Revisjon Øst IKS

FORVALTNINGSREVISJONSRAPPORT

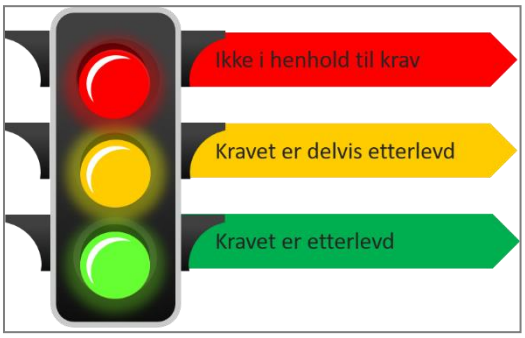
Informasjonssikkerhet i Nord-Odal kommune: Integritet, konfidensialitet og tilgjengelighet

NORD-ODAL KOMMUNE 2022

Postboks 84, 2341 Løten
Telefon: 62 43 58 00
https://www.revisjon-ost.no
E-post: post@rev-ost.no
Org. nr.: 974 644 576 MVA

Forord – om rapporten

Denne rapporten er bygget opp pedagogisk med et kort sammendrag som går gjennom hovedfunnene og konklusjonen i forvaltningsrevisjonsprosjektet i første kapittel.



Vi har valgt å benytte en «trafikklysmodell» for å illustrere hva vi mener er i henhold til krav på området, det som er godkjent med merknad, og det som ikke er i henhold til krav på området. Hver vurdering blir merket med henholdsvis grønt, gul/oransje og rødt.

Vi gjør oppmerksom på at vurderinger med gul/oransje og rødt vil følge av beskrivelser av de mangler og/eller forbedringsmomenter vi mener at tjenesten har. For leseren vil det derfor være nyttig å lese gjennom vurderingene som fremgår av underkapitlene for hver problemstilling, i tillegg til den informasjonen leseren får i sammendraget.

Rapporten er for øvrig utarbeidet med et digitalt tilsnitt og innehar lenker til ulike seksjoner av rapporten. Dette skal gjøre det enklere for leseren å navigere i rapportens innhold. Det er også lenket til de kilder som er digitalt tilgjengelige, for en mer interaktiv opplevelse av rapporten.

Rapporten er bygget opp etter NKRFs krav til sluttrapport i Standard for forvaltningsrevisjon (RSK 001). Dette innebærer minstekravene til

- sammendrag (kap. 1),
- informasjon om bestillingen (kap. 2),
- problemstillingene (kap. 7-9),
- valg av metoder og vurdering av datagrunnlag (kap. 5),
- Analyse av spørreundersøkelsen (kap. 6)
- presentasjon av data (kap. 7-9),
- vurderinger (kap. 7-9),
- konklusjon (kap. 10),
- anbefalinger (kap. 11),
- referanser (kap. 13) og
- kommunedirektørens uttalelse (kap. 12).

I tråd med RSK 001, ønsker vi å fremheve at vi vektlegger at forvaltningsrevisjoner skal «bidra til et godt beslutningsgrunnlag for de folkevalgtes styring og kontroll, og å bidra til læring».

Vi vil takke kontrollutvalget for oppgaven, og administrasjonen for tilrettelegging for en best mulig og effektiv gjennomføring av forvaltningsrevisjonsprosjektet.

Vi håper at leseren finner nytte i rapporten og vil benytte denne videre i forbindelse med en trygg og god forvaltning av tjenesteområdet.

Kongsvinger, den 10. november 2022

Magnus Michaelsen
Oppdragsansvarlig forvaltningsrevisor

Lone Grobøl
Utøvende forvaltningsrevisor

Innholdsfortegnelse

Bilde på forsiden: Helge Eek

Sammendrag

Revisjon Øst IKS har gjennomført en forvaltningsrevisjon for å vurdere om kommunen har etablert planer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte og om kommunen har implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon. Vi har også belyst om kommunalt ansatte har kjennskap til, og praktiserer informasjonssikkerhet på en trygg måte. Med andre ord; at kommunens ansatte praktiserer en god sikkerhetskultur.

Ethvert system er sjelden sterkere enn sitt svakeste ledd. Vi mener derfor at det er viktig at kommunen har gode rutiner og systemer for å håndtere informasjon.

Prosjektet er gjennomført i perioden november 2021 til september 2022. Datainnsamling i prosjektet har foregått fra desember 2021 til september 2022.

Prosjektet har søkt å besvare 3 problemstillinger:

1. Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens IKT-sikkerhet på en tilfredsstillende måte?
2. Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?
3. I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

For å besvare disse problemstillingene har vi gjennomført en spørreundersøkelse rettet mot kommunens ansatte. Vi har også sett nærmere på to av de største systemene som Nord-Odal kommune har:

- Visma Profil som er kommunens elektroniske pasientjournal, samt
- Websak som er kommunens arkiv- og saksbehandlersystem.

Dette er systemer som inneholder mange personopplysninger.

Vi har intervjuet nøkkelpersoner med overordnet ansvar for informasjonssikkerhet, samt systemadministratorer tilknyttet systemene som vi har sett nærmere på. Det er til sammen gjennomført et oppstartsmøte, fire intervjuer, løpende dialog og møter med vår kontaktperson i prosjektet.

Undersøkelsene har utover dette hatt fokus på å undersøke kommunens kvalitetssystem og dokumentasjon knyttet til rammeverket som skal ivareta informasjonssikkerheten i praksis. Vi har hentet inn dokumentasjon relatert til informasjonssikkerhet, hvor de eldste dokumentene er datert tilbake til 2013, mens de nyeste er datert i august 2022.

Den tekniske delen og i mange tilfeller det fysiske «forsvaret» av datasikkerhet/informasjonssikkerhet er det Hedmark IKT (HIKT) som ivaretar. De er ikke omfattet av kontrollen, men det vil gjennom rapporten fremkomme hvordan samarbeidet med HIKT fungerer i praksis med Nord-Odal kommune.

Vi har funnet at Nord-Odal kommune har sikkerhetsmål og sikkerhetsstrategier, et avvikssystem, et personvernombud, rutiner for årlig sikkerhetsrevisjon i ledelsen og et godt samarbeid med HIKT som en kvalitetsinstans for informasjonssikkerhet.

Vi har inntrykk av at Nord-Odal kommune fra sentralt hold jobber bevisst for å ha et godt system for informasjonssikkerhet. Det har spesielt i 2022 tilkommet mange rutiner i kvalitetssystemet som tilfredsstiller sentrale lovkrav og anbefalinger for informasjonssikkerhet, og vi finner at ledelsen utviser bevissthet i informasjonssikkerhetsarbeidet. Det gjenstår fremdeles noe systematisk kartleggingsarbeid før kommunen har en helhetlig oversikt over informasjonssikkerhet og praksis i hele

organisasjonen. En slik oversikt vil kunne hjelpe med å skape og implementere en gjennomgående sikkerhetskultur og risikostyring i hele kommunen.

Vi mener at Nord-Odal kommune har et forbedringspotensial knyttet til:

- Gjennomføring av ROS og DPIA-analyser
- Rutiner for tilgangsstyring
- Oversikt over databehandleravtaler
- Opplæringsrutiner og tiltak
- Klassifisering av informasjonsverdier og en plan for informasjonshåndtering
- Utforming av en tiltaksplan for sikkerhetsrevisjoner
- Avvik og avviksrapportering
- Manglende oversikt om hvorvidt det er nødrutiner i alle enheter

Basert på våre funn, anbefaler vi at Nord-Odal kommune:

- klassifiserer informasjonsverdier og utarbeider en plan for informasjonshåndtering.
- utarbeider en plan for sikkerhetsrevisjoner.
- skaffer seg en helhetlig oversikt over avdelingenes nødrutiner.
- vurderer om informasjonssikkerhet bør inn i kommunens beredskapsplan og eventuelt gjennomføring av øvelser i forbindelse med mulige hendelser.
- reviderer alle rutiner og prosedyrer i Compilo i henhold til angitt revisjonsfrist. Rutiner som er lenket opp i dokumentene og ikke ligger i Compilo, bør legges inn i kvalitetssystemet.
- etablerer en kvalitetssikringsrutine i tilknytning til tilgangsstyring i systemer.
- foretar en gjennomgang av eksisterende databehandleravtaler og sørger for å sikre at systemer som eventuelt mangler databehandleravtaler får dette på plass. Databehandleravtaler bør vurderes å være en del av rutinen i «ledelsens gjennomgang.
- iverksetter tiltak som sikrer implementering og kjennskap til rutiner for informasjonssikkerhet, avvik og avviksrapportering innen informasjonssikkerhet og personvern.
- etablerer rutiner for å sikre at ansatte får en overordnet opplæring om informasjonssikkerhet ved oppstart, og at de til enhver tid har den nødvendige kompetansen til å praktisere god informasjonssikkerhetskultur. Det kan være behov for å kartlegge hva ansatte kan og ikke kan i forhold til informasjonssikkerhet.

1 Bakgrunn for prosjektet

I henhold til kommuneloven § 23-2, punkt c, skal kontrollutvalget påse at det blir gjennomført forvaltningsrevisjon i kommunen. Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak (§ 23-3, første ledd).

I møte 12. februar 2021, sak 9/21, bestilte kontrollutvalget i Nord-Odal kommune en prosjektplan med utgangspunkt i *administrasjon og styring IKT-sikkerhet*. Vedtaket var som følger (utdrag):

1. *Kontrollutvalget viser til vedtatt plan for forvaltningsrevisjon for Nord-Odal kommune for 2021-2024 og bestiller en prosjektplan med utgangspunkt i Administrasjon og styring IKT-sikkerhet*
2. *Prosjektplanen legges frem i møtet i mai*

I møtebehandlingen viser kontrollutvalget til at interimrapportene de siste årene gir en pekepinn på at det er behov for revisjon innen kommunens administrasjon, styring og internkontroll. I tillegg viser kontrollutvalget til at IKT-sikkerhet er et svært viktig område. Utvalget var enig i at det vil være aktuelt med fokus både på IKT-sikkerhet i egen kommune, men også hvordan samarbeidet med HIKT fungerer. Kontrollutvalget mente at problemstillingene er greit formulert i plan for forvaltningsrevisjon. Utvalget mener videre det er viktig å se hen til hva som gikk galt i Østre Toten, der de ansatte i lang tid har vært uten tilgang til sine systemer (hacking-angrep), og at denne type problematikk inkluderes i prosjektet.

Jamfør plan for forvaltningsrevisjon i Nord-Odal kommune for 2021-2021 ble det vedtatt oppstart av et forvaltningsrevisjonsprosjekt knyttet til Administrasjon og styring - IKT-sikkerhet. Vedtaket ble gjort i kontrollutvalgets møte den 20. mai i sak 29/21. Prosjektet har følgende 3 problemstillinger:

1. Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens IKT-sikkerhet på en tilfredsstillende måte?
2. Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?
3. I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

2 Formål og aktualitet

Når man sikrer et bygg for innbrudd innebærer dette ulike former for tiltak, noen ganger er det nok med en dørlås eller å sette opp et gjerde, mens andre ganger kreves det alarm, vakthund eller vektere. Det kan bety at ulike mennesker skal ha tilgang til ulike deler av et bygg og det kan kreve ulike tilpasninger og vedlikehold av disse tilgangene. I prinsippet er dette veldig sammenliknbart med hvordan informasjonssikkerhet skal fungere i praksis. Det må tilpasses sikkerhetsbehovet til den unike organisasjon, og krever kunnskap som er tilpasset den unike bruker slik at det overholdes på riktig vis:

> «Datasikkerhet (informasjonssikkerhet) er noe vi har eller ikke har, noe som er påskrudd eller avskrudd. Det er ikke noe vi kan tenke på en gang i uken eller få hjelp av en nabo til å oppnå. Datasikkerhet er din egen bevissthet om hva hackere og svindlere kan gjøre, samt hvordan du kan hindre at det skjer. Datasikkerhet er også en bevissthet om hvordan du kan minimere skadene. Datasikkerhet er både kunnskap og en måte å tenke på.» [1]

Den digitale trusselen mot norske organisasjoner, både private og offentlige, har vært økende de siste årene. Direktoratet for sikkerhet og beredskap har angitt at trusselbildet er svært høyt. Dette har det også vært flere eksempler på de siste årene, blant de mest omfattende er for eksempel løsepengeangrepet rettet mot Østre Toten kommune. Russlands krigføring i Ukraina, og nasjonalpolitisk støtte og interesser, har ført til at norske offentlige organer kan bli mål i «krigen» på internett. Kommunal og distrikts-departementet og Kommunenes sentralforbund (KS) har sendt et

[1] Tom Heine Natt og Christian F. Heide *«Datasikkerhet, ikke bli svindlerens neste offer»,* side 17

felles brev til kommunene i mars 2022, som har satt teknologisk sikkerhet i kommune-Norge enda tydeligere på agendaen. [2]

En virksomhet skal identifisere og kartlegge, beskytte og opprettholde og aktivt oppdage eventuelle trusler for IKT-sikkerhet i en kommune eller virksomhet, og de skal håndtere og evaluere dette systematisk i hverdagen. De skal også ha en plan for hvordan de skal håndtere eventuelle hendelser, og ha en plan for å gjenopprette systemer ved hendelser som bryter ned systemene.[3] Når det gjelder kommunenes digitale løsninger, så er det avgjørende å sikre informasjon, slik at den ikke kommer på avveie.

Ut fra kontrollutvalgets bestilling og gjeldende risiko- og vesentlighetsvurderinger, er formålet for denne forvaltningsrevisjonen:

Å se etter om Nord-Odal kommune tilfredsstiller sentrale lovkrav og anbefalinger for IKT- sikkerhet.

3 Avgrensninger

I prosjektet har vi foretatt en avgrensning mellom de tekniske løsningene og systemene som HIKT drifter, og det som skal praktiseres av informasjonssikkerhet i kommunen. Årsaken til dette er at HIKT er et vertskommunesamarbeid hvor kontrollutvalget i Hamar kommune er kontrollerende organ.

Vi har kontrollert hvordan informasjonssikkerhet håndteres i organisasjonen i Nord-Odal kommune med hensyn til atferden i disse tekniske løsningene. Dette velger vi å kalle *informasjonshåndtering*. [4] Vi belyser også hvordan Nord-Odal kommune beskriver og opplever samarbeidet med HIKT.

I kommunal tjenesteyting, er det en sammenheng mellom informasjonssikkerhet og personvern. De to områdene har imidlertid to ulike innganger med hensyn til omfanget av en forvaltningsrevisjon. Dette revisjonsprosjektet er derfor avgrenset til å gjelde informasjonssikkerhet knyttet til datateknologi særlig og ikke personvern spesielt.

Området datateknologi inneholder mange begreper, og det opereres med ulike sikkerhetsbegreper som hver for seg belyser ulike deler av risikomomenter tilknyttet datateknologien. De tre mest omtalte formene for sikkerhet er IKT-sikkerhet, informasjonssikkerhet og kybersikkerhet. Prosjektplanen som lå til grunn for kontrollutvalgets bestilling omtalte de tre formene med kun ett begrep; IKT-sikkerhet. Vi har imidlertid definert problemstillingene dithen at forvaltningsrevisjonsprosjektet omhandler informasjonssikkerhet, og har derfor gjennomført forvaltningsrevisjonsprosjektet ut i fra hva dette begrepet omfatter. I det følgende gir vi en kort innføring i de tre begrepene.

3.1 IKT-sikkerhet

IKT-sikkerhet omhandler verktøy og metoder knyttet til drift av IKT-systemer og løsninger, og å beskytte teknologibaserte systemer som lagrer, prosesserer og overfører data. [5] Kort sagt handler IKT-sikkerhet om mye av det konkrete for å forhindre at uvedkommende kan komme seg inn i IKT-løsninger og på datamaskiner, uavhengig av om man er påkoblet internett.

[2] Brev fra kommunal og distriktsdepartementet: *Sikkerhetstiltak i norske kommuner i forbindelse med Russlands invasjon av Ukraina.*

[3] Beskrivelsen er hentet i fra en modell som er beskrevet i Nasjonal sikkerhetsmyndighets grunnprinsipper for sikkerhetsstyring

[4] Helse- og omsorgsdepartementet har brukt samme begrep i et rundskriv for spesialisthelsetjenesten mht. grensegangene mellom taushetsplikt, personvern og informasjonssikkerhet. Kilde: https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049/

[5] Heggernes, T. A. 2020, *Digital forretningsforståelse. Fra store data til små biter* (3. utgave), s. 350.

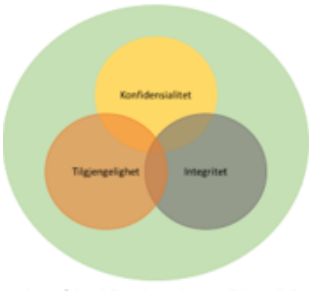
Brudd på IKT-sikkerheten vil kunne medføre nedetid i driftsløsningene og ha konsekvenser for daglige arbeidsoppgaver. Følgene av brudd på IKT-sikkerheten kan omhandle elementer som ligger til informasjonssikkerheten, for eksempel at informasjon og opplysninger kommer på avveie.

3.2 Informasjonssikkerhet

Informasjonssikkerhet omhandler i organisasjoners overordnede prosesser og rutiner for å sikre informasjon og tjenester. Heggernes viser til at informasjonssikkerhet handler om «å sikre kontinuitet i forretningsdriften og å minimere forretningsmessig skade som følge av sikkerhetshendelser». [6]

Forskjellen på IKT-sikkerhet og informasjonssikkerhet handler med andre ord om at IKT-sikkerhet går ut på å lage tekniske løsninger som forhindrer at teknologibaserte systemer tar skade av angrep, mens informasjonssikkerhet handler om beredskap- og beredskapsløsninger som kan iverksettes når en uønsket sikkerhetshendelse inntreffer.

Informasjonssikkerhet handler i prinsippet om å verne alle typer informasjon. For en kommune er informasjon veldig mye forskjellig, ut i fra hvilke oppgaver som skal løses. Fellesnevneren i dette er å beskytte denne informasjonen på et vis som er hensiktsmessig for innholdet i informasjonen. I kommunedirektørens verktøykasse for informasjonssikkerhet og personvern [7] fremgår det at dette handler om å sikre konfidensialitet, integritet og tilgjengelighet. Her illustrert:



Figur 1 Illustrasjon hentet fra kommunedirektørens verktøykasse for informasjonssikkerhet og personvern

Bildet over viser hvordan disse tre delene henger sammen i hverandre, men at de hver for seg er like viktige. I en organisasjon er det derfor viktig å sikre at informasjon i alle former ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og at informasjonen er tilgjengelig ved behov (tilgjengelighet). [8]

I den kommunale hverdagen, der det som oftest er digitale systemer i tilknytning til nesten alle tjenester, følger også økt krav til kunnskap og kontroll innen digital sikkerhet og praktisering av en klar sikkerhetskultur:

> «Økende bruk av digitale tjenester kan føre til enklere drift, bedre mobilitet, økt produktivitet og mer automatisert sikkerhet for virksomheter. Digitalisering kan samtidig føre til økende kompleksitet, flere verdier som eksponeres på offentlige, usikrede nett, og lange digitale verdikjeder som det er vanskelig å ha oversikt over.» [9]

Organisasjonens valg av sikkerhetstiltak må baseres på virksomhetens ordinære risikoarbeid, men grunnprinsippene for IKT-sikkerhet kan hjelpe til med å prioritere utvelgelsen. En virksomhet som ikke implementerer et anbefalt sikkerhetstiltak kan ha en økt risiko som må håndteres. Denne risikoen må vurderes opp mot virksomhetens risikotoleranse, i tillegg til krav i lovverk, bransjenormer og avtaler. Dersom risikoen ikke kan aksepteres, må kompenserende tiltak vurderes.

---

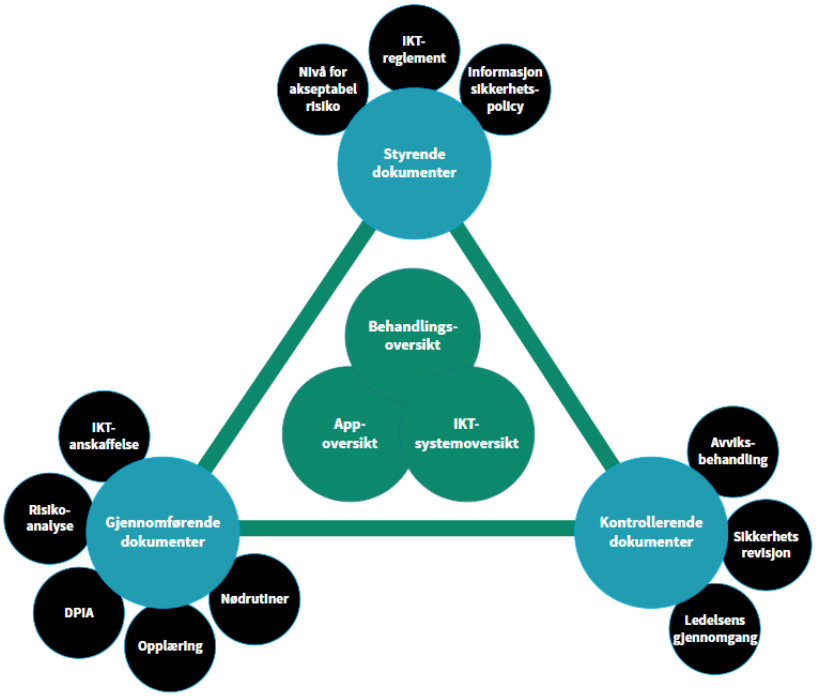
[6] Heggernes, T. A. 2020, *Digital forretningsforståelse. Fra store data til små biter* (3. utgave), s. 352.
[7] Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern, side 6
[8] www.digdir.no
[9] Grunnprinsipper for IKT-sikkerhet versjon 2.0, side 3

I en presentasjon gitt i kontrollutvalget i Kongsvinger kommune den 7. juni, ble modellen i illustrasjonen under benyttet for å illustrere de tre momentene ved informasjonssikkerhet, hva de består av og hva man har behov for kontroll på innenfor disse. Man må ha:

- *Styrende dokumenter,* hvor man setter nivå for akseptabel risiko, har et IKT-reglement og informasjonssikkerhetspolicy.
- *Gjennomførende dokumenter,* hvor det lages rutiner for og gjennomføres IKT-anskaffelser, risikoanalyser, DPIA [10], opplæring og nød-rutiner.
- *Kontrollerende dokumenter,* hvor man har rutiner for og gjennomfører avviksbehandling, sikkerhetsrevisjon og hvor ledelsen foretar en gjennomgang.[11]

Innenfor dette er det behov for en oversikt over opplysninger og informasjon som behandles, en systemoversikt over IKT-systemer, og en oversikt over brukte applikasjoner.

Informasjonssikkerhet er med andre ord i stor grad relatert til internkontrollsystem og internkontroll i praksis.



Figur 1: Hentet fra presentasjon, kontrollutvalget Kongsvinger kommune 7. juni 2022

3.3 Informasjonssikkerhet og personvern

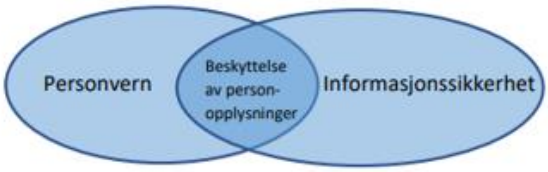
Personvern og informasjonssikkerhet er to ulike fagområder, men overlapper hva gjelder beskyttelse av informasjon, også tilknyttet personer. Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. [12]

[10] Kilde: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

[11] Styrende, gjennomførende og kontrollerende elementer er også beskrevet i datatilsynets veileder for internkontroll

[12] Kilde: Datatilsynet https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/

Informasjonssikkerhet og personvern handler i utgangspunktet om forskjellige ting, men kan henge sammen i praksis:



Figur 2: Hentet fra kommunedirektørens verktøykasse for informasjonssikkerhet og personvern

Illustrasjonen [13] ovenfor viser hvordan disse to fagområdene henger tett sammen. Ved et eventuelt datainnbrudd kan personvernet være truet, men datainnbruddet i seg selv handler hovedsakelig om informasjonssikkerheten.

3.4 Kybersikkerhet

Kybersikkerhet handler om å forhindre negative konsekvenser ved angrep eller uønskede hendelser som foregår over internett, men som ikke direkte berører hensyn til konfidensialitet, integritet eller tilgjengelighet på informasjon. [14] Dataenes konfidensialitet, integritet og tilgjengelighet står sentralt som verdier for både IKT-sikkerhet og informasjonssikkerhet. Som eksempler på kybersikkerhetstrusler, viser Heggernes til nettmobbing, hacking av smart-gjenstander i hjemmet, åndsverkskrenkelse ved fildeling, og kyberterrorisme. Sistnevnte kan imidlertid ha følger for konfidensialitet, integritet og tilgjengelighet.

4 Metode for revisjonen

I NKRFs standard for forvaltningsrevisjon står det at man skal bruke metoder som sikrer at de data som brukes er relevante og pålitelige, og at dataene skal være tilstrekkelige for å besvare prosjektets problemstillinger. Metodene som er brukt skal begrunnes. En måte å sikre dataenes relevans og pålitelighet på, er å innhente data om samme forhold gjennom flere metoder. Bruk av to eller flere metoder kalles metodetriangulering, og bidrar til å sikre gyldigheten og påliteligheten i våre resultater og konklusjoner.

I dette prosjektet har vi brukt metodene dokumentstudier, intervjuer og spørreundersøkelse.

4.1 Dokumentstudier

I denne forvaltningsrevisjonen har vi gjennomgått dokumenter oversendt fra Nord-Odal kommune. Dokumentene omfatter kommunale planer og strategier, rapporter, rutiner og prosedyrer, veiledninger, avtaler og annet. Fokuset har vært å belyse kommunens internkontroll, styringsdokumenter og rutiner i forbindelse med informasjonssikkerhet.

Vi har også i deler av prosjektet, fra juni 2022 til september 2022, hatt tilgang til *Compilo*. Compilo er kommunens kvalitetssystem og består blant annet av et dokumentbibliotek og avviksrapportering for ansatte. Det er også mulig å gjennomføre ROS-analyser i systemet, og det er en egen årshjul-modul i systemet.

Revisjonen har ikke vurdert dokumenter som har blitt lastet opp i Compilo etter 8. september 2022.

[13] Modellen er hentet fra kommunedirektørens verktøykasse for personvern og informasjonssikkerhet, side 6.
[14] Heggernes, T. A. 2020, *Digital forretningsforståelse. Fra store data til små biter* (3. utgave), s. 353.

4.2 Intervjuer

Det er gjennomført 4 intervjuer i prosjektet. Vi har snakket med systemadministratorer tilknyttet de to systemene *Visma Profil*, som er kommunens elektroniske pasientjournal og *Websak*, som er kommunens arkiv- og saksbehandlersystem. Vi har også snakket med IKT-konsulent og informasjonssikkerhetsansvarlig. Leder for HR, stab og service har delegert ansvar som informasjonssikkerhetsansvarlig fra kommunedirektøren. Informasjonssikkerhetsansvarlig og IKT-konsulent i kommunen er et team som daglig ivaretar de overordnede oppgavene tilknyttet informasjonssikkerhet. Informasjonssikkerhetsansvarlig har vært vår kontaktperson gjennom prosjektet.

Det har blitt gjennomført til sammen 7 møter, inkludert oppstartsmøte. Oppstartsmøtet ble avholdt i januar 2022, de øvrige samtalene foregikk mellom mars til og med august 2022. Det har blitt utarbeidet referater i forbindelse med alle samtaler. Alle referater er lest gjennom og verifisert av de deltakende ansatte fra kommunen.

Det har i tillegg vært en del korrespondanse per e-post. Korrespondansen har omhandlet ulike avklaringer og eventuelle oppfølgingsspørsmål. Dette ble gjennomført i tidsrommet januar 2022 til september 2022.

4.3 Spørreundersøkelse

Revisjon Øst IKS gjennomførte en spørreundersøkelse rettet mot de ansatte i Nord-Odal kommune. Undersøkelsen er basert på en undersøkelse NorSIS [15] har utformet, og som tar for seg alle viktige og sentrale områder innen informasjonssikkerhet for å belyse den generelle kunnskapen til ansatte innenfor temaene informasjonssikkerhet og god informasjonssikkerhetskultur. Undersøkelsen ble gjennomført i perioden 15. mars til 22. april.

NorSIS er tydelige på at det er vanskelig å sammenligne sikkerhetskulturer på tvers av organisasjoner og virksomhetsområder, i og med at graden av behovet for sikkerhet er ulik fra virksomhet til virksomhet. Vi mener imidlertid at verktøyet vil kunne bidra til å si noe om sikkerhetskulturen både med hensyn til kartlegging av status og behov.

Spørreundersøkelsen ble sendt til 433 respondenter, der 420 av disse nådde fram til mottaker. Antallet besvarelser ble til sammen 197. Dette er en svarprosent på 47 %. I tillegg hadde 33 åpnet undersøkelsen, men ikke sluttført sine svar, dette utgjør 8 %.

Vi har forsøkt å få en så høy svarprosent som mulig. Det ble derfor sendt ut invitasjon med 3 påfølgende påminnelser, alle per e-post. Invitasjonen gikk ut 23. mars, påminnelser gikk ut henholdsvis 30. mars, 7. april og 19. april. Alle ledere på tvers av sektorer ble oppfordret av informasjonssikkerhetsansvarlig i kommunen til å følge dette opp i sine avdelinger, og sette av dedikert tid slik at ansatte fikk anledning og tid til å gjennomføre undersøkelsen.

Resultatene av undersøkelsen vil brukes opp mot revisjonskriteriene generelt, men vi vil se til de spesielt i tilknytning til problemstilling 3.

[15] Norsk senter for informasjonssikring (NorSIS) er en del av regjeringens helhetlige satsing på informasjonssikkerhet i Norge. NorSIS sin kjernevirksomhet er kunnskapsformidling og utvikling av en digital sikkerhetskultur for å skape bevissthet, påvirke holdninger og å endre sikkerhetsatferd i målgruppen. Målgruppen for NorSIS' aktivitet er norske virksomheter i privat og offentlig sektor.

5 Spørreundersøkelsen – funn og analyse

Spørreundersøkelsen har til formål å kartlegge *kunnskapen og forståelsen* virksomheter har, for å sikre *forsvarlighet* innen informasjonssikkerhet og *god sikkerhetskultur*. Temaene i spørreundersøkelsen kaster lys over atferd og kompetanse i forbindelse med informasjonssikkerhet.

Eksempler på spørsmål er tilknyttet kjennskap til passordsikkerhet, om man låser skjerm når man forlater maskinen sin eller om man kjenner til hva som er sikre og usikre lenker på internett. Spørreundersøkelsen kartlegger også om ansatte har gjennomført *opplæringstiltak* og om det er spesielle ting som ansatte mener kommunen bør se nærmere på. Den røde tråden i undersøkelsen er å finne ut om ansatte har riktig kunnskap og atferd i tilknytning til praktisering av god informasjonssikkerhet.

Undersøkelsen består av fem hovedtemaer med tilhørende spørsmål:

1. Holdninger til digitalisering og digital sikkerhet
2. Risiko-oppfattelse
3. Synet på styring og kontroll
4. Sikkerhetsatferd, og
5. Kunnskap, læring og interesse

Vi har gjennomgått svarprosentene for hvert enkelt spørsmål, og i tillegg gjort analyser hvor vi har sammenlignet ansatte med og ansatte uten lederansvar, samt ledere og ansatte med og uten opplæring. Vi har i tillegg sett nærmere på passord-praksis.

Vi har også undersøkt alle ansatte i forhold til om de bruker samme passord hjemme og på jobb og om de igjen bruker det samme passordet på tvers av systemer. Vi har spesielt sett på dette fordi det kan vise atferd tilknyttet stor risiko for informasjonssikkerheten.

Svaralternativene er i mange av spørsmålene gitt på en skala fra 1-5, samt med et «vet ikke»-alternativ. Selv om det finnes artsgrader har vi valgt å behandle 1 og 2 som felleskategori og 4 og 5 som felleskategori. Dersom man svarer 3, tar man i utgangspunktet ikke stilling til spørsmålet. Det samme gjelder om man svarer vet ikke. Det er med andre ord nyanser i tallmaterialet som vi har valgt å se bort ifra for enkelhets skyld.

5.1 Generelle innledende betraktninger

Over 20 % av de som har svart på undersøkelsen, har oppgitt at de har lederansvar.

5.2 Holdninger til digitalisering og digital sikkerhet

Undersøkelsen viser at de ansatte i Nord-Odal kommune opplever at det er lav terskel for å si ifra til kollegaer dersom en ser at en kollega gjør noe som utgjør en digital sikkerhetsrisiko for virksomheten. Det er likevel slik at få opplever at kolleger gir tilbakemelding på slike forhold. Undersøkelsen er i seg selv ikke i stand til å gi informasjon om slike digitale sikkerhetshendelser forekommer.

De fleste som tar stilling til spørsmålet opplever ledelsen som gode rollemodeller. Ledere uten opplæring i informasjonssikkerhet mener i større grad at ledelsen er gode rollemodeller enn ledere med opplæring.

5.3 Risiko-oppfattelse

Vi spurte ansatte i Nord-Odal kommune om de opplever at de er i stand til å avgjøre hva som er trygt og utrygt å gjøre på internett. 8 av 10 mente de i stor grad var i stand til å vurdere hva som var trygge/utrygge aktiviteter. Her er det en større andel ledere uten opplæring som mener å vite hva som

er trygt og utrygt å gjøre, enn ledere med opplæring. Blant ansatte generelt vurderer de med opplæring seg bedre i stand til å vurdere hva som er utrygt/trygt å gjøre på nett (nærmere 90 %).

Vi spurte de videre om de var bekymret for:

- Å få virus på arbeidsgivers datautstyr
- At man blir lurt til å gi fra seg informasjon
- At virksomhetens systemer blir skadelidende som følge av utilsiktede feil
- At man mister egne og/eller arbeidsgivers data

Resultatene viser at de ansatte er mer eller mindre delt på midten med hensyn til om de tror at digitale trusler kan hende dem. Av de fire punktene, så er ansatte mest bekymret for å miste egne/arbeidsgivers data og å bli lurt til å gi fra seg informasjon.

Vi stilte også spørsmål om de ansatte knyttet høy risiko til:

- Bruk av e-post
- Dele jobb-passord med andre kolleger
- Bruke sosiale medier
- Bruke digitale assistenter, som for eksempel smart-høyttalere eller chatbots
- Bruk av minnepinner og andre fysiske lagringsmedier
- Bruk av sky-tjenester
- Mottak av SMS-er med lenker

De ansatte er opptatt av at det er høy risiko forbundet med å dele jobb-passord, samt å motta SMS-er med lenker. Nærmere 90 % mener det er stor risiko forbundet med å dele jobbpassord og 75 % mener det er stor risiko forbundet med å motta SMS-er med lenker.

De ansatte mener imidlertid at den aktiviteten det er knyttet minst risiko til, er å bruke e-post. Dette står i kontrast til at de aller fleste oppgir at de er i stand til å vurdere hva som er trygt/utrygt å gjøre på nett.

Over 60 % av respondentene gir uttrykk for at de ikke vet, eller ikke tar stilling til om det er høy risiko knyttet til bruk av digitale assistenter. Det kan også hende at digitale assistenter ikke brukes i noen stor grad verken i jobb eller privat sammenheng, men det kan være risikofylt å bruke slike type hjelpemidler. [16]

Over 70 % av de ansatte svarer at det enten er liten risiko, eller at de ikke vet hvilken risiko det utgjør å bruke minnepinner.

Over halvparten er bekymret for at andre/eksterne aktører utgjør en trussel mot informasjonssikkerheten i virksomheten, mens 1 av 5 frykter for at de selv kan gjør en feil eller utgjør en potensiell risiko. 1 av 4 vet ikke hva som kan være en potensiell risiko mot virksomheten.

Ansatte og ledelse som har fått opplæring innen informasjonssikkerhet har en høyere oppfattelse av risiko generelt enn de som ikke har fått opplæring. Ledere uten opplæring er i mindre grad bekymret for å bli lurt fra seg informasjon enn ledere med opplæring. Ansatte med og uten opplæring svarer imidlertid ganske likt på dette spørsmålet. Oppfattelsen av at kommunen er utsatt for mer risiko og trusler knyttet til informasjonssikkerhet er også høyere hos ledelse enn hos ansatte generelt.

Bekymring for å miste egne eller arbeidsgivers data er større hos ledere enn hos ansatte generelt. Nesten 7 av 10 ledere og 45 % av ansatte er bekymret for dette. Her er det også ledere med opplæring og ansatte med opplæring som er mer bekymret enn ansatte uten opplæring.

[16] https://www.nrk.no/kultur/advarer-mot-googles-norske-smarthoyttaler_-_-ikke-en-hvilken-som-helst-husgjest-1.14239760

I forhold til en god del av spørsmålene tilknyttet risiko-oppfattelse, så er det generelt sett en andel som ikke har sterke meninger/ikke tar stilling til (som svarer verken/eller) spørsmålet om risikooppfattelse tilknyttet ulike digitale aktiviteter. Dette kan tolkes i retning av at det er behov for mer opplæring og forståelse av informasjonssikkerhet.

5.4 Syn på styring og kontroll

8 av 10 svarer at Nord-Odal kommune har regler for informasjonssikkerhet. 9 av 10 ledere svarer at virksomheten har regler for informasjonssikkerhet, mens 98 % av ledere med opplæring svarer ja på dette spørsmålet.

De aller fleste (89 %), mener at de vet hvem de skal si ifra til hvis det oppstår en digital sikkerhetshendelse. Spørsmålet i undersøkelsen tillater at den som svarer kan krysse av for flere alternativer. Derfor viser andelene her til hvor stor andel av deltakerne som har svart det enkelte svaralternativ. Summen er følgelig høyere enn 100 %. Nedenfor følger en oversikt over hvem ansatte velger å si ifra til og hvordan fordelingen er:

- Nærmeste leder (89 %)
- IT-konsulent i kommunen (29,5 %)
- HIKT servicedesk (28,7 %)
- Personvernombud (7,9 %)
- Datatilsynet (7,3 %)
- Annet (3 %)
- Superbruker (2,4 %)
- Vet ikke (0 %)

Ca. 60 % mener at ledelsen har kommunisert tydelig sine forventninger og krav til de ansatte når det gjelder informasjonssikkerhet. De fleste av respondentene mener at virksomhetens regler for informasjonssikkerhet ikke er til hinder for deres daglige gjøremål. Her er det flere ledere enn medarbeidere som mener at informasjonssikkerheten ikke er et hinder i det daglige arbeidet.

Det er 4 % som oppgir at de bevisst bryter virksomhetens retningslinjer og ca. 12 % som ikke tar stilling til spørsmålet.

5.5 Sikkerhetsatferd

På spørsmål om de ansatte undersøker nettsider for om hvorvidt de er sikre, oppgir 2 av 3 at de gjør slike vurderinger. 1 av 4 sjekker ikke om vedlegg i e-poster er sikre før de åpner dem.

De aller fleste låser skjermen når de forlater datamaskinen, det er allikevel 1 av 10 som ikke gjør det. De aller fleste deler heller ikke informasjon om arbeidet sitt i sosiale medier. Det er 1 av 5 som gjør det i svært liten grad.

Respondentene ble spurt om hva de ville gjøre dersom de:

- Mottar en mistenkelig e-post
- Mistenker at man har fått virus på virksomhetens datamaskin
- Ser at en kollega begår et sikkerhetsbrudd

3 av 4 sier de vil kontakte nærmeste ledere, helpdesk eller liknende ved mottak av en mistenkelig e-post. 1 av 10 sier de vil ordne opp selv, nærmere 5 % sier de ikke vil gjøre noe hvis de mottar en mistenkelig e-post. Hvis ansatte tror de har et virus eller liknende på datamaskinen melder så mange som 96 % ifra til nærmeste leder/helpdesk. Imidlertid, hvis en ansatt ser en kollega begå et sikkerhetsbrudd, fordeler svarene seg noe annerledes: 1 av 10 vet ikke hva de skal gjøre, mens nærmere 85 % at de varsler enten til nærmeste leder/helpdesk, eller ordner opp selv direkte med kollegaen.

5.5.1 Risiko-atferd - funn i en mindre gruppe

Over 90 % av alle ansatte svarer at de ikke bruker de samme passordene hjemme og på jobb. Det er likevel nesten 10 % som bruker passord på tvers av jobb og privat. Selv om tallene er små, er dette en høyrisiko-atferd med potensielt store konsekvenser. Blant disse 10 % er det også slik at 1 av 3 bruker de samme passordene på tvers i jobbsammenheng, noe som også er en type atferd som høyner risikoen ved et datainnbrudd.

Vi har sett nærmere på om det er en overlapp mellom de som bruker samme passord privat og i jobb og de som bruker samme passord på tvers av systemer på jobb. Det er et lite antall som gjør begge deler, men dette er også en risikogruppe:

- Det er flere av disse som ikke er bekymret for virus på arbeidsgivers datautstyr eller at virksomheten skal bli utsatt for svikt i digitale systemer på bakgrunn av utilsiktede feil, eller å miste egne/arbeidsgivers data.
- Det er en stor andel som ikke er bekymret for å bli lurt til å gi fra seg informasjon eller syns det er risikofylt å dele jobb-passordene med andre. Nesten halvparten mener det ikke er risikofylt å bruke sosiale medier
- De fleste av de som bruker de samme passordene hjemme og på jobb og på tvers av systemer på jobb, anser det ikke som risikofylt å bruke minnepinner
- 1 av 3 låser ikke skjermen når de forlater datamaskinen sin.
- 1 av 5 undersøker ikke om lenker er sikre før de åpner dem.
- 1 av 3 vet ikke, eller gjør ingenting hvis de mottar en mistenkelig e-post
- 9 av 10 har fått opplæring i informasjonssikkerhet og opplæringen har i stor grad foregått gjennom informasjon fra arbeidsgiver og organiserte interne kurs.
- 1 av 3 ønsker ikke mer kunnskap om informasjonssikkerhet på jobb.

Dette tegner en profil av en liten gruppe brukere/ansatte som kan gjøre Nord-Odal kommune spesielt utsatt, og som potensielt kan utgjøre en risiko som brukere av kommunens digitale systemer.

5.6 Kunnskap, læring og interesse

Omtrent halvparten av de som har besvart undersøkelsen har fått opplæring i informasjonssikkerhet. 7 av 10 respondenter ønsker mer opplæring, mens de resterende sier de ikke trenger det.

Ved spørsmål om hvilken opplæring de ansatte får, er det slik at 1 av 5 sier de får organiserte interne kurs eller utdanning. Ca. halvparten sier de er selvlært eller hører om ting fra andre kollegaer i en mer uformell situasjon. 66 % sier de får opplæring gjennom informasjon fra arbeidsgiver. Det er en indikasjon i tallene om at det er mye uformell og egenopplæring av informasjonssikkerhet. 29 % har deltatt på nettkurs i forbindelse med nasjonal sikkerhetsmåned.

5.7 Størst utfordring?

Det ble stilt et åpent spørsmål knyttet til de ansattes egne tanker rundt hva som er kommunens hovedutfordring med informasjonssikkerhet. Innspillene varierer. Av 197 respondenter er det kommet inn 63 unike svar på dette spørsmålet. Disse er gjennomgått og vi har forsøkt å kategorisere svarene for å se hva ansatte mener er mest utfordrende med informasjonssikkerhet, og hva de mener at bør få fokus eller bli endret. Det er ikke mulig å trekke ut klare funn da svarene har stor spredning. Det har kommet en del innspill som kan brukes som utgangspunkt for eventuelle tiltak. Disse presenteres her i kronologisk rekkefølge ut ifra antall:

- Savner to-trinns pålogging
- Stress og arbeidspress
- At det sendes sensitiv informasjon over e-post-systemet
- At vi er avhengige av vår private mobil for å kunne gjennomføre arbeid
- One-drive samkjører ikke, slik at å jobbe hjemmefra kan være en utfordring
- Arkivering i tilknytning med foreldresamtaler og liknende
- Det er mange regler å forholde seg til, og lite mulighet for å dele informasjon med brukere av virksomheten
- Det fins en del skyggesystemer, som ikke er sikret gjennom Hedmark IKT
- Flere benytter samme PC

Noen mener at stress og manglende opplæring kan være fokuspunkter. De største fellestrekkene finner vi rundt en bekymring for at ansattes uvitenhet og ansatte som gjør feil kan skape avvikssituasjoner og være en trussel mot sikkerheten, samt e-postsvindel/hacking som hindrer dem i å få tilgang til den informasjonen de trenger for å gjennomføre arbeidet.

5.8 Oppsummering

Her følger noen oppsummerende punkter:

- De aller fleste (89 %) bruker forskjellige passord på jobb og hjemme.
- Det fremkommer at det er en gruppe med ansatte som har samme passord både hjemme og på jobb, og videre at 1 av 3 i denne gruppen ansatte har de samme passordene på tvers av systemene på jobb.
- Det er lett å si ifra for de fleste når de ser brudd på informasjonssikkerheten, men få opplever at andre sier ifra.
- Halvparten oppgir at de har fått opplæring, og 7 av 10 at de trenger opplæring.
- I spørsmål om hva de ansatte knyttet høyest risiko, svarte mange bruk av e-post. Dette står i kontrast til at de aller fleste oppgir at de er i stand til å vurdere hva som er trygt/utrygt å gjøre på nett.
- Risiko-oppfattelsen er større/høyere blant de som har opplæring enn de som ikke har det.
- I forhold spørsmålene tilknyttet risiko-oppfattelse, så er det mange som ikke har sterke meninger/ikke tar stilling til (som svarer verken/eller) spørsmål om ulike digitale aktiviteter. Dette kan tolkes i retning av at det er behov for mer opplæring og forståelse av informasjonssikkerhet.
- 4 % oppgir at de bevisst bryter virksomhetens regler. 12 % vet ikke om de gjør det.

6 Problemstilling 1 – Etablering av planverk

Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte?

6.1 Revisjonskriterier for problemstilling 1

Følgende er en tabell med de kriterier vi har benyttet for å besvare problemstillingen og våre vurderinger av disse. Kriteriene er gjengitt i kortform. For en full utledning av revisjonskriteriene, se vedlegg A. Tabellen er interaktiv og leseren kan gå rett til den enkelte vurdering ved å trykke på det enkelte kriteriet. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt i kapitlene nedenfor. Vi gjør derfor leseren oppmerksom på at vurderingene må sees opp imot de innhentede data i prosjektet.

	Kriterium 1	Kommunen har beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).
	Kriterium 2	Kommunen og dens øverste ledelse har en tilpasset og risikobasert internkontroll for informasjonssikkerhet. Internkontrollen inneholder både et strategisk og langsiktig perspektiv, samt et operasjonelt perspektiv som omhandler daglig virksomhetsstyring.
	Kriterium 3	Kommunen har gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi, og har en tydelig tiltaksplan som viser hvem som er ansvarlig for ulike tiltak.
	Kriterium 4	Kommunen har rutiner og prosedyrer som sørger for at alle i virksomheten sikrer at informasjon i alle former ikke blir kjent eller endret utilsiktet eller av uvedkommende.
	Kriterium 5	Kommunen har rutiner og prosedyrer som sørger for at alle i virksomheten sikrer at informasjon i alle former er tilgjengelig ut fra tjenstlige behov.
	Kriterium 6	Kommunens ledelse gjennomgår virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året. Følgende punkter skal gjennomgås: - Endringer i behandlinger av helse og personopplysninger (behandlingsprotokoll) - Endringer i organiseringen av arbeidet - Resultat av risikovurderinger og personvernkonsekvensutredninger - Resultat av avviksbehandling - Oppfølging av leverandører og databehandleravtaler - Endring i nivået for akseptabel risiko.
	Kriterium 7	Ledelsens gjennomgang skal dokumenteres.

6.2 Innhentet data

6.2.1 Kommunens styringssystem (internkontroll) for personvern og informasjonssikkerhet

I kommunedirektørens verktøykasse for personvern og informasjonssikkerhet er følgende beskrevet:

> «Kommunedirektøren må sikre god sikkerhetsstyring, dvs. sikre at det blir gjennomført planlagte og systematiske aktiviteter som omfatter planlegging, utførelse, kontroll og korrigering av arbeidet med sikkerhetsloven og sikkerheten i kommunen (internkontroll). For å kunne gjøre dette på best mulig

måte, må du være kjent med hvilke verdier kommunen besitter og hvilke risikoer som gjør seg gjeldende.» [17]

I følge Normen [18] skal alle virksomheter ha et styringssystem for informasjonssikkerhet og personvern (internkontroll). Normen beskriver at et slikt system formaliserer hvordan virksomheten planlegger, gjennomfører, evaluerer/kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler. Informasjonssikkerhet og personvern bør være en del av det totale styringssystemet og ansvaret ligger hos virksomhetens øverste ledelse.

Normen beskriver videre at alle offentlige virksomheter skal beskrive mål og etablere strategi for informasjonssikkerhet, og at dette danner grunnlaget for styringssystemet, eller internkontrollen. Det er beskrevet i kommunedirektørens verktøykasse for personvern og informasjonssikkerhet [19], at for å sikre internkontrollen må kommunen være kjent med hvilke *informasjonsverdier* de besitter og hvilke risikoer som da gjør seg gjeldende. Informasjonsverdier kan klassifiseres i 4 forskjellige kategorier:

- *Kritisk verdi:* Informasjon som er kritisk for kommunen i en krisesituasjon, for eksempel informasjon om samfunnskritiske funksjoner (typisk vannverk, beredskapsplaner etc) og sensitive personopplysninger.
- *Høy verdi:* informasjons som vil være ødeleggende for funksjoner og tjenester som er kritisk for kommunens daglige drift, for eksempel: Strategidokument, eksamensoppgaver før de er gitt og informasjonssystem for lønnsutbetaling.
- *Middels verdi:* Virksomhetsintern informasjon eller informasjon som kan skade kommunens funksjoner og tjenester daglig, som for eksempel: læringsplattform for kommunikasjon mellom elev og skole, informasjon som er unntatt offentligheten.
- *Lav verdi:* Åpen informasjon uten spesielle sikkerhetsbehov, for eksempel: informasjon som ligger åpent på hjemmesiden.

Informasjonsverdiene vil ifølge kommunedirektørens verktøykasse for informasjonssikkerhet og personvern til sammen legge grunnlaget for å kunne vurdere hvilken informasjon som er mest kritisk for kommunens drift og tjenesteproduksjon, og hvilke tiltak som bør prioriteres for å sikre denne informasjonen.

Ifølge IKT-konsulent og informasjonssikkerhetsansvarlig i Nord-Odal kommune, er det ikke foretatt en analyse av informasjonsverdier i kommunen.

Nord-Odal har en prosedyre som beskriver nivå for akseptabel risiko. [20] Hensikten med denne prosedyren er å dokumentere målbare størrelser på sikkerhetsmålene som er fastsatt, slik at det er mulig å kunne kontrollere om sikkerhetsmålene nås. Prosedyren gjelder for de som skal bestemme risikonivå for et IKT-system og bestille tjeneste basert på en slik risikovurdering.

Prosedyren har en tabell hvor den måler i hvilken grad stopp av systemer eller tjenester har en påvirkning på risiko. Hvis nedetid i systemet kan være livstruende for tjenestemottaker, ansees den som kritisk for kommunens drift. Det skal da gjøres en vurdering av akseptabel risiko, og hva kommunen kan tåle av avbruddstid/nedetid før det har potensielle konsekvenser. Kommunen måler dette i 5 ulike kategorier:

- Systemer hvor stopp av tjeneste er livstruende.

[17] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet, side 14
[18] Normen v6, side 13
[19] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet, side 13
[20] Hentet fra Håndbok i informasjonssikkerhet, Compilo februar 2021

- Systemer hvor stopp av tjeneste er alvorlig, for eksempel at det medfører betydelig merarbeid eller tapt effektivitet.
- Systemer hvor stopp av tjeneste kan føre til svekkelse av tjenestemottakers tillit.
- Systemer hvor stopp inntil 72 timer kan aksepteres.
- Systemer som ikke er prioritert.

6.2.2 Kvalitetssystemet Compilo – oppbygging og innhold

Compilo ble tatt i bruk i Nord-Odal kommune fra og med 1. januar 2021. Før denne tid hadde kommunen et kvalitetssystem kalt KF-kvalitet. I følge systemansvarlig i Compilo, har innholdet i dokumentbiblioteket i Compilo blitt bygd opp fra bunnen av. Vi har kun vurdert dokumenter som har vært tilgjengeliggjort for ansatte generelt, gjennom Compilo.

Systemet består av ulike moduler og er tilgjengelig for alle ansatte. Kvalitetssystemet ivaretar en del av den systematiske internkontrollen i praksis. Compilo brukes i dag av ansatte som et felles dokumentbibliotek og som et avvikssystem. Her er det blant annet mulig å gjennomføre ROS-analyser og legge inn avviksmeldinger.

Det er til sammen 21 ulike prosedyrer og beskrivelser tilknyttet informasjonssikkerhet og personvern som har blitt lastet opp siden januar 2021, 12 av disse har blitt lastet opp i tiden som revisjonen har gjennomført dette prosjektet fra januar 2022 til og med august 2022. Vi ser også en sammenheng mellom møter som er gjennomført og temaer som vi har tatt opp i samtaler, og informasjon/dokumenter som da har blitt tilgjengeliggjort eller revidert i Compilo i etterkant av disse samtalene.

Alle dokumenter som er lastet opp i Compilo under «informasjonssikkerhet og personvern» er satt opp til å revideres årlig. Det er en egen fane øverst med *metadata* for hver oppføring. Metadata beskriver hvem som er ansvarlig for prosedyren/rutinen, hvem som har godkjent prosedyren/rutinen, når prosedyren/rutinen ble lastet opp og eventuelt revidert og revisjonsfrist.

Noen av dokumentene har også flere rutiner lenket opp i selve dokumentene, men som ikke er lagt til som egne rutiner eller innlegg i Compilo. Vi går ut ifra at dokumenter som det er lenket til, også skal revideres årlig.

Det er et eget område i Compilos dokumentbibliotek som beskriver informasjonssikkerhet og personvern og føringer/prosedyrer/rutiner. Dette området er delt opp i tre underkategorier:

- Styrende dokumenter
- Gjennomførende dokumenter og
- Kontrollerende dokumenter.

IKT-konsulent i Nord-Odal kommune oppgir at han har bidratt til å utforme mye av dokumentasjonen tilknyttet informasjonssikkerhet og personvern. IKT-konsulent har revisjonsansvar for den delen som handler om informasjonssikkerhet og personvern i Compilo. Ifølge IKT-konsulent, så møter ikke Compilo de kravene til internkontrollsystem som skal ivareta informasjonssikkerhet og personvern.

Prosjektet «HIKT2025» har avdekket at kommunene trenger et system som ivaretar flere funksjoner enn hva HIKT-kommunenes kvalitetssystemer kan tilby per i dag. Kommunen skal i samarbeid med HIKT anskaffe et GDPR-system. Prosessen med anskaffelse av dette systemet er et resultat av prosjektet «Rett og rimelig», som er en del av «HIKT2025». Ifølge informasjonssikkerhetsansvarlig vil det nye systemet gjøre det enklere for kommunen og samarbeide og ivareta informasjonssikkerhet. Dette går spesielt på spesielt på felles behandlingsprotokoll, ROS-analyser og DPIA. Ifølge IKT-konsulent er en del rutiner ikke tilgjengeliggjort for ansatte siden de er tiltenkt å bli tilgjengelige og tas i bruk når det felles GDPR-systemet er anskaffet.

6.2.2.1 Kommunens håndbok for informasjonssikkerhet

Kommunens håndbok for informasjonssikkerhet beskriver hvordan informasjonssikkerhet skal ivaretas i praksis. Det fremgår i håndboken at den er under revisjon. Her er det også listet opp lenker til ulike prosedyrer og veiledninger som er definert inn under styrende, gjennomførende og kontrollerende dokumenter. I håndboka beskrives det at det er en del dokumentasjons- og tiltakskrav til ethvert system som skal tas i bruk i kommunen, for eksempel:

- Det skal gjennomføres risikovurdering, og dette skal foreligge for alle systemer
- DPIA, eller en vurdering av personvernkonsekvenser skal gjennomføres, og sikre personvernet etter nytt personvernregelverk
- Det skal foreligge databehandleravtaler for alle systemer

IKT-konsulenten mener at praksis rundt informasjonssikkerhet er styrket i sektorene oppvekst og eiendom/samfunn. Dette blant annet som følge av større prosjekter gjennom HIKT der sikkerhetstenking er viktig. HIKT-samarbeidets arbeid med felles plattform for velferdsteknologi er et eksempel på et slikt prosjekt som har fokus på sikkerhet.

6.2.2.2 Kommunens sikkerhetsmål og sikkerhetsstrategi

Nord-Odal kommune har et dokument ved navn «Sikkerhetsmål og sikkerhetsstrategi» i sitt kvalitetssystem. Det er beskrevet i dokumentet at det er vedtatt i rådmannens ledergruppe den 18. mars 2021. [21] Nord-Odal kommunes sikkerhetsmål er beskrevet som følger:

> «All informasjon som Nord-Odal forvalter skal behandles etter gjeldende lovverk og på en måte som ivaretar krav til konfidensialitet, integritet, tilgjengelighet, åpenhet, lovlighet og dataminimering. Dette gjelder all informasjon; både det som finnes digitalt, på papir eller kommuniseres muntlig. Informasjonssikkerhet er en nødvendig faktor for at Nord-Odal kommune skal løse sine oppgaver og ha tillit hos innbyggerne».

Dokumentet beskriver ulike tiltakspunkter, eller «sikkerhetsstrategi», under to deler i en tabell; i den ene delen er kommunens ønskede praksis beskrevet, i den andre blir det beskrevet hva kommunen skal gjøre for å nå sikkerhetsmålet. Følgende er noen eksempler fra kommunens ønskede praksis:

- Roller og oppgaver er beskrevet, kjent og etterleves
- Tilgang til informasjon er basert på tjenstlig behov
- Har manuelle rutiner tilgjengelig
- Ansatte kjenner til og etterlever gjeldende plikter og retningslinjer
- Ansatte har kompetanse til å ivareta informasjonssikkerhet
- Ansatte ivaretar innbyggernes rettigheter
- Arbeidet med informasjonssikkerhet er en del av internkontrollen

Punktene som er beskrevet i dokumentet «sikkerhetsmål og sikkerhetsstrategi» er også beskrevet i Normens veileder for internkontroll i informasjonssikkerhet og personvern. [22]

Ifølge informasjonssikkerhetsansvarlig, er sikkerhetsmål og sikkerhetsstrategi tilknyttet informasjonssikkerhet gode. Informasjonssikkerhetsansvarlig har i intervju gitt uttrykk for at det er behov for å stille spørsmål ved om kommunen er gode nok på å få ut informasjon til den enkelte ansatte, og å konkretisere målene for informasjonssikkerhetsarbeidet, samt om dette løses på best mulige praktiske måte.

Som et eksempel på hva kommunen har foretatt seg av informasjonskampanjer rettet mot ansatte i kommunen, har informasjonssikkerhetsansvarlig fortalt at kommunen tidligere har trykket opp og delt

[21] «Sikkerhetsmål og sikkerhetsstrategi», Nord-Odal kommune, 23.3.32 – revidert 8.4.2022 - Compilo

[22] Normens veileder om internkontroll for informasjonssikkerhet og personvern v1.0 er en veileder som er basert på Normens krav.

ut klistremerker som ble klistret på alle datamaskiner, der det stod en påminnelse om at det var viktig å låse maskinen når man forlot den. Informasjonssikkerhetsansvarlig ga uttrykk for at slike tiltak bør settes i system og følges opp jevnlig.

6.2.2.3 IKT-sikkerhetsinstruks – datavettregler

Kommunens datavettregler [23] beskriver hvilket ansvar den enkelte ansatte har for å sikre konfidensialitet, tilgjengelighet, åpenhet og dataminimering. Eksempler på hva dette betyr i praksis er også beskrevet her. Eksempler på slike regler er:

- Person- og helseopplysninger skal ikke deles på e-post, Teams, SMS eller åpne medier på internett. Det skal kun brukes systemer/løsninger som er designet for formålet, og hvor det er gjennomført en ROS-analyse der risikoen ved behandling av disse opplysningene er akseptert.
- Passord skal beskyttes, de skal aldri «lånes ut».
- Bruk av programvare uten lisens og bilder uten tillatelse er forbudt.
- Maskinen må låses eller slås av når man er borte fra arbeidsplassen.
- Sjekk av hvilken skriver som brukes før man sender et dokument til utskrift, og prioritering av sikker print.
- Minnepinner som man ikke kjenner innholdet av, må kontrolleres for datavirus før de blir tatt i bruk.

Det er beskrevet regler rundt informasjonssikkerhet og bruk av følgende handlinger:

- E-post
- Teams/samarbeidsplattformer
- Arbeidsgivers tilgang til internett og andre ressurser
- Utstyr
- Sosiale medier
- Personopplysninger, behandling av sensitive personopplysninger
- Avviksmeldinger og feil og forpliktelse til å sende avvik
- Mistanke om data-angrep
- Avslutning av arbeidsforhold.

IKT-sikkerhetsinstruksen (datavettreglene) omtaler rutiner for hvilke tiltak som må gjennomføres ved mistanke om dataangrep.

6.2.2.4 Sikkerhetsorganisasjonen i Nord-Odal kommune

I Compilo blir sikkerhetsorganisasjonen i Nord-Odal beskrevet. Her fremgår en beskrivelse av organiseringen etter det ulike ansvaret hver av rolleinnehaverne i kommunen har. [24] En del av beskrivelsene i dette dokumentet fremgår også av Normens veileder om internkontroll for informasjonssikkerhet og personvern. [25] Alle ansatte forplikter seg ifølge dokumentet «Sikkerhetsorganisasjonen i Nord-Odal kommune» å sørge for at de gjør seg kjent med kommunens

[23] IKT-sikkerhetsinstruks – datavettregler, Compilo 17. januar 2022
[24] Sikkerhetsorganisasjonen i Nord-Odal kommune, Compilo
[25] Normens veileder om internkontroll for informasjonssikkerhet og personvern v1.0, side 10-12

internkontrollsystem, inklusive rutiner for å melde avvik. Her står det også at alle skal tilegne seg nødvendig kunnskap for å bruke systemene. Andre roller og oppgaver som er beskrevet i tilknytning til sikkerhet er:

- Enhetsledere
- Ledere med personalansvar
- Medlemmer av kommunedirektørens ledergruppe
- Kommunedirektør/informasjonssikkerhetsansvarlig
- Personvernombud
- IKT-konsulent
- Systemforvalter
- Hedmark IKT
- Sikkerhetsansvarlig Hedmark IKT
- IKT-sikkerhetskoordinator

6.2.2.5 Informasjonssikkerhet, risikostyring, risikoanalyse

Kommunens dokument ved navn «Informasjonssikkerhet, risikostyring, risikoanalyse» [26] har til hensikt å beskrive Normens krav til risikohåndtering, risikoanalyse og vurdering av personvernkonsekvenser. Det er beskrevet innledningsvis i dokumentet at dette er en lettere omskrevet versjon av kapittel 3 i Normen. Videre beskriver det vurderingskriterier for ROS-analyse og lenker til behandlingsprotokoll delt på sektor og momentliste for ROS ved anskaffelse av datasystem, samt Compilos veileder for ROS-analyse.

6.2.2.6 Møtevirksomhet og møterutiner

Det beskrives i intervjuer at det skal gjennomføres en del møtevirksomhet:

- Det gjennomføres ledermøter hver 14. dag, og her kobles IKT-konsulent på som fagperson ved behov.

- Informasjonssikkerhetsansvarlig har jevnlig møter med personvernombud.

De største systemene som er i bruk, som for eksempel Visma min skole, Visma Profil og Websak, har såkalte «forvaltningsteam», der systemansvarlig og systemeiere i flere kommuner møtes jevnlig. Forvaltningsteammøtene gjennomføres i regi av HIKT.

6.2.2.7 Ledelsens gjennomgang

I mai 2022 godkjente kommuneledelsen en rutine er kalt «ledelsens gjennomgang – personvern». [27] Formålet med gjennomgangen er å sørge for at internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessig, tilstrekkelig og effektiv og at det tilfredsstiller relevante krav i personvernregelverket. Hensikten med ledelsens gjennomgang [28] er ifølge rutinebeskrivelsen:

- Sørge for at internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessige, tilstrekkelig og effektive og at det tilfredsstiller relevante krav i personvernregelverket.
- Følge opp mål som er satt.
- Vurdere oppfølging av korrigerende tiltak.
- Endring av mål for prosess.

Rutinen definerer også oppgaver og ansvar tilknyttet systemeiere og systemansvarlige.

Kommunedirektøren er blant annet ansvarlig for utarbeidelse og etterlevelse av korrekte rutiner for informasjonsbehandling, etablering og oppfølging av databehandleravtaler og beredskap innenfor

[26] Dokument i Compilo, opprettet 29. august 2022
[27] Compilo, 11.juli 2022
[28] Hentet fra rutinebeskrivelse i kvalitetssystemet Compilo: «Ledelsens gjennomgang – personvern» - Compilo 22. juli 2022

informasjonssikkerhet[29]. Kommunedirektøren har blant annet et overordnet ansvar for kommunens informasjonssikkerhetsstrategi, godkjenne akseptabelt risikonivå og vedta, implementere og følge opp bruken av styringssystem for informasjonssikkerhet. Organisasjonen har også personvernombud, IKT-konsulent og IKT-sikkerhetskoordinator. De to sistnevnte funksjonene bekles av samme person. Kommunen har også systemforvaltere og systemansvarlige for de ulike systemene som er i bruk. [30]

Det er også et krav etter Normen [31], at det minimum skal gjennomføres et årlig møte med ledelsen. Dette omtales som «ledelsens gjennomgang» i ulike faglige veiledere. Ifølge IKT-konsulent brukes kommunens sikkerhetsmål som et utgangspunkt for å utarbeide tiltak, og korrigerende tiltak. Ifølge IKT-konsulent følger Nord-Odal kommune Datatilsynets retningslinjer for internkontroll når det gjelder ledelsens gjennomgang. [32]

Ifølge referatet fra ledelsens gjennomgang i mai 2022, ble følgende gjennomgått:

- *Sikkerhetsmål og strategi.*
- *Roller, funksjoner og struktur*. Ledelsen gikk her gjennom den tidligere nevnte beskrivelsen av «sikkerhetsorganisasjonen i Nord-Odal kommune».
- *Oppfølging av protokoller innen personvernforordningens artikkel 30*. Ledelsen gikk her gjennom arbeidet med behandlingsprotokoller for hvert kommunalområde. Det er beskrevet at gjennomgangen gjennomføres i samarbeid med personvernombudet. Det blir vist til at barnevern og PPT allerede har gjennomført dette på tvers av de samarbeidende kommunene. Her har de konkludert at oversikt over behandlinger er mangelfullt.
- *HIKT-samarbeid.* Ledelsen gikk her gjennom HIKTs vurderinger om det skal opprettes en felles løsning som blant annet ivaretar krav til føring og oppfølging av protokoller. Målet er at kommunene skal kunne samarbeide bedre, og er en del av prosjektet «rett og rimelig». Prosjektet skal se på hva kommunene kan gjøre i fellesskap, eks. ROS- analyser, rutiner og maler.
- *Avviksgjennomgang informasjonssikkerhet og personvern 2021.*
- *Vurdering av endringer i omfang av internkontroll*
- *ROS-analyser.* Ledelsen gikk her gjennom ROS-analyser for kommunens systemer og kom frem til at flere systemer mangler ROS-analyser, samt at enkelte ROS-analyser for systemene ikke er ført i Websak. Dette skulle følges opp i neste ledermøte.
- *KiNS kurs – informasjonssikkerhet*. Det ble bestemt at kommunens ledere skulle gjennomføre dette e-læringskurset før 15.6.2022, og at ansatte skulle gjennomføre aktuelle kurs innen 30.9.2022.
- *Virksomhetskritisk informasjon/og eller systemer.* Ledelsen gikk her gjennom fremdriften i en kartlegging for å finne ut hvilke avdelinger som har manuelle rutiner i tilfelle nedetid (for eksempel som følge av strømbrudd eller datainnbrudd). Det ble konkludert med at det gjenstår en del jobb i forbindelse med kartlegging og nedfelling av rutiner.

[29] Kommunelovens paragraf § 13-1 og § 25-1 (s
[30] Sikkerhetsorganisasjonen i Nord-Odal kommune, Compilo 23. mars 2021, revidert 11.juli 2022
[31] Normen v6, side 14
[32] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/vedlegg/

Det ble ifølge IKT-konsulent også gjennomført et møte med tema informasjonssikkerhet og personvern i øverste ledelse i mars 2021. Temaer i møtet var:

- Flytting og organisering av dokumentasjon og retningslinjer fra KFK til Compilo.
- Oppfordring fra personvernombudet om at det var viktig med ledelsens gjennomgang.
- I tillegg gikk ledelsen igjennom en del relevante rutiner/retningslinjer og reviderte de – deriblant ble grunnlaget for beskrivelsen av «Sikkerhetsorganisasjonen i Nord-Odal kommune» lagt.

I og med at rutinen for ledelsens gjennomgang ble utformet i mai 2022, og det under kontrollen kun er gjennomført et slikt møte, er det forholdsvis lite data om hvordan ledelsen har fulgt opp informasjonssikkerhet.

6.2.3 Øvrige rutiner og prosedyrer som skal sikre riktig tilgang og informasjonshåndtering

6.2.3.1 Tilgangsportalen og tilgangsstyring

Nord-Odal kommune har en egen prosedyre for tilgangsstyring som er lastet opp i «håndbok for informasjonssikkerhet». Dokumentet er udatert, men henviser til at det baserer seg på Normens føringer. Formålet med tilgangsstyringsrutinen er å sikre at informasjon kun er tilgjengelig etter tjenstlig behov. Dette innebærer at brukere autentiseres på en betryggende måte og at tilganger tildeles, administreres, kontrolleres og fjernes.

HIKT har en web-basert tilgangsportal for bestilling av tilganger, denne brukes i Nord-Odal kommune. IKT-konsulent har forklart at det er lederne som administrerer tilganger i tilgangsportalen. Ledere for enhetene har ansvar for å gi beskjed via skjema hvis det er endringer i den ansattes tilganger på deres avdeling. Dette for å sikre at den ansatte får den tilgangen vedkommende trenger for å utføre jobben sin. Ved nyansettelser kommer det bestillinger gjennom HIKT sin tilgangsportal. Ifølge systemansvarlig for Websak, så er ikke alle ledere like flinke til å melde riktig, eller at det kan bli avglemt. Systemansvarlig Websak ga uttrykk for at det mangler gode rutiner på dette området. Systemansvarlig for Websak forklart videre at når det gjelder systematisk gjennomgang av tilganger så foreligger det ikke en skriftlig rutine på dette.

Informasjonssikkerhetsansvarlig mener at tilgangsportalen er et godt hjelpemiddel for å opprettholde og vedlikeholde rett tilgjengelighet for rett bruker.

6.2.3.2 Behandlingsprotokoller

Ifølge kommunedirektørens verktøykasse for informasjonssikkerhet bør en kartlegging av informasjonsverdier være en del av det overordnete arbeidet som gjelder sikkerhetsstrategien og grunnlag for vurdering av tiltak eller en tiltaksplan i organisasjonen.

Det er en prosess i gang med å utarbeide behandlingsprotokoller for alle sektorer. Prosjektet ble satt i gang våren 2022 og skal avsluttes i november i 2022. Behandlingsprotokollen er utarbeidet etter en mal fra Datatilsynet. [33]

Kommunen har ikke bevisst jobbet med kartlegging av hvilken informasjon som må beskyttes mer enn annen informasjon, ifølge informasjonssikkerhetsansvarlig. Det er en del informasjonssystemer som er definert som sårbare gjennom ROS-analyser, men ifølge informasjonssikkerhetsansvarlig har imidlertid ikke kommunen gjennomført ROS-analyser for alle informasjonssystemene.

Informasjonssikkerhetsansvarlig har gitt uttrykk for at databehandlingsprotokollene kan være et viktig verktøy for å vise til hvilke programmer det kan være nødvendig å gjennomføre ROS-analyser og eventuelt DPIA-analyser for, og at dette kan legge grunnlaget for en helhetlig tiltaksplan hvor

[33] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/

informasjon med kritisk, høy, middels og lav verdi er kartlagt, samt at det da kan foreligge en tiltaksplan for hva kommunen skal gjøre ved brudd på informasjonssikkerheten.

6.2.3.3 Databehandleravtaler

Hensikten med å ha en databehandleravtale er å synliggjøre hvilke personopplysninger som lagres hvor og til hvilket formål. Det er også viktig å synliggjøre ansvarsforhold og hvem som har tilgang til opplysningene.[34] I informasjonshåndboka til Nord-Odal står det at alle systemer *skal* ha databehandleravtaler.

I Compilo er det et dokument som heter «Systemoversikt og klassifisering av systemer». Det er til sammen beskrevet 122 forskjellige systemer med informasjon om navn på system, leverandør, risikoaksept og tilgangssone samt databehandleravtale (om det fins eller ikke i tilknytning til systemet). Oversikten viser at noen systemer ikke har databehandleravtaler. Oversikten viser også at det er en del systemer der det fremstår som at det er uklart om det trengs avtale eller ikke, og det er mange av disse der det står et blankt felt under kategorien «databehandleravtaler». [35] Det er i tillegg noen systemer det står at det mangler databehandleravtaler for.

IKT-konsulenten har forklart at de ikke går inn aktivt og kontrollerer/kvalitetssjekker de som de har databehandleravtaler med, så lenge alt virker. Systemeier er den som skal utarbeide databehandleravtaler med leverandør. IKT-konsulenten har forklart at systemeieransvaret som oftest er tillagt kommunens kommunalsjefer. Det er ifølge IKT-konsulent ikke en egen kvalitetssikringsrutine som sikrer at databehandleravtaler kommer på plass, eller sikrer at de er gode nok. IKT-konsulenten spørres noen ganger om råd i forbindelse med etablering og revidering av databehandleravtaler, og andre ganger ikke. Funn tidligere viser at dette ikke er en del av agendaen på ledelsens gjennomgang av informasjonssikkerhet.

6.2.3.4 Personvernombud

Det er etablert felles personvernombud for Nord-Odal, Sør-Odal, Kongsvinger, Eidskog, Åsnes og Grue kommuner. Kongsvinger kommune er vertskommune for samarbeidet. Personvernombudet er rådgiver for de samarbeidende kommunene slik at personopplysninger behandles på en trygg måte i tråd med personvernregelverket. [36] Personvernombudet skal også bistå innbyggerne med å ivareta sine rettigheter.

6.2.4 Visma Profil – kommunens pasientjournalsystem

Kommunens elektroniske pasientjournalsystem, Visma Profil, har ca. 300 brukere (ansatte). Det betyr at det er det systemet med flest brukere i Nord-Odal kommune. Profil er et system der ansatte har ulike roller med ulike tilganger ut ifra arbeidsoppgaver og de ansattes kompetanse; assistenter, sykepleiere, vernepleiere, ledere eller leger er eksempler på ulike roller. Disse rollene gir ulike tilganger i systemet. Det er til sammen 14 ulike tjenestegrupper som representerer ulike områder i helse og omsorgssektoren i kommunen; en tjenestegruppe er for eksempel et sykehjem, en bolig eller en avdeling i hjemmetjenesten og tilgangene på pasienter følger tjenestegruppene. Det er akkurat opprettet en ny tjenestegruppe som vil følge opp flyktninger, med bakgrunn i behovet som har oppstått i forbindelse med krigen i Ukraina.

Systemansvarlig for Profil har forklart at kombinasjonen av at systemet håndterer pasientinformasjon, samt har så mange brukere, stiller et stort krav til systemets brukere og deres evne og kompetanse til informasjonshåndtering. Systemansvarlig har videre opplyst at selve systemet er fysisk sikret uten integrasjoner til andre systemer, annet enn Folkeregisteret.

[34] Datatilsynet , om hvorfor det er viktig med databehandleravtaler
[35] Systemoversikt og klassifisering av systemer, Compilo 21.juli 2021
[36] Informasjonen er hentet fra Nord-Odal kommunes nettsider

Profil har to-faktorautentisering i pålogging. Det er krav til passord i form av tall, små og store bokstaver og bruk av spesialtegn som gir god sikkerhet med tanke på passordbruk. Systemansvarlig ga uttrykk for at Profil derfor er veldig vanskelig å penetrere utenfra.

Profil har en egen tilgangsrutine [37] som oppsummerer tilgangene i systemet. Systemansvarlig er ansvarlig for vedlikehold av tilganger/rollestyring i systemet. Hvis en ansatt sier opp og dennes konto opphører gjennom HIKT, så får systemansvarlig automatisk beskjed om å fjerne brukeren. Ved endringer i roller innenfor helse- og omsorgssektoren er systemansvarlig ansvarlig for å utforme kontrakter for bruk av Profil, og vedlikeholde endringer i tjenestegrupper (tjenestegrupper er den ansattes tilhørighet i ulike områder i helse og omsorgssektoren). Ledere for enhetene har ansvar for å gi beskjed via skjema hvis det er endringer i den ansattes tilganger på deres avdeling. Ved nyansettelser kommer det bestillinger gjennom HIKT sin tilgangsportal. Nord-Odal kommune deltar i et pilotprosjekt i regi av HIKT der man ser på automatisering av tilganger og tilgangsstyring. Per nå er det ledere som fyller ut skjema inne i sikker sone for å bestille tilganger – dette skal automatisere prosessen noe og føre til mindre personlige feil.

I følge systemansvarlig er tilgangene styrt med dokumentasjonskrav hvis det oppstår behov for utvidet tilgang, en såkalt «blålysrolle». Utvidelse av roller går alltid via systemansvarlig, og betyr i praksis tilgang på mer informasjon/personopplysninger. Systemansvarlig har forklart at hjemmetjenesten bruker Profil offline på nettbrett når de er ute hos brukerne. Pasientjournalene/Visma Profil oppdateres så etter hvert skift gjennom påkobling til Visma profils nett. Visma profils system loggfører all aktivitet som brukerne gjennomfører.

Rutinen for tilgangsrettigheter beskriver regler for systemets bruk. Blant annet skal ansatte bare innhente informasjon om de pasienter som det er relevant å hente frem i arbeidssammenheng – det vil si tjenstlige behov. Det føres hele tiden logg i forhold til all aktivitet i systemet. Hvis ledere mistenker at en ansatt har gått inn på en bruker som vedkommende ikke skal inn på – såkalt «snikinnsyn» – så skal de melde fra til systemadministrator, som er de eneste som kan kontrollere denne typen aktivitet.

Systemansvarlig har i intervju fortalt at Compilo skal være kjent som et avvikssystem for ansatte i helse og omsorg, selv om det er generelt lite avviksmeldinger i helse- og omsorgstjenestene. De fleste avvik handler om medisinhåndtering. Systemansvarlig forklarer videre at avvik blir tematisert og jobbet med i personalmøter, eller i de fora der det er behov for å lukke dem.

6.2.5 Websak – kommunens sak- og arkivsystem

Websak er kommunens postjournal, arkiv- og saksbehandlersystem, med 110 brukere, og er levert av Acos. Fagleder for Arkiv er systemansvarlig for Websak. Systemansvarlig for Websak i Nord-Odal kommune er med i «forvaltningsteam Arkiv» sammen representanter fra Sør-Odal, Kongsvinger og Grue kommuner.

Systemansvarlig har forklart at systemet er bygd opp slik at det er satt opp roller i systemet som sikrer tilgangsstyring automatisk. Systemansvarlig har gitt uttrykk for at det også er lett å gjøre endringer i rollene ved behov uten at det er større risiko involvert i dette. Systemansvarlig involverer Acos når det er ønskelig å sikre at det ikke gjøres endringer som kan gå ut over annen funksjonalitet i systemet. Rollene som saksbehandlere/brukere i systemet har, legger begrensninger for hva saksbehandler selv kan gjøre av endringer på sak/journalpost. Systemansvarlig opplever å få tilbakemelding fra brukerne om at tilgangsstyringer nesten kan oppleves som *for* strengt noen ganger. Systemansvarlig har oppgitt at det har blitt gjennomført et grunnarbeid for å skape tydelige og godt oppbygde roller, som sammen med rutinene for skjerming av dokumenter, skal sikre informasjonssikkerhet og personvernet. For eksempel har Nord-Odal kommune gjort et grep der de ikke opprettet elevmapper og personalmapper

[37] «Tilgangsrettigheter i Profil» Compilo, 22. mars 2021 sist revidert 18. januar 2022

per person, men knytter de til emnebaserte mapper, som for eksempel: Tilsettinger, permisjoner og sykemeldinger. Systemansvarlig forklarer at fordelen er at det er mulig å tilgangsstyre dette bedre enn når man samler alle saker tilknyttet en person en all informasjon i en mappe.

Systemansvarlig har forklart at en svakhet ved Websak er at sak-arkivsystemets dokumenter må «sjekkes inn» for at dokumentet skal finne tilbake til sin fil-sti i Websak. Gjøres ikke dette, vil dokumentet bli liggende på et temp-område og kan, om Hedmark IKT gjør en rydde/slettejobb her, miste sitt innhold. Prosessen er tydelig beskrevet i rutiner og brukerdokumentasjon men ikke alle brukerne er like flinke til å huske på dette, og data kan derfor gå tapt.

Systemansvarlig har også opplyst at det kan oppstå risiko for feil når saksbehandlere ferdigstiller dokumenter som ikke er skjermet eller som har feil skjerming. Brukere av systemet kan da ha tilgang til informasjonen i dokumentet uten at dokumentet er kvalitetssikret av Arkiv enda. Siden saker låses for endringer etter at saksbehandler har ferdigstilt dokumentet, kan for eksempel en sakstittel med for mye informasjon bli liggende tilgjengelig for brukerne av Websak. Det samme kan oppstå dersom skjermingskoder med hensyn til taushetspliktige opplysninger blir satt feil i dokumentet. Denne svakheten i systemet har eksistert så lenge Websak har eksistert. Systemansvarlig har forklart at det eneste man kan gjøre er å jobbe med å være så a jour som mulig, alle ansatte har også taushetsplikt.

Websak har loggføring. Man kan ikke se hvem som har sett på de ulike dokumentene, men alle endringer som blir gjort på sak/journalpost loggføres. Systemansvarlig Websak opplever det ikke som problematisk at innsyn ikke loggføres, da det meste er kvalitetssikret gjennom skjerming (å sette tilganger som er tilpasset innholdet). Det er ingen internkontrollrutiner på gjennomgang av logger per nå i Websak.

I følge systemansvarlig, så oppgraderte Nord-Odal Websak i mai i fjor, og kjøpte da også modulen WebSak+. Plussversjonen av Websak er webbasert, har et enklere grensesnitt og mer brukervennlighet enn Websak. Så langt er det kun ledere som har fått opplæring i pluss-versjonen. Systemansvarlig har i intervju forklart at innføringen av pluss-versjonen har gått noe sakte fordi kommunen ikke har nok ressurser til å gjennomføre intern opplæring. Systemansvarlig har oppgitt at ekstern opplæring fra leverandør er dyrt, derfor er foreløpig kun ledere prioritert. Websak+ er heller ikke utviklet med alle funksjoner slik at alle saksbehandlere kan benytte denne på nåværende tidspunkt. Dette gjelder for eksempel byggesaksbehandling. Det vil komme en egen modul som heter Acos Eiendom+ som vil ivareta saksbehandling av slike saker. Websak+ kan brukes på flere flater, også nettbrett og telefon.

6.3 Revisors vurdering

6.3.1 Vurdering av revisjonskriterium 1 – mål og strategi

Kommunen har en egen rutine kalt sikkerhetsmål og sikkerhetsstrategi. Sikkerhetsmålene og –strategien ble vedtatt av rådmannens ledergruppe den 18. mars 2021. Innholdet i dette dokumentet er hentet fra retningslinjer gitt av Normen for E-helse, og inneholder kommunens mål samt tiltakspunkter for å nå kommunens mål for informasjonssikkerhet og personvern.

Vi mener at revisjonskriterium 1 er etterlevd.

Kommunen har beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).

6.3.2 Vurdering av revisjonskriterium 2 – risikobasert internkontroll

Undersøkelsene våre viser at kommunen har rutiner og prosedyrer, som for eksempel sikkerhetsmål og sikkerhetsstrategi, ledelsens gjennomgang, sikkerhetsorganisasjonen med beskrivelser av ulikt ansvar i forbindelse med informasjonssikkerhet, nivå for akseptabel risiko, samt IKT-sikkerhetsinstruks.

Vi har tidligere vist til at informasjon fra intervjuer tyder på at det er et behov for å implementere disse i større grad. Vi har også vist til at HIKT-kommunene gjennom HIKT-samarbeidet er i ferd med å anskaffe et eget kvalitetssystem som etter planen skal ivareta internkontrollen på området i større grad enn i dag. Vi ser at ikke alle rutiner og prosedyrer ikke revideres årlig, som satt opp i kvalitetssystemet, da spesielt alle rutinene som ligger lenket til «håndbok for informasjonssikkerhet».

Flere av dokumentene/rutinene er nye i 2022. Det fremstår slik at avvikssystemet per i dag er lite brukt i organisasjonen, og at det beskrives at risikoanalyser ikke gjennomføres i alle sammenhenger. Vi ser at behandlingsprotokoll og en oversikt over alle manuelle rutiner mangler, slik at den fullstendige oversikten for å kunne ha en tilpasset risikobasert internkontroll er ikke på plass.

Nord-Odal kommune har på plass en formell struktur for å sikre en tilpasset og risikobasert internkontroll for informasjonssikkerhet, men har en vei å gå for å implementere dette over tid.

Vi mener derfor at revisjonskriterium 2 er delvis etterlevd.

Kommunen og dens øverste ledelse har en tilpasset og risikobasert internkontroll for informasjonssikkerhet. Internkontrollen inneholder både et strategisk og langsiktig perspektiv, samt et operasjonelt perspektiv som omhandler daglig virksomhetsstyring.

6.3.3 Vurdering av revisjonskriterium 3 – kartlegging av informasjonsverdier

Som vist til i kapittel 6.2.1, har vi fått opplyst at kommunen ikke har foretatt en kartlegging av informasjon med kritisk, høy, middels og lav verdi.

Vi mener derfor at revisjonskriterium 3 ikke er etterlevd.

Kommunen har gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi og har en tydelig tiltaksplan som viser hvem som er ansvarlig for tiltak knyttet til dette.

6.3.4 Vurdering av revisjonskriterium 4 – informasjonens integritet og konfidensialitet

Vi har undersøkt overordnede retningslinjer, samt rutiner tilknyttet Websak og Visma profil, og våre funn viser at kommunen har rutiner og prosedyrer som i stor grad kommuniserer viktigheten av at informasjon ikke blir endret utilsiktet eller av uvedkommende.

Vi ser imidlertid mangler på rutiner tilknyttet databehandleravtaler. Det finnes en oversikt som viser at det mangler databehandleravtaler på noen systemer, og kommunens IKT-konsulent har forklart at det heller ikke er en egen kvalitetssikringsrutine på dette, men at ansvaret ligger hos den enkelte systemeier. Vi mener at dette ikke gir en helhetlig sikring og oversikt av informasjonen og informasjonshåndteringen.

Vi mener at revisjonskriterium 4 er delvis etterlevd.

Kommunen har rutiner og prosedyrer som sørger for at alle i virksomheten sikrer at informasjon i alle former ikke blir kjent, eller endret utilsiktet eller av uvedkommende.

6.3.5 Vurdering av revisjonskriterium 5 – informasjonens tilgjengelighet

Våre undersøkelser viser at kommunen har rutiner og at systemene har en oppbygging som i stor grad sikrer tilgjengelighet ut ifra tjenstlig behov. Vi har imidlertid også vist til at Websak har svakheter som kan medføre at informasjon blir liggende tilgjengelig for ansatte uten tjenstlig behov, eller føre til at informasjon blir tapt.

Vi har også vist til at rutinene tilknyttet overordnet tilgangsstyring og tilgangsportalen generelt trenger å sikres bedre, da det kan skje at ledere glemmer å fjerne eller endre tilganger til ansatte.

Vi mener revisjonskriterium 5 er delvis etterlevd

Kommunen har rutiner og prosedyrer som sørger for at informasjon i alle former er tilgjengelig ut ifra tjenstlige behov.

6.3.6 Vurdering av revisjonskriterium 6 – ledelsens gjennomgang

Rutinene for ledelsens gjennomgang av informasjonssikkerhet ble vedtatt i ledergruppens møte i mai 2022, og første gjennomgang ble gjennomført i samme møte. I møteprotokollen finner vi at Nord-Odal i dette møtet har:

- vedtatt å etablere oppstart av arbeid med behandlingsprotokoll
- gått gjennom organisering roller, funksjoner og struktur
- gått gjennom og vurdert avviksbehandling.

Vi kan imidlertid ikke se at de har gått gjennom:

- oppfølging av leverandører
- databehandleravtaler og
- vurdert endringer i nivået for akseptabel risiko.

Det ble ikke presentert resultater av risikovurderinger og personvernkonsekvensutredninger utover at det rapporteres at flere områder enda mangler disse utredningene, og at det skal jobbes med å få på plass en oversikt.

Vi mener revisjonskriterium 6 er delvis etterlevd

Kriterium 6	Kommunens ledelse gjennomgår virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året. Følgende punkter skal gjennomgås: - Endringer i behandlinger av helse og personopplysninger (behandlingsprotokoll) - Endringer i organiseringen av arbeidet - Resultat av risikovurderinger og personvernkonsekvensutredninger - Resultat av avviksbehandling - Oppfølging av leverandører og databehandleravtaler - Endring i nivået for akseptabel risiko

6.3.7 Vurdering av revisjonskriterium 7 – dokumentasjon på gjennomgang

Protokollen vi har referert til i kapittel 6.3.6 er dokumentasjon på at ledelsen har gjennomgått virksomhetens informasjonssikkerhet.

Vi mener følgelig at revisjonskriterium 7 er etterlevd.

Ledelsens gjennomgang skal dokumenteres.

6.3.8 Oppsummert vurdering problemstilling 1

Vi har inntrykk av at kommunen har et planverk med rutiner og prosedyrer etablert i kvalitetssystemet Compilo. Mer enn halvparten av oppføringene under «informasjonssikkerhet og personvern» er lastet opp i 2022. Mange rutiner i kvalitetssystemet tilfredsstiller sentrale lovkrav og anbefalinger for informasjonssikkerhet, men vi anbefaler at det settes opp fast revidering av alle rutiner og prosedyrer også de som det er lenket opp til i opplastede dokumenter.

Tilgangsstyringsrutinene kan ifølge intervjuede glippe og har en svakhet ved seg da det skjer at ledere glemmer å oppdatere tilgangene ved endringsbehov hos ansatte.

Vi ser også at kommunen mangler en bevissthet rundt og en overordnet tiltaksplan som identifiserer hvilken informasjon som har høy, middels og lav verdi, og en plan for hvordan denne informasjonen skal forvaltes for å sikre god informasjonssikkerhet. Dette er i veiledere definert som et grunnleggende kartleggingsarbeid som legger forutsetninger for hvordan man skal sikre og håndtere informasjon.

7 Problemstilling 2 – Implementering av sikkerhetstiltak

Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?

7.1 Revisjonskriterier for problemstilling 2

Følgende er en tabell med de kriterier vi har benyttet for å besvare problemstillingen og våre vurderinger av disse. Kriteriene er gjengitt i kortform. For en full utledning av revisjonskriteriene, se vedlegg A. Tabellen er interaktiv og leseren kan gå rett til den enkelte vurdering ved å trykke på det enkelte kriteriet. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt i kapitlene nedenfor. Vi gjør derfor leseren oppmerksom på at vurderingene må sees opp imot de innhentede data i prosjektet.

	Kriterium 8	Kommunen må gjennomføre risikovurderinger på informasjons-sikkerhetsområdet.
	Kriterium 9	Kommunen skal ha en godkjent plan for sikkerhetsrevisjoner.
	Kriterium 10	Kommunen skal gjennomføre sikkerhetsrevisjoner jevnlig, disse skal være dokumenterte.
	Kriterium 11	Kommunen skal følge opp resultater fra disse sikkerhetsrevisjonene.
	Kriterium 12	Kommunen skal ha klare rutiner for avviksrapportering og håndtering.
	Kriterium 13	Kommunen skal ha planer for å gjenopprette normaltilstand etter en fysisk/teknisk hendelse som innebærer informasjon på avveie.

7.2 Innhentet data

7.2.1 Risikovurderinger/ ROS-analyse

«Informasjonssikkerhet – risikostyring, risikoanalyse (ROS) og DPIA» [38] er en rutine som overordnet beskriver hvordan Nord-Odal, sammen med HIKT, bruker Normen for E-helse som sitt grunnlag for informasjonssikkerhet. Det er også en egen ROS- og sårbarhetsanalyse-brukermanual i Compilo, samt en egen DPIA-mal.

IKT-konsulent har i intervju oppgitt at fokus på den daglige driften og løpende individuell oppfølging er det viktigste for å opprettholde god informasjonssikkerhet. IKT-konsulent har forklart at aktiv bruk av ROS-analyser gir et grunnlag for gode rutiner og bevisstgjøring av de valg som skal tas i forbindelse med informasjonssikkerhet. I kombinasjon med god sikkerhetskultur blant ansatte, har han gitt uttrykk for at dette, samlet sett, vil være et godt grunnlag for å unngå sikkerhetsbrudd eller feilhåndtering av informasjon. IKT-konsulenten har forklart at når ansatte i Nord-Odal kommune gjennomfører innkjøp av nye systemer, så er de ikke alltid like flinke til å kvalitetssikre med tanke på informasjonssikkerhet og personvern. Under intervjuet ble vi fortalt at systemeierne har ansvaret for å gjennomføre ROS-analyser, og at en del systemer som har blitt kjøpt inn mangler disse analysene.

IKT-konsulenten forklarer at systemansvarlige skal være deltakere i gjennomføring av ROS-analyser. IKT-konsulenten har fortalt at ROS-analyser og DPIA blir utarbeidet i fellesskap med HIKT når innkjøp gjennomføres sammen med HIKT. IKT-konsulent forteller at når det gjelder ROS-analyse så gjennomføres dette systematisk ved nyanskaffelser så lenge det går via innkjøpsansvarlig/IKT-konsulent.

[38] «Informasjonssikkerhet – risikostyring, risikoanalyse (ROS) og DPIA.» Compilo 29. august 2022

Ifølge informasjonssikkerhetsansvarlig er det gjennomført ROS-analyser for de største systemene, og for noen også DPIA-analyse (personvernkonsekvensvurdering), for eksempel for Profil. [39] Databehandlingsprotokoll og den jobben som gjennomføres ute i sektorene vil gi en fullstendig oversikt over hvilke programmer som enda trenger en risikovurdering og eventuelt en DPIA-analyse.

Ifølge IKT-konsulenten kunne økonomiavdelingen ha vært flinkere til å gjennomføre ROS-analyser ved endringer i systemer. IKT-konsulenten har også fortalt at skolene har blitt flinkere, og at de ofte konsulterer med IKT-konsulent som også er innkjøpsansvarlig, for å sikre at de overholder rutiner og krav før de foretar innkjøp. Dette gjelder særlig mindre systemer, der Nord-Odal ikke samarbeider med andre kommuner.

IKT-konsulenten har gitt uttrykk for at det kan mangle eller være mangelfullt med ROS og DPIA i helsesektoren i kommunen, blant annet er legesenteret et eksempel der ROS ser ut til å mangle i tilknytning til de systemene som de bruker. Dette er meldt som avvik til personvernombudet. Det kan bli aktuelt med en felles ROS for flere kommunale legesentre innenfor personvernombudets virkeområde.

Informasjonssikkerhetsansvarlig ga i intervju uttrykk for at risikovurderinger er en form for sårbarhets-scanninger. Informasjonssikkerhetsansvarlig har videre fortalt at hun mener at kommunen ikke har god nok internkontroll når det gjelder informasjonssikkerhet. Kommunen må jobbe videre med å systematisere og konkretisere sikkerhetsmålene og hva de skal bety i en hverdag for de ansatte. Dette, mener informasjonssikkerhetsansvarlig, vil bidra til en systematisk internkontroll.

Systemansvarlig for Websak vil påpeke at det oppleves at organisasjonen har blitt flinkere på å gjennomføre risikovurderinger generelt sett, og at det har blitt jobbet mye med dette de siste årene.

7.2.1.1 ROS-analyse i Websak og Websak+

Det er gjennomført to ROS-analyser for Websak i henholdsvis 2018 og 2019. [40] [41] Tema og vurderinger for disse risikoanalysene var:

- Manglende avviksmelding. Risikoen for feil er her vurdert som lav da det er så få som har denne tilgangen til systemet.
- Innsyn. Omtaler at dataskjermer må fysisk plasseres slik at uvedkommende ikke får innsyn i opplysninger på skjerm og skjermene må låses, eller systemet må legges ned hvis uvedkommende er i nærheten.
- Feilregistrering og forsinket registrering av informasjon, samt feil data registrert grunnet manglende kompetanse og lagring på feil sted. Det beskrevne tiltaket i analysen er å oppdatere rutinebeskrivelsen for å gjøre den mer oppdatert. Tiltak for manglende kompetanse er å forbedre kunnskap og opplæring rundt bruk av systemet.
- Nedetid i systemet over 15 minutter. Tiltak er ikke omtalt, annet enn at hvis nettet er nede vil det kunne bli behandling hvis det skjer over lengre tid.
- Glemt avlogging. Foreslått tiltak er å låse skjerm.
- Virusangrep, dataangrep, menneskelig lekkasjer av informasjon. Sannsynlighet for dette er vurdert som lav.

[39] Datatilsynets veiledning om vurdering av personvernkonsekvenser (DPIA)
[40] «Risikoanalyse Acos mottak», Lene Jeanette Østby 28. november 2018, oppdatert 12. mars 2019 av Synnøve Grenaker
[41] «Risikoanalyse Acos mottak, tillegg til tidligere ROS», Lene Jeanette Østby, Trine Jeanette Hansen og Paul Reidar Løsnesløkken, udatert.

- Mobile lagringsenheter på avveie. Blir vurdert som lite sannsynlig, fordi tilgangsstyringen er streng og det er få ansatte med tilgang.
- Tilgangspolicy og forglemmelser tilknyttet tilgangspolicy.
- Manglende opplæringsplan. Det blir vist til at det ikke fins egen opplæringsplan for nye brukere av systemet, det er få brukere av systemet og rutine for bruk foreligger. Det er derfor en akseptabel risiko at opplæringsplan ikke foreligger, ifølge analysen.
- Mellomlagring av visse dokumenter på temporært område (ikke i sikker sone) og overføring av dokument til feil mappe. Dette blir beskrevet som en økende problemstilling da noen dokumenter må mellomlagres og muligheten for at informasjon kan komme på avveie er tilstede. Løsningen er dialog med leverandør for å finne bedre løsning for lagring i sikker sone.
- Innbrudd (fysisk), innsyn på dataskjerm.
- Passord og brukernavn på avveie, vurderes som lite sannsynlig.

Ifølge systemansvarlig Websak ble det i «forvaltningsteam arkiv», gjennomført en ROS-analyse ved anskaffelse av Websak+ og Websak+ sin Teams-integrasjon. [42] Systemansvarlig har fortalt at WebSak+ er web-basert, og at man derfor har mulighet for å koble seg opp mot Websak utenfor HIKT sitt nettverk. Det er foreløpig ikke åpnet opp for bruk av Websak utenom HIKT-nettverket. Systemansvarlig har også gitt uttrykk for at kommunen har et ønske om at Teams-integrasjonen som Websak+ tilbyr, sikrer god informasjonshåndtering. Systemansvarlig forteller at det er et ønske blant lederne om overgang til Websak+ da spesielt lederne er mye på «farta» og ønsker mulighet til å gjennomføre enkel saksbehandling, slik som for eksempel å godkjenne oppgaver på sin mobil eller på et nettbrett.

Følgende ble analysert og vurdert i ROS-analysen:

- Brukerfeil, importerer feil dokumentasjon
- Mangel på opplæring og rutiner
- Mangler og feil på gradering av saker og dokumenter
- Manglende ressurser i forhold til kvalitetskontroll
- Manglende to-faktorautentisering
- Pålogging utenfor HIKT sitt nettverk

Spesielt manglende to-faktorautentisering og for lite ressurser til å foreta opplæring for alle ansatte er grunnen for at systemet ikke er tatt i bruk. To-faktorautentiseringsutfordringen skal være løst per juni 2022. Det ble utarbeidet en egen tiltaksliste som samlet alle funnene i ROS-analysen for å beskrive hva som måtte komme på plass for at Websak+ kunne innføres.

7.2.1.2 ROS-analyse i Visma profil

Det ble gjennomført risikoanalyser for Visma Profil i 2017 og 2019. [43] [44] [45] Risikoanalysene omhandlet vurderinger og tiltak ved hendelser som:

- Nedetid i systemet i forbindelse med manglende internett-tilgang, strømbrudd. Her skal det ifølge analysen finnes manuelle rutiner, samt at det skal være mulig å føre oppdateringer i Word i sikker sone mens systemet eventuelt er utilgjengelig.

[42] «Utkast 3 ROS Innføring av WebSak+ og TEAMS integrasjon» ved «Forvaltningsteam Arkiv», 7. mai 2021
[43] Profil: IKT-skker sone, risikoanalyse gjennomført av Paul Vidar Bjørndalen, 27. juni 2017
[44] Plassadministrasjon i Visma profil, risikoanalyse gjennomført av Paul Vidar Bjørndalen, 14. mars 2019
[45] Visma Profil, egenandelsmodulen, risikoanalyse gjennomført av Paul Vidar Bjørndalen, 28. mars 2019

- Hacking av påloggingstrafikken, virusangrep.
- At brukere installerer programvare eller har åpne usikre applikasjoner mens de bruker Profil, som kan føre til at sensitive opplysninger kommer på avveie. Her er One Time Password (OTP) et sikkerhetstiltak. Brukere skal ifølge analysen ikke ha mulighet for å installere egne program på denne typen PC-er.
- Glemt avlogging, brukere som ikke logger seg av systemet før de forlater datamaskinen (fare for personopplysninger på avveie), brukere som ikke slår av skjerm, og at skjermsparer med passord må være aktiv på maskinene. Skjermsparer slår seg på etter 2 minutter.
- Brukere som skriver passordet sitt i brukernavnfeltet.
- Snikinnsyn/snoking i pasientjournaler av ansatte, her er det utarbeidet rutiner som beskriver konsekvensene av snikinnsyn.
- Nettbrett på avveie, noen kan true det til seg. Dette er alltid en politisak hvis det skulle skje.
- Sensitive personopplysninger kommer på avveie grunnet klipp og lim mellom sikker og åpen applikasjon.
- At det glipper i tilgangsrutinen slik at tidligere ansatte fremdeles har tilganger i Profil. Her må det utarbeides en sikker rutine.
- Innsyn fra uvedkommende ved at de titter på skjerm eller bruker/ansatt låner bort PC-en sin.
- Feilregistrering av data grunnet manglende kompetanse, manglende dokumentasjon eller at feil informasjon kommer på feil person grunnet samme fornavn og/eller etternavn.
- Lister med brukernavn og passord er tilgjengelig for andre. Det blir vist til at passord ikke skal skrives ned.

Vi har fått oppgitt at Forvaltningsteamet, som består av systemansvarlige i Nord-Odal, Sør-Odal, Kongsvinger og Eidskog kommuner, jobber med en risikoanalyse og DPIA for Visma Profil som skal være klar i august 2022. Vi har ikke mottatt resultatet av disse.

7.2.2 Organiserte sikkerhetsrevisjoner – plan, dokumentasjon og evalueringer

Det finnes per i dag ikke en egen konkret plan for sikkerhetsrevisjoner i Nord-Odal kommune. Det henvises imidlertid i kommunens håndbok for informasjonssikkerhet til at kommunen benytter seg av Normens faktaark nummer 6 som veiledende for kommunens sikkerhetsrevisjoner. [46]

I faktaarket brukes følgende eksempler på hva sikkerhetsrevisjoner er/kan være:

- Kontrollere nødvendige sikkerhetstiltak i forhold til gjennomførte risikovurderinger
- Vurdere om sikkerhetstiltakene er tilstrekkelige
- Prosedyre for kontroll av hendelsessregistre
- Fysisk sikring av lokaler som benyttes til behandling av informasjon/helse- og personopplysninger
- Sikre at etablerte prosedyrer for sikkerhet benyttes og fungerer etter hensikten

Det er beskrevet i faktaarket at virksomhetens ledelse har et ansvar for at det gjennomføres sikkerhetsrevisjoner. Alle sikkerhetsrevisjoner skal dokumenteres og gjennomgås i forbindelse med ledelsens gjennomgang.

Ifølge IKT-konsulent viser resultater at Nord-Odal kommune, som del av HIKT, kommer godt ut på sårbarhets-scanninger gjennomført på oppdrag fra HIKT. Resultatene fra scanningene er ikke

[46] https://www.ehelse.no/normen/faktaark/faktaark-06-sikkerhetsrevisjon

offentlige, men innholdet blir gjengitt som orienteringssak i HIKT sitt sikkerhetsråd der IKT-konsulenten er medlem. HIKT driver et kontinuerlig sikkerhetsarbeid der såkalte penetrasjonstester bare er en del av arbeidet. Det gjøres for eksempel jevnlige tester internt fra HIKT på om folk bruker for enkle passord.

7.2.3 Kommunens avvikshåndtering og -rapportering

Compilo og kvalitetssystemet har retningslinjer for avvikshåndtering og -rapportering. Det er tilgjengeliggjort rutinebeskrivelser på hvordan man går fram i forbindelse med avvik og rapportering av avvik. Rutinen heter «melding av avvik» [47] og har blant annet til formål å identifisere avvik eller risiko for avvik snarest mulig, bedre måloppnåelse, forhindre gjentakelse av avvik og redusere risikoen for uønskede hendelser og tilstander. Alle ansatte i Nord-Odal kommune har etter rutinen ansvar for å melde avvik så snart som mulig. Det er den enkelte leder sitt ansvar å sørge for at avvik blir meldt og behandlet etter utarbeidete prosedyrer og rutiner. Det er 21 dagers frist for å behandle avviket, eller for eventuelt å løfte avviket til kommunedirektøren.

7.2.4 Manuelle prosedyrer og beredskap

Kommunen har en prosedyre ved dataavbrudd som sist ble revidert i 2016. [48] Prosedyren beskriver at det skal utarbeides egne tilpassede manuelle rutiner i alle avdelinger som sikrer følgende:

- Hvilken informasjon det er nødvendig å ha papirkopier av
- Hvem som er ansvarlig for å vedlikeholde og ta ut disse papirkopiene
- Skjemaer for manuelle registreringer
- Eventuelle elektroniske reserveløsninger

Hver sektor i Nord-Odal kommune har jobbet med en generell beredskapsplan. Ifølge IKT-konsulent er det ikke en egen beredskapsplan for informasjonssikkerhetsområdet i Nord-Odal kommune. IKT-konsulent har forklart at beredskapskoordinatoren ikke har jobbet nevneverdig med IKT-delen av beredskap. IKT-konsulenten har også fortalt at det ikke gjennomføres beredskapsøvelser der IKT-sikkerhet eller informasjonssikkerhet er tema.

Systemansvarlig har gitt uttrykk for at nedetid er en utfordring ved bruk av Visma profil. De siste årene har det vært flere tilfeller av nedetid på grunn av strømbrudd. Nødnettet har samtidig vært nede. I hjemmetjenesten er det derfor rutiner for at de til enhver tid har oppdaterte fysiske lister og rutiner for rapportering for å følge opp brukernes behov. Systemansvarlig mener at dette erfaringsmessig har gått bra. Ved strømbrudd er det likevel flere faremomenter som er knyttet til for eksempel medisinfordelingsmaskiner og trygghetsalarmer, som etter kort tid vil slutte å fungere. Hjemmetjenesten har oversikten over hvem som har trygghetsalarm og medisindisponeringsmaskiner i hjemmene sine.

Ved strømbrudd, er rutinene slik at ansatte ved brannvakta reiser til Sand Bosenter og Mo Bosenter for å assistere med transport av brukere, siden heisene også er ute av funksjon ved strømbrudd. Systemansvarlig for Profil forklarer at det ikke er egne beredskapsplaner/rutiner som adresserer nedetid tilknyttet datasystemer.

IKT-konsulenten har foretatt en kartlegging av praksis og rutiner i forbindelse med nedetid i kommunens systemer. Kartleggingshenvendelsen ble sendt ut til alle avdelinger i kommunen den 22. mars 2022, og svarfristen var satt til 1. april 2022. Resultatet av kartleggingen er delt med ledergruppa i mai i ledelsens gjennomgang. Av 29 forespurte avdelinger er det per 4. august 2022, 17 avdelinger som ikke har gitt tilbakemelding.

[47] Melding av avvik, rutine linket opp «håndbok for informasjonssikkerhet» i Compilo. Rutinen er datert.
[48] Prosedyren heter «prosedyre ved dataavbrudd» og er linket opp i «Håndbok for informasjonssikkerhet», Compilo 21. februar 2021.

IKT-konsulenten mener at mange helse- og omsorgsavdelinger har god praksis for å ivareta pasientsikkerhet hvis det skulle skje at deres systemer opplevde nedetid. Grunnlaget for at IKT-konsulent mener dette er at Nord-Odal kommune har hatt en del strømbrudd den siste tiden, og IKT-konsulent mener derfor mange har manuelle rutiner selv om de ikke er dokumenterte.

7.2.5 Praksiser som kan utgjøres trusler for informasjonssikkerheten

Såkalte «skyggesystemer» og rutiner/prosedyrer som går utenom de formaliserte og besluttede systemene og rutinene/prosedyrene, kan oppstå når det ikke er overordnede retningslinjer og opplæring tilknyttet bruk av digitale systemer, eller dersom datasystemene og digitale verktøy oppleves som tungvinne og/eller uhensiktsmessig utformet:

> «Når IT-systemene ikke harmonerer med brukernes behov, kan det oppstå såkalte «skyggesystemer» – stier i plenen. En del ansatte har litt for lav terskel for å ta i bruk egne verktøy, uten tanke på at dette gjør virksomheten sårbar.» [49]

Ifølge systemansvarlig i Websak, kan det være en viss fare for at det utvikles kultur for «skyggesystemer» eller tilpassede rutiner på funksjonaliteter i Websak, hvor systemet har visse svakheter.

Systemansvarlig har opplyst om at mange lagrer dokumentene på egne områder, før de lastes opp i Websak. Systemansvarlig mener at sak/arkivsystemer kan være litt «sære», i og med at alle dokumenter må sjekkes inn, eller lastes inn i systemet igjen etter at de har blitt jobbet med. Som tidligere nevnt kan saksbehandleren også miste den jobben man har gjort i dokumentet om man ikke går riktig fram. Konsekvensen kan være at noen velger å lagre dokumentet på eget område i stedet for i Websak. Systemansvarlig for Websak mener også at Office 365 og Teams er systemer hvor dokumentfangst kan bli utfordrende, og der innholdet/informasjonshåndteringen ikke er kartlagt.

Informasjonssikkerhetsansvarlig og Arkiv-avdelingen har sett at når en del ledere slutter så blir det oppdaget «skyggearkiver». Arkivene kan bestå av permisjonssøknader og liknende som ledere har valgt å beholde i papir-form. Dette har ført til en bevisst gjennomgang med andre ledere for å få avsluttet en slik type kultur. Permisjonssøknader er et eksempel, der ledere har beholdt fysiske eksemplarer og oppbevart dem på sitt kontor. Vi har fått opplyst at denne praksisen nå i liten grad er eksisterende.

Microsoft Teams er et eksempel der informasjonssikkerhet og personvern kan være sårbart. Informasjonssikkerhetsansvarlig deltar i et prosjekt i samarbeid med HIKT, kalt M365, [50] som har som målsetning å lage felles retningslinjer som skal sikre sikker behandling av og gode rutiner for informasjon, blant annet i Microsoft Teams. Alle kommunene har utpekt personer som skal være ansvarlige for å følge dette opp. Informasjonssikkerhetsansvarlig forklarer at de ansvarlige skal gjennomføre opplæring i alle kommunens enheter. Opplæringen skulle starte i september 2022. Informasjonssikkerhetsansvarlig mener at kommunen har en høy bevissthet på bruk av Teams og at det ikke skal være deling av personopplysninger over Teams.

Ifølge IKT-konsulenten er det et problem at ansatte oppretter kontoer på nettet i Nord-Odal kommunes navn, for eksempel i forbindelse med innkjøpsbehov. Per nå er dette vanskelig å fange opp, både når vedkommende er ansatt og også om disse kontoene termineres når ansatt slutter.

[49] https://www.habberstad.no/fagblogg/it-sikkerhet-slik-sikrer-du-riktig-handtering-av-informasjon
[50] https://www.hedmark-ikt.no/prosjekter/m365/

7.3 Revisors vurdering

7.3.1 Vurdering av revisjonskriterium 8

Kommunen har retningslinjer for gjennomføring av risikovurderinger, eller ROS-analyser. Våre undersøkelser viser at dette gjennomføres i en del av systemene og informasjonssikkerhetsansvarlig har bekreftet at de største systemene har ROS-analyser på plass. Det bekreftes også under intervjuer at det ikke gjennomføres systematisk eller blant alle enheter, og at det per i dag mangler ROS-analyser og DPIA-er for noen systemer i Nord-Odal kommune.

Informasjonssikkerhetsansvarlig og IKT-konsulent mener at arbeidet med utarbeidelse av behandlingsprotokoller, som skal ferdigstilles i løpet av november 2022, vil vise hvilke systemer som mangler ROS-analyser og DPIA per i dag.

Vi mener at revisjonskriterium 8 er delvis etterlevd.

Kommunen må gjennomføre risikovurderinger på informasjonssikkerhetsområdet.

7.3.2 Vurdering av revisjonskriterium 9

Vi finner ikke at Nord-Odal har en egen plan for sikkerhetsrevisjoner.

Vi mener at revisjonskriterium 9 ikke er etterlevd.

Kommunen skal ha en godkjent plan for sikkerhetsrevisjoner.

7.3.3 Vurdering av revisjonskriterium 10

Ledelsens gjennomgang og revidering av etablerte rutiner i kommunens kvalitetssystem, er former for sikkerhetsrevisjoner og internkontroll som vi kan se gjennomføres per i dag. Vi har imidlertid inntrykk av at sikkerhetsrevisjoner ikke er satt i et system, ei heller at det jobbes systematisk og bevisst med sikkerhetsrevisjoner i kommunen. Ifølge IKT-konsulent gjennomføres det også jevnlig sårbarhetsscanninger i regi av HIKT som en del av deres faste sikkerhetsrevisjoner.

Vi mener at revisjonskriterium 10 er delvis etterlevd.

Kommunen skal gjennomføre sikkerhetsrevisjoner jevnlig, disse skal være dokumenterte.

7.3.4 Vurdering av revisjonskriterium 11

Vi viser her til vår vurdering av revisjonskriterium 10. Vi er kjent med at ledelsens gjennomgang og etablerte rutiner og prosedyrer i Compilo er revidert, og at det i dokumentasjonen fra ledelsens gjennomgang er planlagt sikkerhetstiltak for å følge opp resultater. Vi har imidlertid inntrykk av at sikkerhetsrevisjonene ikke følger en fast plan/er satt i et system, eller at det jobbes systematisk og bevisst med sikkerhetsrevisjoner i kommunen.

Vi mener at revisjonskriterium 11 er delvis etterlevd.

Kommunen skal følge opp resultater fra disse sikkerhetsrevisjonene.

7.3.5 Vurdering av revisjonskriterium 12

Våre undersøkelser viser at Nord-Odal kan vise til rutiner for avviksrapportering og håndtering. Disse er å finne i kvalitetssystemet Compilo.

Vi finner revisjonskriterium 12 etterlevd.

Kommunen skal ha klare rutiner for avviksrapportering og håndtering.

7.3.6 Vurdering av revisjonskriterium 13

Nord-Odal har beskrevet egne overordnede rutiner ved dataavbrudd, datainnbrudd eller nedetid. Rutinen har ikke blitt oppdatert siden 2016, og bør revideres på lik linje med alle øvrige rutiner som er lastet opp i Compilo. IKT-konsulenten har vist til at 12 av 29 avdelinger kan vise til at de har manuelle rutiner. De øvrige hadde ved intervjuets gjennomføring ikke besvart IKT-konsulentens henvendelse. Henvendelsen skulle, ifølge satt frist, ha blitt besvart i april 2022.

Beredskapsplanen har ikke en egen del som omhandler IKT-sikkerhet.

Vi mener derfor at revisjonskriterium 13 er delvis etterlevd.

Kommunen skal ha planer for å gjenopprette normaltilstand etter en fysisk/teknisk hendelse som innebærer informasjon på avveie.

7.3.7 Oppsummert vurdering problemstilling 2

Vi finner at kommunen til dels har iverksatt anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon. Nord-Odal gjennomfører ROS-analyser og DPIA, men ikke gjennomgående. I følge våre undersøkelser er det økende aktivitet på disse former for analyser, og blitt gjennomført forbedringsaktiviteter tilknyttet dette. I Compilo er det beskrevet rutiner for dette arbeidet.

Vi finner at det utføres former for sikkerhetsrevisjoner, uten at det er en overordnet plan, eller systematisk oversikt for dette.

Implementering av en god del aktiviteter og rutiner er i startfasen, som for eksempel ledelsens gjennomgang og arbeidet med å utarbeide behandlingsprotokoller for alle behandlingsaktiviteter i fagsystemene.

Kommunen har rutiner for avvikshåndtering og rapportering.

8 Problemstilling 3 – Praktisering av informasjonssikkerhet

I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

8.1 Revisjonskriterier for problemstilling 3

Følgende er en tabell med de kriterier vi har benyttet for å besvare problemstillingen og våre vurderinger av disse. Kriteriene er gjengitt i kortform. For en full utledning av revisjonskriteriene, se vedlegg A. Tabellen er interaktiv og leseren kan gå rett til den enkelte vurdering ved å trykke på det enkelte kriteriet. Vurderingene er knyttet til de data som er samlet inn og som blir gjengitt i kapitlene nedenfor. Vi gjør derfor leseren oppmerksom på at vurderingene må sees opp imot de innhentede data i prosjektet.

	Kriterium 14	Kommunen bør kartlegge kompetansebehovet blant ansatte for å sikre god praktisering av informasjonssikkerhet.
	Kriterium 15	Kommunen bør ha rutiner som gir den enkelte ansatte overordnet og tilpasset opplæring i hvordan ivareta informasjonssikkerheten og personvernet.
	Kriterium 16	Kommunen bør ha rutiner og tiltak som sikrer kontinuerlig og tilstrekkelig kompetanse for å kunne ivareta informasjonssikkerheten i organisasjonen.

8.2 Innhentet data

Ivaretakelse av informasjonssikkerhet og personvern fordrer at ansatte har gode arbeidsrutiner og en klar bevissthet rundt sikkerhet ved bruk av digitale hjelpemidler. [51] De ansattes bidrag og praksis er en viktig del av god informasjonssikkerhet. Etterlevelse, riktig teknologi, god virksomhetsstyring, risikovurderinger og kontinuitet er alt sammen avhengig av menneskers ferdigheter og kunnskap. I en virksomhet favner informasjonssikkerhet alle og krever at alle bidrar og har riktig kunnskap i forhold til hvordan de hjelper til med å sikre informasjonssikkerheten. [52] Temaene i spørreundersøkelsen kaster lys over atferd og kompetanse i tilknytning til informasjonssikkerhet blant ansatte. Dokumentasjon og intervjuer belyser i hvilken grad det jobbes med å kartlegge kompetanse, opplæring og kompetanseutvikling, samt rutiner og sikkerhetstiltak ute i kommunens enheter og blant den enkelte ansatte. De følgende temaene som er kontrollert med hensyn til problemstilling 3, må sees i sammenheng med beskrivelsene vi har gitt under de to foregående problemstillingene.

8.2.1 Kompetansekartlegging

I retningslinjene for «opplæring av ansatte – IKT og informasjonssikkerhet» [53] står det følgende:

> «Nord-Odal har ikke nå en systematisk dokumentasjon på hva den enkelte har tilegnet seg av kompetanse innenfor informasjonssikkerhet og bruk av IKT-systemer. Det er et mål å finne bedre løsninger på dette.»

Slik vi forstår det, er det med andre ord ikke foretatt kartlegging som omhandler informasjonssikkerhet og ansattes kompetanse per januar 2022.

[51] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet
[52] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet
[53] *Opplæring av ansatte – IKT og informasjonssikkerhet*, Compilo, 18.januar 2022, side 2

Det anbefales videre i disse retningslinjene at ledere skal benytte seg av medarbeidersamtaler som et verktøy for å få bedre oversikt over de ansattes kompetanse og behov for opplæring. Dokumentet «Sikkerhetsorganisasjonen Nord Odal kommune» beskriver oppgaver og ansvar som de ulike har i tilknytning til IT-systemene som kommunen bruker, og også litt rundt hva kommunen mener å trenge av kompetanse og opplæring i tilknytning til de ulike rollene.

8.2.2 Kommunens organiserte opplæring av ansatte på informasjonssikkerhetsområdet

8.2.2.1 Rutinebeskrivelsen «opplæring av ansatte – IKT og informasjonssikkerhet»

Rutinebeskrivelsen «Opplæring av ansatte – IKT og informasjonssikkerhet» [54] har til formål å beskrive på et overordnet nivå hvordan opplæring av ansatte i Nord-Odal kommune skal foregå. Her er det beskrevet at ledere til enhver tid skal ha oppdatert kompetanse for å kunne ta stilling til risikohåndtering i virksomheten, og at de skal kjenne til gjeldende krav til informasjonssikkerhet og personvern på området de har ansvar for. Utover dette står det at:

- Ledere har ansvar for at de ansatte får nødvendig opplæring i de ulike fagsystemene.
- Det skal gis beskjed når det kommer aktuelle kurs som er aktuelt for den individuelle ansatte.
- Det er viktig at alle ansatte deltar på nasjonal sikkerhetsmåned og leser informasjon som sendes om dette temaet.
- Den beste opplæringen er å gjøre ting i praksis ut fra behov.
- Ellers er det listet opp ideer til hva Normen beskriver som hensiktsmessige måter å gjennomføre opplæring på.

8.2.2.2 Opplæring

Det skulle ifølge informasjonssikkerhetsansvarlig gjennomføres *KiNS-kurs* for alle ansatte i september 2022. KiNS står for: foreningen for kommunal informasjonssikkerhet. KINS-kursene er e-læringskurs om informasjonssikkerhet og personvern. Dette er korte videoer som forklarer hvordan brudd på informasjonssikkerheten kan oppstå og hva konsekvensene kan bli, hvordan man forebygger disse og hva man gjør hvis uhellet er ute.

Disse små sikkerhetsfilmene omhandler:

- Bruk av e-post
- Taushetsplikt
- Brukerident og passordsikkerhet
- Forsvarlig lagring av data
- Oppslag i fagsystemer (må være i jobbsammenheng, ikke lov med snikinnsyn)
- Mobilsikkerhet
- Phishing
- Ransomware

Informasjonssikkerhetsansvarlig har i intervju fortalt at informasjonssikkerhetsansvarlig og IKT-konsulent i samarbeid med HIKT bruker tid under nasjonal sikkerhetsmåned til å bevisstgjøre og lære opp ansatte generelt om IT-sikkerhet. Informasjonssikkerhetsansvarlig bidro til at det ble gjennomført et e-læringskurs om informasjonssikkerhet i oktober i 2021. Dette kurset hadde dårlig deltakelse på tvers av HIKT-kommunene, men tilbakemeldingen fra HIKT var at Nord-Odal var en av de kommunene med høyest deltakelsesprosent. IKT-konsulent har opplyst om at det ellers kommer ulike kurs og drypp

[54] *Opplæring av ansatte – IKT og informasjonssikkerhet*, Compilo, 18. januar2022, side 2

av informasjon tilknyttet informasjonssikkerhet. IKT-konsulenten mener at dette er en god måte å lære opp ansatte på.

8.2.2.3 Websak og Websak+ og opplæring

Systemansvarlig har i intervju oppgitt at hun gjennomfører kurs for nyansatte som skal jobbe med og i Websak. Systemansvarlig er imidlertid bekymret over at det ikke gjennomføres oppfriskningskurs med jevne mellomrom og ved større endringer i systemet. Dette skyldes blant annet kapasitetsutfordringer. Likevel kan det bli gjennomført oppfriskningskurs dersom det etterspørres fra avdelinger eller saksbehandlere.

Kurset for nyansatte skal også være en innføring i saksbehandling der offentlighetsloven og forvaltningsloven er sentrale. Systemansvarlig for Websak savner at nyansatte får mer organisert oppfølging og kjennskap til offentlighetsloven og mer saksbehandlerkompetanse, spesielt nyansatte med lite bakgrunn fra offentlig forvaltning.

Systemansvarlig for Websak forteller at opplæring og bruk av Websak+ foreløpig bare er innført hos ledelsen. Det ligger begrensninger i budsjettet for å innføre flere moduler av systemet, noe som gjør at det gamle systemet fortsatt er i bruk.

8.2.2.4 Visma profil og opplæring i hjemmetjenesten

Alle som kjører ruter i hjemmetjenesten har egne nettbrett som de bruker for å loggføre aktiviteter i Visma Profil. Alle nyansatte i hjemmetjenesten følger en annen ansatt i fire dager for å få opplæring i tjenstlige oppgaver, bruk av utstyr (også digitalt utstyr og pasientjournal), relevante rutiner og kvalitets- og avvikssystem. Det er en egen sjekkliste for opplæring som er utarbeidet av leder i hjemmetjenesten. Systemansvarlig for Visma Profil har forklart at det ikke fins et overordnet opplæringsopplegg som følges generelt av helse- og omsorgssektoren, og som omhandler Normen, rutiner eller som går spesifikt på informasjonssikkerhet og personvern.

Systemadministrator mener imidlertid at det i helse- og omsorgssektoren er begrenset hvor mye de ansatte sjekker e-post, eller har fått lært om Compilo. Systemadministrator mener at opplæring i Compilo kan gjennomføres i personalmøter med ansatte. Utover dette har systemansvarlig forklart at hun og ledere i hjemmetjenesten har egne sjekklister som beskriver alle punkter for opplæring som nyansatte skal gjennom i oppstarten.

Ifølge IKT-konsulenten har mange ansatte, og kanskje spesielt de som jobber i helse og omsorg, god kompetanse når det gjelder å tenke sikkerhet i informasjonshåndtering. IKT-konsulenten har forklart at han ikke har oversikt over hvordan opplæring foregår i enhetene.

8.2.3 Spørreundersøkelsen og ansattes opplæring, samt kjennskap til informasjonssikkerhetsrutiner og regler i Nord-Odal

Halvparten av de spurte i undersøkelsen sier de har fått opplæring i informasjonssikkerhet, en noe større andel ledere enn ansatte generelt. 7 av 10 deltakere i undersøkelsen ytrer også et ønske om mer opplæring innen informasjonssikkerhet.

I det følgende kobler vi det å ha fått opplæring til de vurderinger disse gjør av informasjonssikkerhet og informasjonssikkerhetsrisiko, som en indikasjon på at opplæring har en positiv effekt på forståelse av informasjonssikkerhet.

Ansatte og ledelse som har fått opplæring innen informasjonssikkerhet har en større forståelse for risiko generelt enn de som ikke har fått opplæring. Ledere uten opplæring er i mindre grad bekymret for å bli lurt fra seg informasjon enn ledere med opplæring. Øvrige ansatte med og uten opplæring svarer imidlertid ganske likt på dette spørsmålet. Oppfattelsen av at respondentene er utsatt for mer risiko og trusler knyttet til informasjonssikkerhet er også høyere hos ledelse enn hos ansatte generelt.

De med opplæring ser i større grad ut til å vite hvilke aktiviteter som er risikofylte, hvordan de skal agere og hva de skal se etter for å jobbe forebyggende i tilknytning til informasjonssikkerhet.

Respondentene svarer forskjellig på spørsmål om hvilken type opplæring de får. Ut ifra svarene ser det ut til at det er mye uformell aktivitet og egenopplæring av informasjonssikkerhet. En av fem sier de får organiserte interne kurs eller utdanning, ca. halvparten sier de er selvlært eller hører om ting fra andre kollegaer i en mer uformell situasjon. To tredjedeler sier de får opplæring gjennom informasjon fra arbeidsgiver og 30 % har deltatt på nettkurs i forbindelse med nasjonal sikkerhetsmåned.

Åtte av ti oppgir at de kjenner til at Nord-Odal kommune har regler for informasjonssikkerhet og seks av ti mener at ledelsen har kommunisert tydelig sine forventinger og krav til de ansatte angående informasjonssikkerhet.

8.2.3.1 Bruk av Compilo som en del av internkontrollen og informasjonssikkerhetspraksis

Compilo er et kvalitetssystem, men også et system der informasjon som er aktuell for alle ansatte er lagret. Systemansvarlig for Websak mener at saksbehandlere har fått for lite opplæring i bruk av dette systemet.

Kommunens IKT-konsulent mener at Compilo ikke nødvendigvis reflekterer hvordan ting gjøres i praksis, det vil si at selv om kvalitetssystemet inneholder førende dokumenter for hvordan ting skal gjøres, er det ikke sikkert at disse praktiseres fullt ut etter intensjonen ute i avdelingene. IKT-konsulenten har forklart at noen sektorer ikke er så flinke til å registrere og protokollere eller gjennomføre formelle ROS-analyser ved endringer i systemene sine, selv om det fins nedskrevne rutiner og prosedyrer for dette.

Systemansvarlig for Profil forklarer at alle ansatte skal ha anledning til å få tilgang til datamaskin i løpet av arbeidsdagen og derfor også fagsystemer og Compilo. Systemansvarlig for Profil forklarer imidlertid at de ansattes e-postadresser i kommunen er lite brukt av de ansatte som jobber i hjemmetjenesten.

8.2.3.2 Avviksgjennomgang

IKT-konsulenten har informert om at det har blitt gitt orienteringer om avviksbehandling i ledergruppens møter de siste 3 foregående årene. IKT-konsulenten fremla avviksrapport fra 2020 som omtalte avvik i forbindelse med informasjonssikkerhetsbrudd. Disse inkluderte mangelfull opplæring av ansatte, menneskelig svikt/avsløring av informasjon, sikkerhetshull i systemer, og manglende sletting av tilganger.

Det ble meldt inn sju avvik på området i 2021: Tre med lav alvorsgrad, tre med middels alvorsgrad og en med høy alvorsgrad. Avvikene omhandler mangler tilknyttet ROS-analyser på datasystem, brudd på personopplysningssikkerheten, manglende innsending av avvik på HMS samt dataproblemer. To av avvikene var ikke lukket ved gjennomføring av ledelsens gjennomgang i mai 2022. IKT-konsulenten har uttrykt at en del av disse avvikene er sendt inn av ham selv.

Når det gjelder avvik innenfor informasjonssikkerhet og personvern er det en oppfattelse av at det ikke er en utbredt kultur for å bruke kvalitetssystemet til dette. Noen av avvikene sendes av IKT-konsulenten i de tilfeller der han ser at det er behov for forbedringer.

Systemansvarlig for Websak har også fortalt at kommunen har et forbedringspotensial på avviksmeldinger. Systemansvarlig har forklart at det er kjent at det tidligere har vært et problem at avvik blir liggende og ikke gjort noe med. Systemansvarlig tror at mange kan føle at poenget med å melde avvik blir borte.

Systemansvarlig for Profil forklarte at de fleste avvik i hjemmetjenesten omhandler medisin, og at avvikene ofte behandles i personalmøter.

8.2.4 Vurdering av revisjonskriterium 14

Våre undersøkelser viser at kommunen ikke har gjennomført en overordnet kartlegging av kompetanse og behov for kompetanse for å sikre god praktisering av informasjonssikkerhet.

Vi mener at revisjonskriterium 14 ikke er etterlevd.

Kommunen bør kartlegge kompetansebehovet blant ansatte for å sikre god praktisering av informasjonssikkerhet.

8.2.5 Vurdering av revisjonskriterium 15

Kommunen har organisert opplæring innen Websak og Visma Profil. Vi finner imidlertid ikke at de har en overordnet plan for opplæring av ansatte. I rutinebeskrivelsen «opplæring av ansatte i IKT og informasjonssikkerhet» [55], står det er at det er et lederansvar å gjennomføre tilpasset opplæring og at det bør foregå underveis og ved behov.

Et funn i spørreundersøkelsen er at ansatte uten opplæring har lavere grad av risiko-oppfattelse enn ansatte med opplæring. De ansatte trenger kunnskap om hvilken betydning informasjonssikkerhet har i de arbeidsoppgavene de utfører, og hvordan de kan gjennomføre arbeidet sitt på en måte som ivaretar behovet for informasjonssikkerhet. Vi mener at Nord-Odal kommune har et forbedringspotensial for å sikre at den enkelte ansatte får denne typen opplæring.

I spørreundersøkelsen har åtte av ti oppgitt at de vet at kommunen har regler for informasjonssikkerhet, men fire av ti mener at ledelsen ikke har kommunisert tydelig hvilke forventninger de har til de ansatte angående informasjonssikkerhet. Det er ulike svar på hvilken type opplæring de ansatte har fått, og svarene i spørreundersøkelsen indikerer at det er mye uformell aktivitet og egenopplæring innen informasjonssikkerhet.

Vi har inntrykk av at det gjennomføres tilpasset opplæring i tilknytning til Websak og Visma Profil som er de to systemene som vi har undersøkt nærmere.

Vi mener følgelig at revisjonskriterium 15 er delvis etterlevd.

Kommunen bør ha rutiner som gir den enkelte ansatte overordnet og tilpasset opplæring i hvordan ivareta informasjonssikkerheten og personvernet.

8.2.6 Vurdering av revisjonskriterium 16

Våre undersøkelser viser at det til en viss grad gjennomføres opplæring. Rutinebeskrivelsen for opplæring innen informasjonssikkerhet beskriver imidlertid at opplæring gjennomføres etter behov som oppstår «underveis». Nord-Odal gjennomfører eksempelvis opplæring for nye saksbehandlere i Websak, men systemansvarlig forteller at det ikke gjennomføres systematiske oppfriskningskurs, hovedsakelig på grunn av kapasitetsutfordringer. Det kan imidlertid gjennomføres oppfriskningskurs på forespørsel.

Compilo inneholder en del informasjon i tilknytning til opplæring, men vi finner ikke at det er en rutine som beskriver sentrale føringer for hvilke områder ansatte bør kjenne konkret til.

Nasjonal sikkerhetsmåned i regi av HIKT, er imidlertid en fast aktivitet som ansatte blir informert om og oppfordres til å delta på.

Vi har inntrykk av at bruk av Compilo og avvikssystemet ikke er tatt i bruk i utstrakt grad. Det kommer frem under intervjuer at opplæring i Compilo ikke har vært tilstrekkelig eller at avvikssystemet ikke er aktivt i bruk av ansatte generelt.

[55] Compilo, 18. januar 2022

Vi mener at revisjonskriterium 16 er delvis etterlevd.

Kommunen bør ha rutiner og tiltak som sikrer kontinuerlig og tilstrekkelig kompetanse for å kunne ivareta informasjonssikkerheten i organisasjonen.

8.2.7 Oppsummert vurdering problemstilling 3

En mer organisert form for opplæring fremstår som et område hvor Nord-Odal kommune har et forbedringspotensial,

Per januar 2022 er det ikke kartlagt kompetanse i tilknytning til informasjonssikkerhet i organisasjonen. Vi finner har kommunen har gjennomført tilpasset opplæring i de sakssystemene som vi undersøkte. Opplæringsansvaret er lagt ut til den enkelte enhet og tilpasset deres oppgaver.

Spørreundersøkelsen viser at 7 av 10 ansatte ønsker mer opplæring i informasjonssikkerhet. Det er ulike svar på hvilken type opplæring de ansatte har, og det er en indikasjon i tallene om at det er mye uformell og egenopplæring av informasjonssikkerhet.

Vi har inntrykk av at avvikssystemet ikke er tatt i bruk i utstrakt grad av ansatte generelt og at det er manglende opplæring på bruk av kvalitetssystemet.

Vi konkluderer derfor med at rutiner, planer og sikkerhetstiltak delvis følges opp av den enkelte ansatte.

9 Konklusjon

I dette forvaltningsrevisjonsprosjektet har vi kontrollert Nord-Odal kommune for overordnede styringsprinsipper for informasjonssikkerhet. Vi har belyst i hvilken grad kommunen har rutiner, prosedyrer og et system for internkontroll som er tilfredsstillende, om kommunen har implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang, samt om ansatte følger opp gjeldende rutiner og sikkerhetstiltak.

Vi har funnet at Nord-Odal kommune har sikkerhetsmål og sikkerhetsstrategier, et avvikssystem, et personvernombud, rutiner for årlig sikkerhetsrevisjon i ledelsen og kommunen har et etablert samarbeid med HIKT som en kvalitetsinstans for informasjonssikkerhet.

Vi har inntrykk av at Nord-Odal kommune fra sentralt hold jobber bevisst for å ha et tilfredsstillende system for informasjonssikkerhet. Det har spesielt i 2022 tilkommet mange rutiner i kvalitetssystemet som tilfredsstiller sentrale lovkrav og anbefalinger for informasjonssikkerhet, og vi finner at ledelsen utviser bevissthet i informasjonssikkerhetsarbeidet.

Det gjenstår fremdeles noe systematikk i kartleggingsarbeid før kommunen har en helhetlig oversikt over informasjonssikkerhet og praksis i hele organisasjonen. Dette inkluderer blant annet en overordnet tiltaksplan og verdifastsettelse av den informasjonen kommunen har i sine informasjonssystemer. En slik oversikt vil kunne hjelpe med å skape og implementere en gjennomgående sikkerhetskultur og risikostyring i hele kommunen.

Vi mener at Nord-Odal kommune har et forbedringspotensial knyttet til:

- Gjennomføring av ROS og DPIA-analyser
- Rutiner for tilgangsstyring
- Oversikt over databehandleravtaler
- Opplæringsrutiner og tiltak
- Klassifisering av informasjonsverdier og en plan for informasjonshåndtering
- Utforming av en tiltaksplan for sikkerhetsrevisjoner
- Avvik og avviksrapportering
- Oversikt om hvorvidt det er nødrutiner i alle enheter

10 Anbefalinger

Basert på våre funn, anbefaler vi at Nord-Odal kommune:

- klassifiserer informasjonsverdier og utarbeider en plan for informasjonshåndtering.
- utarbeider en plan for sikkerhetsrevisjoner.
- skaffer seg en helhetlig oversikt over avdelingenes nødrutiner.
- vurderer om informasjonssikkerhet bør inn i kommunens beredskapsplan og eventuelt gjennomføring av øvelser i forbindelse med mulige hendelser.
- reviderer alle rutiner og prosedyrer i Compilo i henhold til angitt revisjonsfrist. Rutiner som er lenket opp i dokumentene og ikke ligger i Compilo, bør legges inn i kvalitetssystemet.
- etablerer en kvalitetssikringsrutine i tilknytning til tilgangsstyring i systemer.
- foretar en gjennomgang av eksisterende databehandleravtaler og sørger for å sikre at systemer som eventuelt mangler databehandleravtaler får dette på plass. Databehandleravtaler bør vurderes å være en del av rutinen i «ledelsens gjennomgang.
- iverksetter tiltak som sikrer implementering og kjennskap til rutiner for informasjonssikkerhet, avvik og avviksrapportering innen informasjonssikkerhet og personvern.
- etablerer rutiner for å sikre at ansatte får en overordnet opplæring om informasjonssikkerhet ved oppstart, og at de til enhver tid har den nødvendige kompetansen til å praktisere god informasjonssikkerhetskultur. Det kan være behov for å kartlegge hva ansatte kan og ikke kan i forhold til informasjonssikkerhet.

11 Kommunedirektørens uttalelse

Nord-Odal kommune
HR, stab og service
Herredsvegen 2, 2120 Sagstua
62 97 81 00
Org. nr: 964 950 768

Revisjon Øst Iks
Postboks 84
2341 LØTEN

Deres ref:	Vår ref:	Saksbehandler:	Dato:
	22/17644	Trine Jeanette Hansen Dir.tlf.: 91 64 31 25	07.11.2022

"Informasjonssikkerhet i Nord-Odal kommune: Integritet, konfidensialitet og tilgjengelighet" – kommunedirektørens innspill til forvaltningsrevisjonsrapporten

Det vises til mail av 21.10.2022 med oversendelse av forvaltningsrevisjonsrapporten.

Kommunedirektøren har rett til å uttale seg om rapportens innhold. Uttalelsen vil bli tatt inn i rapporten som eget kapittel.

Det bes om en tilbakemelding på følgende:

- Kommunedirektørens syn på rapporten, revisors vurderinger, konklusjoner og anbefalinger.
- Om det planlegges å iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger, og i så fall hvilke tiltak som planlegges og når de er tenkt gjennomført.
- Om rapporten oppfattes som nyttig for kommunen, og en begrunnelse for hvorfor/hvorfor ikke.

Området det er gjennomført forvaltningsrevisjon på berører alle områder i kommunen. Så selv om det er noen særlige fokusområder har rapporten betydning for hele kommunens arbeid med informasjonssikkerhet.

Informasjonssikkerhet er komplekst og omfattende. Det kreves oversikt og gode rutiner innenfor området. Administrasjonen har opplevd at arbeidet med revisjonen har løftet aktuelle temaer og problemstillinger knyttet til informasjonssikkerhet, og generelt økt bevisstheten på området. Det har vært nyttig å få spørsmål fra revisjonen. Revisjonen har også gitt gode innspill til hvordan vi bedre kan ivareta informasjonssikkerhet underveis. Det har gitt grunnlag for å revidere og se på våre dokumenter.

Det ble gjennomført en spørreundersøkelse. Vi synes at analysene som er gjort av revisjonen i etterkant av undersøkelsen er gode. De gir et godt grunnlag for vår videre jobbing med temaet.

Det er 16 kriterier som er vurdert. Funnene i de enkelte kriteriene er i hovedsak gjenkjennbare. Vi ser at det er behov for å jobbe mer med informasjonssikkerhet i tiden fremover. Noen av kriteriene

skal det ikke så mye til for å endre fra gul til grønt, mens andre vil kreve mye arbeid. Mange av kriteriene viser til at det er behov for å gjøre endringer på systemnivå ved å lage rutiner som ivaretar informasjonssikkerhet på en bedre måte enn i dag. Det er også viktig at rutinene som lages blir gjort kjent i organisasjonen. Etter at disse er på plass vil det være behov for øke hele organisasjonens bevissthet knyttet til informasjonssikkerhetsarbeid. Rapporten vil tas opp i møte med kommunens personvernombud slik at vedkommende kan være med å veilede kommunen for å følge opp rapportens anbefalinger på en best mulig måte. I tillegg vil kommunedirektørens ledergruppe gå gjennom rapportens innhold og være sentrale i alle ledd av oppfølging og forbedring.

Rapporten kommer med 9 anbefalinger. Vi vurderer at særlig anbefalingene om klassifisering av informasjonssikkerhet, utarbeide en plan for informasjonshåndtering og kartlegging av ansattes kunnskap samt lage en god plan for overordnet opplæring vil være tidkrevende og utfordrende.

Med vennlig hilsen

Anne Olen Aasen
kommunedirektør

Trine Jeanette Hansen
leder for HR, stab og service

Dette dokumentet er elektronisk godkjent og sendes uten signatur.

12 Referanser

12.1 Litteratur og fagveiledere/standarder

Heggernes, T. A. 2020. *Digital forretningsforståelse. Fra store data til små biter (3. utgave).* Fagbokforlaget

ISO/IEC 27001:2013. *Internasjonal standard for styringssystem for informasjonssikkerhet*

Datatilsynet. 2018. *Veileder: Internkontroll og informasjonssikkerhet*

Digitaliseringsdirektoratet. 2021. Helhetlig styring og kontroll av informasjonssikkerhet

Direktoratet for E-helse. 2021. Veileder om internkontroll for informasjonssikkerhet og personvern

Direktoratet for E-helse. 2020. *Veileder – Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren*

Direktoratet for forvaltning og IKT. 2016. Internkontroll i praksis – informasjonssikkerhet

Kommunal og distriktsdepartmentet og KS. 2022. *Sikkerhetstiltak i norske kommuner i forbindelse med Russlands invasjon av Ukraina.*

KS. 2022. *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet*

KS 2020. *Orden i eget hus – Kommunedirektørens internkontroll*

Nasjonal sikkerhetsmyndighet. 2020. *NSMs grunnprinsipper for IKT-sikkerhet*

Regjeringen. 2015. Elektronisk samhandling med og i forvaltningen

Regjeringen. 2021. Veileder om internkontroll i kommunesektoren

12.2 Lover, forskrifter, NOU'er og rundskriv

Eforvaltningforskriften: https://lovdata.no/dokument/SF/forskrift/2004-06-25-988#KAPITTEL_3

Helseregisterloven: https://lovdata.no/dokument/NL/lov/2014-06-20-43
Lovdata. 2018. *Personvernforordningen av 2018*

Lov om behandling av personopplysninger (personvernloven):
https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#*

Regjeringen. 2018. NOU 2018-14

Regjeringen. 2019. Rundskriv I-3/2019 om informasjonshåndtering i spesialisthelsetjenesten

12.3 Kommunal dokumentasjon – Nord Odal kommune

Oversendt dokumentasjon fra Nord-Odal kommune

2012. Opplæringsmateriell informasjonssikkerhet

2013. Avtale om felles virksomhetsovergripende pasientjournal i formalisert arbeidsfellesskap

2015. Arkivrutiner, Nord Odal kommune

2015. Prosedyre for bruk av trådløs teknologi og regler for sikkerhet i nettverk

2015. Websak, saksbehandlingsrutiner

2017. Databehandleravtale for Acos og Nord-Odal kommune

2020. Prosedyre for bestilling, endring og sletting av brukerkontoer

Udatert. Avtaler med partnere, databehandlere og leverandører

Udatert. Bruk av databehandler

Udatert Brukerinstruks for FEIDE

Udatert. Bruk av elektronisk pasientjournal

Udatert. Handbok for Informasjonssikkerhet inkludert styringssystem

Udatert. Kopi av DPIA mal

Udatert Nivå for akseptabel risiko

Udatert. Nødprosedyrer for manuell drift

Udatert. Overordnede føringer for bruk av informasjonsteknologi

Udatert. Oversikt over behandlinger inklusive formål og hjemmelsgrunnlag for behandlinger

Udatert. Prosedyre for bruk av informasjonssystemene

Udatert. Prosedyre for bruk av mobilt utstyr (PC-telefon-nettbrett-annet)

Udatert. Prosedyre for den registrertes innsyn i helse- og personopplysninger

Udatert. Prosedyre for hendelsesregistrering

Udatert. Prosedyre for håndtering av flyttbare datalagringsmedier og lagring på nett

Udatert. Prosedyre for håndtering av passord

Udatert. Prosedyre for håndtering av utskrifter, oppbevaring og makulering av dokumenter med helse- og personopplysninger

Udatert. Prosedyre for innhenting av informert samtykke

Udatert. Prosedyre for konfigurasjonskontroll

Udatert. Prosedyre for opplæring i informasjonssikkerhet

Udatert. Prosedyre for oppretting og vedlikehold av autorisasjonsregister

Udatert. Prosedyre for sikkerhetskopiering (backup)

Udatert. Prosedyre for tilgangsstyring

Udatert. Prosedyre for å gi informasjon til den registrerte om personvernrettigheter

Udatert. Prosedyre for å forhindre ødeleggende dataprogram

Udatert. Regler for fysisk sikring av lokaler og områder

Udatert. ROS-analyse Acos mottak

Udatert. Ros Innføring av Websak+

Udatert. Rutiner for ROS informasjonssikkerhet

Udatert. Samhandlingsrutine for lokalt IKT-samarbeid

Udatert. Sjekkliste for testtilfeller til samhandlingsrutine til tjenesteavtale nummer 9

Udatert. Taushetserklæring for ansatte ved tiltredelse

Compilo

23.03.2021. Sikkerhetsorganisasjonen i Nord-Odal kommune, sist revidert 11.07.2022

24.03.2021. Sikkerhetsmål og sikkerhetsstrategi, sist revidert 08.04.2022

20.05.2021. Kontroll av postlister før publisering på internett

26.05.2021. Behandlingsprotokoll artikkel 30, *sist revidert 18.01.2022*

29.07.2021. Systemer og ansvarlige Nord-Odal

29.07.2021. Systemoversikt og klassifisering av systemer

04.08.2021. Håndbok Informasjonssikkerhet (Mye i håndbok er under revidering)

04.08.2021. Ivaretakelse av reservasjonsretten, *sist revidert 20.07.2022*

20.08.2021. Retting og sletting av helse- og personopplysninger, *sist revidert 27.1.2022*

20.08.2021. Samtykke som behandlingsgrunnlag for behandling av person og helseopplysninger, *sist revidert 27.01.2022*

25.08.2021. Innsyn i person- og helseopplysninger, *sist revidert 17.01.2022*

17.01.2022. IKT-sikkerhetsinstruks – Datavettregler

18.01.2022. Opplæring av ansatte – IKT og informasjonssikkerhet

24.06.2022. Ledelsens gjennomgang – personvern, *sist revidert 11.07.2022*

12.08.2022. Gjennomføre ROS i Compilo

29.08.2022. DPIA-mal

29.08.2022. Informasjonssikkerhet – Risikostyring, risikoanalyse (ROS) og DPIA

ROS-analyser

27.06.2017. Arkiv Profil: IKT-sikker sone, risikoanalyse gjennomført av Paul Vidar Bjørndalen
28.11.2018. Risikoanalyse Acos mottak. Lene Jeanette Østby 28. november 2018, oppdatert 12.03.2019 av Synnøve Grenaker

14.03.2019. Plassadministrasjon i Visma profil, risikoanalyse gjennomført av Paul Vidar Bjørndalen
28.03.2019. Visma Profil, egenandelsmodulen, risikoanalyse gjennomført av Paul Vidar Bjørndalen

07.05.2021. Utkast 3 ROS Innføring av WebSak+ og TEAMS integrasjon ved «Forvaltningsteam

Udatert. Risikoanalyse Acos mottak, tillegg til tidligere ROS. Lene Jeanette Østby, Trine Jeanette Hansen og Paul Reidar Løsnesløkken, udatert.

HIKT

2011. Sikkerhetsinstruks for ansatte i Hedmark-IKT

2015. Taushetserklæring for ansatte i Hedmark IKT

2021. Årsmelding HIKT. 2021 https://www.hedmark-ikt.no/wp-content/uploads/2021/04/20210423-Hedmark-IKT-Arsmelding-2020.pdf

12.4 Internettreferanser

Aktuell Sikkerhet. 2021. Kommunedata på det «mørke nettet»: Risikerer stort overtredelsesgebyr. https://aktuellsikkerhet.no/cybersecurity-cybersikkerhet-datakriminalitet/kommunedata-pa-det-morke-nettetrisiker-stort-overtredelsesgebyr/692345 (13. april 2021)

Aktuell Sikkerhet. 2021. Østre Toten kommune: - Dataangrepet har kostet oss mer enn 32 millioner. https://aktuellsikkerhet.no/cybersikkerhet-datainnbrudd-it-sikkerhet/ostre-toten-kommune-dataangrepet-har-kostet-oss-mer-enn-32-millioner/700321 (6. mai 2021)

Datatilsynet. Etablere internkontroll: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

Datatilsynet. Databehandlingsprotokoll: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/

Datatilsynet. Hva er personvern? https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/

Datatilsynet. Vurdering av personvernkonsekvenser: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

Digitaliseringsdirektoratet. Begrepsliste informasjonssikkerhet: https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet

Digitaliseringsdirektoratet: www.digdir.no

Digitaliseringsdirektoratet. Hva sier ISO-standarden: https://www.digdir.no/informasjonssikkerhet/kva-seier-ns-isoiec-27001/3060

Digitaliseringsdirektoratet. Hva er digital assistent: https://www.digdir.no/samhandling/hva-er-digital-assistent/2951

Habberstad, om skyggesystemer: https://www.habberstad.no/fagblogg/it-sikkerhet-slik-sikrer-du-riktig-handtering-av-informasjon

Hedmark IKT. Om HIKT https://www.hedmark-ikt.no/hedmark-ikts-historie/

Hedmark IKT. 2020. HIKT Informasjon om e-postangrepet 1. september 2020 https://www.hedmark-ikt.no/viktig-informasjon-vedrorende-svindel/

Hedmark IKT. Om m365 prosjektet: https://www.hedmark-ikt.no/prosjekter/m365/

Hedmark IKT. Prosjektet HIKT 2025 https://hikt2025.hedmark-ikt.no/

Hedmark IKT. Sikkerhetsinformasjon fra HIKT: https://www.hedmark-ikt.no/sikkerhet/

NRK Beta. 2021. «Seks hackergrupper utnyttet Microsoft sårbarhetene før de ble kjent».

KPMG. Datahackingssaken i Østre Toten, rapport fra KPMG: https://www.ototen.no/_f/p1/i5689ceb7-72b4-44d0-970c-a5c4828047e5/endelig-rapport-26082021-kpmg_sladdet.pdf

Nord-Odal kommunes nettsider: https://www.nord-odal.kommune.no/

NRK. 2018. https://www.nrk.no/kultur/advarer-mot-googles-norske-smarthoyttaler_-_-ikke-en-hvilken-som-helst-husgjest-1.14239760

NRK. 2021. https://nrkbeta.no/2021/03/13/seks-hackergrupper-utnyttet-microsoft-sarbarhetene-for-de-ble-kjent/

NRK. 2021. https://www.nrk.no/innlandet/kan-ta-et-halvt-ar-for-ostre-toten-a-rette-opp-dataangrep-1.15364106 (8. februar 2021)

NRK. 2021. https://www.nrk.no/nordland/dette-moter-deg-nar-hackerne-har-fatt-tak-i-din-personlige-informasjon-1.15801932

Regjeringen. Digitalisering 2025: https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2653874/?ch=1

Surveymonkey. Kalkulator for utvalgsstørrelse: https://no.surveymonkey.com/mp/sample-size-calculator/

Østre Toten kommune. 2021. https://www.ostre-toten.kommune.no/dataangrepet/10-1-21-dataangrepet-slik-blir-vare-innbyggere-berort.11988.aspx (18. januar 2021)

Vedlegg A – Utledede revisjonskriterier

Om utledningen av revisjonskriterier

Revisjonskriterier er de krav, normer og/eller standarder som den reviderte enheten skal bli vurdert i forhold til. Utgangspunktet for revisjonskriteriene er problemstillingene, og det skal være utledet revisjonskriterier for hvert forvaltningsrevisjonsprosjekt. Revisjonskriteriene danner med andre ord de krav og forventninger som revisjonen skal bruke i sin vurdering. Revisjonskriterier er beskrevet i § 15 i forskrift om kontrollutvalg og revisjon, og er et skal-krav i ethvert forvaltningsrevisjonsprosjekt.

Kriteriene skal utledes fra autoritative og anerkjente kilder innenfor det reviderte området. Slike kilder kan være lover, forskrifter, forarbeider, rettspraksis, politiske vedtak, mål og føringer, administrative retningslinjer statlige føringer og veiledere, andre myndigheters praksis, anerkjent teori, og reelle hensyn.

Kriteriene skal være relevante, konkrete og i samsvar med kravene som gjelder for den reviderte enheten i den aktuelle tidsperioden for revisjonen. Revisjon Øst IKS bruker RSK 001 som er Norges kommunerevisors forbund sin standard for forvaltningsrevisjon.

Bakgrunn for bestillingen

I henhold til kommuneloven § 23-2, punkt c, skal kontrollutvalget påse at det blir gjennomført forvaltningsrevisjon i kommunen. Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak (§ 23-3, første ledd).

I møte 12. februar 2021 og sak 9/21 bestilte kontrollutvalget i Nord-Odal kommune en prosjektplan med utgangspunkt i *administrasjon og styring IKT-sikkerhet*. Vedtaket var som følger (utdrag):

3. *Kontrollutvalget viser til vedtatt plan for forvaltningsrevisjon for Nord-Odal kommune for 2021-2024 og bestiller en prosjektplan med utgangspunkt i Administrasjon og styring IKT-sikkerhet*
4. *Prosjektplanen legges frem i møtet i mai*

I møtebehandlingen viste kontrollutvalget til at interimrapportene de siste årene gir en pekepinn på at det var behov for revisjon innen kommunens administrasjon, styring og internkontroll. I tillegg viste kontrollutvalget til at IKT-sikkerhet er et svært viktig område. Utvalget var enig i at det ville være aktuelt med fokus både på IKT-sikkerhet i egen kommune, men også hvordan samarbeidet med HIKT fungerer. Kontrollutvalget mente at problemstillingene var greit formulert i plan for forvaltningsrevisjon. Utvalget mente videre at det var viktig å se hen til hva som gikk galt i Østre Toten, der de ansatte i lang tid hadde vært uten tilgang til sine systemer (hacking-angrep), og at denne type problematikk skulle inkluderes i prosjektet.

Jamfør plan for forvaltningsrevisjon i Nord-Odal kommune for 2021-2021 ble det vedtatt oppstart av et forvaltningsrevisjonsprosjekt knyttet til administrasjon og styring - IKT-sikkerhet, i utvalgets møte den 20. mai 2021, under sak 29/21.

Utledning av revisjonskriterier

I det følgende utledes kriteriene som er planlagt benyttet i forvaltningsrevisjonsprosjektet. Utledningen er en gjennomgang og drøfting av hva krav og anbefalinger har å si for forventningene til praksis.

I prosjektet har vi valgt å foreta en avgrensning mellom det som gjelder teknisk drift, og det som kommunen drifter, ivaretar og kontrollerer selv av tjenester og systemer. Mye av det som går på IKT-sikkerhet ligger til tekniske løsninger som Hedmark IKT (HIKT) drifter etter en samarbeidsavtale mellom kommunen og HIKT. HIKT sitt ansvarsområde faller utenfor kontrollen. Vi vil kontrollere hvordan informasjonssikkerhet håndteres i organisasjonen med hensyn til atferden i disse tekniske løsningene. Dette velger vi å kalle *informasjonshåndtering*. [56] Kontrollen gjennomføres gjennom en spørreundersøkelse som sendes alle ansatte, samt intervjuer av nøkkelpersoner i virksomheten tilknyttet informasjonssikkerhet. Vi vil også kontrollere om organisasjonen har gjort tilstrekkelige grep for å ivareta informasjonssikkerhet. Her vil vi se nærmere på to områder spesielt; helse og omsorg og serviceenheten.

Utledning av revisjonskriterier for problemstilling 1

Er det etablert helhetlige planer, retningslinjer og rutiner som kan ivareta kommunens informasjonssikkerhet på en tilfredsstillende måte?

Denne problemstillingen søker å besvare om det foreligger, og er etablert planer og rutiner som kan ivareta informasjonssikkerheten på en måte som sikrer kommunen ut i fra deres behov.

Generelt om informasjonssikkerhet og presentasjon av nasjonale faglige retningslinjer

Informasjonssikkerhet (også omtalt som digital sikkerhet og datasikkerhet) handler om å sikre informasjon og informasjonssystemene som benyttes i en virksomhet tilstrekkelig. Dette inkluderer digitale tjenester, IKT-systemer og komponenter som inngår i IKT-systemer. Det handler om å tilrettelegge arbeidsoppgaver (prosesser) slik at det er enkelt for mennesker å utføre oppgavene sine med sikkerhet i høysetet, og det handler om å sikre tilstrekkelig kompetanse hos de som utfører oppgaver for virksomheten og å jobbe for en kultur som understøtter arbeidet med informasjonssikkerhet. I følge digitaliseringsdirektoratet handler informasjonssikkerhet om å sikre *konfidensialitet*, *integritet* og *tilgjengelighet*:

> «Det er vanlig å si at det handler om å sikre at informasjon i alle former:
>
> - ikke blir kjent for uvedkommende (konfidensialitet)
> - ikke blir endret utilsiktet eller av uvedkommende (integritet)
> - er tilgjengelig ved behov (tilgjengelighet)
>
> Brudd på et eller flere av disse punktene er et brudd på informasjonssikkerheten.» [57]

Forskrift om elektronisk kommunikasjon med og i forvaltningen (e-Forvaltningsforskriften) stiller krav til at forvaltningsorganer skal ha en internkontroll innenfor informasjonssikkerhet som er basert på

[56] Helse- og omsorgsdepartementet har brukt samme begrep i rundskriv for spesialisthelsetjenesten mht. grensegangene mellom taushetsplikt, personvern og informasjonssikkerhet.
[57] www.digdir.no

anerkjente standarder for styringssystemer for informasjonssikkerhet (§ 15). Det finnes flere slike standarder. Direktoratet for e-helse har sammen med helse og omsorgssektoren utarbeidet en standard som ivaretar informasjonshåndtering, informasjonssikkerhet og personvern:

> «Opplysningene må behandles slik at helse- og omsorgstjenester kan tilbys på en forsvarlig måte og samtidig ivaretar innbyggernes tillit til sektoren. God informasjonssikkerhet og godt personvern er en forutsetning for digitalisering. Sektoren må bygge og forvalte robust teknologi, organisasjon og sikkerhetskultur.»[58]

Denne standarden, eller normen blir kalt for Norm for informasjonssikkerhet og personvern, kort kalt Normen. Normen brukes av alle HIKT-kommuner som en standard for informasjonssikkerhet og personvern, også Nord-Odal kommune. Selv om den er rettet mot helse og omsorgssektoren er det fullt mulig å bruke retningslinjene også i andre sektorer i kommunal virksomhet.

Normen stiller følgende krav for å sikre *konfidensialitet* i virksomheten:

- Ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysninger
- Hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten
- Avgrense tilgang for autorisert personell iht. tjenstlig behov og
- Ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten.

Normen stiller følgende krav for å sikre *integritet* i virksomheten:

- At virksomheten sikrer at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er sikret mot utilsiktet eller uautorisert endring eller sletting
- Integritet er en forutsetning for god og forsvarlig hjelp, og det skal logges hvem som har rettet, registrert, endret og slettet informasjon
- Sikre at helse og personopplysninger blir registrert på rett person og at disse føres i henhold til relevant kodeverk/terminologi
- Sikre at opplysninger er korrekte og nødvendig relaterte og forhindre at kopier blir en kilde til utdatert informasjon

Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er *tilgjengelig*:

- Rett informasjon er tilgjengelig til rett tid og ut i fra tjenstlig behov
- Sikre forsvarlig og stabil drift i alle informasjonssystemer
- Sikre at det foretas egnede tiltak for å sikre forebygging, oppdagelse, håndtering og gjenoppretting av informasjon

Brudd på alle disse kravene må behandles som avvik. [59]

Informasjonssikkerhet krever i så måte at en kommune forvalter sine oppgaver i en digital hverdag på forsvarlig vis, og at de ansatte som forvalter dette også er i stand til å kunne utføre oppgavene sine på en sikker måte. Forsvarligheten sikres konkret blant annet gjennom:

- Et etablert tilgangsstyringssystem
- Programvare som loggfører aktivitet og endring av informasjon

[58] Norm for informasjonssikkerhet og personvern

[59] Norm for E-helse, opprinnelig kalt Norm for informasjonssikkerhet og personvern,side 16

- Gjennom klare risiko- og vesentlighetsanalyser for bruk av alle programmer, spesielt de som ikke er godkjente programmer som drives og vedlikeholdes av HIKT.

Kommunens internkontroll

Med ny kommunelov ble internkontrollansvaret tydeliggjort. Dette fordi begrepet ble fjernet fra øvrige lovverk og forskrifter, og at internkontrollansvaret ble «samlet på et sted». Kommunens internkontroll skal tilpasses kommunens behov og risikoforhold. [60] KS har utarbeidet en veileder for kommunedirektørens internkontroll til støtte for hvordan kommunene kan identifisere risiko og utarbeide en risikobasert internkontroll tilpasset kommunens behov. Det fremgår i veilederen at hensikten med internkontrollen i kommunen er å sikre at lover og forskrifter følges.

Kommuneloven angir minstekrav til internkontrollen, og er beskrevet i kommunelovens §25-1:

> «Ved internkontroll etter denne paragrafen skal kommunedirektøren
>
> 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 omfanget som er nødvendig
>
> e. evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.» [61]

Kommunen kan velge å etablere en internkontroll som går lenger enn disse minstekravene. I KS sin veileder «Orden i eget hus – Kommunedirektørens internkontroll», står følgende:

> «God internkontroll handler i stor grad om systematisk arbeid, god organisering og dokumentasjon, arbeidsmetoder og samhandling som kan forebygge lovbrudd og uønskede hendelser». [62]

KS skriver videre at selv om internkontroll og virksomhetsstyring kan overlappe, er internkontrollen mer risikobasert enn mål- og resultatstyrt, slik virksomhetsstyring ofte er.

Kontrollbegrepet kan deles i to perspektiver:

- Et strategisk perspektiv hvor man ønsker å etablere et felles styringssystem og verktøy for å nå en virksomhets mål.
- Et operasjonelt perspektiv hvor man omtaler de løpende prosessene og de praktiske aktivitetene i tjenesteproduksjonen og i støtteprosesser.

Risikobasert utarbeidelse av dokumentasjon for internkontroll, som tilpasses underveis, er derfor et sentralt element ved hvordan internkontrollen bør formes.

eForvaltningsforskriften § 15 viser til følgende:

> *«Forvaltningsorgan 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.»*[63]

[60] KS: Kommunedirektørens internkontroll, side 9
[61] Kommuneloven: Lov om kommuner og fylkeskommuner
[62] KS: Kommunedirektørens internkontroll, side 24
[63] Eforvaltningsforskriften: Forskrift om elektronisk kommunikasjon med og i forvaltningen

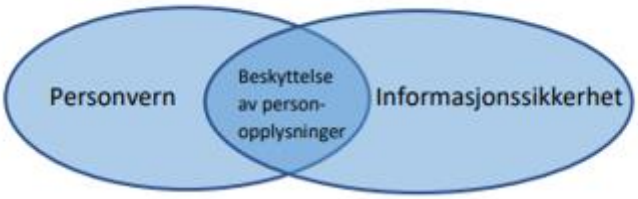
Sikkerhetsstrategi og mål er også beskrevet i Normen: «Alle offentlige virksomheter skal beskrive mål og etablere strategi for informasjonssikkerhet. Dette skal danne grunnlaget for styringssystemet.» [64]

Anbefalinger for informasjonssikkerhet og personvern

KS ga i januar 2022 ut et tillegg til kommunedirektørens internkontroll. [65] Dokumentet er utarbeidet av KPMG og skal fungere som en verktøykasse for kommunedirektører for temaene informasjonssikkerhet og personvern. Her står det følgende:

> «Internkontrollen skal bidra til at kommunen ivaretar beskyttelsesbehovet til informasjon og personopplysninger og er kommunaldirektørens viktigste verktøy for å styre risiko på personvern- og informasjonssikkerhetsområdet». [66]

KPMG viser i dokumentet til at GDPR og ny personvernlovgivning visker ut noen av forskjellene mellom informasjonssikkerhet og personvern. Samtidig viser de også til at informasjonssikkerhet og personvern er to forskjellige fagområder med overlappende temaer. Følgende modell benyttes for å skissere at personvern og informasjonssikkerhet overlapper der hvor det omhandler beskyttelse av personopplysninger:



Figur 3 - hentet fra kommunedirektørens verktøykasse for informasjonssikkerhet og personvern, side 6

Dokumentet inneholder en rekke anbefalinger til hvordan kommunedirektøren best kan ha kontroll med kravene til informasjonssikkerhet og personvern.

Det anbefales i første omgang å tilegne seg en oversikt over hva man har av informasjon og opplysninger, og kategorisere disse etter hva slags verdi de har. Inndelingen som KPMG viser til er ikke en mal, men et eksempel på hvordan dette kan gjøres. KPMG deler først inn informasjonen i ulike verdinivåer med hensyn til hvor viktig informasjonen er for tjenesteytelsen i kommunen:

- Kritisk verdi
  - Informasjon som er kritisk i en krisesituasjon (for eksempel samfunnskritiske funksjoner, beredskapsplaner, helseopplysninger)
- Høy verdi
  - Informasjon som vil være ødeleggende for funksjoner og tjenester som er kritisk for daglig drift (for eksempel strategidokumenter, eksamener/tentamener, informasjonssystem for lønnsutbetaling)
- Middels verdi
  - Informasjon som kan skade kommunens tjenester og funksjoner i daglig drift (for eksempel informasjon unntatt offentlighet, læringsplattform for kommunikasjon mellom elever og skole
- Lav verdi

[64] Norm for e-helse, side 13
[65] KS: Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet.
[66] KS: Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern, side 26

- Åpen informasjon uten særskilte sikkerhetsbehov (for eksempel informasjon fra hjemmesiden til virksomheten)

KPMG skriver at det etter en slik gjennomgang vil være naturlig å starte med den informasjonen det er knyttet størst negativ risiko til. Disse vurderingene skal ende opp i en tiltaksplan. Tiltaksplanen må inneholde hvem som er ansvarlige for det enkelte tiltak og hvilke risikovurderinger som er gjort. Risikovurderingene bør i tillegg kobles opp til den sektorovergripende internkontrollen. I denne internkontrollen bør kommunen vurdere hvor ofte man bør kontrollere tiltakene i forbindelse med evaluering av om iverksatte tiltak fungerer etter hensikten.

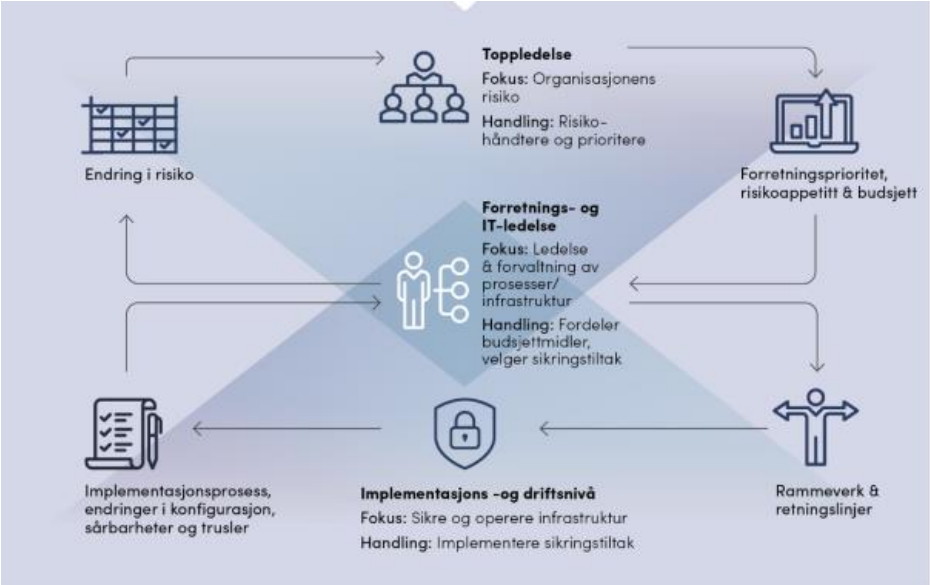
KPMG beskriver ulike sikkerhetstiltak knyttet til om risikoen er relatert til informasjonssikkerhet eller personvern. Informasjonssikkerhetstiltak er ofte knyttet til teknisk drift. Dette er tiltak som for Nord-Odal kommune skal ivaretas av Hedmark IKT gjennom felles samarbeidsavtale. KPMG skriver imidlertid videre at god informasjonssikkerhet og personvern også avhenger av gode arbeidsrutiner og sikkerhetsbevissthet hos de ansatte. Dette kan for eksempel dreie seg om tilgangsstyring, internkontroll, opplæringstiltak og adgangskontroll til fysiske bygg og gjenstander. Andre momenter som kan være viktige er retningslinjer for bruk av sosiale medier, bruk av samme passord over flere plattformer, eller bruk av samme passord både privat og på jobb m.m. Vi mener at det er naturlig å forvente at kommunen kan dokumentere at det er foretatt vurderinger av hvilke typer informasjon kommunen bør prioritere å sikre, og at det er iverksatt tiltak basert på disse prioriteringene.

Særlig ledelsesansvar

Normen beskriver at det ligger et særlig ledelsesansvar i informasjonssikkerhet. Dette innebærer at ledelsen i organisasjonen både har vurdert og bestemt riktig nivå for akseptabel risiko og at det gjennomføres en systematisk og bevisst oppfølging for å sikre organisasjonens informasjonssikkerhet. Dette bør gjenspeiles i virksomhetens aktiviteter, planverk, retningslinjer og kvalitetssystem.

Ledelsesansvaret og forankringen knyttet til informasjonssikkerhet, er tydelig i ISO/IEC 27001 standarden, og i nasjonalfaglige veiledere som er tilknyttet informasjonssikkerhet og personvern. Digitaliseringsdirektoratet beskriver dette som et viktig punkt i sin veileder i informasjonssikkerhet, og i KS sin veileder for kommunedirektørens verktøykasse for informasjonssikkerhet og personvern står det følgende: «I en stadig mer digitalisert verden, er det viktig at toppledere har kunnskap om digital risiko, muligheter for å redusere risiko og hvilke regelverk som må etterleves». [67] Nasjonal sikkerhetsmyndighet viser også til at ledelse og ledelsesforankring skal sikre redusert risiko og kontinuerlig oppfølging av informasjonssikkerhet i en virksomhet, som vist i denne figuren: [68]

[67] KS: Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern, side 4
[68] Nasjonal sikkerhetsmyndighet, «grunnprinsipper for IKT-sikkerhet», side 4



Figur 4 hentet fra Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet, side 4

Nasjonal sikkerhetsmyndighet mener at: «Det er avgjørende at toppledelsen tar eierskap og involverer seg i sikkerhetsarbeidet i egen virksomhet.». [69]

Ledelsens gjennomgang av informasjonssikkerhetsområdet

Nord-Odal kommune henviser til at de bruker Normen for E-helse som grunnleggende veileder for informasjonssikkerhet. Veilederen beskriver følgende om ledelse og ansvar:

> «Virksomhetens øverste ledelse har ansvaret for å sørge for at virksomheten følger gjeldende krav til informasjonssikkerhet og personvern. Dette ansvaret bør ivaretas som en del av arbeidet med virksomhetsstyring og kvalitetsforbedring. Ansvaret inkluderer å bestemme et nivå for akseptabel risiko, håndtering av risiko samt å sørge for velfungerende styring og kontroll. Virksomheten skal dokumentere alle tiltak». [70]

Kommunens øverste ledelse skal, ifølge Normen, helt konkret selv gjennomgå organisasjonens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året. *Formålet er å sikre at styringssystemet for informasjonssikkerhet og personvern er tilstrekkelig og hensiktsmessig ut i fra formål, krav og de risikoene som virksomheten har. Sentrale fagpersoner bør delta på denne gjennomgangen sammen med informasjonssikkerhetsleder og ledergruppen samt eventuelle representanter fra berørte enheter.*

Følgende punkter skal gjennomgås:

- endringer i behandlinger av helse- og personopplysninger (databehandlingsprotokoll)
- endringer i organiseringen av arbeidet
- resultat fra risikovurderinger og personvernkonsekvensvurderinger
- resultat av avviksbehandling
- oppfølging av leverandører og databehandleravtaler
- endring i nivået for akseptabel risiko

[69] Nasjonal sikkerhetsmyndighet: NSMs grunnprinsipper for IT-sikkerhet, side 4
[70] Normen: Veileder om internkontroll for sikkerhet og personvern

Denne gjennomgangen skal gi ledelsen grunnlag for å fatte velinformerte strategiske beslutninger for videre utvikling og forbedringsarbeid på informasjonssikkerhets- og personvernområdet. Dersom gjennomgangen avdekker at virksomhetens risikonivå ikke er akseptabelt, skal det vedtas tiltaksplaner for å rette opp dette, med tidsfrister og plassering av ansvar. Ledelsens gjennomgang skal dokumenteres.

Punktvis oppsummering av revisjonskriterier for problemstilling 1

1. Kommunen har beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).
2. Kommunen og kommunens øverste ledelse har en tilpasset og risikobasert internkontroll for informasjonssikkerhet. Internkontrollen inneholder både et strategisk og langsiktig perspektiv, og et operasjonelt perspektiv som omhandler daglig virksomhetsstyring.
3. Kommunen har gjennomført en kartlegging og risikovurdering av hvilken informasjon som har kritisk verdi, høy verdi, middels verdi og lav verdi, og har en tydelig tiltaksplan som viser hvem som er ansvarlig for ulike tiltak.
4. Kommunen har rutiner og prosedyrer som sørger for at alle i virksomheten sikrer at informasjon i alle former ikke blir endret utilsiktet, eller av uvedkommende.
5. Kommunen har rutiner og prosedyrer som sørger for at alle i virksomheten sikrer at informasjon i alle former er tilgjengelig ut ifra tjenstlige behov.
6. Kommunens ledelse gjennomgår virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året. Følgende punkter skal gjennomgås:
    - endringer i behandlinger av helse- og personopplysninger (behandlingsprotokoll)
    - endringer i organiseringen av arbeidet
    - resultat fra risikovurderinger og personvernkonsekvensvurderinger
    - resultat av avviksbehandling
    - oppfølging av leverandører og databehandleravtaler
    - endring i nivået for akseptabel risiko

    Dersom gjennomgangen avdekker at virksomhetens risikonivå ikke er akseptabelt, skal det vedtas tiltaksplaner for å rette opp dette, med tidsfrister og plassering av ansvar.
7. Ledelsens gjennomgang skal dokumenteres.

Utledning av revisjonskriterier for problemstilling 2

Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?

Denne problemstillingen tar sikte på å belyse om kommunen har satt i gang og implementert de konkrete sikkerhetstiltakene som trengs for å sikre seg mot uautorisert tilgang på informasjon.

Risikoforståelse

Datatilsynet skriver at vurderinger av risiko er en viktig del av det kontinuerlige arbeidet innenfor informasjonssikkerhet:

> «*Risiko* betegner forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse. Risikovurderingen må ses i sammenheng med etablerte akseptkriterier for risiko, og den behandlingsansvarlige skal iverksette nødvendige tiltak for å oppnå tilfredsstillende *informasjonssikkerhet*». [71]

KS viser til at det å ha en rettmessig forståelse av risiko innebærer en forståelse av hvilken risiko virksomheten kan være utsatt for:

> «Kommunen bør ha oppdatert innsikt i overordnede trender og utviklingen i kommunens risikobilde. Fagpersoner på informasjonssikkerhets- og personvernområdet bør ha i oppgave å ivareta denne type risikovurderinger». [72]

Risikobildet er i stadig endring og krever at det følges med i utviklingen. Sikkerhetstiltak må tilpasses ut fra:

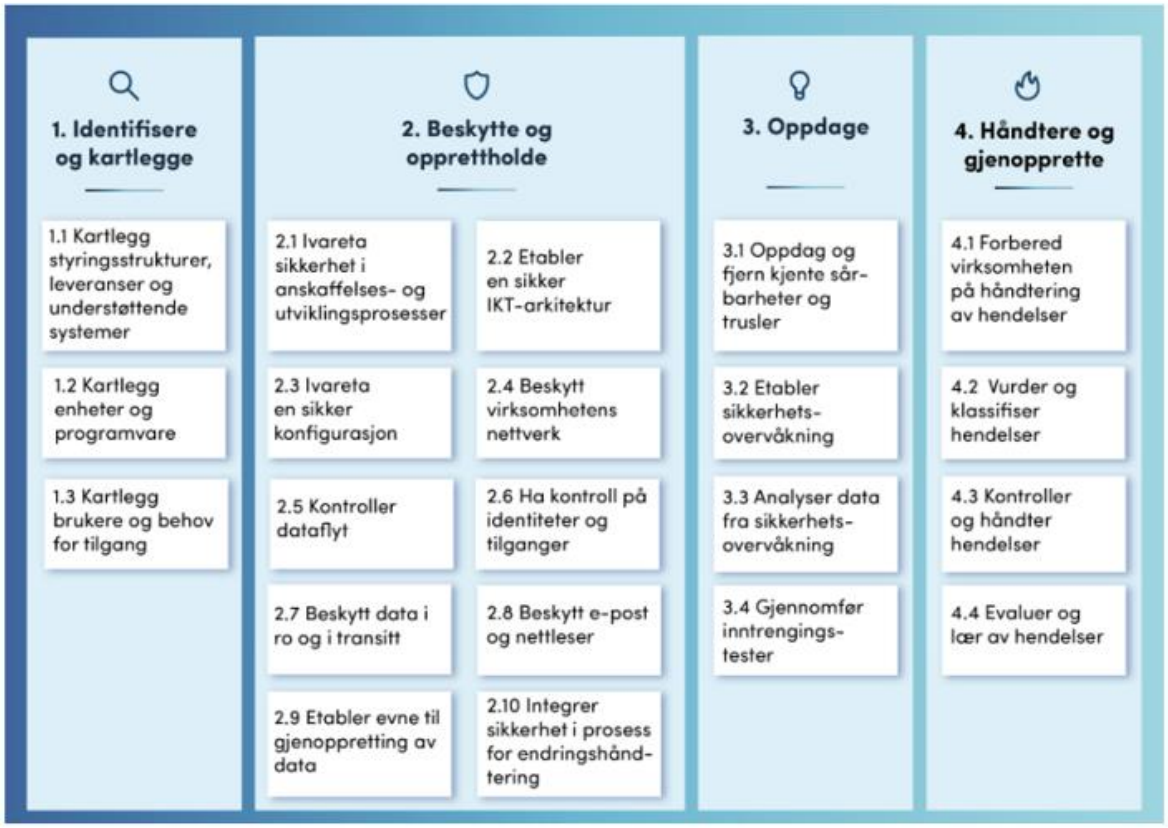
- Sikkerhetshendelser og hackerangrep som oppstår
- Læring av egne feil eller når ting gjøres riktig
- Anvendelse av ny teknologi eller programvare
- Utvikling av ulike arbeidsmetoder
- Sektorovergripende internkontrollaktiviteter
- Hvordan iverksetting av ulike sikkerhetstiltak samvirker med tekniske, organisatoriske og menneskelige faktorer

Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern anbefaler derfor:

> «…å bygge et rammeverk som stiller krav til sikkerhetstiltak, som bidrar til at kommunen forholdsvis enkelt kan få en god informasjonssikkerhet og godt personvern som bidrar til å håndtere mange risikoer». [73]

Dette kan være rutiner og roller i organisasjonen som sikrer at alle systemer er risikovurdert ved oppstart, og at de jevnlig risikovurderes i tilknytning til større endringer i systemet. Et eksempel på rammeverk er NSMs grunnprinsipper for IKT-sikkerhet:

[71] Datatilsynet: Virksomhetens plikter innen informasjonssikkerhet og internkontroll: Risikovurdering
[72] KS: Kommunedirektørens verktøykasse for informasjonssikkerhet, side 16
[73] KS: Kommunedirektørens verktøykasse for informasjonssikkerhet, side 20

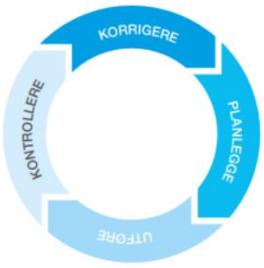


Figur 5 Oversikt over NSMs grunnprinsipper for IKT-sikkerhet, kilde: www.nsm.no

Risiko og vesentlighetsvurderinger, sikkerhetsrevisjoner

Digitaliseringsdirektoratet (Digdir) viser til at risikovurderinger er et viktig verktøy som må være en del av virksomhetens sikkerhetstiltak: «Vurdering av risiko er «hjertet» i internkontrollen. Risiko som angår informasjonssikkerhet må identifiseres, analyseres og evalueres». [74]

Datatilsynet, Digdir, Normen og KS (Kommunedirektørens verktøykasse for informasjonssikkerhet og personvern) presenterer modeller for internkontroll og risikovurderinger som er relativt like i sine prinsipper, der kontinuerlig forbedring sikres gjennom at de er sirkulære i sine aktiviteter. KS sin modell har fire aktiviteter, eller faser; planlegge, utføre, kontrollere, korrigere. Felles for alle disse modellene er at de sikrer kontinuitet, og at det jevnlig gjennomføres revisjoner etter at en risikovurdering er gjennomført. KS og Normen bruker «Demings sirkel» som modell for å beskrive dette best:



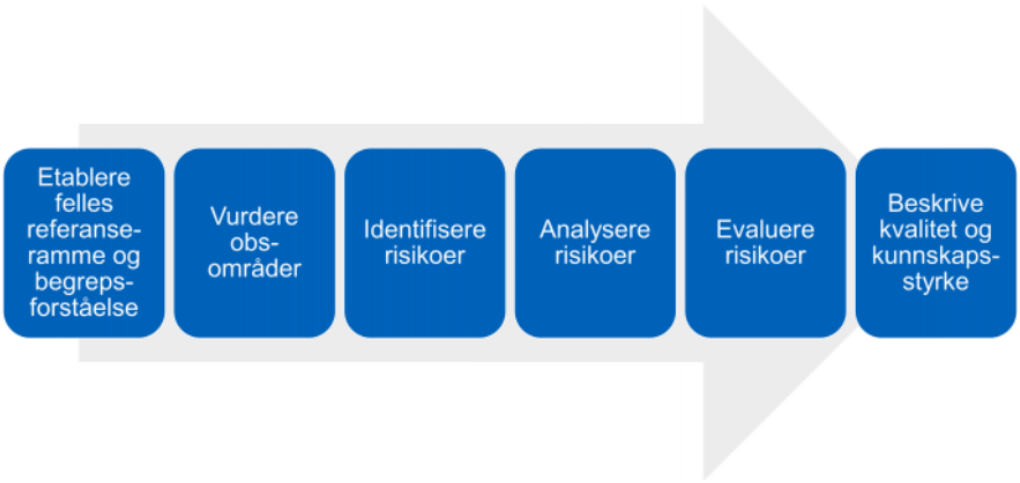
Figur 8: Demings sirkel: Plan, Do, Check, Act

Figur 6 Demings sirkel, kilde: www.ks.no

[74] Digitaliseringsdirektoratet: *Gjennomføre en risikovurdering*

Uønskede hendelser har to komponenter som kan føre til at ting går galt, eller at det oppstår såkalte uønskede hendelser. Det ene er sårbarhetene som kommunen selv har, og det andre er de truslene som kommunen står overfor. Eksempler på uønskede hendelser kan være feilkoding av saker som fører til at personlig informasjon havner på postlister, en brann kan oppstå som fører til at en server blir ødelagt, en skole kan bli hacket og informasjon kan lekkes, en ansatt kan bli utsatt for phishing og gi uønskede tilgang til informasjon, eller at det kan innføres skyggesystemer av enheter som ikke er sikret gjennom de faste prosedyrer som virksomheten har for informasjonssikkerhet og anskaffelser. Slike henvendelser har ofte omdømmemessige og økonomiske konsekvenser for virksomheter.

Vurdering av risiko er viktig i arbeidet med informasjonssikkerhet. Dette må organiseres på en god måte, for å gi et godt grunnlag for håndtering av risiko. Digitaliseringsdirektoratet har beskrevet følgende modell for risikovurdering i forbindelse med informasjonssikkerhet:



Figur 7 - Kilde: Digitaliseringsdirektoratet, Gjennomføre en risikovurdering

I Normen står det at virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner. Formålet med en sikkerhetsrevisjon er å gjennomføre kontrollaktiviteter og kvalitetssikring av etablerte tiltak og fastsatte rutiner. Det skal foreligge en godkjent plan for sikkerhetsrevisjoner. Det viktigste med å ha en kontinuitet i revisjonene er å sikre kontinuerlig forbedring, slik at virksomheten sikrer at de er oppdaterte og videreutvikler sine systemer i takt med trusselbildet. [75]

Avvikshåndtering og gjenopprettelse av IT-drift

Hvis det oppstår hendelser som fører til at IKT-tjenestene er nede og at informasjon som er nødvendig å gjennomføre ikke er tilgjengelig, er det viktig å ha beredskapsplaner og jevnlige øvelser som sikrer at man kan gjenopprette normal drift ved en digital sikkerhetshendelse. Her er det viktig at disse planene er utformet slik at de ivaretar kravene til personvern og informasjonssikkerhet. [76] *Det er også viktig å ha rutiner for å registrere, håndtere, evaluere og følge opp avvik i drift:*

> «For å sikre at regelverket følges skal det etableres avviksrutiner slik at avvik oppdages og at årsak til avviket, korrigerende tiltak, læring og rapportering blir dokumentert. Avvikshåndtering kan også iverksettes ved tilfeller av manglende eller uhensiktsmessige rutiner. Virksomheten skal samle inn fakta

[75] Normen: Veileder om internkontroll for sikkerhet og personvern
[76] Kommunedirektørens verktøykasse for informasjonssikkerhet, side 20

om hendelsesforløpet for etablering av korrigerende tiltak og effekten av korrigerende tiltak skal vurderes og eventuelle andre tiltak skal settes i verk ved behov». [77]

Det er den enkelte ansatte som er ansvarlig for å rapportere avvikshendelser.

Punktvis oppsummering av revisjonskriterier for problemstilling 2

8. Kommunen må gjennomføre risikovurderinger på informasjonssikkerhetsområdet.
9. Kommunen skal ha en godkjent plan for sikkerhetsrevisjoner.
10. Kommunen skal gjennomføre sikkerhetsrevisjoner jevnlig, disse skal være dokumenterte.
11. Kommunen skal følge opp resultater fra disse sikkerhetsrevisjonene.
12. Kommunen skal ha klare rutiner for avviksrapportering og håndtering.
13. Kommunen skal ha planer for å gjenopprette normaltilstand etter en fysisk/teknisk hendelse som innebærer informasjon på avveie, eller at informasjon er utilgjengelig. Planen(e) opprettholder drift så tilnærmet ordinær drift som mulig.

Utledning av revisjonskriterier for problemstilling 3

I hvilken grad følges planer, rutiner og sikkerhetstiltak opp i kommunens enheter og av den enkelte ansatte?

Denne problemstillingen søker å besvare om de ansatte følger opp sin rolle i tilknytning til informasjonssikkerhet og om de har den kompetansen som behøves for å kunne gjøre dette.

Forankring av rutiner

I KS sin veileder for internkontroll blir det omtalt ulike områder som vil avkreve sektorovergripende regler. Her blir blant annet datasikkerhet og håndtering av personopplysninger nevnt. KS skriver at det vanligvis ikke er mangel på rutiner som er utfordringen ved internkontrollen, men at rutinene ikke følges. For å sikre at rutinene følges, må disse gjøres kjent for de ansatte. I enkelte tilfeller vil det også være behov for opplæring i rutinene. En annen årsak til at rutiner ikke følges, kan være at rutinene fremstår som rigide eller tungvinne sett opp mot andre krav i arbeidshverdagen i den enkelte tjeneste. Dette er spesielt kjent innenfor IKT-sikkerhet hvor man lett kan sikre systemer ved å lukke de fullstendig fra tilgang på internett eller fastsette krav til komplekse passord og flertrinnsverifisering ved enhver pålogging, noe som vil være lite hensiktsmessig dersom brukerne av systemene skal være i stand til å gjennomføre arbeidsoppgavene sine på en effektiv måte. Det er derfor viktig at regler og rutiner er utarbeidet og tilpasset den faktiske situasjonen for kommunen og kommunens tjenester.

Den menneskelige faktoren, en viktig del av god informasjonssikkerhet

Mange tenker at fysiske og tekniske sikkerhetstiltak, eksempelvis kryptering, tilgangsstyring, passordstyrke eller utvikling av sikre IKT-systemer, er det som skal til for å ivareta krav til informasjonssikkerhet og personvern. Den menneskelige faktoren er likeså viktig, og god informasjonssikkerhet og godt personvern er også avhengig av ansatte med gode arbeidsrutiner og en

[77] Normen: Veileder om internkontroll for sikkerhet og personvern

klar bevissthet rundt sikkerhet i bruk av digitale hjelpemidler. [78] De ansatte er en viktig del av god informasjonssikkerhet, og noe som man til syvende og sist er helt avhengig av for at skal fungere på en bra måte i organisasjonen. Etterlevelse, riktig teknologi, god virksomhetsstyring, risikovurderinger og en kontinuitet er alt sammen avhengig av menneskers ferdigheter og kunnskap. I en virksomhet favner informasjonssikkerhet alle og krever at alle bidrar og har riktig kunnskap i forhold til hvordan de hjelper til å sikre informasjonssikkerheten. [79]

Digitaliseringsdirektoratet har utarbeidet en egen veileder som omhandler kompetanse og kulturutvikling innen digital sikkerhet. [80] Deriblant er det også utarbeidet egne kompetansebeskrivelser som angir krav til både nøkkelpersoner innen IT, ansatte generelt og ledelsen i virksomheten. Det legges generelt vekt på en kontinuitet i forståelsen av hvilke handlinger som kompromitterer informasjonssikkerheten og at man generelt må ta ansvar for å skape både et planverk og kontinuerlige aktiviteter i virksomheten som sikrer informasjonssikkerhet og som skaper en kultur som ivaretar informasjonssikkerheten. De ansatte trenger kunnskap om hvilken betydning informasjonssikkerhet har i de arbeidsoppgavene de utfører, og hvordan de kan gjennomføre arbeidet sitt på en måte som ivaretar behovet for informasjonssikkerhet. Her handler det blant annet om å inneha en tilfredsstillende forståelse av trusler og risiko, slik at de utfører arbeidsoppgavene på en sikker måte. De må også forstå hvordan uønskede hendelser kan hindre dem i å få gjort jobben sin slik de skal, eller hvordan dette kan få konsekvenser for andre parter. Det er viktig at ansatte kjenner til kommunens interne rutiner for varsling av informasjonssikkerhetshendelser. [81]

Punktvis oppsummering av revisjonskriterier for problemstilling 3

14. Kommunen bør kartlegge kompetansebehovet blant ansatte for å sikre god praktisering av informasjonssikkerhet.
15. Kommunen bør ha rutiner som gir den enkelte ansatte overordnet og tilpasset opplæring i hvordan ivareta informasjonssikkerheten og personvernet.
16. Kommunen bør ha rutiner og tiltak som sikrer kontinuerlig og tilstrekkelig kompetanse for å kunne ivareta informasjonssikkerheten i organisasjonen.

[78] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet
[79] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet
[80] Veileder i kompetanse og kulturutvikling innen digital sikkerhet
[81] Kompetansebeskrivelser for roller innen styring og kontroll av informasjonssikkerhet

Referanser

Datatilsynet (2019). *Virksomhetens plikter innen informasjonssikkerhet og internkontroll: Risikovurdering*

Det kongelige helse og omsorgsdepartement (2019). *Informasjonshåndtering i spesialisthelsetjenesten* (Rundskriv I-3 2019)

Digitaliseringsdirektoratet. *Kompetansebeskrivelser for roller innen styring og kontroll av informasjonssikkerhet*

Digitaliseringsdirektoratet. *Styring av informasjonssikkerhet: Gjennomføre en risikovurdering*

Digitaliseringsdirektoratet. *Veileder i kompetanse og kulturutvikling innen digital sikkerhet*

Direktoratet for e-helse (2021). *Normen for informasjonssikkerhet og personvern i helsesektoren*

E-forvaltningsforskriften (2020). *Forskrift om elektronisk kommunikasjon med og i forvaltningen*

Kommuneloven (2018). *Lov om kommuner og fylkeskommuner*

Kommunenes sentralforbund (2020). *«Orden i eget hus: Kommunedirekteørens internkontroll»*

Kommunenes sentralforbund (2022).*Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet*, Utarbeidet av KPMG for kommunenes sentralforbund.

Nasjonal sikkerhetsmyndighet (2020). *NSMs grunnprinsipper for IT-sikkerhet*

Standard Norge (2017). *Informasjonsteknologi – Sikringsteknikker – Ledelsessystemer for informasjonssikkerhet – Krav (ISO/IEC 27001: 2014 innbefattet Cor 1:2014 og Cor 2:2015)*