- Overordnet sikkerhetskrav for risikostyring, under arbeid.
- Rammer for bruk av kvalitetssystemets avviksmodul. Versjon 1.0, godkjent av Åge Solheim, 7.1.2021.
- Registrering, behandling og rapportering av avvik. Versjon 1.0, godkjent av Åge Solheim, 7.1.2021.
- Prosedyre for avvik personvern og informasjonssikkerhet, godkjent av Åge Solheim, 20.8.2021.
- Overordnet krisehåndteringsplan for Innlandet fylkeskommune, vedtatt av fylkeskommunedirektøren, siste revisjon 10.1.2021.

3.2.2 PROBLEMSTILLING 2

Elements
Følgende dokumenter er gjennomgått:

- Standard tjenestenivå for Elements Cloud, SSA – L[17].
- Avtale om kjøp av ny sak-/arkivløsning til Innlandet fylkeskommune, SSA – L, datert 5.4.2019.
- Oppsummering av risikovurdering, Elements Cloud. Versjon 1.1, 3.12.2019.
- Oppfølging av tiltak etter gjennomført risikovurdering. Oppdatert 3.5.2021.
- Databehandleravtale vedr. Elements Cloud mellom EVRY Norge AS og Innlandet fylkeskommune, signert 2.1.2020.
- Rutine for tilgangsstyring i Elements. Godkjent av Åge Solheim, 7.5.2021.
- Nødprosedyre ved utilgjengelig sak-/arkivsystem Elements, godkjent av Åge Solheim 5.5.2021.

[17] Statens standardavtale for løpende tjenestekjøp (SSA – L).

Skyssweb
Følgende dokumenter er gjennomgått av revisjonen:

- Brukerveiledning for Skyssweb, datert 13.6.2017.
- Risikovurdering av Skyssweb, 28.6.2019.

3.3 INTERVJUER

3.3.1 PROBLEMSTILLING 1

Det er gjennomført intervju/samtale med følgende personer i forbindelse med problemstilling 1:

- Dejan Ljusic, rådgiver i seksjon for Kvalitet, sikkerhet og beredskap, på Teams den 19.5.2021 og 9.11.2021.

3.3.2 PROBLEMSTILLING 2

Elements
Det er gjennomført et gruppeintervju på Teams den 31.5.2021 med aktuelle personer i fylkeskommunen som har ansvar for Elements:

- Åge Solheim (tjenesteeier - administrasjonssjef)
- Daiva Skoglund (tjenesansvarlig – enhetsleder Dokumentasjonsforvaltning)
- Dejan Ljusic (fagansvarlig for informasjonssikkerhet og personvern)
- Yngve Nordseng (daværende enhetsleder IKT – Prosjekt og utvikling (risikovurderinger))
- Mona Ring Nyheim (tjenesteforvalter - integrasjonsansvarlig)
- Hanne A. Østvang (tjenesteforvalter – systemadministrator)

Skyssweb
Det er gjennomført et intervju med Per Solbakken på Teams den 9.6.2021. Per Solbakken er rådgiver i avdeling for Digitale tjenester i Innlandstrafikk. Det har også vært e-post korrespondanse i november 2021.

3.4 KVALITETSSIKRING – RELEVANS OG PÅLITELIGHET

Dataenes relevans er knyttet til om undersøkelsen representerer den virkelige situasjonen. Vi mener data som er samlet inn i denne undersøkelsen er egnet til å svare på problemstillingene. Det er likevel viktig å være oppmerksom på at de opplysninger som framkommer i rapporten nødvendigvis er et utvalg av fakta.

Fylkeskommunen er en relativt fersk organisasjon, og vi har mottatt dokumenter undervegs i prosjektet som er nylig utarbeidet. Det tar tid å innarbeide rutiner for en ny organisasjon, men kravene på området er ikke nye.

Med pålitelighet menes at data skal være mest mulig presise og nøyaktige. Dette er blant annet ivaretatt ved verifisering av intervjureferater og ved innhenting av uttalelse fra fylkeskommunedirektøren på utkast til rapport.

4. REVISJONSKRITERIER

I en forvaltningsrevisjon skal revisor utlede revisjonskriterier. Kilder til revisjonskriterier er de lover, forskrifter, retningslinjer, kommunale vedtak, faglige standarder, eller andre anerkjente kilder, som sier noe om hvordan den (fylkes)kommunale virksomheten skal drives innenfor det området vi ser på. Hensikten med revisjonskriteriene er å sette opp noen autoritative[18] standarder som (fylkes)kommunens praksis kan måles opp mot, og som er grunnlaget for revisjonens vurderinger.

I henhold til Standard for forvaltningsrevisjon (RSK 001), punkt 15, skal revisjonskriteriene være «relevante, konkrete og i samsvar med de kravene som gjelder for revidert enhet innenfor den aktuelle tidsperioden».

Revisjonen mener at revisjonskriteriene vi har satt opp er gyldige for Innlandet fylkeskommune i den tidsperioden vi ser på.

Vi benytter følgende kilder til revisjonskriterier i dette prosjektet:

- Kommunelovens bestemmelse om internkontroll, § 25 – 1.
- eForvaltningsforskriften med tilhørende veiledning.
- Personopplysningsloven med personvernforordningen.
- Digitaliseringsdirektoratets veiledningsmateriell for internkontroll på informasjonssikkerhetsområdet.
- Nasjonal Sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet, versjon 2.0.
- Standard for styringssystem for informasjonssikkerhet (ISO/IEC 27001).

Nedenfor bruker vi kildene til å utlede konkrete revisjonskriterier som vi kan måle fylkeskommunens praksis opp mot.

4.1 UTLEDNING AV KONKRETE REVISJONSKRITERIER

4.1.1 INTERNKONTROLL

4.1.1.1 Kommuneloven

Lovens kapittel 25 inneholder bestemmelser om kommunedirektørens internkontroll.

§ 25-1 lyder slik:
«*Kommuner og fylkeskommuner skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Kommunedirektøren i kommunen og fylkeskommunen er ansvarlig for internkontrollen. Internkontrollen skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Ved internkontroll etter denne paragrafen skal kommunedirektøren*

[18] Autoritativ: toneangivende, med myndighet/autoritet.

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

§ 25-2[19] sier:
Kommunedirektøren skal rapportere til kommunestyret og fylkestinget om internkontroll og om resultater fra statlig tilsyn minst én gang i året.

Kommunedirektøren skal etablere og dokumentere nødvendige rutiner og prosedyrer for å sikre at lover og forskrifter følges, samt evaluere og forbedre etablerte prosedyrer og tiltak for internkontroll. Videre skal status for internkontrollen rapporteres til fylkestinget minst én gang i året. Dette vil også gjelde på informasjonssikkerhetsområdet.

4.1.1.2 eForvaltningsforskriften

Forskriften har som formål å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen og gjelder bruk av IKT-systemer til saksbehandling og kommunikasjon med og i forvaltningen.

Forskriften gir konkrete føringer for bruk av elektronisk kommunikasjon i et forvaltningsorgan. Risiko for uberettiget innsyn i opplysningene ved bruk av elektronisk kommunikasjon må «være forebygget på tilfredsstillende måte», jf. § 5 første ledd.

Videre følger det av forskriften § 15 at det er krav til internkontroll på informasjonssikkerhetsområdet. Forvaltningsorganet som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Kommunal- og moderniseringsdepartementet har utarbeidet en veiledning til eForvaltningsforskriften[20]. Veilederen består av tre deler og del 3 viser forskriftens bestemmelser med tilhørende kommentarer (noter).

I kommentar til § 15 (note 88) står det blant annet: «*Forvaltningsorganet har plikt til å utarbeide sikkerhetsmål og sikkerhetsstrategi. Sikkerhetsmålene beskriver hva som ønskes oppnådd på informasjonssikkerhetsområdet. De skal understøtte og bidra til realisering av forvaltningsorganets overordnede mål, etterlevelse av lover og regler og kostnadseffektiv drift. Sikkerhetsstrategien beskriver hvordan forvaltningsorganet skal nå sikkerhetsmålene. Enkelte forvaltningsorgan velger å legge overordnede prinsipper og kanskje andre føringer inn i et eget dokument kalt informasjonssikkerhetspolicy. Forskriftens bruk av sikkerhetsstrategi dekker alle de overordnede føringene fra ledelsen, uavhengig av omfang, om innholdet kalles policy, strategi eller annet og om det styrende innholdet samles i ett eller flere dokument».*

[19] Gjelder fra 1.1.2021.
[20] Veileder til eForvaltningsforskriften, Kommunal- og moderniseringsdepartementet (2015).

Det følger videre av forskriften § 15 andre ledd at internkontrollen på informasjonssikkerhetsområdet skal basere seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Omfang og innretning på internkontrollen skal være tilpasset risiko. I kommentar til § 15 (note 91) står det:

«*I det ligger en klar føring om at det ikke er tilstrekkelig å basere seg på generelle rammeverk eller standarder for virksomhetsstyring alene. Når det gjelder informasjonssikkerhetsområdet må forvaltningsorganet basere seg på de standarder som er utviklet innenfor informasjonssikkerhetsområdet spesielt og som oftest omtales som styringssystem for informasjonssikkerhet. De må i tillegg være anerkjente. Samtidig gir eForvaltningsforskriften gjennom nøkkelordene «basere seg på» et viktig handlingsrom til det enkelte forvaltningsorgan for å tilpasse anvendelsen av anerkjente standarder på informasjonssikkerhetsområdet til egne behov og egen helhetlig virksomhetsstyring. Selv om den anerkjente standarden en velger å basere seg på stiller spesifikke krav, må forvaltningsorganet selv beslutte ut fra egen risikovurdering om det enkelte kravet i standarden er noe forvaltningsorganet faktisk skal følge eller ikke. Alle kravstandarder om internkontroll/styringssystem blir derfor i eForvaltningsforskriftens forstand veiledende. Vesentlige avvik fra valgt kravstandard bør imidlertid begrunnes, da de er ment å representere god praksis «for de fleste».*

eForvaltningsforskriften gir altså konkrete krav til forvaltningsorganet/fylkeskommunen om å etablere internkontroll på informasjonssikkerhetsområdet. Internkontrollen skal være tilpasset risiko, innrettes med grunnlag i utarbeidde sikkerhetsmål og sikkerhetsstrategi, og skal baseres på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontroll på informasjonssikkerhetsområdet kan også omtales som et styringssystem/ledelsessystem for informasjonssikkerhet.

4.1.1.3 Personopplysningsloven

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. Forordningen er delt inn i to deler; fortalen og artiklene. Fortalen er en tolkningshjelp som skal utfylle eller forklare artiklene.

Personopplysningsloven handler om behandling av personopplysninger[21]. Den nye personopplysningsloven har som mål å sikre vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger.

Fylkeskommunen behandler personopplysninger om innbyggere, politikere og ansatte og er derfor pliktige til å følge regelverket som gjelder for personopplysninger.

Artikkel 5 i personvernforordningen angir grunnleggende prinsipper for behandling av personopplysninger. Ett av prinsippene er at personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet, herunder

[21] 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).

vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak (integritet og konfidensialitet).

Videre framgår det av artikkel 24 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. Nevnte tiltak skal gjennomgås på nytt og oppdateres ved behov. Tiltakene skal omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger. Dette kan oppsummeres som rutiner og tiltak for informasjonssikkerhet, eller internkontroll for informasjonssikkerhetsområdet.

Ved utforming av tiltak skal det tas hensyn til «behandlingens art, omfang, formål og sammenheng, samt hva sannsynligheten og konsekvensen er for at uønskede hendelser skal inntreffe. Kravene til styringssystem for informasjonssikkerhet (eForvaltningsforskriften) vil i stor grad sammenfalle med kravene som følger av personvernregelverket.

I artikkel 32 står det at både den behandlingsansvarlige og databehandleren plikter å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen». Den behandlingsansvarlige er den som er overordnet ansvarlig i virksomheten for å overholde personvernprinsippene og regelverket. I dette prosjektet vil det være Innlandet fylkeskommune som er den behandlingsansvarlige. En databehandler er en som behandler personopplysninger på vegne av den behandlingsansvarlige, i dette tilfellet vil det være IT-leverandørene til fylkeskommunen. Ved vurdering av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen av personopplysningene, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Personopplysningsloven slår altså fast at virksomheter som behandler personopplysninger skal etablere internkontroll for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med krav. Internkontrollen skal bestå av egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som står i forhold til risikoen forbundet med behandlingen av personopplysningene (konfidensialitet og integritet), og skal omfatte egnede retningslinjer for vern av personopplysninger. Tiltakene skal gjennomgås og oppdateres ved behov.

4.1.1.4 Digitaliseringsdirektoratets veiledningsmateriell for internkontroll på informasjonssikkerhetsområdet

Digitaliseringsdirektoratet (Digdir) er utpekt av Kommunal- og moderniseringsdepartementet (KMD) til det organ som skal gi anbefalinger knyttet til internkontroll på informasjonssikkerhetssområdet, etter efvf § 15. Digdir har utarbeidet veiledningsmateriell, tilgjengelig på Digdir.no, som beskriver hvordan virksomheter kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet.

Veiledningen er basert på den internasjonale IT-standarden ISO/IEC 27001 og konkretiserer de mest sentrale delene av standarden[22]. ISO/IEC 27001 er den mest anerkjente standarden ved etablering av internkontroll på informasjonssikkerhetsområdet.

Helhetlig styring og kontroll

I veiledningsmateriellet understrekes det at for å sikre god styring og kontroll av informasjonssikkerhet må en jobbe helhetlig, og se informasjonssikkerhet som en del av virksomhetsstyringen. Nedenfor presenteres kort grunnleggende aktiviteter i arbeidet med helhetlig styring og kontroll (eller innhold i et styringssystem for informasjonssikkerhet):

Ledelsen må lede an, og ha det overordnede ansvaret for at arbeidet med informasjonssikkerhet gjennomføres på en hensiktsmessig måte. Ledelsen må sørge for at styringsaktiviteter blir etablert og fulgt opp, samt sikre tilstrekkelige ressurser til arbeidet. Videre må ledelsen sørge for en hensiktsmessig organisering av arbeidet, og at *roller og ansvar* er klart beskrevet og formidlet. Ledere av risikoområder må kjenne sitt ansvarsområde og gjøres i stand til å vurdere og håndtere risikoen innenfor sitt område.

For å oppnå og opprettholde nødvendig informasjonssikkerhet må arbeidet være prosessorientert med *systematiske aktiviteter*. Styring og kontroll av informasjonssikkerhet handler om å *styre risikoen* i oppgaver og tjenester som er avhengig av digital teknologi og digitale tjenester. Arbeidet må tilpasses virksomhetens egenart, risiko og vesentlighet. En del av risikostyringen innebærer å etablere sikkerhetstiltak som står i forhold til den risikoen som skal håndteres, samt etablere gode føringer for å forstå, vurdere, og håndtere risiko. Det må finnes gode anvendbare kriterier for å akseptere risiko.

En forutsetning for arbeidet med styring og kontroll er å sørge for at organisasjonen innehar riktig *kompetanse,* samt å bygge en sterk *sikkerhetskultur* som understøtter de målsettingene en har i informasjonssikkerhetsarbeidet.

Arbeidet med styring og kontroll av informasjonssikkerhet skal være en del av virksomhetens styringssystem, og må være gjenstand for *kontinuerlig oppfølging* og korrigering. Eksempler på kilder som kan benyttes til forbedring av arbeidet er analyser etter sikkerhetshendelser, øvelser, tester, avvikssystem, eller internrevisjon. Status på virksomhetens arbeid med informasjonssikkerhet bør også regelmessig gjennomgås i den øverste ledelsen av virksomheten.

Styringsaktivteter og sikkerhetstiltak

I arbeidet med styring og kontroll er «styringsaktiviteter» og «sikkerhetstiltak» to sentrale begreper. På digdir.no omtales disse begrepene slik:

[22]I referansekatalogen for IT-standarder, under bruksområde «Internkontroll/styringssystem/ledelsessystem for informasjonssikkerhet», anbefaler Digdir at internkontrollen baseres på den internasjonale standarden ISO/IEC 27001:2013 (nå erstattet med en oppdatert versjon: ISO/IEC 27001:2017).

Referansekatalogen er en oversikt over IT-standarder som er obligatoriske eller anbefalte for offentlig sektor. Standardene er sortert etter aktuelle bruksområder.

Med «styringsaktiviteter» menes de lederstyrte aktivitetene som utgjør kjernen i styring og kontroll på informasjonssikkerhetsområdet. Det er blant annet snakk om aktiviteter for å vurdere og håndtere risiko. Det handler om å ta beslutninger, prioritere oppgaver, fordele ressurser og følge opp arbeidet – å styre dette området som en del av den helhetlige styringen av virksomheten.

Med «sikkerhetstiltak» menes de varige tiltakene som virksomheten etablerer og forvalter for å redusere risikoen for informasjonssikkerhetsbrudd. Dette er tiltak som velges og etableres ved gjennomføring av styringsaktivitetene «risikovurdering» og «risikohåndtering».

Man kan skille mellom tiltak som har som formål å forebygge uønskede hendelser, tiltak som skal oppdage og avdekke hendelser, og tiltak som skal benyttes i respons på hendelser som er under utvikling eller har funnet sted.

Sikkerhetstiltak deles inn i følgende grupper;

- organisatoriske tiltak (roller og ansvar, retningslinjer, prosedyrer og rutiner mv.)
- menneskelige tiltak (kompetanse og kultur)
- tekniske tiltak

Styringsaktivitetene er svært like uavhengig av hvilket område som styres (informasjonssikkerhet, personvern, sikkerhetsstyring iht. sikkerhetsloven, ansattes helse iht. HMS-regelverk, osv.). De konkrete sikkerhetstiltakene vil variere ut ifra hvilket område som styres.

Når det gjelder styring og kontroll på informasjonssikkerhetsområdet følger krav til styringsaktiviteter av ISO/IEC 27001 (kapittel 4 til 10), mens krav til sikkerhetstiltak følger av ISO/IEC 27002[23] eller Tillegg A til ISO/IEC 27001. Digitaliseringsdirektoratets veiledning for styring og kontroll på informasjonssikkerhetsområdet beskriver styringsaktivitetene. Nasjonal sikkerhetsmyndighets (NSM) [24] grunnprinsipper for IKT-sikkerhet inneholder sentrale sikkerhetstiltak en virksomhet kan ha behov for, og uthever de viktigste sikringstiltakene i ISO/IEC 27002:2017.

4.1.1.5 ISO/IEC 27001

ISO 27001 er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet (internkontroll for informasjonssikkerhet).[25] Standarden beskriver en risikostyringsprosess som skal sikre nødvendig konfidensialitet, integritet og tilgjengelighet til virksomhetens informasjon. Det er forventet at ledelsessystemet for informasjonssikkerhet skaleres i samsvar med virksomhetens behov.

Kravene i standarden er generelle og er ment å være anvendelige for alle virksomheter.

IS0 27001 er strukturert rundt sju hovedkapitler. Disse er:

---

[23] ISO/IEC 27002 er en standard for administrasjon av sikringstiltak knyttet til informasjonssikkerhet.

[24] Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). https://nsm.no.

[25] Norsk standard NS-EN ISO/IEC 27001: 2017. Informasjonsteknologi, Sikringsteknikker, Ledelsessystemer for informasjonssikkerhet, Krav. (ISO/IEC 27001:2013 innebefattet Cor 1:2014 og Cor 2:2015)

Organisasjonens kontekst (kap. 4)
Kapitlet slår fast at virksomheten skal etablere, implementere, vedlikeholde og kontinuerlig forbedre et ledelsessystem for informasjonssikkerhet. For å fastslå omfanget av systemet må en kartlegge og forstå interne og eksterne forhold som er viktige for virksomhetens formål, struktur og rammer.

Lederskap (kap. 5)
Den øverste ledelsen skal vise lederskap og forpliktelse til ledelsessystemet for informasjonssikkerhet, blant annet ved å;

- Etablere en informasjonssikkerhetspolicy.
- Sikre nødvendige ressurser.
- Sørge for at ansvar og myndighet relevant for informasjonssikkerheten er delegert og kommunisert.

Planlegging (kap. 6)
Ved planlegging av et ledelsessystem for informasjonssikkerhet skal virksomheten bestemme risikoer og muligheter som er nødvendige å håndtere, samt planlegge tiltak for å håndtere risikoene og mulighetene. Virksomheten skal definere og benytte en prosess for risikovurdering av informasjonssikkerheten. Informasjonssikkerhetsrelaterte kriterier skal etableres og vedlikeholdes, herunder kriterier for risikoaksept og risikovurderinger. Virksomheten skal også definere og benytte en prosess for håndtering av informasjonssikkerhetsrisikoene.

Videre skal virksomheten fastsette informasjonssikkerhetsmål for relevante funksjoner og nivåer, som er konsistente med informasjonssikkerhetspolicyen og tar hensyn til gjeldende krav til informasjonssikkerhet og resultater fra risikovurdering og -håndtering. Det skal foreligge en plan for hvordan målene skal oppnås.

Støtte (kap. 7)
Virksomheten skal definere og skaffe nødvendige ressurser for etablering, iverksetting, vedlikehold og kontinuerlig forbedring av styringssystemet for informasjonssikkerhet. Virksomheten skal sikre nødvendig kompetanse for personer som kan påvirke informasjonssikkerheten, samt at ansatte kjenner til informasjonssikkerhetspolicyen og konsekvensene dersom kravene ikke oppfylles.

Drift (kap. 8)
Virksomheten skal implementere og styre prosessene som er nødvendige for å oppfylle informasjonssikkerhetskravene og nå informasjonssikkerhetsmålene. Det skal gjennomføres risikovurderinger med planlagte intervaller eller når endringer er foreslått eller inntreffer. Planen for håndtering av risikoer skal iverksettes. Virksomheten skal gjennomgå konsekvensene av utilsiktede endringer og treffe tiltak for å begrense ugunstige virkninger.

Prestasjonsevaluering (kap. 9)
Virksomheten skal evaluere prosesser og tiltak knyttet til informasjonssikkerheten gjennom overvåking, måling, og analyse, og bestemme egnede metoder og tidspunkt. Organisasjonens øverste ledelse skal gjennomgå ledelsessystemet for informasjonssikkerhet med planlagte mellomrom.

Forbedring (kap. 10)
Virksomheten skal reagere på avvik og treffe korrigerende tiltak, samt håndtere konsekvenser.

ISO 27001 inneholder også et tillegg A, som beskriver sikringsmål og sikringstiltak, direkte avledet og i tråd med ISO/IEC 27002. Disse skal brukes i sammenheng med punkt 6.1.3 i ISO 27001, som sier at virksomheten skal definere og benytte en prosess for håndtering av informasjonssikkerhetsrisikoene til å blant annet fastsette alle sikringstiltak som er nødvendige for å håndtere informasjonssikkerhetsrisikoene.

4.1.2 OVERORDNEDE STYRENDE DOKUMENTER

Å etablere overordnede styrende dokumenter er fundamentet i internkontrollen. Disse er en forutsetning for at de systematiske aktivitetene gjennomføres i tilstrekkelig omfang og på riktig måte. Det påpekes at virksomhetsledelsen bør engasjere seg aktivt både ved utforming og godkjenning av disse dokumentene, og at de bør kommuniseres og forankres bredt i organisasjonen (Digdir.no).

Policy/strategi for informasjonssikkerhet

ISO 27001 (5.2) gir krav om at den øverste ledelsen skal etablere en informasjonssikkerhetspolicy[26] som blant annet skal inneholde mål for informasjonssikkerheten. Policyen skal formidle ledelsens føringer for informasjonssikkerhetsarbeidet. Det er lite informasjon å finne om hva informasjonssikkerhetspolicyen for øvrig bør inneholde. I Digitaliseringsdirektoratets (Digdir) veiledningsmateriell er policy for informasjonssikkerhet anbefalt som et overordnet styrende dokument som bør utarbeides ved etablering av internkontrollen, men det er ikke gitt noen utdypende beskrivelse. ISO 27001 sier at policyen skal omfatte ledelsens forpliktelse til å oppfylle aktuelle krav til informasjonssikkerhet og til kontinuerlig forbedring av internkontrollen, og at den skal gjennomgås med planlagte intervaller. En overordnet policy/strategi vil ofte ha et langsiktig perspektiv.

Vi har vist at eForvaltningsforskriften § 15 gir krav til forvaltningsorganet om å etablere internkontroll på informasjonssikkerhetsområdet med grunnlag i sikkerhetsmål og sikkerhetsstrategi. I veiledningen til evfv § 15 står det at *sikkerhetsstrategien skal dekke alle de overordnede føringene fra ledelsen, uavhengig av omfang, om innholdet kalles policy, strategi eller annet.* Vi mener derfor at policy, strategi og mål kan ses under ett og samles i ett dokument.

Videre står det i veiledningen til efvf § 15 at *sikkerhetsmålene* beskriver hva virksomheten ønsker å oppnå på informasjonssikkerhetsområdet. De skal understøtte og bidra til realisering av forvaltningsorganets overordnede mål, etterlevelse av lover og regler og kostnadseffektiv drift. Ifølge ISO 27001 (6.2) skal informasjonssikkerhetsmålene være konsistente med sikkerhetspolicyen, altså ikke gi føringer som står i motsetning til policyen. De skal være målbare, hvis praktisk mulig, og de skal ta hensyn til gjeldene krav til informasjonssikkerhet og resultater fra risikovurdering og -håndtering. Målene skal kommuniseres og oppdateres ved behov og det skal foreligge en plan for hvordan de skal oppnås.

I veiledningens omtale av *sikkerhetsstrategi* står det at denne beskriver hvordan forvaltningsorganet skal nå sikkerhetsmålene. Videre står det at det er virksomhetens kompleksitet, risiko og behov som bør avgjøre omfang, innretning og detaljeringsnivå på sikkerhetsmål, sikkerhetsstrategi og omfanget av internkontrollen. Dette er i samsvar med ISO.

[26] Policy defineres som et handlingsprogram, retningslinje, framgangsmåte, taktikk (Språkrådets ordbok).

Roller og ansvar i internkontroll- og sikkerhetsarbeidet

Ifølge ISO 27001 (5.3) er det toppledelsens ansvar å sørge for en hensiktsmessig organisering av arbeidet med informasjonssikkerhet, og det er viktig at roller og ansvar er klart beskrevet og formidlet til de det gjelder. Alt ansvar for informasjonssikkerhet skal være definert og tilordnet. Ledelsen skal tildele ansvar og myndighet for å rapportere til øverste ledelse om hvordan ledelsessystemet for informasjonssikkerhet fungerer. Rolle- og ansvarsfordelingen skal være dokumentert.

I tillegg A i ISO 27001 er det listet opp ulike sikkerhetstiltak som er knyttet til mål om å etablere et styringsrammeverk for forvaltning av informasjonssikkerhet i organisasjonen (A.6.1). Disse inkluderer blant annet å opprette hensiktsmessig kontakt med relevante myndigheter på området, og med spesialiserte sikkerhetsfora eller profesjonelle foreninger.

Prosess for risikovurdering, -forstå, vurdere og håndtere risiko

Det er et krav i ISO 27001 (6.1.2) at virksomheten skal utarbeide en prosess for risikovurdering som;

- Etablerer kriterier for risikoaksept og risikovurderinger.
- Sikrer at gjentatte risikovurderinger er sammenlignbare.
- Identifiserer risikoene knyttet til informasjonssikkerheten (tap av konfidensialitet, integritet og tilgjengelighet).
- Identifiserer risikoeiere.
- Analyserer informasjonssikkerhetsrisikoene, konsekvenser og sannsynligheter.
- Evaluerer informasjonssikkerhetsrisikoene.

Risikovurderingsprosessen skal være dokumentert.

4.1.3 KRAV TIL SIKKERHETSTILTAK

4.1.3.1 NSM grunnprinsipper

Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet et sett med grunnprinsipper og anbefalte tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade og misbruk. NSMs grunnprinsipper for IKT-sikkerhet er utarbeidet i samarbeid med virksomheter som forvalter kritiske samfunnsfunksjoner og/eller kritisk infrastruktur. Grunnprinsippene er relevante uavhengig av om virksomheten er underlagt sikkerhetsloven eller ikke. De skal være et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet, og uthever de viktigste sikringstiltakene i ISO/IEC 27002:2017.

Grunnprinsippene er delt inn i fire kategorier. Hvert grunnprinsipp har tilknyttede sikkerhetstiltak som beskriver hva som bør gjøres for å følge grunnprinsippet. Hvert prinsipp/tiltak har en kobling til ISO/EOC 27001 Tillegg A.

Nedenfor beskriver vi de ulike kategoriene og noen sentrale sikkerhetstiltak (hentet fra ISO 27001 tillegg A og NSM sikkerhetstiltak) for hver kategori.

1. *Identifisere og kartlegge*

Denne kategorien utgjør grunnlaget for en effektiv implementering av de andre kategoriene. Den vurderer risiko og legger en plan for risikohåndtering basert på en forståelse av virksomheten/IKT-systemet og den verden

virksomheten opererer i. Det er vesentlig å identifisere informasjonsverdiene som skal beskyttes. Regelverk, lovkrav, bransjenormer som har innvirkning på sikringen må kartlegges. For eksempel må betydningen av personvernlovgivningen være kjent. Virksomheten skal benytte den risikovurderingsprosessen som er definert for virksomheten (ISO 6.1.2). Risikovurderinger skal gjennomføres i planlagte intervaller og når vesentlige endringer planlegges eller oppstår (ISO 8.2).

Basert på risikovurderingen skal virksomheten velge hensiktsmessig håndtering av de risikoene som krever håndtering ut fra risikokriteriene, og bestemme hvilke tiltak som er nødvendige å innføre (ISO 6.1.3). Det skal utarbeides en plan for håndtering av risikoene. I Digdir sitt veiledningsmateriell beskrives ulike aktiviteter i virksomhetens prosess for risikohåndtering. Her står det blant annet at det skal utpekes en håndteringsansvarlig/tiltakseier som har ansvar for å utarbeide handlingsplan for hvordan det enkelte tiltak skal følges opp. Handlingsplanen bør beskrive hvordan tiltaket er tenkt gjennomført, hvem som er ansvarlig og når det skal være utført.

2. *Beskytte og opprettholde* (forebygge)

Kategorien innebærer å etablere og ivareta en forsvarlig sikring av IKT-systemet og opprettholde den sikre tilstanden over tid og ved endringer. Informasjonssikkerheten skal ivaretas i hele systemets levetid, fra anskaffelse til avhending.

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 A.7.2.2)

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. 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.

Grunnprinsipp 2.3 er *å ivareta en sikker konfigurasjon* som innebærer å tilpasse maskin- og programvare slik at den tilfredsstiller virksomhetens behov for sikkerhet. De fleste IKT-produkter leveres med en standardkonfigurasjon. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. Systemer som ikke er eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte. Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for, samt fjerne standard-innstillinger og standardpassord (forhåndsinnstillinger satt opp av produsent/leverandør).

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 er tilgjengelig for uvedkommende, eller at den er uleselig dersom den kommer på avveie.

Ved bruk er det viktig at kun personer som har tjenstlig behov er autorisert for tilgang (A.9.4). Det er også viktig å sikre informasjon som overføres innenfor virksomheten og med eksterne enheter, samt informasjon som overføres i nettverk (A.13.1, A.13.2), f.eks. ved hjelp av kryptering (NSM 2.7.3, 2.7.4). Dette vil også gjelde data under oppbevaring (lagret), både i ro, og dersom mediet dataene er lagret på transporteres eller avhendes (A.8.2.3, A.8.3).

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.

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 generere bevis er et sikringsmål i ISO 27001 (A.12.4). Foreslåtte sikringstiltak er å produsere, oppbevare, gjennomgå og beskytte hendelseslogger som registrerer brukeraktiviteter, avvik, feil og hendelser. Systemadministratorers og systemoperatørers aktiviteter skal loggføres særskilt, for å ivareta sporbarhet.

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*.

4. Håndtere og gjenopprette (respons)

Hensikten med 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. ISO A 17.1. Planen skal ivareta behovet for kontinuitet ved uønskede hendelser og krise. ISO A.16.1.5 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.17.2.1, dvs. at systemet skal ha tilstrekkelig redundans.

4.1.3.2 Andre styrende dokumenter/retningslinjer

ISO 27001 tillegg A angir at det bør utarbeides en rekke retningslinjer for relevante tiltaksområder. At retningslinjene følges bidrar til å opprettholde ønsket sikkerhetsnivå. Det er blant annet anbefalt egne retningslinjer for: informasjonsklassifisering (ISO A.8.2), behandling av personopplysninger (ISO A.18.1.4), leverandørforhold (ISO A.15.1.1), samt avviks- og hendelseshåndtering (ISO A.17.1).

<u>Klassifisering av informasjon</u>
ISO 27001) A.8.2 handler om klassifisering av informasjon (A.8.2), der målet er å sikre at informasjonen har et tilstrekkelig beskyttelsesnivå i samsvar med dens betydning for virksomheten. Et anbefalt sikkerhetstiltak er å klassifisere informasjon i henhold til juridiske krav, verdi, kritikalitet og sensitivitet forbundet med uautorisert utlevering eller modifisering (tilpassing). Retningslinjen skal gi føringer for informasjonsklasser, f.eks. strengt hemmelig, hemmelig, osv., og hva slags informasjon som hører hjemme i hver klasse.

Det skal videre utarbeides prosedyrer for merking (av sikkerhetsnivå) av informasjon i samsvar med organisasjonens ordning for informasjonsklassifisering. Virksomheten bør også ha en prosedyre for hvordan klassifiseringen operasjonaliseres i organisasjonen, hvem gjør hva, hvilken betydning klassifiseringen har for det enkelte IT-system, etc.

<u>Behandling av personopplysninger</u>
ISO 27001 A.18.1 handler om at virksomheten skal sikre at den ikke bryter juridiske, lovfestede, regulatoriske eller kontraktsmessige forpliktelser knyttet til informasjonssikkerhet. A.18.1.4 sier at personvern og beskyttelse av personlig identifiserbar informasjon skal sikres som påkrevd i relevante lover og forskrifter. A.18.1.1 sier at virksomhetens tilnærming til å oppfylle kravene skal være dokumentert og oppdatert for virksomheten og hvert system.

<u>Policy for leverandørforhold</u>
ISO 27001 A.15.1 har som mål å sikre at virksomhetsaktiva som er tilgjengelig for leverandører er beskyttet. A.15.1.1 sier at virksomheten skal utarbeide en informasjonssikkerhetspolicy for leverandørforhold der krav til informasjonssikkerhet for å redusere risiko forbundet med leverandørtilgang skal avtales med leverandøren og dokumenteres.

<u>Retningslinje for avviks- og hendelseshåndtering</u>
ISO 27001 A.17.1 handler om kontinuitet, eller opprettholdelse, av informasjonssikkerheten også ved uønskede situasjoner, krise eller katastrofe. A.17.1.2 sier at virksomheten skal etablere, dokumentere, implementere og vedlikeholde prosesser, prosedyrer og tiltak for å sikre nødvendig nivå av kontinuitet i en uønsket situasjon.

4.2 KONKRETE REVISJONSKRITERIER FOR PROBLEMSTILLING 1

Som vi har sett i utledningen gir kommuneloven krav til systematisk internkontroll og om rapportering av status til politisk nivå, mens personopplysningsloven og eforvaltningsforskriften gir krav om internkontroll på informasjonssikkerhetsområdet spesielt. Innholdet i internkontrollen skal basere seg på anerkjente standarder. Digitaliseringsdirektoratet anbefaler den internasjonale standarden ISO/IEC 27001, som er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet (internkontroll for informasjonssikkerhet). Se referanser til ISO i vedlegg 2.

Problemstilling 1:
Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i fylkeskommunen?

Vi har utledet følgende konkrete revisjonskriterier for problemstilling 1.

- Fylkeskommunen skal ha en policy for informasjonssikkerhet som viser ledelsens overordnede føringer for arbeidet med informasjonssikkerhet. Policyen skal inneholde;
    - Sikkerhetsmål som beskriver hva fylkeskommunen ønsker å oppnå på informasjonssikkerhetsområdet. Målene skal være risikobasert, samt målbare hvis praktisk mulig.
    - En strategi/plan for hvordan fylkeskommunen skal nå sikkerhetsmålene.
    - En forpliktelse til kontinuerlig forbedring av styringssystemet.
- Fylkeskommunen skal ha etablert en hensiktsmessig intern organisering for arbeidet med informasjonssikkerhet. Herunder
    - Roller og ansvar skal være hensiktsmessig fordelt, klart beskrevet, formidlet og dokumentert.
    - Det skal sikres at nødvendige ressurser er tilgjengelig.
    - Det skal være gjennomført nødvendig opplæring.
    - Det bør være opprettet kontakt med relevante myndigheter og interessefora på informasjonssikkerhetsområdet.
- Fylkeskommunen skal ha etablert en overordnet retningslinje for gjennomføring av risikovurderinger som en del av sikkerhetsarbeidet.
- Fylkeskommunen skal ha utarbeidet nødvendige rutiner og prosedyrer, som skal gjennomgås i planlagte intervaller. Fylkeskommunen bør ha utarbeidet følgende sentrale styrende retningslinjer;
    - Retningslinje og prosedyre for klassifisering av informasjon.
    - Retningslinje for behandling av personopplysninger.
    - Retningslinje for informasjonssikkerhet i leverandørforhold.
    - Retningslinje for avviks- og hendelseshåndtering.

- Arbeidet med styring og kontroll av informasjonssikkerheten skal være gjenstand for kontinuerlig evaluering og forbedring, og status for fylkeskommunens arbeid med informasjonssikkerhet bør rapporteres regelmessig til den øverste politiske og administrative ledelsen.

4.3 KONKRETE REVISJONSKRITERIER FOR PROBLEMSTILLING 2

Revisjonskriteriene er utledet fra ISO 27001 tillegg A og NSM grunnprinsipper versjon 2.0. Se referanser til ISO (og NSM) i vedlegg 2.

Problemstilling 2: I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?

Vi har utledet følgende revisjonskriterier for problemstilling 2.

Identifisere og kartlegge:

- Fylkeskommunen 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.
- Fylkeskommunen bør oppdatere risikovurderingen i faste intervaller og ved betydelige endringer.

Beskytte og opprettholde:

- Fylkeskommunen skal ha gjennomført sikkerhetsopplæring av systemets brukere.
- Det bør være etablert et regime for sikkerhetsoppdatering av systemet.
- Fylkeskommunen bør ha gjennomgått IT-systemets funksjonaliteter og unødvendig funksjonalitet bør ha blitt slått av.
- Systemets standardpassord bør ha blitt byttet.
- Fylkeskommunen bør beskytte data i IT-systemet under oppbevaring i samsvar med gjennomført klassifisering av systemets informasjonsverdier.
- Fylkeskommunen bør beskytte data i systemet under overføring (dataflyt) i samsvar med gjennomført klassifisering av systemets informasjonsverdier.
- Informasjonsverdier lagret på medier bør være tilstrekkelig sikret i samsvar med gjennomført informasjonsklassifisering, ved:
    - Bruk
    - Flytting/transport
    - Avhending/Arkivering
- Fylkeskommunen bør ha sikret muligheten til å gjenopprette systemets data.
- Det bør ha blitt gjennomført regelmessige tester for å verifisere at sikkerhetskopien fungerer.

Oppdage:

- Fylkeskommunen bør ha opprettet en hendelseslogg for hvert system.
- Loggføring bør inneholde informasjon om systemadministrators og systemoperatørers aktiviteter.
- Systemets logger bør være tilstrekkelig sikret.
- Det bør være etablert sikkerhetsovervåking av systemet.
- Det bør være gjennomført penetrasjonstest av systemet.

Håndtere og gjenopprette:

- Fylkeskommunen bør ha utarbeidet en hendelseshåndteringsplan for systemet.
- Fylkeskommunen bør ha vurdert redundansmuligheter som sikrer tilgjengelighetskrav.

5. OVERORDNET STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET

I dette kapitlet besvarer vi problemstilling 1.

Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i fylkeskommunen?

Vi starter med å presentere innhentet informasjon, deretter vurderer vi informasjonen opp mot de konkrete revisjonskriteriene. Informasjonen baserer seg på dokumentanalyse, samt intervju med rådgiver i seksjon for Kvalitet, sikkerhet og beredskap, også kalt fagansvarlig for informasjonssikkerhet og personvern, samt med personvernkoordinator i avdeling for Kompetanse og tannhelse. Personvernkoordinatoren har bidratt i seksjon for Kvalitet, sikkerhet og beredskap sitt arbeid med å utarbeide dokumenter som inngår i internkontrollsystemet. Sikkerhets- og beredskapssjefen har også gjennomgått informasjonen presentert i datakapitlet og gitt kommentarer.

5.1 DATA

I dette kapitlet beskriver vi relevante deler av fylkeskommunen sitt internkontrollsystem for informasjonssikkerhet. Fylkeskommunen betegner internkontrollsystemet for *styringssystem for personvern og informasjonssikkerhet.*

Ifølge fagansvarlig for informasjonssikkerhet og personvern er det fortsatt flere dokumenter som må utarbeides for å ha et fullstendig styringssystem. Dette skyldes manglende kapasitet. Fagansvarlig mener at dette arbeidet må prioriteres og at det er viktig at ledelsen har fokus på informasjonssikkerhet. Han sier at arbeidet går fremover, men siden fylkeskommunen fortsatt er en ny organisasjon så tar det tid å implementere nye rutiner.

5.1.1 SIKKERHETSPOLICY

Ordet policy er et begrep som brukes i ISO-standarden, og av mange offentlige instanser. Innlandet fylkeskommune har kalt sitt overordnede dokument på området for «*Styringsdokument for personvern og informasjonssikkerhet*[27]».

I styringsdokumentet står det at fylkeskommunen har systematisert sitt arbeid med personvern og informasjonssikkerhet gjennom etableringen av et styringssystem for personvern og informasjonssikkerhet. Styringssystemet skal sikre god styring av sikkerheten og består av tre nivåer, hvorav *Styringsdokument for personvern og informasjonssikkerhet* beskriver nivå en og to, se figur 5.1 nedenfor.

[27] Styringsdokument for personvern og informasjonssikkerhet, godkjent av avdelingssjef for administrasjon 7.4.21.

Hensikten med styringsdokumentet er å gi overordnede føringer for organisering, etablering, oppfølging, vedlikehold og kontinuerlig forbedring av personvern- og informasjonssikkerhetsarbeidet i Innlandet fylkeskommune. Dokumentet skal beskrive rammer, mål, myndighet og ansvar som ligger til grunn for sikkerhetsarbeidet (Nivå 1), samt overordnede sikkerhetskrav som gjelder for fylkeskommunen (Nivå 2). Nivå tre skal beskrive hvordan sikkerhetsarbeidet skal foregå i praksis og bestå av detaljerte retningslinjer med veiledninger. Dette arbeidet er ifølge fagansvarlig for personvern og informasjonssikkerhet ikke ferdigstilt.

Figur 5.1. Styringssystem for personvern og informasjonssikkerhet. Innlandet fylkeskommune.

Styringsdokumentet gjelder all informasjonsbehandling som skjer i fylkeskommunen, med unntak av skjermingsverdig informasjon som følger sikkerhetslovens krav. Målgruppen er ansatte som har en rolle i å etablere, vedlikeholde og dokumentere tiltak som gir tilstrekkelig internkontroll innen personvern og informasjonssikkerhet.

Ansvar

Fylkeskommunedirektør har det overordnede ansvaret for personvern og informasjonssikkerhet, og er ansvarlig for at styringsdokumentet realiseres og etterleves. Sikkerhets- og beredskapssjef i fylkeskommunen har ansvaret for den daglige oppfølgningen av dokumentet, herunder å gjøre nødvendige endringer. Substansielle endringer skal godkjennes av Fylkeskommunedirektøren før iverksetting.

Mål for personvern og informasjonssikkerhet

Dokumentets punkt/avsnitt 1 har overskrift *Mål for personvern og informasjonssikkerhet*. Her står det at ved å etterleve kravene til personvern og informasjonssikkerhet sikres grunnlaget for god styring og kontroll i fylkeskommunen. Som en del av personvernet fastsettes det også minimumskrav for informasjonssikkerhet. Innlandet fylkeskommune må fremstå som en seriøs samfunnsaktør og en pådriver i å fremme godt personvern og god sikkerhetskultur.

Videre står det at målet for personvern og informasjonssikkerhet i fylkeskommunen innebærer konkret å ivareta den registrertes rettigheter og friheter gjennom å:

- forstå organisasjonens plikter i personvernforordningen.
- etablere praktiske rutiner som beskriver og gir føringer på hvordan den daglige håndteringen av personopplysninger skal foregå.
- bare behandle personopplysninger i samsvar med personvernprinsippene.
- ivareta krav til konfidensialitet, integritet og tilgjengelighet.
- sørge for at alle medarbeidere kjenner til og etterlever interne retningslinjer for personvern i egen oppgaveløsning.

Det overordnede målet er å ha god styring og kontroll på informasjonssikkerhet og personvern, sier fagansvarlig for informasjonssikkerhet og personvern. Styringssystemet for personvern og informasjonssikkerhet er et verktøy for å oppnå dette. Han sier at fylkeskommunen pr nå ikke har et fullverdig styringssystem, på grunn av ressursmangler.

På spørsmål om fokus på personvern kontra informasjonssikkerhet i de konkrete målene oppgitt i styringsdokumentet (og ellers i styringsdokumentet), sier fagansvarlig for informasjonssikkerhet og personvern at de har valgt å samle styring og kontroll av både personvern og informasjonssikkerhet i et felles dokument. Han mener at krav til konfidensialitet, integritet og tilgjengelighet favner all informasjonssikkerhet, og at informasjonssikkerhet derfor også er ivaretatt i målene. Fylkeskommunen har et stort fokus på personvern, og dette gjenspeiles i styringsdokumentet, sier han.

Revisjonen spurte fagansvarlig for informasjonssikkerhet og personvern om hans vurdering av målbarheten til målene i styringsdokumentet. Han mener at det er mulig å måle om fylkeskommunen har implementert et styringssystem for informasjonssikkerhet. Det er for eksempel et mål å etablere rutiner, og dette er målbart. Personvernkoordinatoren revisjonen har snakket med sier at målene er målbare, en kan f.eks. måle om det er brudd på konfidensialitet, integritet og tilgjengelighet.

Krav til personvern og informasjonssikkerhet

Dokumentets punkt/avsnitt 2 har som overskrift *Overordnede krav til personvern og informasjonssikkerhet*. Her presenteres først grunnleggende prinsipper for personvern, som følger de grunnleggende prinsippene for behandling av personopplysninger i personvernforordningen (artikkel 5). Videre er det oppgitt grunnleggende prinsipper for informasjonssikkerhet. Disse er (ikke ordrett);

- Ansvar og myndighet for personvern og informasjonssikkerhet skal som hovedregel følge linjeansvaret.
- Arbeidet med informasjonssikkerhet skal være risikobasert.
- All tilgang til personopplysninger og systemer skal basere seg på tjenstlig behov.
- Behov for kontinuerlig drift og robusthet i prosesser skal sikres.
- Et sikkerhetstiltak skal koste mindre enn det koster å leve med risikoen som tiltaket skal forhindre.

Punkt/avsnitt 3 i styringsdokumentet har overskrift *Krav til personvern og informasjonssikkerhet.* Dette er krav som skal ivaretas for at fylkeskommunen skal nå sine mål knyttet til informasjonssikkerhet og etterleve personvernforordningens prinsipper.

Fagansvarlig for informasjonssikkerhet og personvern sier at det skal utarbeides retningslinjer for hvert av kravene, men at alle ikke er på plass enda (pr mai 2021).

Kravene er satt opp i sju kulepunkt. Disse er (ikke ordrett);

- *Kompetanse*. Sørge for at ansatte er oppmerksomme på trusler, og har kunnskap om viktige tiltak og rutiner. Ansatte må få opplæring.
- *Roller og ansvar*. Identifisere nødvendige roller og funksjoner og fastsette tilhørende myndighet.
- *Eierskap og klassifisering*. All informasjon og alle systemer skal ha en eier, som er linjeleder. Informasjonen skal klassifiseres etter hvor viktig den er, og i henhold til krav til beskyttelse.
- *Risikostyring*. Risikostyring skal gi fylkeskommunen en oppdatert oversikt over risikobildet og styre risikoen til et akseptabelt nivå.
- *Kontinuitet og avvikshåndtering*. Planer og systemer skal etableres, testes og vedlikeholdes for å opprettholde kontinuitet. Avvik og uønskede hendelser skal rapporteres og håndteres.
- *Samsvar og status på tilstand*. Arbeidet med personvern og informasjonssikkerhet skal baseres på anerkjente standarder og veiledninger, blant annet ISO 27000 – serien, og være i samsvar med gjeldende lover, forskrifter og internt reglement. Det skal utarbeides årlig tilstandsrapport til ledelsen.
- *Programvaresikkerhet og innebygd personvern.* Det skal være krav til innebygd personvern i alle anskaffelser eller utvikling av nye løsninger. Det skal inngås databehandleravtaler med presise og tilstrekkelige krav i alle anskaffelser av systemer som behandler personopplysninger.

Ifølge fagansvarlig for informasjonssikkerhet og personvern er det utarbeidet retningslinjer for punktene Roller og ansvar, Eierskap og klassifisering, samt Avvikshåndtering. Rutine for risikostyring er under arbeid, og ikke endelig vedtatt[28]. De skal etter hvert utarbeide en retningslinje for kontinuitet, men dette er ikke startet opp enda[29].

Retningslinje for kompetanse er under arbeid. Fagansvarlig for informasjonssikkerhet og personvern og personvernombudet har utarbeidet en opplæringspakke som gjelder personvern og informasjonssikkerhet. Denne er foreløpig ikke implementert, og det er opp til HR å bestemme hvordan pakken skal distribueres til de ansatte. HR skal avgjøre om sikkerhetsinstruksen skal inngå i «onboardingen» til nyansatte, eller om den skal gjelde alle ansatte. Fylkeskommunen har i dag ingen obligatorisk generell sikkerhetsopplæring utover den opplæringen som gis knyttet til bruk av de ulike tjenestene. De har kampanjer og foredrag rettet mot informasjonssikkerhet og personvern, men alt er frivillig.

Når det gjelder krav til programvaresikkerhet og innebygd personvern er dette noe de jobber med i anskaffelser. Fylkeskommunen utvikler ikke egne IT-systemer, men de passer på at tjenestene de kjøper/forvalter har innebygd personvern som standard innstilling. Punktet om samsvar og status på tilstand følges opp gjennom utarbeidelse av et årshjul. Dette gjelder også ledelsens gjennomgang.

[28] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at rutine for risikostyring ble godkjent den 16.11.2021. Revisjonen har ikke sett det endelige dokumentet.

[29] Revisjonen har mottatt en oversikt over dokumentstrukturen i styringssystem for personvern og informasjonssikkerhet (nov. 2021). Her er det satt opp 14 ulike dokumenter som skal utgjøre overordnede sikkerhetskrav. Av disse er fem ferdige og godkjent, tre under arbeid, og seks ikke påbegynt.

Punkt/avsnitt 4 i styringsdokumentet beskriver roller og ansvar som er viktige i arbeidet med å ivareta personvern og informasjonssikkerhet. Disse er beskrevet nærmere i dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* som vi omtaler i kapittel 5.1.2 nedenfor.

5.1.2 INTERN ORGANISERING/ ROLLER OG ANSVAR

5.1.2.1 Roller og ansvar for informasjonssikkerhet og personvern

Fylkeskommunen har utarbeidet et dokument som heter *Roller og ansvar for informasjonssikkerhet og personvern*[30]. Hensikten med styringsdokumentet er å beskrive de rollene som har et ansvar for arbeidet med informasjonssikkerhet og personvern i Innlandet fylkeskommune. Dokumentets omfang og målgruppe er den samme som for overordnet styringsdokumentet for personvern og informasjonssikkerhet, omtalt i kapittel 5.1.1 (sikkerhetspolicy).

Dokumentet starter med en generell del, der det opplyses at ansvaret for arbeidet med informasjonssikkerhet som hovedregel skal følge linjen. I tillegg er det noen særskilte roller som har informasjonssikkerhet som hovedoppgave, som er organisert i ansvarsområder i linjen. Dette gjelder rollene sikkerhets- og beredskapssjef og personvernrådgivere. Sikkerhets- og beredskapssjefen er leder av Kvalitet, sikkerhet og beredskap, som er en seksjon i administrasjonsavdelingen.

Det presiseres i dokumentet at tydelige roller med tilhørende ansvar og myndighet er viktig for å kunne følge opp, vedlikeholde og kontinuerlig forbedre arbeidet med informasjonssikkerhet. Alle de ulike rollene skal få nødvendig kompetanse, verktøy og støtte for å kunne ivareta sitt ansvar og utøve sin myndighet.

Videre står det at arbeidet med informasjonssikkerhet i Innlandet fylkeskommune skjer på strategisk, taktisk og operativt nivå. På strategisk nivå skal mål og strategi for informasjonssikkerhet etableres. Ansvaret er i hovedsak å beslutte hva som skal gjøres i et langsiktig og overordnet perspektiv. På dette nivået inngår blant annet beslutningen om å etablere et styringssystem for personvern og informasjonssikkerhet, akseptabelt risikonivå og metode for risikostyring. På taktisk nivå skal mål og strategi operasjonaliseres i et mellomlangt tidsperspektiv. På dette nivået inngår helhetlig styring og kontroll med informasjonssikkerhet i Innlandet fylkeskommune, samt risikostyring og kontroll med virksomhetsinterne systemer. Operativt ansvar innebærer å iverksette operasjonaliseringen gjennom de daglige oppgavene.

Under avsnitt/punkt 2 i dokumentet er de ulike rollene med tilhørende ansvarsområder beskrevet. Disse rollene er fylkeskommunedirektør, avdelingssjefer, sikkerhets- og beredskapssjef, personvernombud, og andre medarbeidere. I avsnitt/punkt 3 i dokumentet er det beskrevet hvem som har ansvar for sikkerhetsarbeid i prosjektorganisasjon og endringsledelse, samt hva ansvaret består av. Vi går ikke nærmere inn på disse rollene her. I avsnitt/punkt 4 er roller og ansvar for sikkerhetsarbeidet knyttet til de digitale tjenestene beskrevet. Disse rollene er tjenesteeier og tjenesteansvarlig. Disse har ansvar for informasjonssystemer knyttet til digitale tjenester. Nedenfor går vi igjennom de ulike rollene.

[30] Roller og ansvar for informasjonssikkerhet og personvern, godkjent av avdelingsleder for Administrasjon,1.3.2021.

Fylkeskommunedirektør

Fylkeskommunedirektøren har det overordnede ansvaret for at styringssystem for personvern og informasjonssikkerhet realiseres og etterleves. Fylkeskommunedirektør skal sørge for at det etableres mål og strategi innen personvern og informasjonssikkerhet. Videre skal fylkeskommunedirektøren ivareta fylkeskommunens plikter som behandlingsansvarlig etter personopplysningsloven og har myndighet til å styre og akseptere all risiko i Innlandet fylkeskommune.

Fylkeskommunedirektøren skal:

- Godkjenne styrende dokumenter for informasjonssikkerhet og personvern.
- Sikre nødvendig kapasitet og kompetanse til arbeidet med personvern og informasjonssikkerhet.
- Ivareta at tydelige roller og ansvar for personvern og informasjonssikkerhet er etablert, med tilhørende myndighet.
- Sørge for at ansvar for personvern og informasjonssikkerhet er i henhold til personopplysningsloven, forvaltningsloven, annen lovgivning og fylkeskommunens eget regelverk.
- Vedta og ivareta akseptabelt risikonivå for fylkeskommunen.
- Behandle restrisiko for fylkeskommunen.
- Sørge for at styring av personvern og informasjonssikkerhet inngår i fylkeskommunen ordinære virksomhetsstyring. Herunder å etterspørre informasjonssikkerhetstilstanden for avdelingene.
- Følge opp alvorlige hendelser innen personvern og informasjonssikkerhet og at nødvendige tiltak blir iverksatt for å hindre gjentakelse.

Avdelingssjefer

Avdelingssjefer skal systematisk styre, kontrollere og følge opp tilstanden og arbeidet med personvern og informasjonssikkerhet for sitt ansvarsområde. Myndighet og spesifikke sikkerhetsoppgaver kan delegeres til underliggende nivå.

Avdelingssjef skal:

- Ivareta personvern og informasjonssikkerhet i egen avdeling i henhold til personopplysningsloven, forvaltningsloven, annen lovgivning og interne regler.
- Holde oversikt over myndighetskrav for å ivareta taushetsplikt, personvern og informasjonssikkerhet.
- Sikre tilstrekkelig kapasitet og kompetanse for å sikre at informasjonssikkerhets- og personvernkravene etterleves tilfredsstillende.
- Påse at sine medarbeidere får nødvendig opplæring og har en atferd som bidrar til å ivareta sikkerheten, veilede sine medarbeidere og søke bistand hvis nødvendig.
- Utpeke Tjenesteeier for de digitale tjenestene som avdelingen leverer (internt eller eksternt).
- Verdivurdere informasjon som avdelingen eier og behandler.
- Oppdatere behandlingsoversikter for personopplysninger.
- Gjennomføre risikovurderinger og personvernkonsekvensvurderinger for aktiviteter og digitale tjenester gjennom hele tjenestens levetid i henhold til standard for risikostyring.
- Iverksette nødvendige tiltak og/eller fremlegge restrisiko ut over akseptabelt risikonivå til fylkeskommunedirektør.
- Påse at vedtatte sikkerhetstiltak er iverksatt og fungerer etter hensikten.
- Utarbeide årsplan for personvern og informasjonssikkerhet knyttet til egen avdeling.

- Omgående rapportere uønskede informasjonssikkerhetshendelser i egen avdeling i samsvar med dokumenterte rutiner.
- Søke støtte hos sikkerhetssjef og informasjonssikkerhetsrådgiver for ivaretakelse av ansvaret.

Sikkerhets- og beredskapssjef
Sikkerhets- og beredskapssjefen har fagansvaret for personvern og informasjonssikkerhet, og skal utarbeide og forvalte styringssystemet for personvern og informasjonssikkerhet på vegne av fylkeskommunedirektøren. Sikkerhets- og beredskapssjefen skal bistå i kompetanseheving og bidra til daglig oppfølging av linjeansvaret. Sikkerhets- og beredskapssjef skal rapportere direkte til fylkesrådmann ved kritiske sikkerhetshendelser eller ved observerte situasjoner som medfører eller kan medføre høy risiko. Sikkerhets- og beredskapssjefen skal bidra til at det utarbeides et tilstrekkelig beslutningsgrunnlag slik at risikoeiere kan vurdere informasjonssikkerhetsrisiko i henhold til Standard for risikostyring.

Sikkerhets- og beredskapssjefen skal:

- Utarbeide og oppdatere styrende og utførende dokumenter for personvern og informasjonssikkerhet.
- Utarbeide og presentere helhetlig trusselvurdering.
- Rapportere sikkerhetstilstand på informasjonssikkerhet og personvern til fylkeskommunedirektørens ledergruppe.
- Legge til rette for helhetlig risikostyring innen informasjonssikkerhet og personvern.
- Bidra til å utforme krav og styringsprinsipper (arkitekturprinsipper) knyttet til fylkeskommunens digitale tjenester.
- Følge opp utviklingen av fylkeskommunens tjenester og tilhørende informasjonssystemer for å sikre innebygd informasjonssikkerhet og personvern.
- Være kontaktperson mot Datatilsynet.
- Delta i spesifisering, design, utvikling og implementering av digitale løsninger for å sikre en effektiv tilnærming til akseptabel risiko i fylkeskommunens tjenester og informasjonssystemer.
- Formidle Styringssystem for personvern og informasjonssikkerhet på en hensiktsmessig måte til alle ansatte, samarbeidspartnere og relevante interessenter.
- Planlegge og utføre ledelsens gjennomgang.
- Verifisere etterlevelse av interne og eksterne krav gjennom helhetlig sikkerhetsrevisjon.
- Sikre videreutvikling av Styringssystem for personvern og informasjonssikkerhet.
- Planlegge årshjul for sikkerhetsaktiviteter.
- Bistå i håndteringen av sikkerhetsavvik.
- Gjennomføre sikkerhetsrevisjon.
- Sørge for god IKT hendelses- og krisehåndtering for Innlandet fylkeskommune.
- Ivareta Innlandet fylkeskommunes IT beredskap og oppfyllelse av krav for beredskap i henhold til sikkerhetsloven.
- Holde beredskapsplan og kontinuitetsplaner oppdaterte.

Personvernombud
Personvernombudet har en uavhengig rolle og hovedoppgaver er regulert i personvernforordningen.

Personvernombudet skal blant annet:

- Informere, gi råd og opplæring om forpliktelsene i personvernforordningen.
- Kontrollere overholdelsen av personvernlovgivningen og andre relevante regelverk, samt virksomhetens egne interne retningslinjer for personvern.
- Bistå avdelingssjefer ved avvik (brudd på personopplysningssikkerheten), eller andre hendelser som kan ha konsekvenser for personvernet.

Andre medarbeidere
Medarbeidere skal blant annet:

- Gjøre seg kjent med og etterleve rutiner som bidrar til tilfredsstillende personvern og informasjonssikkerhet knyttet til egen stilling.
- Rapportere avvik knyttet til personvern og informasjonssikkerhet i henhold til etablerte prosedyrer for avvikshåndtering.
- Forstå og etterleve konkrete krav til informasjonssikkerhet som bidrar til å sikre fylkeskommunenes digitale verdier.

Tjenesteeier
Rollen som tjenesteeier innebærer en lederrolle i virksomheten og har det overordnede ansvaret for informasjonssikkerhet og personvern innenfor den konkrete tjenesten. Tjenesteeier er ansvarlig for å dokumentere at informasjonssikkerhet og personvern er ivaretatt i tjenesten i henhold til standard for risikostyring. Tjenesteeier kan ikke akseptere restrisiko som går ut over akseptabelt risikonivå. Dette må rapporteres videre til fylkeskommunedirektøren. For virksomhetskritiske fellestjenester bør rollen som tjenesteeier være organisert i toppledelsen. På denne måten sikres handlekraft og robusthet i tjenesten. For konkrete oppgaver knyttet til rollen som tjenesteeier henvises til «Forvaltningsmodell for digitale tjenester».

Tjenesteansvarlig
Rollen som tjenesteansvarlig ivaretar de daglige oppgavene knyttet til informasjonssikkerhet og personvern gjennom å identifisere, iverksette og kontrollere tjenesten. Tjenesteansvarlig må rapportere sikkerhetsavvik til tjenesteeier. Tjenesteansvarlig har delegert myndighet fra tjenesteeier og kan iverksette sikkerhetstiltak innenfor den definerte rammen for tjenesteutvikling, men kan ikke akseptere restrisiko. Restrisiko opp til akseptabelt risikonivå må løftes opp til tjenesteeier som kan akseptere risiko, mens restrisiko som går over akseptabelt nivå må løftes opp til fylkeskommunedirektør. For konkrete oppgaver knyttet til rollen som tjenesteansvarlig henvises til «Forvaltningsmodell for digitale tjenester».

5.1.2.2 Ressurser på informasjonssikkerhetsområdet

Seksjon for Kvalitet, sikkerhet og beredskap har fagansvar for fylkeskommunens styringssystem for personvern og informasjonssikkerhet. Seksjonen består av leder pluss tre rådgivere, hvorav én av rådgiverne jobber med informasjonssikkerhet.

Rådgiver for informasjonssikkerhet og personvern (fagansvarlig) opplyser at de fleste av seksjonens oppgaver som gjelder informasjonssikkerhet er delegert videre til han. Som fylkeskommunens fagperson på informasjonssikkerhet utfører han eller deltar i de fleste av oppgavene på informasjonssikkerhetsområdet. Dette er et omfattende arbeid, og det er liten kapasitet til å drive utviklingsarbeid. For eksempel bistår han avdelingene med å utføre ROS-analyser når det skal installeres ny programvare, noe som tar en del tid.

Seksjonen har i tillegg hjelp fra personvernkoordinatoren i avdeling for Kompetanse og tannhelse (20%). Hun mener også at det er lite ressurser på informasjonssikkerhetsarbeidet i fylkeskommunen. Det er en stor utfordring å få alt på plass i en ny organisasjon med så begrensede ressurser, sier hun.

Fagansvarlig for informasjonssikkerhet og personvern opplyser at det er fire personer som jobber dedikert med informasjonssikkerhet og personvern i fylkeskommunen (som har dette som hovedoppgave). Disse er fagansvarlig for informasjonssikkerhet og personvern, personvernombud, personvernrådgiver (koordinator) og en sikkerhetsarkitekt på IT-avdelingen. I tillegg kommer hele IT-avdelingen pluss alle ute i organisasjonen som er tildelt ansvar for visse oppgaver (tjenesteeier, tjenesteansvarlig, etc.).

5.1.3 KONTAKT MED RELEVANTE MYNDIGHETER

Fylkeskommunen er medlem av Foreningen Kommunal Informasjonssikkerhet (KiNS) som har som formål å bidra til å øke informasjonssikkerhet og personvern i kommuner og fylkeskommuner. Foreningen tilbyr aktiviteter som årlige konferanser og kurs, faglige fora og møteplasser, rådgivning, m.m.

Det er blitt tatt initiativ fra Viken fylkeskommune om å etablere et fylkeskommunalt informasjonssikkerhetsforum. Fylkeskommunen deltar i dette forumet. I tillegg deltar fylkeskommunen i fylkeskommunalt forum for sikkerhet og beredskap og i KS sitt Strategisk Nettverk for Informasjonssikkerhet og Personvern (SNIP).

I forbindelse med det fylkeskommunale samarbeidet om systemet VIGO[31] har Innlandet fylkeskommune tatt initiativ til å ha et sikkerhetsforum med andre fylkeskommuner. Fylkeskommunen har besluttet å delta i Kommune-CSIRT.

Personvernombudet deltar i personvernforum, samt i nettverk for personvernombud.

Fylkeskommunen har også kontakt med Nasjonal Sikkerhetsmyndighet (NSM) når det gjelder informasjonssikkerhetsarbeid med graderte systemer og i en krisesituasjon, og de har blant annet hatt et foredrag for ledere.

5.1.4 OVERORDNET RETNINGSLINJE FOR RISIKOSTYRING

Ifølge *Styringsdokument for personvern og informasjonssikkerhet*, jf. kapittel 5.1.1, er det et overordnet krav til personvern og informasjonssikkerhet at arbeidet skal være risikobasert. For å oppnå fylkeskommunens mål knyttet til informasjonssikkerhet et det videre et krav å utarbeide rutine for risikostyring. Fylkeskommunedirektøren med ledergruppe skal beslutte kriterier for risikoaksept og skala for konsekvens og sannsynlighet.

I dokumentet *Roller og ansvar for informasjonssikkerhet og personvern*, jf. kapittel 5.1.2, står det at beslutningen om å etablere et akseptabelt risikonivå og metode for risikostyring inngår i fylkeskommunens arbeid med informasjonssikkerhet på strategisk nivå.

[31] Vigo er en internettportal for søking til videregående opplæring, og er eid av Vigo IKS som er et inter(fylkes)kommunalt selskap. Selskapet er et samarbeid mellom alle fylkene i Norge i tillegg til Oslo kommune.

Avdelingssjefer og tjenesteeiere skal gjennomføre risikovurderinger og personvernkonsekvensvurderinger for aktiviteter og digitale tjenester i henhold til standard for risikostyring.

Revisjonen har fått oversendt utkast til dokumentet, «*Overordnet sikkerhetskrav for risikostyring av personvern og informasjonssikkerhet*», eller «Standard for risikostyring». Ifølge sikkerhets- og beredskapssjefen er dette dokumentet ikke endelig vedtatt i påvente av beslutning om risikostyringsmetodikk for fylkeskommunen[32], og kan derfor ikke benyttes som fakta.

I dokumentet står det at risikostyringen skal bestå av følgende element; risikovurdering, risikobehandling, risikoeiers aksept av risiko, kommunikasjon og lederforankring, og revidering og oppdatering av risikovurderinger.

Fagansvarlig for informasjonssikkerhet og personvern sier at dokumentet delvis er i bruk i organisasjonen og at det skal fungere som en mal for å gjøre risikovurderinger av systemene.

Fagansvarlig for informasjonssikkerhet og personvern forteller at det er satt ned en prosjektgruppe som skal utarbeide en risiko- og sårbarhetsanalyse (ROS) for hele fylkeskommunen, der også informasjonssikkerhet skal inkluderes. Han mener det bør etableres en egen ROS for hver enkelt avdeling før det lages en overordnet ROS av hele informasjonssikkerhetsområdet i fylkeskommunen. Han sier han kan bistå avdelingene i dette arbeidet slik at avdelingene utfører risikovurderinger med felles mal og metodikk. Etter dette kan seksjon for Kvalitet, sikkerhet og beredskap lage rapporter om sikkerhetstilstand til hver enkelt avdeling, samt en felles rapport for hele fylkeskommunen.

Når avdelingene gjør ROS-vurderinger av et system/tjeneste skal den sendes til seksjon for Kvalitet, sikkerhet og beredskap for kvalitetssikring, og større risikoer skal meldes videre til ledergruppa.

5.1.5 ANDRE STYRENDE RETNINGSLINJER

5.1.5.1 Klassifisering av informasjon

Det følger av *Styringsdokument for personvern og informasjonssikkerhet* at fylkeskommunen skal utarbeide en rutine for klassifisering av informasjon. Informasjonen skal klassifiseres på en slik måte at den indikerer viktigheten for fylkeskommunen og ivaretar lovkrav til beskyttelse. I dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* er avdelingsleder gitt ansvar for å vurdere verdien av informasjonen som avdelingen eier og behandler.

Revisjonen har fått oversendt dokumentet *Overordnende sikkerhetskrav for informasjonsklassifisering*[33]. Hensikten med dokumentet er å etablere en strukturert tilnærming, enhetlig begrepsbruk og en felles forståelse for klassifisering av informasjon og informasjonssystemer. Fylkeskommunedirektøren har det overordnede ansvaret for at dokumentet realiseres og etterleves, mens Sikkerhet- og beredskapssjefen har ansvaret for den daglige oppfølgingen.

---

[32] Info pr 14.9.2021. Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at dokumentet «Overordnet sikkerhetskrav for risikostyring» ble godkjent den 16.11.2021 og at risikostyringsmetodikk for fylkeskommunen ble godkjent den 5.12.2021. Revisjonen har ikke sett disse godkjente dokumentene.

[33] Godkjent 7.4.2021 av avdelingsleder for Administrasjonsavdelingen.

Omfang og målgruppe er som for de andre styringsdokumentene som gjelder styringssystem for informasjonssikkerhet og personvern.

Dokumentet beskriver rollene som har et særskilt ansvar for at kravene til klassifisering oppfylles;

- Avdelingssjef har ansvar for at informasjonen som behandles på avdelingen er klassifisert iht. sikkerhetskravene.
- Tjenesteeier har ansvar for at det blir gjennomført en klassifisering av informasjonssystemet og at sikringstiltak er iverksatt.
- Tjenesteansvarlig har ansvar for å etablere og oppdatere en oversikt over informasjonstyper med tilhørende klassifisering i tjenesten. Informasjonstyper er kategori av informasjon, f.eks. personopplysning, vedtak, etc.
- Medarbeidere har ansvar for å klassifisere informasjonsobjektene etter vedtatte retningslinjer. Informasjonsobjekter er informasjon som er lagret på et medium, f.eks. dokument, bilde, e-post, videofil, m.fl.

Dokumentet gir krav om at all informasjon som behandles i Innlandet fylkeskommune, både i digital og analog form, skal kategoriseres i informasjonstyper og klassifiseres etter behovet for å ivareta konfidensialitet, integritet og tilgjengelighet. Behov for sikkerhet vurderes enkeltvis for konfidensialitet, integritet og tilgjengelighet, og klassifiseres i sikkerhetsklassen åpen, beskyttet eller sensitiv. Alle informasjonstyper og tilhørende sikkerhetsklasse skal fremkomme i en samlet oversikt som skal være tilgjengelig for alle medarbeidere.

Videre skal alle informasjonssystemer i IFK klassifiseres ut fra behovet for å ivareta konfidensialitet, integritet, og tilgjengelighet. Sikkerhetsklassifiseringen skal ta hensyn til alle informasjonstypene som behandles i informasjonssystemet. Alle informasjonssystemer og tilhørende sikkerhetsklasse skal inngå i en samlet oversikt som er en del av tjenestebeskrivelsen.

For hver definerte sikkerhetsklasse skal det være krav til sikkerhetstiltak for å ivareta informasjonssystemets behov for konfidensialitet, integritet, og tilgjengelighet. Behov for ytterligere sikkerhetstiltak skal baseres på konkret risiko og beslutninger fra risikoeiere. Det skal gå fram av oversikten hvem som har godkjent sikkerhetsklassifiseringen, når dette ble gjort og hvem som har akseptert.

Sikkerhetsklassifiseringen er førende for fylkeskommunens videre arbeid med konsekvensutredninger (BIA) og ROS-analyser. Fylkeskommunen har et eget verktøy for konsekvensutredning (BIA).

Personvernkoordinatoren sier at de har en behandlingsoversikt (oversikt over hvilke personopplysninger som behandles) pr avdeling. Der står det hvilke opplysninger som er lagret hvor. Noen av disse ligger i ehåndboka i kvalitetsverktøyet.

På spørsmål om fylkeskommunen har utarbeidet prosedyrer for hvordan informasjonsklassifiseringen skal foregå i praksis sier fagansvarlig for informasjonssikkerhet og personvern at tjenesteeier har ansvar for å utarbeide egne prosedyrer som følger overordnede sikkerhetskrav for informasjonsklassifisering. Rutinen skal brukes som mal for hvordan informasjonen i systemene skal vurderes. Personvernkoordinatoren sier at de ikke har noen operasjonelle prosedyrer eller retningslinjer som understøtter dokumentet *Overordnede sikkerhetskrav for informasjonsklassifisering.*

Revisjonen har fått oversendt dokumentet *Bruk av «følsomhet», klassifisering i Office 365.* Dokumentet er ikke påført dato for godkjenning eller signatur. Dokumentet beskriver hvordan dokumenter med sensitiv informasjon kan lagres og deles i Office 365 ved å bruke funksjonen «følsomhet». Følsomhetsnivå skal bestemmes ved lagring av nytt dokument. Dette avgjør hvor dokumentet kan lagres, hvem det kan deles med og hvordan det kan deles.

5.1.5.2 Behandling av personopplysninger

Fylkeskommunen har ikke en egen rutine/retningslinje for personvern, som er et bevisst valg de har tatt, sier fagansvarlig for informasjonssikkerhet og personvern. *Styringsdokumentet for personvern og informasjonssikkerhet* skal gjelde både personvern og informasjonssikkerhet. Det vises også til at fylkeskommunen følger prinsippet for innebygd personvern. Dette følger også av fylkeskommunens arkitekturprinsipper[34]. Arkitekturprinsippene er styringsprinsipper for valg av løsninger ifm. innføring, utvikling og forvaltning av fylkeskommunens digitale tjenester

Fylkeskommunen har blant annet rutiner for

- Innsyn i egne personopplysninger
- Behandlingsoversikt (protokoll)
- Sikkerhetskrav for hemmelig adresse
- Databehandleravtalemal og sjekkliste for databehandleravtaler
- Ivaretagelse av personvern og databehandleravtaler i anskaffelser

På hjemmesiden til Innlandet fylkeskommune har de en personvernerklæring som beskriver hva slags personopplysninger de samler inn, hvordan de samler dem inn og hva personopplysningene brukes til. Det står også om de registrertes rettigheter og innsyn i egne personopplysninger.

5.1.5.3 Leverandørforhold

Fylkeskommunen har ingen egen retningslinje for leverandørforhold, men de er i gang med utarbeidelsen av en rutine som de kaller «Overordnet sikkerhetskrav i leverandørforhold». Ifølge fagansvarlig for informasjonssikkerhet og personvern har anskaffelsesteamet i IFK fått en liste over krav til informasjonssikkerhet og personvern som brukes i anskaffelser av IT-systemer. Både fagansvarlig for informasjonssikkerhet og personvern og personvernkoordinator er med i anskaffelsesprosessen og bidrar med evaluering av leverandørene. Det vises også til arkitekturprinsippene for Innlandet fylkeskommune som stiller krav til personvern og informasjonssikkerhet ved anskaffelser.

5.1.5.4 Hendelses- og avvikshåndtering

Fylkeskommunen har pr i dag ikke en egen IKT-beredskapsplan, men IKT-avdelingen har rutiner som iverksettes i forbindelse med hendelser. Conexus-saken[35] viser at de hadde et system som fungerte. Fagansvarlig for informasjonssikkerhet og personvern opplyser til revisjonen at fylkeskommunen har som mål å starte opp et arbeid med å utarbeide retningslinje/prosedyre for hendelseshåndtering for IKT-hendelser i løpet av høsten 2021.

[34] Arkitekturprinsipper for Innlandet fylkeskommune, godkjent av fylkesrådmann IFK 10.08.2020.
[35] Sikkerhetsbruddet hos selskapet Conexus i perioden 23.3.2020-5.5.2020. IFK ble berørt, og systemet hadde persondata om elever, lærere og enkelte ansatte i fylkesadministrasjonen.

Det presiseres at dette er en plan på IKT-området og ikke en generell hendelseshåndtering for fylkeskommunen.

Fylkeskommunen har en overordnet krisehåndteringsplan, vedtatt 11.12.2019. Denne er ment å håndtere hele spekteret av hendelser som nødvendiggjør en koordinert kriseledelse, også brudd knyttet til informasjonssikkerhet, sier sikkerhets- og beredskapssjefen. Det er utarbeidet tiltakskort som beskriver oppgaver ved ulike hendelser/situasjoner. Ett tiltakskort gjelder langvarig bortfall av IKT-tjenester som har betydning for krav til tilgjengelighet, men det er ingen spesifikke tiltakskort som gjelder andre større informasjonssikkerhetshendelser.

Revisjonen har fått oversendt dokumentet *Prosedyre for avvik personvern og informasjonssikkerhet*[36]. Hensikten med prosedyren er å sikre riktig og hensiktsmessig kartlegging, vurdering og iverksetting av tiltak ved behandling av avvik og uønskede hendelser knyttet til personvern og informasjonssikkerhet. Prosedyren baserer seg på *Prosedyre for registrering, behandling og rapportering av avvik*[37] samt fylkeskommunens plan- og styringssystem. Registrering og videre håndtering av avviket gjøres i fylkeskommunens avvikssystem Netpower. Det er også utarbeidet et skjema/prosedyre for varsling av personvernavvik.

Et avvik defineres som et forhold som ikke er i samsvar med lovgivning, forskrift, avtaler, eget internt reglement og instrukser. Et avvik omfatter brudd på personvern eller informasjonssikkerheten.

Dersom avviket er av et så stort omfang at det truer liv og helse, kritiske prosesser eller fylkeskommunens omdømme, skal avviket rapporteres umiddelbart til fylkeskommunedirektøren samt sikkerhets- og beredskapssjefen. I slike tilfeller skal det vurderes om avviket skal behandles iht. fylkeskommunens krisehåndteringsplan.

Kartlegging av avvik og vurdering av konsekvens og risiko gir grunnlag for fastsetting av avvikets alvorlighetsgrad, melding til eksterne parter, samt identifisering og prioritering av tiltak. Tiltak skal identifiseres basert på kartlegging og vurdering av risikoene som følger av avviket. Tiltak skal begrense skadeomfang, redusere risiko som følger av avviket og forebygge at avvik inntreffer på nytt. Tiltak registreres i avvikssystemet. Seksjon for Kvalitet, sikkerhet og beredskap er ansvarlig for regelmessig rapportering av vesentlige avvik til ledelse og fylkeskommunedirektør.

Revisjonen har også fått oversendt dokumentet *Rammer for bruk av kvalitetssystemets avviksmodul* [38] . Dokumentet angir hvilke typer avvik det skal rapporteres på. Her er informasjonssikkerhet og personvern inkludert.

5.1.5.6 Rutine for gjennomgang av styrende dokumenter

Fagansvarlig for informasjonssikkerhet og personvern opplyser at fylkeskommunen bruker kvalitetssystemet Netpower for å varsle om at rutiner skal følges opp. Systemet er bygget slik at man kan velge hvordan varslingen skal foregå. Hvert styringsdokument har en fast dato for gjennomgang. Dato for gjennomgang legges inn i kvalitetssystemet og eieren av dokumentet får en generert e-post med påminnelse før dato går ut.

---

[36] Prosedyre for avvik personvern og informasjonssikkerhet, godkjent 20.8.21 av avdelingsleder Administrasjon.
[37] Prosedyre for registrering, behandling og rapportering av avvik, godkjent 7.1.2021 av avdelingsleder Administrasjon.
[38] Rammer for bruk av kvalitetssystemets avviksmodul, godkjent 7.1.2021 av avdelingsleder for Administrasjon.

Når fagansvarlig for informasjonssikkerhet og personvern utarbeider en rutine har den vanligvis to års varighet, men noen er satt med kortere levetid siden fylkeskommunen er en ny organisasjon. Sikkerhets- og beredskapssjefen opplyser at standard varighet for rutiner i fylkeskommunens kvalitetsverktøy er 12 måneder.

Alle styringsdokumenter og rutinedokumenter skal godkjennes av en avdelingssjef. Dokumentene/rutinene er datert med det tidspunktet som de er godkjent, men ikke tidspunkt for neste revisjon. Det gjennomføres opplæring i bruken av verktøyet. Sikkerhet- og beredskapssjefen mener at fylkeskommunens kvalitetsverktøy sikrer at det til enhver tid er siste gjeldende versjon av en rutine som er tilgjengelig.

5.1.5 KONTINUERLIG EVALUERING OG FORBEDRING

Ledelsens gjennomgang

I *Styringsdokument for personvern og informasjonssikkerhet* står det at fylkeskommunen skal utarbeide tilstandsrapport for personvern og informasjonssikkerhet årlig som skal rapporteres til fylkesutvalget. Fagansvarlig for informasjonssikkerhet og personvern sier at det ikke er endelig bestemt om tilstandsrapporten skal gå til politisk nivå eller til fylkeskommunedirektørens ledergruppe. Tilstandsrapporten skal oppsummere status fra avdelingene og staber, hendelser innen personvern og informasjonssikkerhet, samt viktige tiltak som er iverksatt i fylkeskommunen. I dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* står det at sikkerhets- og beredskapssjefen skal planlegge og utføre ledelsens gjennomgang.

Sikkerhet- og beredskapssjefen har informert revisjonen om at tilstand for 2020 er utarbeidet og presentert fylkeskommunedirektøren og hans ledergruppe. Revisjonen har fått oversendt dokumentet, dokumentet er ikke datert eller signert. I dokumentet er det gjort en vurdering av tilstanden i Innlandet fylkeskommune sett opp mot anbefalte tiltak som virksomheter i offentlig og privat sektor bør gjennomføre iht. *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*[39]. Dokumentet presenterer status og hvilke oppgaver seksjon for Kvalitet, sikkerhet og beredskap mener må prioriteres basert på anbefalingene. Hvert punkt har en fargeangivelsene som angir tilstand. Tre av ni punkter er røde, mens tre er gule.

Annen rapportering

Det står også i dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* at sikkerhets- og beredskapssjefen har ansvar for å rapportere sikkerhetstilstand på informasjonssikkerhet og personvern til fylkeskommunedirektørens ledergruppe. Rådgiver i seksjon for Kvalitet, sikkerhet og beredskap opplyser at sikkerhets- og beredskapssjefen rapporterer tertialvis til ledergruppen. Rapporteringen gjelder alle tre områdene kvalitet, sikkerhet og beredskap. Dette er en overordnet rapportering som ikke inneholder alle detaljer. Den administrative tertialrapporteringen til politisk nivå inneholder også status på arbeidet med informasjonssikkerhet.

Revisjonen har i tillegg fått opplyst at det gjennomføres månedlige møter mellom fylkeskommunedirektøren, personvernombudet, sikkerhets- og beredskapssjefen og rådgiver i seksjon for Kvalitet, sikkerhet og beredskap (fagansvarlig for informasjonssikkerhet og personvern).

[39] Utarbeidet i tilknytning til *Nasjonal strategi for digital sikkerhet,* Regjeringen Solberg, januar 2019.

Rådgiver i seksjon for Kvalitet, sikkerhet og beredskap sier at de nå er i ferd med å bestemme en modell for rapportering på informasjonssikkerhetsområdet[40]. Det er et mål å lage systematiske rapporter som sammenfatter risikobildet i fylkeskommunen og iverksatte tiltak.

Kontinuerlig forbedring av styringssystemet

I *Styringsdokument for personvern og informasjonssikkerhet* står det at hensikten med dokumentet blant annet er å gi overordnede føringer for kontinuerlig forbedring av personvern- og informasjonssikkerhetsarbeidet i Innlandet fylkeskommune. Dokumentet inneholder imidlertid ingen punkter om evaluering og forbedring. I dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* står det at sikkerhets- og beredskapssjefen har ansvar for å sikre videreutvikling av styringssystemet for personvern og informasjonssikkerhet. Dette dokumentet beskriver roller og ansvar og gir ingen føring for hvordan utviklingsarbeid skal systematiseres.

Det står heller ikke noe om evaluering og forbedring i dokumentet *Prosedyre for avvik personvern og informasjonssikkerhet*, men i dokumentet *Rammer for bruk av kvalitetssystemet avviksmodul* står det at «Det å avdekke og følge opp avvik og risiko for avvik er et viktig element i internkontrollen og i det kontinuerlige forbedringsarbeidet. Det er viktig å sørge for at læring og forbedring skjer på organisasjonsnivået og ikke kun på individnivået. Et avvikssystem vil være et godt hjelpemiddel for å jobbe systematisk med forbedringer på organisasjonsnivå.» Det henvises til *Prosedyre for registrering, behandling og rapportering av forbedringsforslag* for nærmere beskrivelse av roller, ansvar og oppgaver i arbeidet med forbedringsforslag. En samlet oversikt over innkomne forbedringsforslag skal legges fram for fylkeskommunedirektørens kvartalsvise ledermøte.

Når det gjelder rapportering av avvik står det i dokumentet *Rammer for bruk av kvalitetssystemets avviksmodul* at i henhold til plan- og styringssystemet skal vesentlige avvik tas inn i tertialrapporten til fylkestinget. Aggregert informasjon om interne avvik (HMS, personvern, informasjonssikkerhet og tjenestekvalitet/prosesser) overføres manuelt fra avviksmodulen (Netpower) til rapporteringsverktøyet (Corporater), og tas inn i den helhetlige rapporteringen.

Seksjon for Kvalitet, sikkerhet og beredskap er, ifølge *Prosedyre for avvik personvern og informasjonssikkerhet*, ansvarlig for regelmessig rapportering av vesentlige avvik til ledelse og direktør. Rådgiver i seksjon for Kvalitet, sikkerhet og beredskap sier at dette er en del av den kvartalsvise rapporteringen fra sikkerhets- og beredskapssjefen til ledergruppen. Hittil i 2021 er det meldt inn 28 avvik som gjelder personvern og informasjonssikkerhet, hvorav 22 er lukket og 6 under behandling (pr november 2021). Alle avvik på personvern og informasjonssikkerhetsområdet går i kopi til fagansvarlig for informasjonssikkerhet og personvern og personvernombudet slik at de kan følge opp og etterspørre status.

I dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* står det at sikkerhets- og beredskapssjefen skal planlegge et årshjul for sikkerhetsaktiviteter. Likeens skal avdelingsledere utarbeide årsplan for personvern og informasjonssikkerhet knyttet til egen avdeling. Fagansvarlig for informasjonssikkerhet og personvern forteller at det ikke foreligger et godkjent årshjul for sikkerhetsarbeidet enda, og det er heller ikke utarbeidet av avdelingsledere. Det må avklares med fylkesledelsen hvilket godkjenningsnivå slike årshjul skal ha.

[40] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at modell for rapportering ble vedtatt den 19.11.2021. Revisjonen kjenner ikke til detaljene i modellen.

5.2 REVISJONENS VURDERING

Kapitlet er organisert slik at for hvert tema starter vi med å presentere de aktuelle revisjonskriteriene, og deretter vurderer vi de innsamlede dataene i kapittel 5.1 opp mot kriteriene.

5.2.1 SIKKERHETSPOLICY

- **Fylkeskommunen skal ha en policy for informasjonssikkerhet som viser ledelsens overordnede føringer for arbeidet med informasjonssikkerhet. Policyen skal inneholde;**
    - **Sikkerhetsmål som beskriver hva fylkeskommunen ønsker å oppnå på informasjonssikkerhetsområdet. Målene skal være risikobasert, samt målbare hvis praktisk mulig.**
    - **En strategi/plan for hvordan fylkeskommunen skal nå sikkerhetsmålene.**
    - **En forpliktelse til kontinuerlig forbedring av styringssystemet.**

Ledelsens overordnede føringer
Fylkeskommunen har utarbeidet dokumentet *Styringsdokument for personvern og informasjonssikkerhet.* Dokumentet utgjør det overordnede fundamentet i fylkeskommunens styringssystem for personvern og informasjonssikkerhet, hvor hensikten er å gi føringer for organisering, etablering, oppfølging, vedlikehold og kontinuerlig forbedring av personvern- og informasjonssikkerhetsarbeidet i Innlandet fylkeskommune. Disse føringene er gitt i form av mål for personvern og informasjonssikkerhet og en rekke krav og prinsipper for personvern og informasjonssikkerhet som fylkeskommunen skal ivareta for å oppnå målene.

Revisjonen mener at føringene gitt i styringsdokumentet er relativt generelle og ikke er knyttet opp mot fylkeskommunens status og situasjon på informasjonssikkerhetsområdet. En sikkerhetspolicy skal være tilpasset virksomhetens kompleksitet, risiko og behov, og angi en strategi/plan for hva virksomheten skal jobbe mot og på hvilken måte.

Sikkerhetsmål og sikkerhetsstrategi
Sikkerhetsmålene skal vise hva fylkeskommunen ønsker å oppnå på informasjonssikkerhetsområdet, mens strategien skal angi hvordan målene skal nås. I styringsdokumentet, under punktet for mål for personvern og informasjonssikkerhet, står det at det konkrete målet er å ivareta den registrertes rettigheter og friheter gjennom blant annet å forstå organisasjonens plikter i personvernforordningen, etablere retningslinjer for håndtering av personopplysninger, etterleve interne retningslinjer for personvern i egen oppgaveløsning, samt ivareta krav til konfidensialitet, integritet og tilgjengelighet.

Revisjonen mener at målene i styringsdokumentet har et for stort fokus på personvern. Fylkeskommunens konkrete mål på informasjonssikkerhetsområdet er å ivareta den registrertes rettigheter og friheter. Revisjonen mener at informasjonssikkerhet handler om å verne all informasjon, inkludert personopplysninger, og at fylkeskommunens sikkerhetsmål i større grad bør balanseres mellom personvern og informasjonssikkerhet.

Videre vurderer revisjonen at fylkeskommunens mål er lite spesifikke i forhold til fylkeskommunens status og behov på informasjonssikkerhetsområdet.

ISO 27001 legger vekt på at styringssystemet for informasjonssikkerhet skal planlegges ut ifra risikoer som er nødvendige å håndtere i virksomheten og at mål for informasjonssikkerhet skal ta hensyn til resultater fra risikovurderinger og –håndteringer. Revisjonen finner ikke at fylkeskommunens sikkerhetsmål baserer seg på en vurdering av fylkeskommunens risikonivå knyttet til informasjonssikkerhet.

Når det gjelder målenes målbarhet henger dette sammen med hvor konkrete målene er. En kan måle hvorvidt en retningslinje er på plass, men det er ikke like enkelt å måle om retningslinjen er forstått og fulgt. Et mål på dette kan være antall avvik, men dersom regelverket ikke er forstått vil det helder ikke bli meldt avvik. Dersom målene er overordnet bør de konkretiseres i undermål som er målbare. Revisjonen vurderer at målene i styringsdokumentet er lite konkrete og dermed vanskelige å måle.

Styringsdokumentet angir ingen strategi for å nå målene, med unntak av å utarbeide retningslinjer på konkrete fokusområder. Revisjonen vurderer at dette er relevante fokusområder som er i henhold til krav i ISO 27001, og hvor det er viktig å få på plass retningslinjer. Revisjonen finner imidlertid ikke at styringsdokumentet har en kobling mellom mål og strategi, hvor det er gitt en beskrivelse av hvordan det enkelte mål skal oppnås. På hvilken måte skal fylkeskommunen oppnå at de ansatte bare behandler personopplysninger i samsvar med personvernprinsippene, når skal dette være oppnådd, hvilke ressurser må til, og hvordan kan det måles?

I styringsdokumentets avsnitt om mål for personvern og informasjonssikkerhet står det også at fylkeskommunen må fremstå som en pådriver i å fremme godt personvern og god sikkerhetskultur. Det framgår ikke av dokumentet hvordan fylkeskommunen skal oppnå en rolle som en pådriver i informasjonssikkerhetsarbeidet.

Forpliktelse til kontinuerlig forbedring av styringssystemet
Det er videre et krav i ISO 27001 at informasjonssikkerhetspolicyen skal inneholde en forpliktelse til kontinuerlig forbedring av styringssystemet. Det står i styringsdokumentet til fylkeskommunen at hensikten med dokumentet blant annet er å gi overordnede føringer for kontinuerlig forbedring av personvern- og informasjonssikkerhetsarbeidet i Innlandet fylkeskommune. Revisjonen finner ikke at dette punktet er fulgt opp i dokumentet og vurderer at fylkeskommunens informasjonssikkerhetspolicy/styringsdokument ikke inneholder en forpliktelse til kontinuerlig forbedring av styringssystemet.

5.2.2 INTERN ORGANISERING/ROLLER OG ANSVAR

- **Fylkeskommunen skal ha etablert en hensiktsmessig intern organisering for arbeidet med informasjonssikkerhet. Herunder**
    - **Roller og ansvar skal være hensiktsmessig fordelt, klart beskrevet, formidlet og dokumentert.**
    - **Det skal sikres at nødvendige ressurser er tilgjengelig.**
    - **Det skal være gjennomført nødvendig opplæring.**
    - **Det bør være opprettet kontakt med relevante myndigheter og interessefora på informasjonssikkerhetsområdet.**

Roller og ansvar

Dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* beskriver de rollene som har ansvar for arbeidet med informasjonssikkerhet og personvern i Innlandet fylkeskommune.

I hvilken grad de ulike rollene er tildelt og formidlet er det vanskelig for revisjonen å vurdere, men vårt inntrykk er at organiseringen er «satt» og de ansatte kjenner sine roller. Når det gjelder ansvarsområdene knyttet til den enkelte rolle ser vi at det er lagt relativt mye ansvar for sikkerhetsarbeidet til sikkerhets- og beredskapssjefen. Ifølge dokumentet *Roller og ansvar* skal sikkerhets- og beredskapssjefen utarbeide, oppdatere og formidle både styrende og utførende dokumenter i styringssystem for personvern og informasjonssikkerhet, sikre videreutvikling av styringssystemet, ivareta fagansvaret for informasjonssikkerhet og bidra til daglig oppfølging av linjeansvaret, samt verifisere etterlevelsen av interne og eksterne krav gjennom sikkerhetsrevisjoner.

Revisjonen har fått opplyst at sikkerhets- og beredskapssjefens ansvar på informasjonssikkerhetsområdet i praksis er delegert videre til rådgiver (fagansvarlig) for informasjonssikkerhet og personvern. Dette er svært mye ansvar og arbeid tildelt én person og framstår som noe sårbart.

Ifølge fylkeskommunens styringssystem skal ansvaret for arbeidet med informasjonssikkerhet og personvern som hovedregel følge linjen. Dette medfører at avdelingssjefene har ansvar for å ivareta informasjonssikkerhet i egen avdeling, som igjen innebærer å gjennomføre verdivurderinger, risikovurderinger, iverksette tiltak, kontrollere tilstand, følge opp hendelser, tildele roller, samt sikre nødvendig kapasitet og kompetanse. Revisjonen er ikke kjent med hvordan dette ansvaret er ivaretatt, men vurderer at avdelingsledere har en omfattende og kritisk rolle i informasjonssikkerhetsarbeidet, og at det er viktig at disse er sitt ansvar bevisst og har nødvendige ressurser og støtte.

Nødvendige ressurser

Digitaliseringsdirektoratet (og ISO 27001), som er det organ som er utpekt av departementet til å gi anbefalinger knyttet til internkontroll på informasjonssikkerhetsområdet, legger vekt på at ledelsen skal lede an og ha det overordnede ansvaret for at sikkerhetsarbeidet gjennomføres på en hensiktsmessig måte, herunder sikre nødvendige ressurser. I dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* står det at fylkeskommunedirektøren skal sikre nødvendig kapasitet og kompetanse til arbeidet med personvern og informasjonssikkerhet.

Revisjonen setter spørsmålstegn ved om det er avsatt tilstrekkelig ressurser til sikkerhetsarbeidet. Dette gjelder spesielt ressurser til å utføre oppgavene under sikkerhets- og beredskapssjefens ansvarsområde som er svært omfattende. Revisjonen mener også at avdelingsledere har en omfattende og kritisk rolle i arbeidet med personvern og informasjonssikkerhet og at det er viktig at de har nødvendig støtte og kapasitet til å utføre dette arbeidet.

Opplæring

Når det gjelder opplæring har revisjonen fått opplyst at fylkeskommunen ikke har en obligatorisk generell sikkerhetsopplæring for alle ansatte, men at alle får opplæring knyttet til de ulike tjenestene/systemene, samt tilbud om foredrag, kampanjer, etc. Det arbeides med en egen opplæringspakke for personvern og informasjonssikkerhet og en sikkerhetsinstruks. I tillegg er det utarbeidet en prosedyre for opplæring i personvern og informasjonssikkerhet som er lagt fram for godkjenning.

Ifølge ISO 27001 skal virksomheten fastslå nødvendig kompetansebehov og sikre passende opplæring. Revisjonen vurderer at alle ansatte bør ha opplæring tilpasset sin rolle, og at det bør sikres at alle ansatte har fått nødvendig opplæring.

I dokumentet *Roller og ansvar for informasjonssikkerhet* og *personvern* står det i dokumentets del 1 at arbeidet med informasjonssikkerhet i Innlandet fylkeskommune skjer på strategisk, taktisk og operativt nivå. Deretter er det gitt en beskrivelse av de tre nivåene. Revisjonen mener at dette er en informativ beskrivelse av styringssystemet for personvern og informasjonssikkerhet som naturlig også hører hjemme i overordnet styringsdokument for personvern og informasjonssikkerhet.

Kontakt med relevante myndigheter og interessefora
Fylkeskommunen er medlem av Foreningen Kommunal Informasjonssikkerhet (KiNS) og andre fylkeskommunale fora for informasjonssikkerhet. Det er nå besluttet å delta i Kommune-CSIRT. Fylkeskommunen har også opprettet kontakt med Nasjonal Sikkerhets myndighet (NSM).

Revisjonen vurderer at fylkeskommunen har kontakt med myndigheter/interessegrupper som er relevante for informasjonssikkerheten.

5.2.3 OVERORDNET RETNINGSLINJE FOR RISIKOSTYRING

- **Fylkeskommunen skal ha etablert en overordnet retningslinje for gjennomføring av risikovurderinger som en del av sikkerhetsarbeidet.**

Overordnet retningslinje for risikostyring
Ifølge dokumentet *Roller og ansvar for informasjonssikkerhet og personvern* skal fylkeskommunen etablere en metode for risikostyring som en del av det overordnede arbeidet med informasjonssikkerhet. Fylkeskommunen hadde ikke en godkjent retningslinje for risikostyring i revisjonsprosjektets prosjektperiode[41]. Revisjonen fikk opplyst i informasjonsinnhentingen at dokumentet *Overordnet sikkerhetskrav for risikostyring* var under arbeid, men at rutinen ikke var endelig godkjent fordi det først måtte på plass en beslutning om fylkeskommunens risikostyringsmetodikk[42]. Revisjonen har ikke vurdert det foreløpige dokumentet.

Fylkeskommunen har opplyst at den foreløpige rutinen delvis har vært i bruk og at den fungerer som en mal for å gjøre risikovurderinger av systemene. Det er ikke gjennomført en overordnet risiko- og sårbarhetsanalyse (ROS) av informasjonssikkerhetsområdet i fylkeskommunen, men det skal utarbeides en overordnet ROS for hele fylkeskommunen der også informasjonssikkerhet skal inkluderes.

Revisjonen mener at risikostyring er grunnleggende i et styringssystem for informasjonssikkerhet og at overordnet retningslinje for risikostyring er et fundament for å få på plass en risikovurderingstankegang i det øvrige sikkerhetsarbeidet. Det er derfor viktig at en overordnet retningslinje for risikostyring kommer på plass og at metodikken implementeres på en hensiktsmessig måte.

---

[41] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at retningslinjen ble godkjent den 16.11.2021.
[42] Fylkeskommunen har opplyst etter at rapporten ble sendt på høring at risikostyringsmetodikk ble godkjent den 5.12.2021. Revisjonen har ikke sett denne metodikken.

5.2.4 ANDRE STYRENDE RETNINGSLINJER

- **Fylkeskommunen skal ha utarbeidet nødvendige rutiner og prosedyrer, som skal gjennomgås i planlagte intervaller. Fylkeskommunen bør ha utarbeidet følgende sentrale styrende retningslinjer som bidrar til å opprettholde ønsket sikkerhetsnivå;**

    - **Retningslinje og prosedyre for klassifisering av informasjon.**
    - **Retningslinje for behandling av personopplysninger.**
    - **Retningslinje for informasjonssikkerhet i leverandørforhold.**
    - **Retningslinje for avviks- og hendelseshåndtering.**

Retningslinje og prosedyre for klassifisering av informasjon
For å drive risikostyring er det vesentlig å kjenne hvilke informasjonsverdier som skal beskyttes og klassifisere informasjonen i henhold til behov for å sikre konfidensialitet, integritet og tilgjengelighet. En retningslinje for klassifisering av informasjon skal gi føringer for hvilke informasjonsklasser fylkeskommunen skal ha og hvilke typer informasjon som hører hjemme i de ulike klassene. En prosedyre for klassifisering av informasjon beskriver den operasjonelle delen, hvordan dette skal gjennomføres ute i organisasjonen.

Fylkeskommunen har utarbeidet dokumentet *Overordnet sikkerhetskrav for informasjonsklassifisering*. Revisjonen vurderer at fylkeskommunen har på plass en styrende retningslinje for klassifisering av informasjon.

Når det gjelder prosedyrer eller operasjonelle retningslinjer sier fylkeskommunen at tjenesteeier har ansvar for å utarbeide egne prosedyrer. Etter det revisjonen forstår er det på nåværende tidspunkt ikke utarbeidet egne prosedyrer for hvordan informasjonsklassifiseringen skal foregå i praksis, med unntak av en rutine for *Bruk av «følsomhet», klassifisering i Office 365*, som beskriver hvordan dokumenter med sensitiv informasjon kan lagres og deles i Office 365. Revisjonen vurderer at det ikke er utarbeidet prosedyrer for informasjonsklassifisering, med unntak for Office 365.

Retningslinje for behandling av personopplysninger
Fylkeskommunen har ikke etablert en egen retningslinje for behandling av personopplysninger, og sier at dette er ivaretatt i dokumentet *Styringsdokument for personvern og informasjonssikkerhet*. Ifølge fylkeskommunen har de egne rutiner for flere områder som gjelder personvern.

Det er positivt at fylkeskommunen har utarbeidet rutiner på personvernområdet. Revisjonen mener likevel at det ville gitt en bedre oversikt over krav til personverntiltak om disse var samlet i ett dokument, og dermed større trygghet for en systematisk etterlevelse. Revisjonen vil også påpeke at styringsdokumentet er en overordnet policy og ikke en retningslinje.

Retningslinje for informasjonssikkerhet i leverandørforhold
Fylkeskommunen har ingen egen rutine for informasjonssikkerhet i leverandørforhold. En slik rutine skal sikre beskyttelse av fylkeskommunens aktiva som er tilgjengelig for leverandører. Fylkeskommunen er i gang med utarbeidelsen av en rutine som de kaller «Overordnet sikkerhetskrav i leverandørforhold».

Det er anskaffelsesteamet i IFK som ivaretar krav til informasjonssikkerhet og personvern i anskaffelsene, men fagansvarlig for informasjonssikkerhet og personvern og personvernkoordinatoren bidrar med evaluering av leverandørene.

Selv om fylkeskommunen sier at sikkerhetskrav ivaretas i anskaffelsene vurderer revisjonen at en egen rutine for leverandørforhold vil ivareta en systematisk tilnærming til informasjonssikkerhet i forhold til alle leverandører, ikke bare ved anskaffelser.

Retningslinje for avviks- og hendelseshåndtering

Avviks- og hendelseshåndtering handler om å ha en plan for hvordan avvik og hendelser skal håndteres når de oppstår. Avvik og uønskede hendelser skal registreres og behandles, med formål om å lære hvordan en kan unngå at avviket gjentar seg. Dersom det oppstår uønskede hendelser eller kriser med et stort omfang eller med alvorlige konsekvenser må det reageres umiddelbart. Det bør foreligge en beredskapsplan for hvordan virksomheten skal håndtere slike akutte større hendelser, der oppgaver og roller i beredskapen er kjent og øvd på.

Fylkeskommunen har utarbeidet dokumentet *Prosedyrer for avvik personvern og informasjonssikkerhet*, som baserer seg på fylkeskommunens overordnede prosedyre for registrering, behandling og rapportering av avvik. Avvikene skal registreres og håndteres i fylkeskommunens avvikssystem Netpower. Revisjonen vurderer at fylkeskommunen har på plass en retningslinje for behandling av avvik og mindre alvorlige hendelser.

Revisjonen vil påpeke at dersom avviks- og hendelseshåndtering skal fungere er det en forutsetning at de ansatte kjenner til og forstår hvilke hendelser som skal defineres som et avvik og hvilket område avviket gjelder. Prosedyredokumentet inneholder en generell definisjon på avvik, men kunne med fordel ha gitt eksempler på eller konkretisert hvilke typer avvik som er å anse som brudd på informasjonssikkerheten eller personvernet, eller vist til hvilke krav og instrukser som er gjeldende.

I *Prosedyre for avvik personvern og informasjonssikkerhet* står det at det skal vurderes om avviket skal behandles iht. fylkeskommunens krisehåndteringsplan dersom avviket er av et så stort omfang at det truer liv og helse, kritiske prosesser, eller fylkeskommunens omdømme. Krisehåndteringsplanen inkluderer ikke tiltakskort for et scenario som omhandler større hendelser knyttet til informasjonssikkerhet. Det er heller ikke utarbeidet en egen beredskapsplan for IKT-området, men det er et mål å utarbeide en retningslinje for kontinuitet. Revisjonen vurderer at fylkeskommunen ikke har en tilfredsstillende plan for håndtering av akutte hendelser og kriser knyttet til informasjonssikkerhet.

Rutine for gjennomgang av styrende dokumenter

Fylkeskommunen benytter kvalitetssystemet Netpower for å varsle om at rutinedokumenter skal følges opp. Eieren av dokumentet skal legge inn dato for neste gjennomgang og metode for varsling. Dette sikrer at alle dokumenteiere blir varslet om at det er tid for ny gjennomgang. Det er imidlertid ikke opplyst hvordan oppdateringen av dokumentene skal gjennomføres; hvem har ansvar for at oppdateringen gjennomføres, og på hvilken måte oppdateringen skal skje.

Revisjonen vurderer at det er positivt at kvalitetssystemet benyttes til å systematisere oppdatering av rutinedokumenter, men bemerker at rutinen kan være noe sårbar hvis det er opp til den enkelte dokumenteier å bestemme hvordan oppdateringen skal foregå.

5.2.5 KONTINUERLIG EVALUERING OG FORBEDRING

- **Arbeidet med styring og kontroll av informasjonssikkerheten skal være gjenstand for kontinuerlig evaluering og forbedring, og status for fylkeskommunens arbeid med informasjonssikkerhet bør rapporteres regelmessig til den øverste politiske og administrative ledelsen.**

Fylkeskommunen opplyser at de er i ferd med å utarbeide en modell for rapportering på informasjonssikkerhetsområdet, og at denne foreløpig ikke er endelig implementert[43].

Ifølge fylkeskommunens styringsdokumenter skal sikkerhets- og beredskapssjefen planlegge og utføre ledelsens gjennomgang. Dette er en årlig tilstandsrapport for personvern og informasjonssikkerhet som oppsummerer status, hendelser og tiltak. Fylkeskommunen opplyser at det ikke er endelig avgjort om denne rapporteringen skal gå til politisk nivå eller fylkeskommunedirektørnivå[44]. I tillegg skal sikkerhets- og beredskapssjefen rapportere tertialvis til fylkeskommunedirektørens ledergruppe om status for sine ansvarsområder.

Revisjonen vurderer at fylkeskommunen har utarbeidd retningslinjer for regelmessig rapportering av status for informasjonssikkerheten til ledelsen. Det er viktig at innhold og nivå på rapporteringen fastsettes. Revisjonen mener at fylkeskommunens tilstand på informasjonssikkerhetsområdet også bør kommuniseres til politisk nivå.

Rapportering om status for tilstand bør gi et beslutningsgrunnlag for videre forbedring og behov for endringer. Kontinuerlig forbedring av internkontrollsystemet følger både av kommuneloven § 25, personvernforordningen, ISO 27001 og NSM grunnprinsipper.

I fylkeskommunens prosedyre for avvik personvern og informasjonssikkerhet står det at seksjon for Kvalitet, sikkerhet og beredskap er ansvarlig for å rapportere vesentlige avvik til fylkeskommunedirektøren, men det står ikke noe om hvordan avvikene skal følges opp i videre arbeid. I fylkeskommunens generelle rutine for bruk av kvalitetssystemets avviksmodul finner vi at det å avdekke og følge opp avvik er et viktig element i internkontrollen og i det kontinuerlige forbedringsarbeidet. Det er videre utarbeidet en rutine for registering, behandling og rapportering av forbedringsforslag.

Revisjonen mener det er positivt at fylkeskommunen har etablert rutiner for avvikshåndtering og forbedringsforslag, men finner ikke at det er etablert rutine for systematisk evaluering og forbedring av styringssystem for personvern og informasjonssikkerhet. Oppfølging av avvik et er ett eksempel på en kilde som kan benyttes til forbedring av styringssystemet. Andre eksempler er analyser etter sikkerhetshendelser, øvelser, tester, eller interne revisjoner.

---

[43] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at modell for rapportering ble godkjent 19.11.2021. Revisjonen kjenner ikke innholdet i modellen.
[44] Viser til note 43.

6. INFORMASJONSSIKKERHET I ELEMENTS CLOUD

Problemstilling 2 besvares i to deler. I dette kapitlet undersøker vi hvordan informasjonssikkerheten er ivaretatt i fylkeskommunens sak- og arkivsystem Elements Cloud[45].

I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i sak- og arkivsystemet Elements?

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 fylkeskommunen som har ansvar for Elements, samt fylkeskommunens svar på skriftlige henvendelser.

6.1 DATA

Om Elements

Elements Cloud er fylkeskommunens sak- og arkivsystem som ble anskaffet i forbindelse med fylkessammenslåingen. Systemet inneholder store mengder personopplysninger, både personopplysninger om ansatte og om brukere av en fylkeskommunal tjeneste. Systemet ble offisielt tatt i bruk fra 1.1.20. Avtalen om anskaffelse av Elements Cloud ble inngått våren 2019 med Evry Norge AS, som senere ble overtatt av Sikri AS.

Informasjonen som behandles i Elements kan systematiseres i hovedtyper. Informasjonen i systemet finnes i personalmapper, elevmapper, politiske saker, saker knyttet til anskaffelser, eller saker knyttet til generell saksbehandling. I tillegg vil det være informasjonsverdier i e-poster.

Elements Cloud er et skybasert system (cloud), som innebærer at programvaren ligger på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett, og ikke er installert lokalt. Kjøpsavtalen inkluderer både drift og vedlikehold av systemet. Dette innebærer at leverandøren gjør mye av sikkerhetsarbeidet, men hovedansvaret hviler likevel på fylkeskommunen som må sikre at leverandøren har tiltak som gir trygghet for ønsket sikkerhetsnivå.

Ansvarsfordelingen for sikkerhet i Elements er slik:

1) IFK har ansvar for sikkerheten knyttet til IFK's infrastruktur, nettverk, påloggingspolicy og autentisering av brukere til Elements.
2) Tjenesteforvalter for Elements hos IFK har ansvar for administrasjon av brukere og roller, samt tilgangsstyring.
3) Sikri har ansvar for verifisering av brukernes pålogging til systemet og sikkerheten i og rundt Elements på skyplattformen.

[45] Cloud indikerer at systemet er skybasert.

6.1.1 IDENTIFISERE OG KARTLEGGE

Risikovurderinger

Revisjonen har fått oversendt en risikovurderingsrapport for Elements Cloud, datert den 3.12.2019. Risikovurderingen er gjennomført av en arbeidsgruppe for sak-/arkivløsningen i Innlandet fylkeskommune med bistand fra en prosessveileder. Metoden er basert på Norsk standard 5814 og OFK/HFK[46] sine akseptkriterier for risiko. Målet for risikovurderingen var å vurdere informasjonsverdiene som behandles, identifisere trusler/farer/sårbarheter med særlig vekt på behandling av personopplysninger, analysere uønskede hendelser som kan oppstå og indentifisere mulige tiltak for å redusere risiko.

Det står i risikovurderingsrapporten fra 2019 at selve risikovurderingen er dokumentert i et egenutviklet verktøy i en Excel-arbeidsbok. Rapporten sammenfatter hovedpunkter og hovedkonklusjoner. Utdyping og detaljer er dokumentert i arbeidsboken.

Verdivurderingen av informasjonsverdiene som behandles i Elements viste at det er høy risiko forbundet med brudd på konfidensialitet og integritet, og middels risiko forbundet med tilgjengelighet.

Ifølge fylkeskommunen revideres ikke risikoanalysen til faste tidspunkt, men når det oppstår hendelser/endrede risikoer. Det er ikke gjennomført revisjoner etter 2019. Innlandet fylkeskommune sier de følger ISO-standarden som innebærer at det gjøres ny risikovurdering dersom det skjer endringer som tilsier at risikoen i systemet øker. Rådgiver i seksjon for Kvalitet, sikkerhet og beredskap sier at de følger med på trusselbildet og varsler tjenesteeier/ tjenesteansvarlig ved behov for nye risikovurderinger.

Det ble gjennomført en vurdering av risiko og håndtering av data (januar 2021) da Elements Cloud-kunder skulle migreres til ny skyplattform. Denne ble utarbeidet av Sikri og gjennomgått sammen med fylkeskommunen i et felles forberedende møte.

Oppfølging av tiltak

Det er satt opp en tiltaksplan[47] som følger opp tiltakene fra risikovurderingen fra desember 2019. Det er til sammen satt opp 53 tiltak. Det framgår av planen hvilke tiltak som er gjennomført (30 stk.), hvilke som er påbegynt (3 stk.), hvilke som Sikri (leverandøren) har ansvar for (8 stk.), og hvilke som ikke er påbegynt (4 stk.). Det er ikke satt tidsfrister for tiltakene, men for tiltak «Påbegynt» og «Ikke påbegynt/ikke prioritert» er det satt inn årstall for når tiltaket skal gjennomføres.

Av de fire tiltakene som ikke er påbegynt skal, ifølge tiltaksplanen, to av dem gjennomføres i løpet av 2021/2022, og to i løpet av 2022. Ett av tiltakene som ikke er påbegynt gjelder penetrasjonstest, som er planlagt gjennomført i tilknytning til en skjemaløsning som er integrert med Elements. Det er besluttet å vente med testen til etter at denne skjemaløsningen er migrert over til skyplattform 1. kvartal 2022.

Noen av tiltakene gjennomføres fortløpende/kontinuerlig (8 stk.), som f.eks. tiltak for kompetanse/kultur, opplæring, automatiseringstiltak, og oppfølging av databehandleravtalen.

---

[46] Oppland fylkeskommune (OFK) og Hedmark fylkeskommune (HFK).
[47] Oppfølging av tiltak etter gjennomført risikovurdering, sist oppdatert 3.5.2021

Noen tiltak er ikke gjennomført fordi de henger sammen med det overordnede styringssystemet (som er under arbeid), og må derfor avvente til dette er ferdig.

Ifølge tiltaksplanen er Sikri ansvarlig for noen av tiltakene. Det står ingenting om hvorvidt disse tiltakene er gjennomført, eller på hvilken måte de følges opp fra fylkeskommunen. Fylkeskommunen presiserer at tiltaksplanen kun omhandler tiltak som fylkeskommunen har ansvar for og kan gjennomføre. Ved behov for ytterligere innsyn i leverandørens arbeid med sikkerhet/ risikovurderinger (altså utover den dokumentasjonen som allerede foreligger), må leverandør kontaktes.

Av de 53 tiltakene er 16 knyttet til hendelser som har høy risiko dersom ikke tiltak iverksettes. Av disse er åtte gjennomført, to er påbegynt, ett er ikke påbegynt, tre er leverandørens ansvar, og to skal gjennomføres fortløpende. De fortløpende tiltakene gjelder bygging av sikkerhetskultur/kompetanse, samt bevissthet og gode rutiner rundt bruk av e-post.

Rådgiver i seksjon for Kvalitet, sikkerhet og beredskap sier at alle tiltak knyttet til hendelser med rød risiko skal ha en tiltakseier og en fristdato. Dette fremgår ikke av tiltaksplanen, kun årstall for når tiltaket skal gjennomføres.

Hendelser med gul og grønn risiko kan aksepteres uten at tiltak innføres. Det gjøres en vurdering av kost/nytte for tiltakene. Rutiner vedrørende risikoanalyser og tiltak skal stå beskrevet i «Overordnet sikkerhetskrav for risikostyring», men dette dokumentet er ikke endelig godkjent enda[48].

Fylkeskommunen opplyser at det alltid er tjenesteeier som er overordnet ansvarlig for sikkerheten i tjenesten og for gjennomføringen av risikoreduserende tiltak, mens tjenesteansvarlig er utførende. Rådgiver i seksjon for Kvalitet, sikkerhet og beredskap sier at tiltakseier ikke nødvendigvis må tilhøre avdelingen, det er graderingen av risiko som bestemmer hvem som har ansvaret. Gradering av risiko, og rutiner for hvem som har ansvar, følger av det overordnende styringssystemet, sier han.

6.1.2 BESKYTTE OG OPPRETTHOLDE

Sikkerhetsopplæring
Det gjennomføres kontinuerlig kompetanseheving/opplæring gjennom brukerhjelp, kurs, og webinarer knyttet til Elements. Disse gjelder også nyansatte. Webinarene er en serie temaer som bygger på hverandre, og som er tilgjengelig på intranettet (INNsia). Fylkeskommunen tilbyr også en egen e-læring som er tilgjengelig for alle ansatte. Når det gjelder opplæring i informasjonssikkerhet har de egne tema som bl.a. pålogging, tilgangsstyring, klassifisering, skjerming av informasjon, bruk av sikre kanaler for forsendelse av post/dokumenter, håndtering av personopplysninger, bruk av e-post osv. De har også mange skriftlige rutiner for Elements og daglig brukerstøtte.

Andre arenaer for opplæring er:
- Nettverk for personvernkoordinatorer i IFK
- Sikkerhetsmåned i regi av personvernombudet: mikroleksjoner, klistermerke-kampanje o.l.

[48] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at dokumentet ble godkjent 16.11.2021. Revisjonen har ikke vurdert dette dokumentet.

• Informasjon på intranettet – ulike tema, bl.a. dataangrep, phishing
• Informasjonssikkerhet/personvern for ledere, jf. ledersamling 25. mars 2021

Regime for sikkerhetsoppdatering av systemet
Når det gjelder sikkerhetsoppdatering sier fylkeskommunen at dette ivaretas og overvåkes av leverandøren Sikri.

Videre opplyser fylkeskommunen følgende om utvikling/vedlikehold av Elements:

- Nye versjoner lanseres minst to ganger i måneden.
- Sikri sender infobrev til IFK om endringer, nye versjoner og installasjon i testmiljø.
- Systemteamet (Dokumentasjonsforvaltning) deltar i Sikris gjennomgang av endringene.
- Systemteamet tester endringene i testmiljø.
- Ny versjon installeres i produksjonsmiljø.
- Systemteamet legger ut informasjon om ny versjon på intranettet.
- Ved omfattende endringer informerer systemteamet support IKT, endringsansvarlig og superbrukere for Elements direkte, og organiserer opplæring/informasjon for brukere i form av digitale møter.
- Sikri setter opp webinarer for alle cloud-kunder én gang pr måned.

All ny funksjonalitet eller feilrettinger blir testet og kvalitetssikret gjennom Sikri sine prosedyrer for utvikling og test, slik at IFK har trygghet for at brukerne er sikret en stabil og tilgjengelig løsning. Sikri har en egen testrutine for Elements Cloud. Fylkeskommunen har mottatt både testmetodikk og rutiner. I tillegg har fylkeskommunen og Sikri løpende dialog om forbedring av testing/oppfølging av nye versjoner både hos Sikri og hos fylkeskommunen.

Revisjonen har spurt fylkeskommunen om de får jevnlig informasjon fra Sikri om tekniske sårbarheter. Fylkeskommunen sier at de ikke får egne rapporter om tekniske sårbarheter som oppstår. De får månedlige rapporter knyttet til bruken av systemet; statistikk, åpne hendelser, feilhåndtering, etc. De har løpende dialog med leverandøren. Det ble gjennomført møter i forbindelse med flytting av Elements til ny skyplattform. Det gjennomføres også møter i forkant av systemoppgraderinger, hver 14. dag. Sikri skal varsle fylkeskommunen om vesentlige endringer i tjenesten. Risikoer/sårbarheter tas opp i møter med Sikri; månedlig med deres FAM (Functional Account Manager), som er fylkeskommunenes faste kontaktperson hos leverandøren, og kontraktsmøter hvert kvartal.

På spørsmål om fylkeskommunen evaluerer de tekniske sårbarhetene selv svarer de at de i utgangspunktet har ansvar for sikkerheten selv, men Sikri som leverandør er delegert den tekniske/operative sikkerheten. Fylkeskommunen opplyser at de selv må kvalitetssikre at Sikri leverer det de sier de skal levere. De har et forum der fylkeskommunen kan ta opp problemstillinger overfor leverandøren, som deretter gir forslag til løsninger.

Gjennomgang av funksjonalitet
På spørsmål om systemets funksjonaliteter har blitt gjennomgått og om unødvendig funksjonalitet er slått av svarer fylkeskommunen følgende:

- Konfigurasjon av Elements ble gjennomført både i testmiljø og i produksjonsmiljø ved oppstart av systemet, sammen med Sikri.
- Det kan være behov for å gjøre justeringer, f.eks. ved tilgang på ny/endret funksjonalitet i systemet.
- Dokumentert i konfigurasjonsdokumentet (ikke oversendt).

Standardpassord
Vi har spurt fylkeskommunen om systemets standardpassord er byttet. Fylkeskommunen sier at leverandøren ivaretar dette i henhold til egne sikkerhetsrutiner.

Beskyttelse av data under oppbevaring
På spørsmålet om hvordan data beskyttes i systemet under oppbevaring sier fylkeskommunen at dette ivaretas og overvåkes av leverandøren. De viser til underlagsmateriale for risikovurdering av Elements (Sikri, 1.11.19) og til databehandleravtale knyttet til Elements Cloud (2.1.2020), samt til rutine om tilgangsstyring i Elements. Sikris tekniske og organisatoriske tiltak knyttet til ivaretakelse av informasjonssikkerhet er beskrevet i møteprotokoll 4.3.2019 (ikke oversendt revisjonen).

Ved lagring er alle data kryptert, ofte kalt encryption at rest. For noen typer data er dette løst ved kryptering på filsystemnivå, på andre med innebygd støtte i produktet. For sikring av SQL Server benyttes Transparent Data Encryption (TDE).

For øvrig viser fylkeskommunen til disse punktene:

- Autorisasjon av brukere /påloggingspolicy.
- Tilgangsstyring i Elements.
- Skjerming av opplysninger.

Brukernes pålogging til fylkeskommunens nettverk og applikasjoner styres av fylkeskommunens felles passord-policy. Dette gjelder også for Elements. Pålogging utenfor fylkeskommunens nettverk skjer via «Mine applikasjoner» med to-faktor autentisering. Innenfor fylkeskommunens nettverk skjer autentisering via Single-Sign–On (SSO). Det kreves bekreftelse fra bruker også ved pålogging til Elements og tilknyttede applikasjoner (M365) for dokumentproduksjon og arkivering av e-post fra Outlook.

Alle brukerkontoer for ansatte vedlikeholdes via Visma HRM (Human Resource Management). Elements benytter en egen tjeneste, Elements IdentityServer, for pålogging. Denne kan føderere (samordne, integrere) med en rekke ulike påloggingsløsninger via standardene SAML2 og ws-federation.

Skjerming av opplysninger inngår i mange rutiner, f.eks. anskaffelsessaker. Personalmapper (personalarkiv) og utdanningsmapper (elevarkiv) skjermes automatisk. I flere integrasjoner for automatisk dokumentoverføring fra andre fagsystemer til Elements er skjerming av dokumenter definert på forhånd. Dette gjelder også for dokumentfangst via digitale skjemaer.

Fylkeskommunen har utarbeidet en egen prosedyre for tilgangsstyring i Elements, godkjent 7.5.2021. Formålet med prosedyren er å sikre at opplysninger i Elements kun er tilgjengelig etter tjenstlig behov. Dette innebærer at brukere autentiseres på en betryggende måte og at tilganger tildeles, administreres, kontrolleres og fjernes. Brukere av Elements skal gis tilgang til opplysninger bare i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt og annen særskilt autorisering. Rutinen skal bidra til at tilgangsstyring i Elements blir kjent, forstått og etterlevd. Tilganger til informasjon i Elements gis ved at bruker knyttes til en rolle i systemet. Ulike roller gir tilgang til ulike funksjoner i systemet, f.eks. journalføre dokumenter, fordele post og godkjenne dokumenter.

Beskyttelse av dataflyten i systemet (nettverk og overføring mellom enheter)
Fylkeskommunen sier at dette overvåkes av leverandørens overvåkingsavdeling. De viser til underlagsmateriale for risikovurdering av Elements utført av Sikri. Fylkeskommunen fremhever følgende punkt:

- Nettverkstrafikk (data in transit) er sikret ved at all ekstern trafikk mot Elements Cloud gjøres via https/tls.
- Backend-trafikk ((trafikken bak applikasjonen, det «usynlige» grunnlaget for hvordan systemet fungerer) mellom Docker-containerne krypteres av Docker.
- Systemet genererer logger og rapporter som følges opp ved behov.
- Nye integrasjoner testes nøye: først i testmiljø deretter i produksjonsmiljø.
- Dataoverføring mellom systemene logges både i Elements og i fagsystemene som er integrert med Elements.
- Rapporter som inneholder feilmeldinger/stans ved dataoverføring følges opp daglig.

Det er ikke mulig å logge på eller få direkte tilgang til virtuelle maskiner, docker-containere, data og annet som potensielt kan inneholde kundedata.

Beskyttelse av informasjonsverdier lagret på medier
Fylkeskommunen sier at beskyttelse av informasjonsverdier som er lagret i medier ivaretas av leverandøren. De viser til underlagsmateriale for risikovurdering av Elements utført av Sikri og til databehandleravtale knyttet til Elements Cloud.

Fylkeskommunen framhever følgende punkt som er på plass:

- Autorisasjon av brukere /påloggingspolicy.
- To-faktorpålogging.
- Tilgangsstyring i Elements.
- Skjerming av opplysninger.
- Kryptering ved lagring.
- For å sikre at driftspersonell hos Sikri ikke skal få utilsiktet tilgang, er alle data inkl. database-backup kryptert ved lagring (Encryption at rest.) Antiviruskontroll utføres fortløpende på dokumentlager.
- Automatisk konvertering av dokumenter til godkjent arkivformat.
- IFK's bevarings- og kassasjonsplan (ikke oversendt).

Gjenopprettelse av data
På spørsmål om systemet har evne til å gjenopprette data svarer fylkeskommunen at dette ivaretas av leverandøren. De framhever følgende:

- IFK kan få tilgang til backup/sikkerhetskopi ved bestilling etter nærmere avtale.
- For å sikre segmentering/isolering av kundedata, lagres disse i ulike SQL Server-databaser og filområder. Dette forenkler også backup og returnering av data til kunden ved ev. avslutning av kundeforhold.
- Det er strenge krav til testing av rekonstruksjon for å kunne levere raskt i Cloud. Oppdages feil når endringer pushes ut, kan Sikri rulle tilbake til forrige versjon umiddelbart.

Sikri har etter forespørsel fra fylkeskommunen informert om at det ikke tas offline backup, men at back-up lagres på egen storage account på et annet datasenter med 30 dagers backup.
Det finnes tre typer backuper:

- Full back-up: ukentlig
- Inkrementell back-up: daglig
- Back-up av logg på transaksjoner: Hver time

Test av sikkerhetskopi
Fylkeskommunen sier at testing av sikkerhetskopiene blir ivaretatt av leverandøren, og at IFK kan bestille tester ved behov.

Fylkeskommunen har ikke fått noen rapporter om at det er utført tester. Men når det har vært feil i systemet i forbindelse med ny versjon, har de måtte rulle tilbake til forrige versjon og dette har fungert. Fylkeskommunen antar derfor at sikkerhetskopien fungerer. Det er ingen avtale med Sikri om at de skal rapportere på testingen. Slike rapporter kan etterspørres ved behov.

6.1.3 OPPDAGE

Hendelseslogg
Fylkeskommunen opplyser at Elements har hendelseslogg knyttet til ulike aktiviteter som utføres av brukere. I tillegg logges det dataoverføring fra/til andre fagsystemer og registre.

I tillegg til standard NOARK-logger, logges en rekke hendelser til en Elastic database, med dashboards i Kibana. Disse loggene er ikke direkte tilgjengelig for sluttbrukere, men brukes til å monitorere ytelse og uønskede hendelser.

Fylkeskommunen gjennomgår interne logger (NOARK-rapporter) løpende. Tjenesteforvaltere gjennomfører daglig kontrolloppgaver knyttet til dette. Eksempler på kontrolloppgaver kan være overvåking av logger/ rapporter knyttet til konvertering av dokumenter til arkivformater, digital utsendelse av dokumenter, signeringsoppdrag, overføring av data/dokumenter via integrasjoner osv.

Loggføring av aktiviteter
På spørsmål om systemet har en loggføring av administratorers og operatørers aktiviteter viser fylkeskommunen til det som er skrevet under hendelseslogg.

Beskyttelse av logger
Når det gjelder beskyttelse av logg for aktuelt objekt (sak eller journalpost) svarer fylkeskommunen at disse er tilgjengelig for alle som har tilgang til det aktuelle objektet (jf. tilgangsstyring). Fylkeskommunen er ikke kjent med at det er noen logger som kun er tilgjengelig for systemadministrator, men de tror at det er noen logger som i prinsippet kun er tilgjengelig for Sikri.

Ulike logger håndteres ulikt. Noen overvåkingslogger slettes etter at feilsituasjoner er løst. Logger som dokumenterer brukernes aktiviteter i systemet blir arkivert og bevart.

På spørsmål om hvordan integriteten i loggene er ivaretatt svarer fylkeskommunen at teknisk logging ligger hos Sikri. Sikri har informert om at Noark-logger ligger i hver database. Systemlogger lagres i Elastic Search som kun er tilgjengelig for autorisert personale og kun fra innsiden av nettverket, ikke via internett. Det ligger feillogger og NOARK-logger i Elements som IFK har tilgang til.

Sikkerhetsovervåking av systemet
Sikkerhetsovervåkingen av systemet skal styres av Sikri, dette følger av avtalen som er inngått ved kjøp[49]. Fylkeskommunen opplyser at sentralt i løsningen er Docker Enterprise installasjon, egen overvåkningsløsning, virtuelle maskiner, SQL Server og kryptert fillagring. Dette driftes av Digital Platform Services (DPS), en egen avdeling i Sikri.

Sikri har en egen avdeling som jobber med sikkerhet. IFK har dialog med Sikri om overvåkning i forbindelse med innføring av nye versjoner. Nye versjoner inneholder feilrettinger og forbedringer, men kan også inneholde uønskede endringer eller feil på funksjoner som fungerte tidligere.

I tillegg utfører fylkeskommunen egen overvåking. Systemteamet (Dokumentasjonsforvaltning) og integrasjonsansvarlig overvåker Elements daglig gjennom ulike kontroller og følger opp rapporter med feilmeldinger. IKT-enheter overvåker klientsiden med nettverk og brukernes autorisering og pålogging. Det er også mulig å hente ut anonymisert statistikk over bruksmønster.

Penetrasjonstest
Det er planlagt en penetrasjonstest for å avdekke sårbarheter i den tekniske infrastrukturen (opsjon i tjenesteavtalen). Testen skal bestå av:

- Ekstern sikkerhetstest: Simulere et angrep som kommer fra internett.
- Intern sikkerhetstest: Simulere et angrep som kommer fra det interne nettverket.
- Sosial manipulering: Prøve å lure våre ansatte for å skaffe seg tilgang til nettverket.

Fylkeskommunene har besluttet å prioritere sikkerhetstesten knyttet til skjemaløsning ACOS Interact som er integrert med Elements. Fylkeskommunen vil vente med en slik sikkerhetstest til etter at ACOS Interact er migrert over til skyplattform 1. kvartal 2022.

6.1.4 HÅNDTERE OG GJENOPPRETTE

Hendelseshåndteringsplan
Det finnes ikke en egen hendelseshåndteringsplan for Elements, men det finnes en overordnet krisehåndteringsplan for Innlandet fylkeskommune. Fylkeskommunen jobber med en rutine for Elements som skal angi hvem som skal gjøre hva, hvis situasjoner oppstår.

Personvernavvik skal varsles i samsvar med egen rutine. De har en nødprosedyre (rutine) som skal brukes hvis Elements er nede.

[49] Avtale om løpende tjenestekjøp over internett (SSA-L) og Standard tjenestenivå Elements Cloud (SSA-L,5.april 2019, punkt 6.4).

Det er et mål å oppdage, rapportere, registrere og håndtere eventuelle hendelser, avvik og informasjonssikkerhetsbrudd tidligst mulig, og håndtere raskest mulig. Det jobbes med kultur for systematisk rapportering av hendelser, avvik og brudd.

I tillegg viser fylkeskommunen til:

- Oppfølging av avvik/hendelser knyttet til tjenestekvalitet via IFK's kvalitetssystem.
- Sikri overvåker systemet i henhold til avtale for tjenestekjøp.
- Det jobbes med evaluering, kontinuerlig forbedring og kompetanseheving.
- Prosedyre - Overvåking og hendelseshåndtering - Elements Cloud (under arbeid).

Fylkeskommunen har spurt Sikri om en hendelseshåndteringsplan og hvor hendelseshåndtering skjer hos Sikri. Sikri informerer om at de benytter runbook for dette, samt at de informerer kunder og andre involverte via Statuspage (eller e-post). I tillegg har de Disaster/Recovery planer og driller.

De har ikke hatt noen øvelse om hendelser knyttet til sikkerhet. Når det har skjedd feil i systemet har man fått testet hvordan samarbeidet foregår i praksis. Sikri har rullet ut nye versjoner med feil, og da har de trukket denne tilbake. De har mulighet til å kjøpe ekstraøvelser.

Redundansmulighet

På spørsmål om Elements har redundansmuligheter som sikrer tilgjengelighetskrav svarer fylkeskommunen at det er avtalt tjenestenivå på 99,5 % tilgjengelighet med leverandør. Sikri tar sikkerhetskopier og har ansvar for rekonstruksjon av data.

Sikri viser til at Microsoft er ansvarlig for tilgjengeligheten av sine Azure-datasentre, og at det skal være tilstrekkelig redundans for å ivareta krav til tilgjengelighet.

6.2 REVISJONENS VURDERING

For hvert tema starter vi med å presentere de aktuelle revisjonskriteriene, og deretter vurderer vi de innsamlede dataene i kapittel 6.1 opp mot kriteriene.

6.2.1 IDENTIFISERE OG KARTLEGGE

- **Fylkeskommunen 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.**
- **Fylkeskommunen bør oppdatere risikovurderingen i faste intervaller og ved betydelige endringer.**

Elements Cloud ble anskaffet i forbindelse med opprettelsen av nye Innlandet fylkeskommune. Det ble gjennomført en risikovurdering i forkant av innføringen av systemet. Denne er ikke revidert. Ifølge fylkeskommunen skal risikovurderingen revideres dersom det oppstår endringer som påvirker risikoen. Revisjonen mener at risikovurderingen i tillegg bør revideres med faste mellomrom, slik at organisasjonen må gjennomgå øvelsen med å tenke igjennom hvilke uønskede hendelser som kan oppstå. Dette kan også være hendelser som ikke er knyttet til det ytre trusselbildet, men som kan være relatert til avvik, etterlevelse av rutiner, etc.

Det er satt opp en plan/oversikt over anbefalte tiltak i risikovurderingen (sist oppdatert 3.5.21) hvor det framgår status for det enkelte tiltak. De fleste tiltakene er gjennomført, men fire tiltak var ikke påbegynt ved siste oppdatering av planen. Ett av disse tiltakene er knyttet til en hendelse med høy risiko og er planlagt gjennomført i 2022, tre år etter at risikovurderingen ble gjennomført. Revisjonen mener at tiltak knyttet til hendelser med høy risiko bør ha høy prioritet for gjennomføring.

Ifølge fylkeskommunen skal hendelser med rød (høy) risiko påføres tiltakseier og en fristdato. Dette framkommer ikke av tiltaksplanen, men påbegynte og ikke påbegynte tiltak har påført årstall for gjennomføring. Revisjonen vurderer at årstall for gjennomføring ikke tilsvarer fristdato, og at frist for gjennomføring kunne vært mer spesifisert. Når tiltakseier ikke er påført kan det være tvil om hvem som har det faktiske ansvaret for å gjennomføre tiltaket.

Noen tiltak er det leverandøren som har ansvar for å gjennomføre og tre av disse er knyttet til hendelser med høy risiko. Fylkeskommunen har ikke kontrollert statusen på disse. Revisjonen vurderer at fylkeskommunen bør følge opp om leverandøren har på plass kritiske tiltak. Dersom dette gjelder tiltak som er kontrollert gjennom kravspesifikasjon ved anskaffelsen eller databehandleravtalen behøver de ikke stå oppført som tiltak i tiltaksplanen. Dersom fylkeskommunen ikke kjenner til om leverandøren har på plass de aktuelle tiltakene medfører dette at fylkeskommunen ikke kjenner den faktiske risikoen forbundet med systemet.

Det er også flere tiltak i tiltaksplanen som ikke har fastlagt en endelig tidsfrist, men som skal gjennomføres kontinuerlig/fortløpende. To av disse tiltakene er knyttet til hendelser med høy risiko. Revisjonen mener at slike kritiske tiltak bør følges opp i henhold til en plan, slik at det er mulig å vurdere tiltakets status.

Et av tiltakene gjelder kompetanse/bevissthet/gode rutiner/lojalitet knyttet til bruk av e-post. Dersom dette er et viktig tiltak for å redusere en hendelse med høy risiko bør det legges en plan for hvordan en kan sikre at kompetansen/rutinene er på plass, og for hvordan dette kan måles.

6.2.2 BESKYTTE OG OPPRETTHOLDE

- **Fylkeskommunen skal ha gjennomført sikkerhetsopplæring av systemets brukere.**

Det gjennomføres kontinuerlig kompetanseheving/opplæring av systemets brukere som omfatter ulike temaer knyttet til informasjonssikkerhet. Revisjonen vurderer at fylkeskommunen har etablert et regime for opplæring av systemets brukere. Revisjonen kjenner ikke til i hvilken grad fylkeskommunen sikrer at alle brukere har fått tilpasset opplæring, og at alle relevante temaer er gjennomgått, men mener at dette er vesentlig for risikostyringen av systemet.

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

It-systemer er under kontinuerlig endring når løsninger først er satt i drift. Dette kan skyldes nye brukerbehov, endringer i trusselbildet, nyoppdagede sårbarheter, m.m. Det er derfor viktig å oppgradere og verifisere konfigurasjonen med jevne mellomrom.

Det er leverandøren som ivaretar sikkerhetsoppdateringer av Elements. Det lanseres nye systemoppgraderinger minst to ganger i måneden. Fylkeskommunen får informasjon om endringer i forkant og deltar i testing av nye versjoner. Risikoer og sårbarheter tas opp i møter med leverandøren. De får månedlige rapporter knyttet til bruken av systemet.

Revisjonen vurderer at fylkeskommunen har etablert et tilfredsstillende regime for sikkerhetsoppdatering av systemet.

- **Fylkeskommunen bør ha gjennomgått IT-systemets funksjonaliteter og unødvendig funksjonalitet bør ha blitt slått av.**
- **Systemets standardpassord bør ha blitt byttet.**

Systemer som ikke er eksplisitt konfigurert har ofte sårbarheter som en angriper kan utnytte. Det er derfor viktig å «herde» systemene ved å ta bort funksjonalitet det ikke er tjenstlig behov for, samt fjerne standardinnstillinger.

Fylkeskommunen har opplyst at det ble gjennomført konfigurasjon av systemet ved oppstart, hvor både fylkeskommunen og leverandøren deltok. Konfigurasjonen ble først gjennomført i testmiljø. Revisjonen kan ikke ut ifra denne informasjonen vurdere om unødvendig funksjonalitet er slått av.

Når det gjelder hvorvidt standardpassord er byttet ut, sier fylkeskommunen at leverandøren ivaretar dette iht. egne sikkerhetsrutiner. Revisjonen kan ikke vurdere om kriteriet er oppfylt ut ifra denne informasjonen.

Revisjonen bemerker at siden pålogging til Elements skjer enten via tofaktor-autentisering (utenfor nettverk) eller Single-Sign-On (innenfor) at problemstillingen i dette tilfellet ikke er relevant. Disse prosessene benytter ikke forhåndsinnstilte passord.

- **Fylkeskommunen bør beskytte data i IT-systemet under oppbevaring i samsvar med gjennomført klassifisering av systemets informasjonsverdier.**

Det er leverandøren som ivaretar ansvaret for å beskytte data i systemet under oppbevaring, men fylkeskommunen styrer tilganger og autoriseringen av brukere. Fylkeskommunen har gjennomført en verdivurdering av informasjonsverdiene som behandles i Elements. Denne viste at systemet behandler informasjonsverdier som har behov for høy beskyttelse.

Leverandøren sikrer at alle data under oppbevaring er kryptert. Fylkeskommunen har utarbeidet egen rutine for tilgangsstyring i Elements som skal sikre at opplysninger er tilgjengelig etter tjenstlig behov. Pålogging til Elements styres av fylkeskommunens felles påloggingspolicy, som innebærer to-faktor autentisering utenfor nettverk og Single-Sign-On innenfor. Det er også utarbeidet rutiner for skjerming av sensitiv informasjon, hvor for eksempel elevmapper og personalmapper skjermes automatisk.

Revisjonen vurderer at fylkeskommunen har en tilfredsstillende beskyttelse av data under oppbevaring i systemet og at denne er i tråd med gjennomført informasjonsklassifisering.

- **Fylkeskommunen bør beskytte data i systemet under overføring (dataflyt) i samsvar med gjennomført klassifisering av systemets informasjonsverdier.**

Dataflyt betegner data som transporteres i et nettverk eller som overføres innenfor virksomheten og med eksterne parter.

Fylkeskommunen sier at dataflyten knyttet til Elements overvåkes av leverandørens overvåkingsavdeling. Nettverkstrafikk er sikret ved at all ekstern trafikk mot Elements gjøres via https/tls, og back-end trafikk er kryptert. Det genereres logger og rapporter som følges opp ved behov. Feilmeldinger følges opp daglig. Dette gjelder både for Elements og integrerte fagsystemer.

Revisjonen vurderer at fylkeskommunen har en tilfredsstillende beskyttelse av data under overføring som er i tråd med gjennomført informasjonsklassifisering.

- **Informasjonsverdier lagret på medier bør være tilstrekkelig sikret i samsvar med gjennomført informasjonsklassifisering, ved:**
  - **Bruk**
  - **Flytting/transport**
  - **Avhending/Arkivering**

Når det gjelder beskyttelse av informasjonsverdier ved bruk av Elements viser fylkeskommunen til deres påloggingspolicy, rutine for tilgangsstyring, samt rutine for skjerming.

Når systemet er skybasert vil det ikke være lagret informasjon på ulike medier. Programmet hentes opp via internett. Det er derfor ikke like viktig med beskyttelse av fysisk utstyr, etc, i denne sammenheng. Dersom en ikke-autorisert bruker oppnår tilgang skal informasjonen være uleselig. Alle data, inklusive database back-up, er kryptert ved lagring, samt at det utføres antiviruskontroll fortløpende.

Revisjonen vurderer at fylkeskommunen har en tilfredsstillende beskyttelse av informasjonsverdier når systemet er i bruk, eller som er lagret på medier, som er i tråd med risikovurderingen av informasjonsverdiene.

- **Fylkeskommunen bør ha sikret muligheten til å gjenopprette systemets data.**
- **Det bør ha blitt gjennomført regelmessige tester for å verifisere at sikkerhetskopien fungerer.**

Dataangrep kan medføre at kritiske konfigurasjoner, kritisk programvare eller kritisk informasjon endres eller gjøres utilgjengelig, jf. hendelsen i Østre Toten kommune. Det er derfor et viktig sikkerhetstiltak å etablere en evne til å gjenopprette data og ha tilgjengelig sikkerhetskopier. Det er også viktig å teste sikkerhetskopier for å kontrollere at disse fungerer.

Det er leverandøren som ivaretar ansvaret for gjenoppretting av data. Fylkeskommunen kan få tilgang til back-up/sikkerhetskopi ved bestilling. Oppdages feil ved lansering av nye systemoppdateringer kan de gå tilbake til forrige versjon umiddelbart. Det tas back-up både hver time, daglig og ukentlig, og back-up lagres på trygt sted i 30 dager.

Testing av sikkerhetskopier blir også ivaretatt av leverandøren. Fylkeskommunen kan bestille tester ved behov, eller etterspørre testrapport. Fylkeskommunen har ikke etterspurt testrapporter, men det har hendt at tjenesten har blitt rullet tilbake til forrige versjon ved lansering av nye versjoner når det har oppstått feil.

Revisjonen vurderer at fylkeskommunen har sikret muligheten til å gjenopprette systemets data og til å gjennomføre testing av sikkerhetskopier. Revisjonen kan ikke vurdere om det har blitt gjennomført regelmessige tester, men det at rullering tilbake til tidligere versjoner har vært vellykket viser at sikkerhetskopiene har fungert.

6.2.3 OPPDAGE

- **Fylkeskommunen bør ha opprettet en hendelseslogg for hvert system.**
- **Loggføring bør inneholde informasjon om systemadministrators og systemoperatørers aktiviteter.**
- **Systemets logger bør være tilstrekkelig sikret.**

Det er viktig å registrere og analysere brukeraktiviteter, avvik, feil og hendelser, for å oppdage eventuelle mistenksomme hendelser/aktiviteter, samt at loggingen er tilstrekkelig sikret mot uvedkommende.

Fylkeskommunen opplyser at Elements har hendelseslogg knyttet til ulike aktiviteter som utføres av brukere. I tillegg logges det dataoverføring fra/til andre fagsystemer og registre. Fylkeskommunen gjennomgår løpende interne logger. Det er i tillegg etablert standard nettverksovervåking for å avdekke uønsket trafikk.

Revisjonen vurderer at fylkeskommunen har opprettet tilfredsstillende hendelseslogg for systemet og at denne også ivaretar systemadministrator og -operatørers aktiviteter.

Når det gjelder sikring av loggene viser fylkeskommunen til rutinen for tilgangsstyring. IFK har tilgang til feillogger og NOARK-logger, mens den tekniske loggingen er ivaretatt av leverandøren. Systemlogger er kun tilgjengelig for autorisert personale, og kun fra innsiden av nettverket. Noen logger slettes etter at situasjonen er løst, mens andre logger av brukeraktivitet arkiveres og bevares.

Det er ikke opplyst hvilke muligheter som finnes til å endre eller slette logger for de som har tilgang.

Revisjonen vurderer at systemets logger er sikret, men det er vanskelig å vurdere om sikringen er tilstrekkelig med bakgrunn i tilgjengelig informasjon.

- **Det bør være etablert sikkerhetsovervåking av systemet.**

Å etablere en sikkerhetsovervåking av systemet er viktig for å oppdage sårbarheter eller forhold av sikkerhetstruende karakter. Mangelfull sikkerhetsovervåking kan innebære at angripere kan skjule tilstedeværelse, handlinger og aktiviteter i systemet.

Sikkerhetsovervåking av systemet styres i utgangspunktet av leverandøren, men fylkeskommunen har også en egen overvåking som utføres av systemteamet. Leverandøren har en egen overvåkningsløsning med elementer som vurderes å innebære en profesjonell løsning.

Revisjonen vurderer at fylkeskommunen har etablert en tilfredsstillende sikkerhetsovervåking av systemet.

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

Fylkeskommunen bør teste egen forsvarsevne ved å gjennomføre inntrengningstest (penetrasjonstest), for å identifisere mangler og svakheter i systemet.

Det er planlagt en penetrasjonstest i løpet av 2022 for å avdekke sårbarheter i den tekniske infrastrukturen. Dette er et tiltak i risikoanalysen fra desember 2019 som foreløpig ikke er gjennomført.

Revisjonen vurderer at fylkeskommunen ikke har gjennomført penetrasjonstest av systemet. Revisjonen mener at slike tester kan gjennomføres jevnlig og ikke nødvendigvis bare i forbindelse med spesielle hendelser

6.2.4 HÅNDTERE OG GJENOPPRETTE

- **Fylkeskommunen bør ha utarbeidet en hendelseshåndteringsplan for systemet.**

En hendelseshåndteringsplan er en beredskapsplan som skal gjøre fylkeskommunen i stand til å håndtere sikkerhetshendelser knyttet til systemet og gjenopprette normaltilstand.

Det finnes ikke en egen hendelseshåndteringsplan for Elements, men fylkeskommunen viser til overordnet krisehåndteringsplan for Innlandet fylkeskommune. De har en nødprosedyre som skal brukes hvis Elements er ute av funksjon. Det jobbes nå med en prosedyre for overvåking og hendelseshåndtering for Elements. De har ikke gjennomført øvelser knyttet til sikkerhetshendelser.

Leverandøren har en egen prosedyre for hendelser som de må håndtere.

Revisjonen vurderer at fylkeskommunen ikke har utarbeidet en hendelseshåndteringsplan for Elements. Dersom en alvorlig sikkerhetshendelse oppstår er det fylkeskommunen som sitter med ansvaret knyttet til konsekvensene av sensitiv informasjon på avveie, ikke leverandøren. Det er derfor viktig at hendelseshåndteringen skjer i fylkeskommunen.

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

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

Fylkeskommunen sier at det er avtalt tjenestenivå på 99,5% med leverandør, som blant annet sikres gjennom sikkerhetskopier og rekonstruksjon av data. Leverandøren viser til at Microsoft er ansvarlig for tilgjengeligheten av sine datasentre, og at dette skal gi tilstrekkelig redundans for å ivareta krav til tilgjengelighet.

Revisjonen vurderer at fylkeskommunen har tilfredsstillende redundansmuligheter.

7. INFORMASJONSSIKKERHET I SKYSSWEB

Problemstilling 2 besvares i to deler. I dette kapitlet undersøker vi hvordan informasjonssikkerheten er ivaretatt i saksbehandlingssystemet Skyssweb.

> I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i saksbehandlingssystemet Skyssweb?

Vi starter med å presentere innhentet informasjon, deretter vurderer vi informasjonen opp mot de konkrete revisjonskriteriene. Informasjonen baserer seg i hovedsak på informasjon i form av skriftlige svar fra fylkeskommunen og intervju med rådgiver i avdeling for digitale tjenester i Innlandstrafikk som er systemansvarlig for Skyssweb. Fylkeskommunen ved Innlandstrafikk er også gitt anledning til å gå igjennom datakapitlet for å kontrollere og eventuelt supplere informasjonen.

7.1 DATA

Om Skyssweb
Skyssweb er et saksbehandlingssystem som benyttes til å behandle søknader om skoleskyss for elever i grunnskole og videregående skole. Systemeier er Innlandet fylkeskommune ved Innlandstrafikk. Systemet behandler personopplysninger om elever som har behov for skoleskyss. For skoleåret 2020/2021 var det 23.364 elever som hadde godkjent skoleskyss i en eller annen form.

Kommunene melder inn skysselever i grunnskolen og timeplaner for offentlige og private grunnskoler i kommunen innen 1. mars hvert år. Elevene ved videregående skole søker selv om skoleskyss, så snart de er tildelt skoleplass, via portalen MinSkyss som er et brukervennlig webgrensesnitt mot Skyssweb (fra 2015).

Systemet benyttes av elever ved videregående skoler, skyssansvarlig i kommunene eller ved skolene og rute- og transportplanleggere i Innlandstrafikk. Transportører (drosje) har også tilgang til opplysninger om elever de skal frakte.

For elevene registreres fullt navn, fødselsnummer, bostedsadresse(r), skoletilhørighet, skolens start- og sluttider, holdeplass, samt skyss-kode som kan angi om eleven har spesielle behov. Elever som søker om skoleskyss gjennom MinSkyss blir også bedt om å oppgi mobiltelefonnummer, e-postadresse og et passord. Legeattester og annen dokumentasjon som bekrefter rett til skoleskyss, for eksempel på medisinsk grunnlag, lastes opp i Skyssweb av skyssansvarlig i kommunene og via MinSkyss for elever i videregående skole.

Systemet ble opprinnelig anskaffet i Opplandstrafikk i 2009. Leverandør og utvikler av systemet er Trapeze. Systemet driftes av fylkeskommunens IKT-avdeling via en lokal server. Leverandøren foretar endringer i systemet og utfører teknisk support.

7.1.1 IDENTIFISERE OG KARTLEGGE

Risikovurderinger

Det er gjennomført en risikovurdering av Skyssweb i 2019. Vurderingen er gjennomført av en intern arbeidsgruppe i Oppland fylkeskommune med bistand av en prosessveileder.

Styrende dokumenter for personvern og informasjonssikkerhet i Oppland fylkeskommune (OFK) påla systemeiere å foreta jevnlige risikovurderinger. Risikovurderingen skulle avdekke om bruken av systemet oppfylte de kravene som skoleeier stilte til sikring av personopplysningenes konfidensialitet, integritet og tilgjengelighet. Metoden som er brukt er basert på Norsk standard 5814 og OFK sine akseptkriterier for risiko. Deler av det metodiske grunnlaget stammer også fra veilederen «Sikker håndtering av personopplysninger i skolen» (Senter for IKT i utdanningen, 2011).

Arbeidsgruppen gjennomførte innledningsvis en verdivurdering av informasjonen i systemet. Den viste at det potensielt er informasjon i systemet som har høy verdi i et konfidensialitetsperspektiv. Systemet behandler søknader om skoleskyss som kan være dokumentert med legeattester eller andre sensitive personopplysninger. Videre ble beskyttelse av tilgjengelighet satt til middels høy verdi, der kritisk nedetid ble vurdert til mer enn ett døgn.

Det ble identifisert fem uønskede hendelser. Risikovurderingen viste at det var behov for å iverksette risikoreduserende tiltak for flere uønskede hendelser. Arbeidsgruppen anbefalte en liste med tiltak som skulle iverksettes og at restrisikoen ble akseptert. Etter arbeidsgruppens vurdering ville implementering av tiltakene redusere det totale risikobildet. Tiltakene ble gitt prioritet 1 – bør gjennomføres snarest, prioritet 2 – bør gjennomføres, og prioritet 3 - gjennomføres ikke.

Risikovurderingen er avgrenset til bruken av Skyssweb og omfatter ikke risikovurdering av drift og vedlikehold av systemet og databasen.

Områder som er behandlet er;

- Håndtering av sensitiv personinformasjon
- Tilgangsstyring
- Kontroll av tilganger og tilgangsstyring
- Logging
- Dokumentasjon
- Personell
- Integrasjon mot andre systemer
- Hendelseshåndtering, forbedringer
- Samsvar med lover og annet regelverk

I samtale med systemansvarlig ble det opplyst at det ikke har vært fastsatt en bestemt dato for revidering av risikovurderingen. Han sier at de har planlagt å utarbeide en ny ROS-analyse i løpet av 2021 i forbindelse med en større oppgradering av systemet.

Seksjon for Kvalitet, sikkerhet og beredskap skal hjelpe dem med dette. Revisjonen har ikke fått svar på om ROS-analysen er gjennomført[50].

Oppfølging av tiltak
Det ble identifisert til sammen fem risikoreduserende tiltak i risikovurderingen fra 2019. Fire med prioritet 1 og én med prioritet 2. Det ble ikke satt noen tidsfrist for gjennomføring, eller tildelt ansvar for gjennomføring.

Ifølge systemansvarlig er status for gjennomføringen av tiltak slik pr november 2021:

Disse tiltakene er gjennomført:

- Ny teknisk løsning slik at transportører henter oppdrag direkte fra Skyssweb, pålogging via ID-porten.

Disse tiltakene er delvis gjennomført:

- Databehandleravtaler med transportørene er under arbeid.
- Rutiner for dialog med transportører er i bruk, men ikke godt nok dokumentert.

Disse tiltakene er ikke gjennomført:

- Databehandleravtaler med kommunene.
- Penetrasjonstester for å verifisere at webapplikasjonene tilfredsstiller kravene til OWASP Application Security Verification Standard (prioritet 2).
- Fortsette bevisstgjøring og holdningstiltak på fagenhetsmøter. Ikke utført noe spesielt for Skyssweb. Bare gjennomført generelt for hele Innlandstrafikk.

Når det gjelder databehandleravtale med kommunene sier systemansvarlig at de ikke har fått en vurdering som sier at dette er noe de må ha. Dette i lys av at både fylkeskommunen og kommunene er ansvarlige for organiseringen av skoleskyssen. Det foreligger ikke en plan for når de resterende tiltakene skal gjennomføres. I etterkant av risikovurderingen er det også innført innlogging via ID-porten for alle eksterne brukere (ikke for MinSkyss)[51]. ID-porten er en felles innloggingsløsning til offentlige tjenester på internett som tilbyr sikker innlogging ved bruk av elektronisk ID.

7.1.2 BESKYTTE OG OPPRETTHOLDE

Sikkerhetsopplæring
I intervju har systemansvarlig oppgitt at det ikke er gitt opplæring utover den generelle opplæringen som blir gitt i fylkeskommunen om behandling av personopplysninger. Behandling av personopplysninger er et tema som jevnlig er oppe i ulike møter/fora i Innlandstrafikk. Det blir gitt generell opplæring for brukere av systemet[52].

[50] Revisjonen har mottatt en foreløpig ROS-analyse den 10.1.22. Denne er ikke gjennomgått.
[51] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at det er innført innlogging via ID-porten også for interne brukere i desember 2021.
[52] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at det ble innført faste brukerforum/møter i nov-21 både for eksterne (kommuner og skoler) og interne brukere, der sikkerhet er en del av opplæringen.

Det er flest nye brukere ute i kommunene, og da gir fylket tilgang gjennom ID-porten. Brukere på skolene lærer opp hverandre. Systemet har en egen brukerveiledning som ligger i systemet når man logger inn. Brukerne på skolene får brukerstøtte ved behov via Innlandstrafikk sitt kundesenter og fra to medarbeidere i faggruppen Digitale tjenester.

Regime for sikkerhetsoppdatering av systemet

Systemansvarlig opplyser at systemet (Skyssweb) ikke blir patchet[53] fortløpende, men det kommer oppgradering ca. én gang pr år. IKT-avdelingen i fylket utfører vedlikehold på servere og annen infrastruktur siste torsdag hver måned og i tillegg ved behov.

Det er planlagt en større oppgradering av systemet høst 2021. Systemansvarlig sier at denne har blitt forsinket på grunn av tiltak i forbindelse med sikkerhet og tilhørende konfigurasjon av ny løsning. IKT-avdelingen har stilt strenge krav som leverandøren har brukt lang tid på å tilpasse seg. De er nå i gang igjen med oppgraderingen (november-21), men dette er samtidig et utviklingsløp der nye deler /moduler kommer til etter hvert som de blir testet og godkjent.

På spørsmål om fylkeskommunen evaluerer de tekniske sårbarhetene selv svarer de at det er IKT-avdelingen som styrer tilgang til servere. Det er IKT som drifter serveren som Skyssweb ligger på og som styrer åpninger i brannmur. Systemansvarlig opplyser at ROS-analysen som skal gjennomføres nå også skal inkludere IKT-avdelingen.

Leverandøren (Trapeze) foretar endringer i systemet og utfører support for det tekniske. Det gis tidsbegrenset tilgang etter gjeldende prosedyrer. Representant hos leverandør undertegner personlig «Taushetserklæring konsulenter IFK» når vedkommende skal ha tilgang[54].

Gjennomgang av funksjonalitet

Ifølge systemansvarlig er Skyssweb delvis utviklet spesielt for fylkeskommunen (Oppland) etter en anbudskonkurranse og tilhørende kravspesifikasjon. Det er derfor lite unødvendig funksjonalitet. De funksjonene som ikke er nødvendige er gjort utilgjengelige for de vanlige brukerne, altså ansatte på skolene og skyssansvarlige i kommunene.

Standardpassord

Systemansvarlig sier at alle eksterne brukere på skolene og i kommunene logger på via ID-porten. Når det gjelder passord for interne brukere har fylkeskommunen ingen fast rutine for at disse skal skiftes, og brukere blir ikke tvunget til dette. Det er planlagt innføring av innlogging via ID-porten også for interne brukere høsten 2021, men dette er foreløpig ikke på plass (nov-21)[55].

---

[53] I denne sammenhengen betyr å «patche» å modifisere eller endre en del av den originale programvaren, typisk for å fikse en feil eller legge til ny funksjonalitet. Wikipedia.

[54] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at de har en Service Level Agreement (SLA) med leverandøren. Dette er en avtale som sier noe om avtalt nivå på ytelser, leverandørens ansvar for å opprettholde ytelsene, f.eks. tidsramme for respons og problemløsning. Revisjonen kjenner ikke innholdet i avtalen.

[55] Se note 51. Fylkeskommunen opplyser også i forbindelse med oversendt høringsutkast at passord-bruken for administratorer er strammet opp ila høsten 2021. Det er nå etablert rutine for regelmessig skifte av passord. Revisjonen har ikke sett denne.

Beskyttelse av data under oppbevaring
Fylkeskommunen informerer om at det kun er autorisert personell/administratorer som har utvidet tilgang i systemet. Øvrige brukere er kategorisert i fire grupper; interne brukere, kommune/skole, taxi og videregående elev.

Systemet har også en standardbruker, en bruker som følger med systemet og har alle rettigheter, og som kan brukes ved kriser. Denne kommer med et spesifikt passord/standardpassord. Systemansvarlig opplyser at hvis noen hacker seg inn på en standardbruker, vil vedkommende kunne gjøre store endringer i systemet. En må avveie om slike brukere skal deaktiveres opp mot nytten dersom det oppstår hendelser. Det er en svakhet at rollen standardbruker har for store tilganger i systemet. Dette er påpekt overfor leverandøren, men er foreløpig ikke endret.

Data er lagret i en SQL-database med SQL-autentisering. Det er ingen kryptering av data i databasen eller på disken. IKT Driftsenter, hvor serverne står, er sikret i bunker med låsekontroll på dør. Det er videre opplyst at det er installert antivirus-program (Checkpoint Endpoint Security) på alle serverne.

Bruker av systemets service-konto, som gjør alt mot databasen, har DBO-rettigheter. Ifølge systemansvarlig innebærer dette for store tilganger og er ikke i samsvar med beste praksis. Dette er påpekt overfor leverandør, men er foreløpig ikke endret.

Ifølge fylkeskommunen kom det på plass databehandleravtale med leverandøren høsten 2021, men revisjonen har ikke sett denne.

Beskyttelse av dataflyten i systemet (nettverk og overføring mellom enheter)
Ifølge systemansvarlig er all trafikk på utsiden (internett) kryptert.

Intern trafikk som er ukryptert gjelder all trafikk mellom applikasjonen og databasen. Dette er ifølge fylkeskommunen en ordinær kobling mellom applikasjon og SQL-database som anses som sikkert nok. Dette er trafikk mellom to servere i samme v-lan via intern brannmur. Det er kun autorisert IKT-personell som kan «se» den interne trafikken, sier systemansvarlig.

Beskyttelse av informasjonsverdier som er lagret på medier
Når det gjelder å beskytte informasjonsverdiene i systemet ved bruk så opplyser systemansvarlig at eksterne operatører (på skoler og i kommuner) gis tilgang til «sine» elever, og gis rettigheter gruppevis.

De ansatte på skolene og i kommunene logger inn i Skyssweb via ID-porten og har fått brukertilgang av fylket. ID-porten er ikke tatt i bruk på MinSkyss, men det jobbes med det. Transportørene (taxi) har også tilgang via ID-porten. Inne i systemet ser de bare opplysninger om de som de har blitt tildelt ansvar for å kjøre. For de som jobber i Innlandstrafikk er det ikke tofaktor-pålogging i systemet. De må logge på systemet med eget brukernavn og passord (ekstra innlogging etter man har logget på pc-en). De skal over til innlogging via ID-porten[56]. Skyssweb har tidsbegrensing, slik at en blir logget ut automatisk etter 30 minutter.

[56] Se note 51.

Interne brukere har samme tilgang som eksterne når det gjelder rettigheter i databasen, men det er forskjell når det gjelder funksjoner i systemet. De interne er saksbehandlere og har dermed tilgang til andre funksjoner og data.

Når det gjelder å beskytte informasjonsverdiene i systemet ved overføring (flytting, transport) sier systemansvarlig at det ikke er nødvendig med overføring av data som f.eks. USB minnepenner.

Når det gjelder arkivering og sletting sier systemansvarlig at disker som tas ut av servere blir avmagnetisert om det er roterende disker, mens SSD-disker foreløpig blir samlet opp på sikkert sted i påvente av anskaffelse av en løsning for å kverne opp disker, telefoner, iPader, etc.

Gjenopprettelse av data
Fylkeskommunen har opplyst følgende om back-up (sikkerhetskopi):

- Det blir tatt back-up av systemet hver natt.
- Det kjøres back-up av transaksjonslogger hver time på dagtid.
- All back-up kjøres til en sentral server på kveld.
- All back-up på dagtid speiles til en server nr. to.

Ved en eventuell krasj, gjenopprettes databasen fra kvelden før. Back-up regimet er ikke noe som er spesielt for Skyssweb, alle system som ligger på servere hos fylkeskommunen blir med i samme back-up. Back-up tas etter gjeldende rutiner for standard drift i IKT- seksjonen.

Fylkeskommunen har to back-up servere som er plassert i to forskjellige brannmursoner, utenfor IKT Driftssenter og i forskjellige sikrede rom. Back-up serverne er ikke medlemmer av domenet, men står selvstendig med forskjellige systemkontoer. Fylkeskommunen vurderer denne løsningen som sikker i forhold til påvirkning fra utsiden[57].

Test av sikkerhetskopi
Systemansvarlig sier at de ikke har testet sikkerhetskopien, og at de ikke har konkrete planer for å gjøre dette. De har noen få ganger hatt behov for å hente ut deler av sikkerhetskopi, hvilket har fungert godt. Å teste sikkerhetskopien fullt ut krever at de bruker applikasjonen mot de «gjenopprettede» dataene.

7.1.3 OPPDAGE

Hendelseslogg
Systemansvarlig opplyser at det er en hendelseslogg internt i systemet som registrerer en del operasjoner som operatørene utfører i systemet, som for eksempel på- og avlogging og hendelser i saksbehandlingen. Dette gjelder også administratorer. Loggen ligger i tabeller i databasen på linje med informasjon i basen/systemet for øvrig. Loggen går to måneder bakover, eldre data slettes automatisk.

[57] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at det settes opp en ny bacup-løsning i Innlandet fylkeskommune som skal ta høyde for sikring av data mot påvirkning utenifra. Arbeidet starter opp i desember 2021.

Interne brukere har tilgang til loggene for å kunne se «hva som har skjedd» når de opplever at det tilsynelatende er gjort noe med en søknad de ikke forstår, men de kan ikke endre denne informasjonen. Saksbehandlere kan naturligvis endre navn som er feil skrevet, endre adresse når elever har flyttet, godkjenne/avslå søknader osv., men dette blir logget. Fylkeskommunen gjennomgår hendelsesloggene, men ikke regelmessig.

Å endre data i loggen er mulig dersom man har tilgang til databasen og har dataverktøy for å gjøre dette. Det er kun administratorer som har denne muligheten. Denne tilgangen må man ha for å kunne «feilsøke» når brukerne opplever problemer i det daglige arbeid.

Sikkerhetsovervåking av systemet
Fylkeskommunen har ikke en egen sikkerhetsovervåking av systemet [58]. Når det gjelder den generelle infrastrukturen i fylkeskommunen logges all trafikk inn og ut fra brannmuren. Det er etablert overvåkning utover brannmur for aktiviteter i nettverket.

Det er i tillegg etablert sikkerhetsovervåkning fra AntiMalware på alle servere (Checkpoint Endpoint Security antivirus).

Penetrasjonstest
Systemansvarlig opplyser at det ikke er foretatt noen penetrasjonstest av systemet, og det er heller ikke planlagt noen slik test.

7.1.4 HÅNDTERE OG GJENOPPRETTE

Hendelseshåndtering
På spørsmål om det finnes en hendelseshåndteringsplan for systemet vises det til overordnet krisehåndteringsplan for IFK.

Hvis Skyssweb stopper opp kontakter Innlandstrafikk IKT-avdelingen. Hvis systemet går ned midt på dagen risikerer man å miste det man har utført i systemet den dagen. I backup-systemet finnes transaksjonslogger frem til krasj. Dette kan de skru av eller på i Skyssweb-databasen. Hvis noen av de eksterne brukerne i kommunene ikke kommer inn i systemet kontakter de systemansvarlig hos fylkeskommunen som formidler beskjed videre til IKT-avdelingen. Hvis IKT-avdelingen ikke finner feilen, kontakter de leverandøren.

Redundansmulighet
Skyssweb i seg selv har ingen redundans, ifølge systemansvarlig. Det er lagt opp til mye redundans i infrastrukturen hos fylkeskommunen. Bl.a. brannmurer, proxy-servere, kjernenettverk, servermaskinvare og lagring. Data i seg selv er ikke redundant utover back-up.

Systemet er ikke vurdert til å ha høy kritikalitet i forhold til nedetid, jf. risikovurderingen (kap. 7.1.1) der kritisk nedetid ble vurdert til mer enn ett døgn.

[58] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst at de er i ferd med å iverksette et driftsovervåkningverktøy som skal gjelde alle systemer i Innlandet plattformen.

7.2 REVISJONENS VURDERING

Kapitlet er organisert slik at for hvert tema starter vi med å presentere de aktuelle revisjonskriteriene, og deretter vurderer vi de innsamlede dataene i kapittel 7.1 opp mot kriteriene.

7.2.1 IDENTIFISERE OG KARTLEGGE

- **Fylkeskommunen 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.**
- **Fylkeskommunen bør oppdatere risikovurderingen i faste intervaller og ved betydelige endringer.**

Oppland fylkeskommune gjennomførte en risikovurdering av systemet i juni 2019, denne inkluderte ikke den tekniske driften av systemet. Det er ikke fastsatt dato for oppdatering av risikovurderingen, men det er planlagt en ROS-analyse i forbindelse med en større oppgradering av systemet høsten 2021. Denne er forsinket og revisjonen har ikke fått verifisert at det er gjennomført ny ROS-analyse. Revisjonen vurderer at fylkeskommunen bør planlegge oppdatering av risikovurderingen i faste intervall i tillegg til ved betydelige endringer.

Det ble satt opp forslag til fem risikoreduserende tiltak, hvorav fire fikk prioritet 1 og én fikk prioritet 2. Det er ikke satt opp en tidsplan for gjennomføring av tiltakene, eller hvem som er tiltakseier i risikovurderingsrapporten. Pr november 2021 er flere tiltak ikke gjennomført, blant annet å utarbeide databehandleravtaler med kommuner og transportører. Revisjonen vurderer at tiltakene i risikovurderingen ikke er gjennomført i henhold til en fastsatt plan.

Revisjonen mener at fylkeskommunen også bør gjennomføre en risikovurdering som inkluderer drift og vedlikehold av systemet. Dette er vesentlig for å kunne ivareta nødvendig teknisk sikkerhet.

7.2.2 BESKYTTE OG OPPRETTHOLDE

- **Fylkeskommunen skal ha gjennomført sikkerhetsopplæring av systemets brukere.**

Det er ikke gitt egen sikkerhetsopplæring i forbindelse med bruk av Skyssweb utover den generelle opplæringen som blir gitt i fylkeskommunen om behandling av personopplysninger. Dette er et tema som er jevnlig opp i ulike fora.

Revisjonen vurderer at det ikke er gjennomført systematisk sikkerhetsopplæring av systemets brukere.

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

IT-systemer er under kontinuerlig endring når løsninger først er satt i drift. Dette kan skyldes nye brukerbehov, endringer i trusselbildet, nyoppdagede sårbarheter, m.m. Det er derfor viktig å oppgradere og verifisere konfigurasjonen med jevne mellomrom.

Fylkeskommunen opplyser at systemet oppgraderes ca. én gang i året. I tillegg utfører IKT-avdelingen vedlikehold på server og annen infrastruktur én gang i måneden og ellers ved behov.

Det er behov for en større oppgradering av systemet som er planlagt gjennomført i 2021. Fylkeskommunen er i gang med denne prosessen i samarbeid med leverandøren og opplyser at sikkerhet er et av de områdene som blir ivaretatt på en bedre måte i den nye løsningen.

Revisjonen finner at det er vanskelig å vurdere om fylkeskommunen har etablert et regime for sikkerhetsoppdatering av systemet basert på den informasjonen som foreligger. Årlige oppgraderinger er svært sjeldent og medfører risiko for at kritiske sårbarheter forblir i systemet over tid. Revisjonen kjenner ikke til om det foreligger en avtale med leverandøren vedrørende sikkerhetshendelser og om hvorvidt leverandøren kan oppdatere og tette «hull» og sårbarheter underveis. Det er heller ikke kjent hvordan oppgraderinger og ny funksjonalitet implementeres, om IFK er involvert i testing og kvalitetssikring, eller om leverandøren har alt ansvar.

- **Fylkeskommunen bør ha gjennomgått IT-systemets funksjonaliteter og unødvendig funksjonalitet bør ha blitt slått av.**
- **Systemets standardpassord bør ha blitt byttet.**

Systemer som ikke er eksplisitt konfigurert har ofte sårbarheter som en angriper kan utnytte. Det er derfor viktig å «herde» systemene ved å ta bort funksjonalitet det ikke er tjenstlig behov for, samt fjerne standardinnstillinger.

Skysswb er delvis utviklet spesielt for fylkeskommunen (Oppland) og inneholder derfor lite unødvendig funksjonalitet. Funksjonalitet som ikke er nødvendig for eksterne brukere er gjort utilgjengelig. Når det gjelder standardpassord sier fylkeskommunen at alle eksterne brukere, med unntak av elever i videregående skole, bruker ID-porten i dag. Interne brukere har ikke brukt ID-porten fram til nå, men i henhold til nye opplysninger[59] er dette gjennomført i desember 2021. Det er også opplyst at passord-regimet for administratorer er strammet opp.

Revisjonen vurderer at Skyssweb er tilfredsstillende konfigurert i forhold til funksjonalitet.

Når det gjelder standardpassord mener revisjonen at det var forbundet risiko med passord-regimet til interne brukere slik dette ble gjennomført frem til desember 2021. Ny informasjon medfører at problemstilling knyttet til standardpassord ikke er relevant for interne og eksterne brukere. Revisjonen bemerker at rutine for skifte av passord for administratorer bør være skriftlig.

Standardbrukeren i systemet, en konto med alle rettigheter som kan benyttes i kriser, kommer med ett spesifikt passord/standardpassord. Det er ikke opplyst om dette passordet er byttet. Revisjonen mener at dette passordet bør byttes.

[59] Fylkeskommunen har gitt supplerende og ny informasjon i desember 2021 i forbindelse med oversendelse av høringsutkast.

- **Fylkeskommunen bør beskytte data i IT-systemet under oppbevaring i samsvar med gjennomført klassifisering av systemets informasjonsverdier.**

Fylkeskommunen har gjennomført en verdivurdering av informasjonsverdiene som behandles i Skyssweb i forbindelse med risikovurderingen som ble gjennomført i 2019. Denne viste at systemet behandler informasjonsverdier som har behov for høy beskyttelse.

Systemansvarlig har opplyst at data i databasen eller på disken ikke krypteres. Det er kun autorisert personell/administrator som har tilgang til alle data, og påloggingsprosedyrer for disse er strammet opp i høst. Det er likevel en svakhet at rollen standardbruker har for store tilganger og at det opereres med et standardpassord. Det er også opplyst at service-konto bruker har for store rettigheter.

Når det gjelder fysisk sikkerhet av server opplyser fylkeskommunen at serverne er sikret i en bunker med låsekontroll. Det er også installert antivirus-programmer på serverne.

Revisjonen vurderer at fylkeskommunen ikke i tilfredsstillende grad beskytter data i systemet under oppbevaring i samsvar med gjennomført verdivurdering. Det er sårbarheter knyttet til tilganger til ukrypterte data.

Det foreligger ingen risikoanalyse som grunnlag for de ulike tekniske sikkerhetstiltakene, for eksempel om hvorvidt kryptering av data er nødvendig. Det er også et spørsmål om hvordan den fysiske sikkerheten av serveren er ivaretatt. Hvis mange har direkte tilgang til serveren kan de hente ut ukrypterte data ved å koble seg opp mot databasen som ligger på serveren/disken.

- **Fylkeskommunen bør beskytte data i systemet under overføring (dataflyt) i samsvar med gjennomført klassifisering av systemets informasjonsverdier.**

Dataflyt betegner data som transporteres i et nettverk eller som overføres innenfor virksomheten og med eksterne parter.

Fylkeskommunen opplyser at all trafikk på utsiden (internett) er kryptert, men intern trafikk er ukryptert. Intern trafikk er ifølge fylkeskommunen en ordinær kobling mellom applikasjonen og databasen, som de anser som sikker nok. Det er vanskelig å vurdere om sikringen av dataflyten er tilfredsstillende. Det foreligger ingen risikovurdering eller dokumentasjon som viser at gjennomført sikring av internt nettverk er god nok. Hvordan adgangskontrollen til server-rommet gjennomføres vil også ha betydning for tilgangen til ukrypterte data.

- **Informasjonsverdier lagret på medier bør være tilstrekkelig sikret i samsvar med gjennomført informasjonsklassifisering, ved:**

  - **Bruk**
  - **Flytting/transport**
  - **Avhending/Arkivering**

Når det gjelder beskyttelse av data ved bruk av systemet opplyser fylkeskommunen at eksterne operatører kun har tilgang til «sine» elever og at transportører (drosjer) kun ser opplysninger om elever de skal frakte. Interne brukere har samme rettigheter som de eksterne når det gjelder rettigheter i databasen. Alle brukere med unntak av administrator-rollen, har pålogging via ID-porten (og videregående elever).

Det er viktig at bare de som skal ha tilgang er autorisert for tilgang. Revisjonen har ikke fått informasjon om hvordan tilgangsrettigheter håndteres når en ansatt slutter eller skifter rolle.

Sikring av data under flytting/transport er ikke så aktuelt da programmet er web-basert som vil si at pålogging kan skje fra alle enheter, og trafikken mellom brukers enhet og server er sikret ved kryptering.

Når det gjelder rutiner for avhending/arkivering kan ikke revisjonen vurdere om disse er bra nok, men påpeker at all sikring av data som er lagret bør basere seg på en risikovurdering.

Revisjonen vurderer at data som er lagret er tilstrekkelig sikret ved bruk.

- **Fylkeskommunen bør ha sikret muligheten til å gjenopprette systemets data.**
- **Det bør ha blitt gjennomført regelmessige tester for å verifisere at sikkerhetskopien fungerer.**

Dataangrep kan medføre at kritiske konfigurasjoner, kritisk programvare eller kritisk informasjon endres eller gjøres utilgjengelig, jf. hendelsen i Østre Toten kommune. Det er derfor et viktig sikkerhetstiltak å etablere en evne til å gjenopprette data og ha tilgjengelig sikkerhetskopier. Det er også viktig å teste sikkerhetskopier for å kontrollere at disse fungerer.

Fylkeskommunen har et back-up regime som gjelder alle system som ligger på lokale servere. Back-up tas etter gjeldene rutiner for standard drift. Back-upene kjøres til to separate back-up servere i to ulike sikrede rom utenfor IKT-driftssenter, men på huset.

Når det gjelder testing for å verifisere at sikkerhetskopien fungerer har de ikke rutiner for å gjøre dette regelmessig, men de har noen få ganger hentet ut deler av sikkerhetskopi som har vært vellykket.

Revisjonen vurderer at fylkeskommunen har etablert evne til å gjenopprette systemets data. Fylkeskommunens back-up løsning anses som god, men ville ha vært enda bedre hvis en tredje kopi ble lagret offline/utenfor huset. Med dagens løsning vil begge back-uper bli rammet dersom det skjer en hendelse i serverparken eller i bygget, jf. Østre Toten.

Fylkeskommunen har verifisert at sikkerhetskopien fungerer noen få ganger. Revisjonen mener at fylkeskommunen bør innarbeide rutiner for regelmessig gjenopprettingstest. Back-up regimet bør være basert på risikovurderinger. Dvs. at verdien av dataene avgjør regelmessighet på sikkerhetskopieringen, krav til sikring ved lagring og flytting (over nett), og krav til tilgangsrettigheter.

7.2.3 OPPDAGE

- **Fylkeskommunen bør ha opprettet en hendelseslogg for hvert system.**
- **Loggføring bør inneholde informasjon om systemadministrators og systemoperatørers aktiviteter.**
- **Systemets logger bør være tilstrekkelig sikret.**

Fylkeskommunen har opprettet en hendelseslogg internt i systemet som registrerer operatørers og administratorers operasjoner. Loggene blir gjennomgått, men ikke regelmessig. Administratorer har i prinsippet mulighet til å endre data i loggene. Loggen bevares i to måneder før den slettes.

Revisjonen finner at fylkeskommunen har opprettet en hendelseslogg for systemet som også gjelder systemadministratorer. Revisjonen vurderer imidlertid at fylkeskommunens sikring av loggene ikke er tilfredsstillende. I henhold til ISO 27001 skal logger beskyttes mot misbruk og uautorisert tilgang, og det bør derfor ikke foreligge mulighet til å endre loggene. Brukere med slike tilganger bør i så fall være sterkt kontrollert. Det er også en svakhet at loggene kun oppbevares i to måneder, da hendelser kan gå lenger tilbake enn to måneder. Logger bør ikke slettes, men arkiveres, slik at ikke relevante spor blir borte.

- **Det bør være etablert sikkerhetsovervåking av systemet.**

Å etablere en sikkerhetsovervåking av systemet er viktig for å oppdage sårbarheter eller forhold av sikkerhetstruende karakter. Mangelfull sikkerhetsovervåking kan innebære at angripere kan skjule tilstedeværelse, handlinger og aktiviteter i systemet.

Fylkeskommunen har ingen egen sikkerhetsovervåking av systemet, men det er etablert overvåking av aktiviteter i nettverket og antivirusprogram på alle servere.

Revisjonen vurderer at fylkeskommunen ikke har etablert en tilfredsstillende sikkerhetsovervåking av systemet. Det er kun gjennom sporadisk gjennomgang av logger at de har mulighet til å oppdage avvik/hendelser.

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

Fylkeskommunen bør teste egen forsvarsevne ved å gjennomføre inntrengningstest (penetrasjonstest) for å identifisere mangler og svakheter i systemet.

Fylkeskommunen opplyser at det ikke er foretatt penetrasjonstest av systemet, og heller ikke planlagt en slik test.

Revisjonen vurderer at det ikke er gjennomført penetrasjonstest av systemet. Revisjonen observerer at penetrasjonstest er et foreslått tiltak i risikovurderingen fra 2019 som ikke er gjennomført (prioritet 2). Revisjonen mener derfor at det burde foreligge en plan for gjennomføring av test.

7.2.4 HÅNDTERE OG GJENOPPRETTE

- **Fylkeskommunen bør ha utarbeidet en hendelseshåndteringsplan for systemet.**

En hendelseshåndteringsplan er en beredskapsplan som skal gjøre fylkeskommunen i stand til å håndtere sikkerhetshendelser knyttet til systemet og gjenopprette normaltilstand.

Fylkeskommunen viser til overordnet krisehåndteringsplan for Innlandet fylkeskommune, og ellers til noen uformelle rutiner ved brudd på tilgjengeligheten til systemet. Det foreligger ikke informasjon som sier noe om hvordan fylkeskommunen håndterer andre brudd enn tilgjengelighet, for eksempel løsepengevirus, og om det er formalisert roller og ansvar ved et brudd på datasikkerheten.

Det er heller ikke opplyst hvilket ansvar leverandøren har når det oppstår feil eller hendelser, hvilke plikter leverandør har til å svare og følge opp, eller om det er fastsatt rettetid. I henhold til risikovurderingen fra 2019 behandler systemet informasjon som krever høy beskyttelse av konfidensialitet. Dette tilsier at hendelser bør håndteres deretter.

Revisjonen vurderer at fylkeskommunen ikke har utarbeidet en hendelseshåndteringsplan for Skyssweb.

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

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

Systemet har ikke redundans i seg selv, men sikkerhetskopi av data vil beskytte mot informasjonstap. Dette forutsetter at sikkerhetskopien er intakt. Fylkeskommunen viser til at det er mye redundans i infrastrukturen.

Det er ikke opplyst om det er redundansmuligheter som gir tilgjengelighet dersom strømmen blir borte, men ifølge risikovurderingen fra 2019 er kritisk nedetid satt til mer enn ett døgn, slik at det kanskje er vurdert at det ikke er nødvendig med ytterligere tiltak mot strømstans.

Revisjonen mener at fylkeskommunen har vurdert redundansmuligheter som sikrer tilgjengelighetskrav.

8. KONKLUSJONER OG ANBEFALINGER

8.1 KONKLUSJONER

Revisor skal konkludere i forhold til problemstillingene. Dersom revisor finner vesentlige avvik, skal dette komme tydelig til uttrykk i forvaltningsrevisjonsrapporten.

Konklusjonene gis med bakgrunn i revisjonens vurderinger i kapittel 5, 6 og 7.

Problemstilling 1:

Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i Innlandet fylkeskommune?

Konklusjon:
Innlandet fylkeskommune har ikke etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet.

Innlandet fylkeskommune er en relativt ny organisasjon og det jobbes med å få på plass et fullverdig styringssystem for personvern og informasjonssikkerhet (internkontrollsystem for informasjonssikkerhet). Det er godkjent flere styrende dokumenter underveis i perioden revisjonsprosjektet har pågått. Revisjonen finner likevel at det er mangler ved styringssystemet ved revisjonsprosjektets slutt. En av utfordringene synes å være manglende kapasitet til å utvikle styringssystemet.

Begrunnelse:
Revisjonen har vurdert om fylkeskommunen har på plass en rekke sentrale krav til et styringssystem (internkontrollsystem) for informasjonssikkerhet.

Fylkeskommunen har etablert en intern organisering av arbeidet med informasjonssikkerhet. Det er definert og tildelt roller og ansvar. Revisjonen mener at rollene sikkerhets- og beredskapssjef og avdelingsleder har fått tildelt svært omfattende ansvarsområder, og at dette kan framstå som noe sårbart. Sikkerhets- og beredskapssjefen har en sentral rolle i å bygge opp styringssystemet, og samtidig det faglige ansvaret for fylkeskommunens sikkerhet på personvern- og informasjonssikkerhetsområdet. Dette arbeidet utføres i praksis av noen få personer, og revisjonen mener at kapasitetsproblemer er en utfordring for framdriften i fylkeskommunens arbeid med å utvikle styringssystemet for personvern og informasjonssikkerhet. I henhold til ISO 27001 skal ledelsen sikre at de nødvendige ressursene for internkontrollsystemet er tilgjengelig og at den interne organisasjonen er hensiktsmessig.

Et viktig element i styringssystemet er en policy eller en strategi for informasjonssikkerhet som skal vise ledelsens mål for arbeidet med informasjonssikkerhet og hvordan målene er tenkt oppnådd. En slik policy/strategi skal danne grunnlaget for virksomhetens internkontroll på informasjonssikkerhetsområdet. Fylkeskommunen har utarbeidet dokumentet *Styringsdokument for personvern og informasjonssikkerhet* som utgjør deres overordnede styringsdokument for arbeidet med personvern og informasjonssikkerhet.

Revisjonen vurderer at målene gitt i styringsdokumentet er lite spesifikke og ikke basert på fylkeskommunens risiko og behov på informasjonssikkerhetsområdet. Det gis ingen plan for hvordan det enkelte mål skal oppnås. Revisjonen mener også at styringsdokumentet i for stor grad har et personvernperspektiv.

Når det gjelder andre styrende rutinedokumenter som skal være en del av internkontrollsystemet finner revisjonen at fylkeskommunen ikke har på plass godkjente rutiner for kompetanse og opplæring, sikkerhet i leverandørforhold, samt kontinuitet og beredskap/hendelseshåndtering. Overordnet retningslinje for risikostyring, samt sikkerhetsinstruks og opplæringspakke for personvern og informasjonssikkerhet er under arbeid[60]. Revisjonen mener at risikostyring er grunnleggende i arbeidet med informasjonssikkerhet og at det er viktig at rutiner for metodikk og kriterier for risikoaksept kommer på plass.

Ifølge ISO 27001 skal virksomheten kontinuerlig evaluere og forbedre internkontrollsystemet for informasjonssikkerhet. Revisjonen mener at arbeidet med kontinuerlig evaluering og forbedring av fylkeskommunens styringssystem for personvern og informasjonssikkerhet ikke er systematisert i tilstrekkelig grad. Når det gjelder rapportering av status for informasjonssikkerhetsarbeidet til ledelsen er det ikke etablert en endelig modell for hvordan denne skal foregå[61].

Problemstilling 2:

I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?

Revisjonen har svart på denne problemstillingen gjennom å kontrollere informasjonssikkerheten i to utvalgte IKT-system.

Elements Cloud:

Konklusjon:
Innlandet fylkeskommune ivaretar i høy grad informasjonssikkerheten i sak- og arkivsystemet Elements Cloud.

Begrunnelse:
Elements behandler informasjonsverdier som krever høy beskyttelse av konfidensialitet og integritet. Dette betyr at informasjon på avveie kan medføre alvorlige konsekvenser. Elements er et skybasert system som innebærer en fordeling av sikkerhetsansvaret mellom fylkeskommunen og leverandøren. Revisjonen mener at fylkeskommunen i stor grad har sikret at informasjonen i systemet er beskyttet i samsvar med risikovurderingen av informasjonsverdiene.

Revisjonen vil peke på at det er noen sårbarheter knyttet til ivaretagelsen av informasjonssikkerheten. Det er ikke utarbeidet en hendelseshåndteringsplan, hverken for informasjonssikkerhetshendelser generelt, eller for Elements spesielt.

[60] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst (16.12.21) at dokumentet «*Overordnet sikkerhetskrav for risikostyring av personvern og informasjonssikkerhet*» ble godkjent den 16.11.21 og at fylkeskommunens risikostyringsmetodikk ble godkjent den 5.12.21. Revisjonen har ikke sett disse dokumentene.
[61] Fylkeskommunen har etter at rapporten ble sendt på høring opplyst (16.12.21) at modell for rapportering ble godkjent 19.11.21. Revisjonen har ikke sett denne modellen.

Det er viktig at organisasjonen har tenkt igjennom ulike scenarioer for hva som kan skje og er forberedt dersom en større hendelse skulle oppstå. Revisjonen mener også at det er en svakhet at det ikke er gjennomført en penetrasjonstest av systemet. Dette er viktig for å teste egen forsvarsevne og avdekke systemets sårbarheter.

Når det gjelder risikovurdering mener revisjonen at det bør utarbeides en rutine for revidering av risikovurderingen med faste mellomrom, og at tiltak iverksettes i henhold til en fastlagt plan som konkretiserer tiltakseier og tidsfrist.

Skyssweb:

Konklusjon:
Basert på den informasjonen som foreligger konkluderer revisjonen med at Innlandet fylkeskommune ikke i tilstrekkelig grad ivaretar informasjonssikkerheten i skoleskyss-systemet Skyssweb. Revisjonen finner flere mangler ved informasjonssikkerheten.

Begrunnelse:
Skyssweb behandler informasjonsverdier som krever høy beskyttelse av konfidensialitet. Systemet driftes av fylkeskommunen og informasjonssikkerheten ivaretas gjennom fylkeskommunens sikkerhetsrutiner. Revisjonen finner ikke at organisatoriske og tekniske tiltak er basert på risikovurderinger.

Når det gjelder organisatoriske tiltak finner revisjonen at det mangler rutine for tilgangsstyring. Det er sårbarheter knyttet til for høye tilgangsrettigheter. Fylkeskommunen sier at dette skal bli bedre når ny versjon av Skyssweb er implementert. Det er ikke kjent hvordan tilgang til brukere med utvidede rettigheter vil bli sikret etter oppgraderingen, eller når den nye versjonen blir implementert.

Når det gjelder tekniske tiltak påpeker revisjonen følgende:

- Rutine for sikkerhetsoppdateringer medfører risiko for at kritiske sårbarheter forblir i systemet over tid.
- Den tekniske sikringen av data under oppbevaring og i transitt (dataflyt) er vanskelig å vurdere basert på den informasjonen som foreligger. Data under oppbevaring og intern datatrafikk er ikke kryptert, men det foreligger ingen vurdering som sier at dette er i samsvar med risiko. Dersom den fysiske sikringen av serverne har sårbarheter, vil dette kunne medføre at inntrengere kan få tilgang til ukrypterte data.
- Det er etablert evne til å gjenopprette data. Det oppbevares to separate sikkerhetskopier, men det er ikke etablert offline back-up. Dersom det ikke foreligger sikkerhetskopier utenfor det interne nettverket, vil eventuelle inntrengere kunne kryptere/låse all back-up.
- Det er opprettet en hendelseslogg for systemet, men revisjonen stiller spørsmålstegn ved om loggene er tilstrekkelig sikret. Det er uheldig at det finnes muligheter til å endre logger og at loggene slettes etter relativt kort tid.
- Det er ikke etablert en tilfredsstillende sikkerhetsovervåking av systemet. Dette kan medføre risiko for at hendelser ikke oppdages i tide.
- Det er ikke utarbeidet en hendelseshåndteringsplan/beredskapsplan, hverken for systemet eller for informasjonssikkerhetsområdet generelt. Dette kan medføre at organisasjonen ikke er forberedt på hvilke hendelser som kan oppstå, og hvordan de kan håndteres.

8.2 ANBEFALINGER

Revisjonen har følgende anbefalinger:

Problemstilling 1:

- Fylkeskommunen bør sikre nødvendige ressurser til informasjonssikkerhetsarbeidet. Dagens arbeidsfordeling gir et omfattende ansvar til enkeltpersoner.
- Fylkeskommunen bør sikre at alle ansatte har fått nødvendig opplæring i informasjonssikkerhet som samsvarer med sine roller.
- Fylkeskommunen bør etablere en rutine for systematisk forbedringsarbeid på informasonssikkerhetsområdet.
- Fylkeskommunen bør utarbeide en beredskapsplan/hendelseshåndteringsplan for informasjonssikkerhetsområdet.
- Fylkeskommunen bør utarbeide en policy for informasjonssikkerhet i leverandørforhold.
- Fylkeskommunen bør redigere *Styringsdokument for personvern og informasjonssikkerhet* slik at det blir bedre balanse mellom personvern og informasjonssikkerhet.
- Fylkeskommunen bør redigere *Styringsdokument for personvern og informasjonssikkerhet* slik at fylkeskommunens overordnede mål for informasjonssikkerhet blir bedre tilpasset fylkeskommunens risiko og behov på informasjonssikkerhetsområdet. Det bør videre beskrives en plan/strategi for hvordan målene skal oppnås.

Problemstilling 2:

- Fylkeskommunen bør utarbeide en rutine for å gjennomføre og revidere risikovurderinger av informasjonssystemene i faste intervaller.
- Risikovurderinger av systemer som driftes lokalt bør også inkludere teknisk drift og vedlikehold.
- Fylkeskommunen bør utarbeide en rutine for iverksetting av risikoreduserende tiltak knyttet til risikovurderinger, slik at ansvaret for iverksetting er tildelt og gitt en frist.
- Fylkeskommunen bør sikre en tilfredsstillende sikkerhetsopplæring av brukere av informasjonssystemer.
- Fylkeskommunen bør gjennomføre penetrasjonstester for å teste egen forsvarsevne.
- Fylkeskommunen bør gjennomgå interne rutiner for sikring av IKT-systemer som driftes lokalt. Hvert system skal ha en tilpasset sikring som står i forhold til verdien av informasjonen som behandles. Viktige element i sikringen er:
    - Regelmessige sikkerhetsoppdateringer
    - Rutiner for tilgangsstyring og passord-policy
    - Standardpassord for standardbruker bør byttes
    - Tilstrekkelig sikring av data under oppbevaring og i transitt (dataflyt)
    - Tilstrekkelig sikring av back-up
    - Tilstrekkelig sikring av logger
    - Rutine for sikkerhetsovervåking
    - Tilstrekkelig fysisk sikring av serverpark

9. REFERANSER

Lover og forskrifter:
Lov om kommuner og fylkeskommuner (kommuneloven), LOV-2018-06-22-83.
Lov om behandling av personopplysninger (personopplysningsloven), LOV-2018-12-20-116.
Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), FOR-2004-06-25-988.

Andre dokumenter:
Kommunal- og moderniseringsdepartementet, veileder til eForvaltningsforskriften, 24.6.2015.
NOU 2018:14, IKT-sikkerhet i alle ledd.
Meld St. 38 (2016-2017) IKT-sikkerhet. Et felles ansvar.
ISO/IEC 27001:2017
NSM; Grunnprinsipper for IKT-sikkerhet versjon 2.0, sist oppdatert 15.4.2020.
Digdir.no: Veiledningsmateriell om informasjonssikkerhet.
Datatilsynet.no; Varsel om vedtak om overtredelsesgebyr og pålegg. Østre Toten kommune (18.10.2021).
SSB: Artikler og statistikk fra serien: «Bruk av IKT i offentlig sektor».
KPMG (26.8.2021); IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021.
PST.no; Nasjonal trusselvurdering 2021 (8.2.2021).
KS.no; Oppfordring til kommuner om å være oppmerksom på unormal aktivitet (11.1.2021).

Dokumenter fra Innlandet fylkeskommune:
Styringssystem for informasjonssikkerhet:
Styringsdokument for personvern og informasjonssikkerhet, godkjent 7.4.2021.
Roller og ansvar for informasjonssikkerhet og personvern, godkjent 1.3.2021.
Overordnende sikkerhetskrav for informasjonsklassifisering, godkjent 7.4.2021.
Rutine for følsomhet, klassifisering i Office 365, udatert.
Arkitekturprinsipper for Innlandet fylkeskommune, august 2020.
Sikkerhetskrav i anskaffelsen, ikke ferdig utarbeidet.
Overordnede sikkerhetskrav i risikostyring, ikke ferdig utarbeidet.
Overordnet krisehåndteringsplan for Innlandet fylkeskommune, 10.1.2021.
Rammer for bruk av kvalitetssystemets avviksmodul, 7.1.2021.
Registrering, behandling og rapportering av avvik, 7.1.2021.
Prosedyre for avvik personvern og informasjonssikkerhet, godkjent 20.8.2021.

Elements:
Oppsummering av risikovurdering Elements Cloud. Rapport, 03.12.2019.
Risikovurdering av Elements – underlagsmateriale, Evry 1.11.2019.
Risiko analyse og datahåndtering. Migrering av Elements Cloud til ny skyplattform, Sikri 22.1.2021
Risk Report for Elements, Evry 28.8.2018.
Oppfølging av tiltak etter gjennomført risikovurdering, sist oppdatert 3.5.2021.
Avtale om løpende tjenestekjøp over internett SSA-L, med bilag. Ny sak- /arkivløsning til IFK, 5.4.2019
Standard tjenestenivå Elements Cloud SSA-L, 5.4.2019.
Databehandleravtale Elements Cloud, 2.1.2020.
Rutine tilgangsstyring i Elements, 7.5.2021.

Nødprosedyre ved utilgjengelig Elements, 5.5.2021.

Skyssweb:
Risikovurdering av Skyssweb, ferdigstilt den 28.6.2019.

VEDLEGG 1: REVISJONSKRITERIER MED KILDEHENSVISNINGER

Problemstilling 1:
Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i fylkeskommunen?

«A» refererer til Annex i ISO/IEC 27001

Kriterium	Kilde
Har det blitt etablert en rutine for gjennomgang av styrende dokumenter i faste intervaller?	ISO27001, A.5.1.2
Har fylkeskommunen etablert en policy for informasjonssikkerhet som inneholder mål og strategi for å nå målene?	ISO 27001, 5.1, 5.2, 6.2 A.5.1.1
Har virksomheten etablert en hensiktsmessig intern organisering for informasjonssikkerheten?	ISO27001, 5.3, 7.2 A.6.1.1-5
Har virksomheten etablert en prosedyre for risikostyring?	ISO27001, 6.1
Har virksomheten etablert en retningslinje for å klassifisere informasjon i henhold til lovverk og krav til konfidensialitet, integritet og tilgjengelighet?	ISO27001, A.5.1.1, A.8.2.1
Har virksomheten etablert en prosedyre for sikkerhetsmerking av informasjon?	ISO27001 A.8.2.2
Har virksomheten etablert en retningslinje for behandling av personopplysninger?	GDPR artikkel 5 og 24. ISO27001 A.18.1.4
Har virksomheten etablert en retningslinje for leverandørforhold?	ISO27001, A.15.1.1
Har virksomheten etablert en retningslinje/prosedyre for effektiv hendelseshåndtering?	ISO27001, A.16, A.17
Har virksomheten etablert en retningslinje for avvikshåndtering og korrigerende tiltak?	ISO27001 10.1 og 10.2

Problemstilling 2:
I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?

Tema	Kriterium	Kilde
Identifisere og oppdage	Har det blitt gjennomført risikovurdering av systemet?	ISO 27001, 6.1.2, 8.2
Identifisere og oppdage	Har tiltakene blitt gjennomført i henhold til fastsatt plan?	ISO27001, 6.1.3
Beskytte og opprettholde	Har virksomheten gjennomført sikkerhetsopplæring av systemets brukere?	ISO 27001 A.7.2.2, A.12.2.1
Beskytte og opprettholde	Har virksomheten etablert et regime for sikkerhetsoppdatering av systemet?	ISO 27001 A.12.6.1
Beskytte og opprettholde	Hvordan beskyttes data i IT- systemet under oppbevaring?	ISO 27001 A.8.2.3, A.14.1
Beskytte og opprettholde	Hvordan beskyttes dataflyten i IT-systemet? (styring av nettverkssikkerhet og informasjonsoverføring)	ISO 27001 A.8.2.3, A.13.1.1-3, A.13.2.3, A.14.1
Beskytte og opprettholde	Hvordan beskyttes informasjonsverdiene lagret på medier ved - Bruk - Flytting/transport - Avhending/Arkivering	ISO 27001 A.8.2.3, A.8.3. A.11.2.5-7.
Beskytte og opprettholde	Har systemets funksjonaliteter blitt gjennomgått og har unødvendig funksjonalitet blitt slått av?	ISO 27001 A.14.1.1 Se også NSM grunnprinsipp 2.3.
Beskytte og opprettholde	Har alle systemets standardpassord blitt byttet?	ISO 27001 A.14.1.1 NSM grunnprinsipp 2.3.

Beskytte og opprettholde	Har det blitt opprettet en evne til å gjenopprette systemets data?	ISO 27001 A.12.3.
Beskytte og opprettholde	Blir det gjennomført regelmessige tester for å verifisere at sikkerhetskopien fungerer?	ISO 27001 A.12.3.
Oppdage	Har systemet en hendelseslogg?	ISO 27001 A.12.4.1
Oppdage	Har systemet en loggføring av administrators og operatørers aktiviteter?	ISO 27001 A.12.4.3
Oppdage	Hvordan beskyttes systemets logger?	ISO 27001 A.12.4.2
Oppdage	Hvordan blir systemet sikkerhetsovervåket? (eventuelt enklere: Har det blitt etablert sikkerhetsovervåking av systemet)	ISO 27001 A.13.1.1 Se også NSM grunnprinsipp 3.2.
Oppdage	Har det blitt gjennomført penetrasjonstest av systemet?	ISO 27001 A.18.2.3 NSM grunnprinsipp 3.4.
Håndtere og gjenopprette	Har det blitt utarbeidet en hendelseshåndteringsplan for systemet?	ISO 27001 A.16.1.1, A.16.1.5, A.17.1.1-2
Håndtere og gjenopprette	Har systemet redundansmuligheter som sikrer tilgjengelighetskrav?	ISO 27001 A.17.2.1

VEDLEGG 2: FYLKESKOMMUNEDIREKTØRENS UTTALELSE

Innlandet fylkeskommune

Innlandet Revisjon IKS
Postboks 153

2626 LILLEHAMMER

Offl. § 5 1. ledd

Deres ref:	Vår ref:	Dato:
2022-083/IS	2021/11853-8 Daiva Skoglund	24.02.2022

Fylkeskommunedirektørens uttalelse til forvaltningsrevisjonsrapport nr. 17-2021 - Informasjonssikkerhet i IKT-systemer

Fylkeskommunedirektøren er i oversendelsesbrev av 16.1.2022 bedt om en uttalelse i forbindelse med rapportutkast etter forvaltningsrevisjon «Informasjonssikkerhet i IKT-systemer».

Fylkeskommunedirektøren tar forvaltningsrevisjonens konklusjoner og anbefalinger på alvor og skal sørge for at dette blir fulgt opp i fylkeskommunen. Uttalelsen sorteres med utgangspunkt i spørsmålene fra oversendelsesbrevet.

Fylkeskommunedirektøren har følgende tilbakemeldinger når det gjelder selve gjennomføringen av forvaltningsrevisjonen:

1. **Har informasjonen om prosjektets formål og gjennomføring vært god nok?**

   Informasjonen om formål og plan for gjennomføring av forvaltningsrevisjonsprosjektet oppleves som god.

   Fylkeskommunedirektøren har følgende bemerkninger til dette punktet:

   - Gjennomføring av forvaltningsrevisjonen har tatt lang tid. En rekke forhold knyttet til informasjonssikkerhetsarbeid i fylkeskommunen og systemene har endret seg underveis, da organisasjonen er under kontinuerlig utvikling og forbedring.
   - Vurderingene går i noen grad ut over det som er fokusområdet i revisjonen, der enkelte konklusjoner kan diskuteres basert på ståsted, og ikke utfra objektive kriterier. Det favnes for vidt når vurderingen for et enkelt system (Skyssweb) blir til en total vurdering av plattform.

2. **Har dere kommentarer til prosjektets metode, anvendte kilder eller beskrivelse av fakta?**

   Valg av metode og anvendte kilder vurderes som hensiktsmessig sett opp mot prosjektets formål. Når det gjelder beskrivelse av fakta, er det gitt anledning til å kvalitetssikre dette i prosessen. Fylkeskommunedirektøren opplever det som utelukkende positivt at revisjonen har knyttet til seg ekstern ekspertise for å kvalitetssikre revisjonskriterier, metode og vurderinger.

   Fylkeskommunedirektøren har følgende bemerkninger:

   - Det er nødvendig å knytte til seg riktig teknisk kompetanse internt i fylkeskommunen, når man gjør tekniske vurderinger med gjennomgang av spørsmål mot faktagrunnlag.
   - Det ville vært en fordel å ha noen flere felles arbeidsmøter for å avstemme spørsmål/svar med fagpersoner i prosessen. Dette ville sikre at det til enhver tid er tilknyttet riktig kompetanse på de ulike områder som behandles.
   - Det savnes en betraktning fra revisjonen om fylkeskommunens ståsted som en ny organisasjon og behovet for organisasjonsbygging der mye skal på plass samtidig.

3. **Har dere kommentarer til revisjonskriteriene som ligger til grunn for våre vurderinger og konklusjoner?**

   Fylkeskommunedirektøren mener at gjennomgang av revisjonskriteriene burde vært bedre avstemt internt i fylkeskommunen og i samarbeid med revisjonen før revisjonskriteriene ble endelig bestemt.

   Revisjonen benytter seg av flere kilder for å utlede revisjonskriteriene. En av kildene er personopplysningsloven (bl.a. artikler 5, 24 og 32), og rapporten omtaler forhold knyttet til personvern. Internkontrollsystemet og informasjonssikkerhet er viktige fundamenter for å ivareta personvernet og personopplysningssikkerheten.

   Det er imidlertid ikke spesifisert hvilke revisjonskriterier som er hentet fra disse kildene, men mange av revisjonskriteriene kan knyttes direkte eller indirekte til krav i personopplysningsloven. Personopplysningsloven inneholder en rekke krav utover de nevnte artiklene, som ikke inngår i revisjonen. Selv om kilder og kriterier fra personopplysningsloven benyttes, så har vi ikke oppfattet at dette er en revisjon av personvernet.

4. **I hvilken grad oppfattes rapporten som nyttig?**

   Fylkeskommunedirektøren opplever rapporten som nyttig i det videre arbeidet med informasjonssikkerhet i fylkeskommunen.

5. **Har dere kommentarer til rapportens oppbygning og språk?**

   Rapportens oppbygning og språk er generelt bra, men fylkeskommunedirektøren kunne ønsket at særlig anbefalingene, men også revisjonskriteriene, var nummerert i stedet for opplistet med kulepunkter. Dette for å sikre korrekte henvisninger ved bl.a. tiltaksoppfølging.

6. **Hva er fylkeskommunedirektørens samlede vurdering av revisjonsrapportens vurderinger, konklusjoner og anbefalinger?**

   Fylkeskommunedirektørens samlede vurdering er at revisjonsrapporten gir et representativt situasjonsbilde av problemstillingene på revisjonstidspunktet. Det er grunn til å bemerke at flere deler av styringssystemet for informasjonssikkerhet og personvern, eller internkontrollsystemet, er implementert etter at revisjonen satte punktum for sitt arbeid. Derfor er dagens situasjon noe annerledes enn det bildet rapporten tegner.

Fylkeskommunedirektørens konkrete tilbakemeldinger i forhold til forvaltningsrevisjonens problemstilling 1 og 2 gis nedenfor.

Problemstilling 1: Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i Innlandet fylkeskommune?

Konklusjon: Innlandet fylkeskommune har ikke etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet.

Fylkeskommunedirektørens kommentar:

Selv om fylkeskommunen er en relativt ny organisasjon er det utarbeidet en rekke styrende og gjennomførende dokumenter som inngår i internkontrollsystemet og som revisjonen selv påpeker at *"Det er godkjent flere styrende dokumenter underveis i perioden revisjonsprosjektet har pågått."*

Det tar tid å utvikle og implementere et internkontrollsystem for informasjonssikkerhet i en ny organisasjon. Fylkeskommunen har en tydelig plan for dette arbeidet, og underveis i revisjonsperioden har vi kommet nærmere målet gjennom at stadig nye tiltak har blitt implementert.

Problemstilling 2: I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?

Elements Cloud:

Konklusjon: Innlandet fylkeskommune ivaretar i høy grad informasjonssikkerheten i sak- og arkivsystemet Elements Cloud.

Skyssweb:

Konklusjon: Basert på den informasjonen som foreligger konkluderer revisjonen med at Innlandet fylkeskommune ikke i tilstrekkelig grad ivaretar informasjonssikkerheten i skoleskyss-systemet Skyssweb. Revisjonen finner flere mangler ved informasjonssikkerheten.

Fylkeskommunedirektørens kommentar:

Fylkeskommunedirektøren vil sørge for en nøye vurdering og nødvendige oppfølgingstiltak basert på de anbefalinger som er påpekt i rapporten.

Fylkesdirektørens konkrete tilbakemeldinger på de enkelte av forvaltningsrevisjonens anbefalinger:

Problemstilling 1:

Fylkeskommunedirektøren kan informere om iverksetting av følgende tiltak:

- Fagområdet styrkes med en fagressurs knyttet til arbeid med informasjonssikkerhet.
- Det er etablert årshjul for informasjonssikkerhet med konkrete aktiviteter som skal sørge for en enklere og mer systematisk oppfølging.
- Rollen som fagansvarlig for informasjonssikkerhet og personvern, med hovedfokus på implementering av styringssystem og internkontroll, er tydeliggjort.

Problemstilling 2:

Fylkeskommunedirektøren kan informere om at iverksetting av tiltak er påbegynt for følgende anbefalinger:

- Revidere risikovurdering for Skyssweb og utarbeide en ny tiltaksplan
- Etablere rutiner for tilgangsstyring og passord-policy i Skyssweb

Fylkeskommunedirektøren vil sørge for at følgende oppfølgingstiltak for de øvrige anbefalingene legges inn i planene for informasjonssikkerhetsarbeidet i 2022:

- Utarbeide hendelseshåndteringsplan for systemer i fylkeskommunen, inkludert Elements Cloud og Skyssweb
- Revidere risikovurdering for Elements Cloud og utarbeide en ny tiltaksplan
- Gjennomføre planlagt penetrasjonstest for Elements Cloud og Skyssweb

Fylkeskommunedirektørens vurdering av hvordan den endelige rapporten skal presenteres i forhold til offentlighet

Fylkeskommunedirektøren vurderer at det ikke er grunnlag for at hele eller deler av rapporten skal unntas offentlighet.

Med vennlig hilsen

Tron Bamrud
Fylkeskommunedirektør

Dette dokumentet er elektronisk godkjent og sendes uten signatur.