Forvaltningsrevisjon 2018/2019.

Utarbeidet av Hedmark Revisjon IKS på oppdrag fra kontrollutvalget i Åsnes kommune.

IKT-sikkerhet i Åsnes kommune

-Personvern og generell IKT-sikkerhet-

(I rapporten er sladdede opplysninger unntatt offentligheten etter offentlighetsloven § 24 tredje ledd)

Hedmark Revisjon IKS

Postboks 84, 2341 Løten
Telefon: 62 43 58 00
www.hedmark-revisjon.no
E-post: post@hedmark-revisjon.no

Forord

Denne rapporten er et resultat av forvaltningsrevisjonsprosjektet: *IKT-sikkerhet i Åsnes kommune.* Rapportutkastet har vært sendt rådmannen i Åsnes kommune til uttalelse, og rådmannens uttalelse fremkommer av rapporten. Rapporten, som utgjør prosjektets sluttprodukt, avleveres herved til revisjonens oppdragsgiver; kontrollutvalget i Åsnes kommune.

Forvaltningsrevisor Kjetil Kalager har vært utøvende revisor for prosjektet og har ført rapporten i pennen. Lina Høgås-Olsen har vært oppdragsansvarlig forvaltningsrevisor for prosjektet og har vært tillagt oppgaven med å kvalitetssikre arbeidet. Forvaltningsrevisor Karoline Hovstad har bistått som prosjektdeltaker.

Revisjonen ønsker å takke kommunens administrasjon for god tilrettelegging og bistand i prosjektforløpet.

Hedmark Revisjon IKS takker kontrollutvalget i Åsnes kommune for oppdraget.

Løten, den 25. april 2019

Lina Høgås-Olsen
Oppdragsansvarlig forvaltningsrevisor

Kjetil Kalager
Utøvende forvaltningsrevisor

Forsidebilder: Freedigitalphotos.net

Innholdsfortegnelse

Sammendrag

Kontrollutvalget i Åsnes kommune fattet i møte den 14. februar 2018 vedtak om at det, med bakgrunn i utarbeidet prosjektplan, skulle gjennomføres et forvaltningsrevisjonsprosjekt rettet mot IKT-sikkerhet i kommunen. Området inngår som et tema i kontrollutvalgets plan for forvaltningsrevisjon (2017-2020).

Problemstillinger og metode

Problemstillingene gjør seg gjeldende i følgende hovedspørsmål:

I. I hvilken grad har kommunen etablert tilfredsstillende rutiner og systemer for å ivareta krav til IKT-sikkerhet?
    a. Personvern
    b. Kriseløsninger, sikkerhetskopiering av data (backup) mv.

II. I hvilken grad fungerer fastlagte rutiner og systemer for IKT-sikkerhet i praksis?

I undersøkelsen er det intervjuet fem personer. Respondentene fordeler seg på rådmannens stab, IKT-avdelingen, sektor for helse, omsorg velferd, samt sektor for oppvekst. I relasjon til problemstillingen er det foretatt enkelte tester og observasjoner rutiner og praksis. Hensikten har vært å supplere intervjudataene.

Forvaltningsrevisjonens innsamlede data er vurdert opp mot utledede revisjonskriterier, herunder kriterier fra blant annet følgende kilder:

- Personvernforordningen[1] (2018).
- Kommuneloven (1992).
- E-forvaltningsforskriften (2004).
- ISACA (2009): Grunnleggende retningslinjer for god IT-skikk.

[1] Personvernforordningen omtales også som GDPR. I Norge trådte forordningen i kraft 20. juli 2018.

Hovedkonklusjon og anbefalinger

Revisors samlede konklusjon at Åsnes kommunes praksis innen det reviderte området i hovedsak synes å fungere tilfredsstillende. Revisor fremmer samtidig enkelte anbefalinger:

- Kommunen har utarbeidet en prosedyre for beredskapsplanlegging innen IKT. Av prosedyren, som er datert 6. april 2018, går det frem at kommunen skal utarbeide en kriseplan for tilfeller der vesentlige deler av informasjonssystemet faller ut. I undersøkelsen blir det opplyst at kriseplanen så langt ikke er utarbeidet, men at en er i startgropen med å påbegynne dette arbeidet.

  Revisor anbefaler at kommunen følger opp arbeidet med å utarbeide en kriseplan for IKT-området, herunder at planen inneholder tiltak knyttet til å gjennomføre regelmessige øvelser innen området.

- [redacted]

  Revisor vil anbefale at kommunen vurdere disse tiltakene nærmere.

- I undersøkelsen blir det tilkjennegitt at det trolig foreligger forskjellig kjennskap og kunnskap knyttet til personvern og generell IKT-sikkerhet i kommunens ulike avdelinger, hvilket også inkluderer utarbeidede prosedyrer innen området. En utbredt erkjennelse blant respondentene er at den største sikkerhetsrisikoen innenfor IKT er knyttet til menneskelig svikt i hverdagen. Flere respondenter gir uttrykk for at det hadde vært formålstjenlig om alle medarbeidere, som benytter kommunens datasystemer, ble gitt et kort kurs / gjennomgang av kommunens retningslinjer for informasjonssikkerhet/personvern, herunder at de ansatte måtte undertegne på at retningslinjene var forstått og at de forpliktet seg til å følge dem. Dette er også et tiltak som er inntatt i kommunens sikkerhetsstrategi for informasjonssikkerhet, men som ennå ikke er gjennomført. Det opplyses imidlertid at ulike kurstilbud er til vurdering i kommuneadministrasjonen.

  Revisor vil anbefale at kommunen følger opp ovennevnte tiltak overfor medarbeiderne i kommunen.

1 Innledning

1.1 Bestilling og hjemmel for forvaltningsrevisjon

I henhold til forskrift om kontrollutvalg av 15. juni 2004, skal kontrollutvalget påse at kommunens virksomhet årlig blir gjenstand for forvaltningsrevisjon. Kontrollutvalget i Åsnes kommune fattet i møte den 14. februar 2018, jf. sak 8/18, vedtak om at det, med bakgrunn i utarbeidet prosjektplan, skulle gjennomføres et forvaltningsrevisjonsprosjekt rettet mot IKT-sikkerhet i kommunen. Området inngår som et tema i kontrollutvalgets plan for forvaltningsrevisjon (2017-2020).

1.2 Kommunikasjon med rådmannen/revidert enhet

Den 30. oktober 2018 sendte revisjonen oppstarts brev til rådmannen hvor det ble informert om igangsettelsen av inneværende forvaltningsrevisjon mv. Revisjonen mottok svarbrev med oppnevnelse av kommunens kontaktpersoner den 6. november 2018.

Utkastet til forvaltningsrevisjonens revisjonskriterier ble sendt rådmannen til uttalelse den 26. februar 2019. Den 15. mars 2019 mottok revisor tilbakemelding fra rådmannen. Det ble opplyst at kommunen anså kriteriene som relevante for undersøkelsen.

Forvaltningsrevisjonsrapporten ble sendt rådmannen til uttalelse den 4. april 2019. Den 24. april 2019 mottok revisor rådmannens uttalelse som er inntatt i rapportens kapittel 6.

1.3 Kort om kommunes IKT-avdeling

Åsnes kommunes IKT-avdeling inngår i rådmannens stab og ledes av IKT-lederen. Avdelingen består av tre faste stillinger samt av en lærling.

IKT-avdelingen har ansvar for drift og vedlikehold av kommunens datanettverk og IKT-løsninger, brukerstøtte, videre utvikling av de tekniske løsningene, klargjøring av maskinvare og programvare. Avdelingen deltar i prosjekter sammen med kommunens fagavdelinger i forbindelse med valg, kjøp og innføring av nye dataløsninger i kommunen.

1.4 Rapportens videre strukturelle oppbygging

I kapittel 2 gis det en beskrivelse av prosjektets formål og av prosjektets problemstilling.

Prosjektets kilder til revisjonskriterier presenteres i kapittel 3.

Kapittel 4 utgjør rapportens metodekapittel. Her presenteres undersøkelsens metodiske fremgangsmåte.

Data innhentet i forbindelse med undersøkelsen presenteres i kapittel 5 og analyseres med henblikk på revisjonskriteriene. Her fremkommer revisors vurderinger, anbefalinger og samlede konklusjon knyttet til analysen.

Rådmannens uttalelse til rapporten fremkommer av kapittel 6.

2 Formål, problemstillinger og avgrensning

Prosjektets formål og problemstillinger er basert på risiko- og vesentlighetsvurderinger som er trukket opp i overordnet analyse og plan for forvaltningsrevisjon.

2.1 Formål

Formålet med forvaltningsrevisjonen er å undersøke i hvilken grad kommunen har etablert tilfredsstillende IKT-sikkerhetstiltak, samt om tiltakene fungerer i praksis.

2.2 Problemstillinger

Problemstillingene gjør seg gjeldende i følgende hovedspørsmål:

I. I hvilken grad har kommunen etablert tilfredsstillende rutiner og systemer for å ivareta krav til IKT-sikkerhet?

   a. Personvern

   b. Kriseløsninger, sikkerhetskopiering av data (backup) mv.

II. I hvilken grad fungerer fastlagte rutiner og systemer for IKT-sikkerhet i praksis?

2.3 Avgrensning

Informasjonssikkerhet omfatter både muntlig, papirbasert og digital behandling av informasjon. Denne forvaltningsrevisjonen er primært avgrenset til digital behandling av informasjon, nærmere bestemt IKT-sikkerhet. I en del tilfeller benyttes imidlertid informasjonssikkerhet som et generelt begrep i rapporten. Dette skyldes blant annet at mange av kommunens rutiner omfatter informasjonssikkerhet i sin alminnelighet, og ikke kun IKT-sikkerhet.

3 Revisjonskriterier

3.1 Valg av revisjonskriterier

Revisjonskriterier skal begrunnes i/utledes av autoritative kilder innenfor det reviderte området. Autoritative kilder kan være lover, forskrifter, forarbeider, rettspraksis, politiske vedtak/mål/føringer, administrative retningslinjer/mål/føringer, statlige føringer/veiledere, andre myndigheters praksis, teori og reelle hensyn som vurderinger av hva som er rimelig/formålstjenlig/effektivt[2].

Revisjonskriteriene velges ut med bakgrunn i problemstillingen og danner grunnlaget for hva de innhentede data vurderes opp mot. I og med at revisjonskriteriene er uttrykk for en norm eller et ideal for hvorledes tilstanden bør være på området, er kriteriene også med på å danne utgangspunktet for revisors anbefalinger.

I dette prosjektet benyttes revisjonskriterier fra følgende kilder:

- Personvernforordningen (2018).
- Kommuneloven (1992).
- Odelstingsproposisjon nr. 70 (2002–2003): Vedrørende div. endringer i kommuneloven.
- E-forvaltningsforskriften (2004).
- ISACA (2009): *Grunnleggende retningslinjer for god IT-skikk.*
- COSO (2005): *Helhetlig risikostyring - et integrert rammeverk.*
- Kommunaldepartementet (2009): *85 tilrådingar for styrkt eigenkontroll i kommunane.*
- Datatilsynet (2009): *En veiledning om internkontroll og informasjonssikkerhet.*
- Datatilsynet (2018): *Veileder. Internkontroll og informasjonssikkerhet.*
- Direktoratet for forvaltning og IKT (2016): *Internkontroll i praksis – informasjons-sikkerhet. Grunnleggende innføring.*

[2] Norges Kommunerevisorforbund (2011): RSK *001 Standard for forvaltningsrevisjon.*

- Implementeringsteori.

For nærmere utledning av revisjonskriterier vises det til vedlegg B.

4 Metode for revisjonen

4.1 Om metodevalget

Det er hva problemstillingen ønsker å undersøke som bør avgjøre metodevalget (Holme og Solvang: 1996). Etter en samlet vurdering har det blitt gjennomført kvalitative intervjuer samt enkelte tester og observasjoner av rutiner og praksis.

Metodevalget begrunnes ut ifra problemstillingens komplekse karakter. På denne måten kan det, i form av kvalitative intervjuer, bringes til veie dybde og detaljrikdom vedrørende IKT-sikkerhet i Åsnes kommune. Enkelte tester og observasjoner kan, på sin side, supplere intervjudataene. Det er således tale om en kombinasjon av ulike metoder, det vil si metodetriangulering.

4.2 Utvalg

I undersøkelsen er det intervjuet fem personer, det vil si undersøkelsens totale antall respondenter. Følgende personer er intervjuet:

- Spesialrådgiver hos rådmannen. Spesialrådgiveren leder kommunens sikkerhetsutvalg for informasjonssikkerhet og har et koordineringsansvar for kommunens iverksettelse av personvernforordningen.
- Leder for kommunens IKT-avdeling og arkiv.
- Avdelingsleder for koordinering, fag og forvaltning i sektor for helse, omsorg og velferd.
- Skole- og barnehagefaglig rådgiver hos sektorleder for oppvekst.
- Konsulent i IKT-avdelingen. Konsulenten arbeider med IKT mot kommunens skoler.

Det er et bevisst valg å intervjue representanter ifra ulike avdelinger i kommunen, herunder ifra sektor for helse, omsorg og velferd samt ifra sektor for oppvekst. Dette utgjør store sektorer som håndterer mange sensitive personopplysninger. Utgangspunktet er at intervju-respondentene innehar ulike posisjoner og roller. I rolleteorien forklares atferd som en konsekvens av forventninger. Rolleteorien bygger på begrepet posisjon i organisasjonen (hierarkiet) (Andersen, J. A.: 1995). Til den som innehar en bestemt posisjon finnes det forventninger ifra andre, for eksempel ifra kollegaer, samarbeidspartnere og offentligheten,

om hvorledes vedkommende skal håndtere sitt arbeid. Den som innehar posisjonen har dessuten sine egne forventninger til hvorledes han eller hun bør fylle sin rolle og løse oppgavene. Informasjonen som det enkelte intervjuobjekt gir vil svært ofte være påvirket av posisjonen og dermed også rollen som det enkelte intervjuobjekt innehar.

I relasjon til problemstillingen er det foretatt test av rutine for backup samt observasjon av enkelte fysiske sikringstiltak på [redacted] serverrom. Hensikten har, som nevnt, vært å supplere intervjudataene.

***

For angivelse av undersøkelsens reliabilitet og validitet vises det til vedlegg C.

5 Innhentende data og analyse

I dette kapittelet fremkommer undersøkelsens innhentede data, som igjen analyseres med henblikk på revisjonskriteriene og angis i form av revisors vurderinger og anbefalinger. Deretter angis revisors samlede konklusjon for det gjennomførte forvaltnings-revisjonsprosjektet.

5.1 Hovedspørsmål I: Rutiner og systemer for å ivareta IKT-sikkerhet

Hovedspørsmål I, jf. punkt 2.2, fokuserer på i hvilken grad kommunen har etablert tilfredsstillende rutiner og systemer for å ivareta krav til IKT-sikkerhet. I denne forbindelse omfatter dette:

a. Personvern

b. Kriseløsninger, sikkerhetskopiering av data (backup) mv.

Av punkt 9.1 i vedlegg B går det frem at revisor legger til grunn følgende oppsummerte revisjonskriterier for hovedspørsmål I:

- Kommunen har beskrevet mål og strategi for IKT-sikkerhet i virksomheten. Dette benevnes som sikkerhetsmål og sikkerhetsstrategi og skal danne grunnlaget for forvaltningsorganets internkontroll innen området. Omfang og innretning på internkontrollen skal være tilpasset risiko og bør utgjøre en integrert del av virksomhetens helhetlige styringssystem.
- Kommunen har gjennomført en risikovurdering og utarbeidet nødvendige skriftlige rutiner for håndtering av personopplysninger.
- Kommunen har fokus på kriseløsninger innen IKT-området. Dette innebærer behov for planverk, tekniske løsninger samt regelmessige øvelser.
- Kommunen har etablert tiltak som kan bidra til driftskontinuitet og til å forebygge alvorlige hendelser innen IKT-området. Blant annet vil dette innbefatte å sikre:
    - Klart definerte roller og arbeidsdeling.
    - Jevnlig oppdatering av operativsystem, programvarer, antivirus-program og brannmur.

- Rutiner for sikkerhetskopiering av data (backup).
- Tilgangsstyring til systemer.
- Tiltak mot innbrudd, vannskader, brann o.l.

5.1.1 Innhentede data

I undersøkelsen blir det gitt uttrykk for at kommunen har nedlagt et betydelig arbeid knyttet til informasjonssikkerhet, herunder personvern og generell IKT-sikkerhet. Kommunen nedsatte i 2017 en felles prosjektgruppe til å forberede innføringen av personvernforordningen (GDPR) mv. Personvernforordningen ble iverksatt som norsk lov fra 20. juli 2018.

Den nedsatte prosjektgruppen, som fremdeles er virksom, er bredt sammensatt med deltakere fra følgende avdelinger:

- Rådmannens stab, herunder funksjonene HR, lønn, IKT, arkiv samt spesialrådgiver.
- Sektor for helse, omsorg og velferd.
- Sektor for oppvekst.

Som et resultat av prosjektet er det foretatt kartlegging i relasjon til hva hvert av kommunens ca. 70 datasystemer inneholder av personopplysninger, herunder om systemene inneholder sensitive og/eller ikke-sensitive personopplysninger. I denne forbindelse er det utarbeidet en protokoll for hvert datasystem. Noen systemer inneholder ingen personopplysninger av noe slag.

Den ovennevnte prosjektgruppen har utarbeidet en del skriftlige rutiner (prosedyrer) relatert til personvernforordningen og generell informasjonssikkerhet (se oversikt i vedlegg E). Prosedyrene er inndelt i kategoriene *styrende, gjennomførende, daglige* og *kontrollerende.* Kommunen har også utarbeidet sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet, herunder tilhørende prosedyrer for risikobasert internkontroll mv.

En rekke ansatte i kommuneadministrasjonen har, ved siden av prosjektgruppens medlemmer, deltatt i arbeidet med å utarbeide prosedyrene. Enkelte kommunale avdelinger har samtidig etablert undergrupper til å arbeide med tematikken. Selv om kommunen også har hatt prosedyrer forut for innføringen av personvernforordningen, blir det opplyst at det

har forekommet et betydelig behov for å oppdatere gamle prosedyrer og utarbeide en rekke nye.

Noen av de utarbeidede prosedyrene er overordnede og omfatter hele kommunens organisasjon, mens andre er utarbeidet for bestemte avdelinger. Dette skyldes blant annet at avdelingene må tilpasse seg ulike særlover og krav. Helse- og omsorgstjenesten, oppvekstsektoren og NAV har eksempelvis utarbeidet egne tilleggsprosedyrer i relasjon til personvernforordningen m.m. Videre har Åsnes kommune utarbeidet en personvernerklæring som er publisert på kommunens hjemmeside. Denne erklæringen er primært rettet mot kommunens innbyggere og inneholder grunnleggende informasjon om kommunens behandling av personopplysninger mv.

I undersøkelsen går det frem at den nedsatte prosjektgruppen har foretatt en risikovurdering knyttet til hva kommunen har behov for av prosedyrer innen personvern og generell informasjonssikkerhet. Det blir tilkjennegitt at kommunens utarbeidede prosedyrer dekker Datatilsynets rutineangivelse på en risikobasert og tilfredsstillende måte, nærmere bestemt i forhold til områdene hvor tilsynet har anført at det kan være hensiktsmessig med egne rutiner for håndtering av personopplysninger (jf. punkt 9.1). På den annen side utelukker ikke respondentene at det kan være behov for å gjøre endringer i kommunens prosedyrer etterhvert, blant annet som følge av at personvernforordningen representerer et omfattende og til dels nytt område. Det blir tilkjennegitt at innføringen av personvernforordningen har medført et visst tidspress i kommunen når det gjelder å utarbeide prosedyrer innen området. I denne forbindelse blir det uttalt at enkelte prosedyrer trolig kan være noe overlappende og representere ulike vinklinger til samme tematikk. Følgelig kan det være behov for noen redaksjonelle endringer etterhvert.

I undersøkelsen går det frem at alle de utarbeidede prosedyrene er gjort gjeldende. De er lagret i kommunens elektroniske kvalitetssystem *Compilo* og ligger åpent for alle ansatte med tilgang til kommunens datasystemer. Når prosedyrene, herunder prosedyrene for internkontroll, blir lagret i kommunens kvalitetssystem Compilo, utgjør de en integrert del av kommunens helhetlige styringssystem. Compilo er et søkbart system og inneholder både overordnede prosedyrer og styringsdokumenter, samt egne mapper for ulike avdelinger og fagområder.

***

Åsnes kommune har utarbeidet en prosedyre for beredskapsplanlegging innen IKT. Av prosedyren, som er datert 6. april 2018, går det frem at kommunen skal utarbeide en kriseplan for tilfeller der vesentlige deler av informasjonssystemet faller ut. I undersøkelsen blir det opplyst at kriseplanen så langt ikke er utarbeidet, men at en er i startgropen med å påbegynne dette arbeidet.

Kommunens sektor for helse, omsorg og velferd har utarbeidet skriftlige rutiner for kriseløsninger. Sektoren har som ordning å alltid oppbevare papirkopi av pasientenes hovedkort[3] og legemiddelkort. Dette utgjør en sikkerhet dersom det skulle oppstå nedetid for det elektroniske pasientjournalsystemet. En av de største risikoene innen helse- og omsorgsfeltet, opplyses å være nedetid for pasientjournalsystemet over lengre tid. Dette forekommer imidlertid meget sjeldent. En respondent forteller at det har skjedd i forbindelse med ekstremværet Dagmar i 2011 samt to dager knyttet til en planlagt hendelse.

Av undersøkelsen går det frem at kommunen har etablert flere tiltak som kan bidra til å sikre driftskontinuitet og til å forebygge alvorlige hendelser innen IKT-området. Dette inkluderer blant annet:

- Klart definerte roller og arbeidsdeling. I undersøkelsen blir det tilkjennegitt at kommunen har vektlagt å definere roller og arbeidsdeling innen IKT-området. Det er utarbeidet en skriftlig prosedyre som definerer sikkerhetsorganisasjon og ansvar. I prosedyren beskrives funksjonene til følgende stillinger/organ:
    - Rådmannen
    - Rådmannens sikkerhetsutvalg for informasjonssikkerhet
    - Spesialrådgiver hos rådmannen
    - Sektorledere / enhetsledere / avdelingsledere
    - IKT-leder

[3] Hovedkortet inneholder opplysninger om hvem pasienten er, pasientens sykdomssituasjon, tjenestene som mottas, samt hvem pårørende er.

- Personvernombud
- Arkivleder

- Jevnlig oppdatering - operativsystem, programvarer, antivirusprogram og brannmur. Det blir opplyst at det foretas automatisk oppdatering av operativsystem og antivirusprogram, mens programvarer og brannmur oppdateres manuelt. I undersøkelsen blir det tilkjennegitt at IKT-avdelingen er løpende inne på server for å undersøke om det foreligger aktuelle oppdateringer for programvarer og brannmur.
- Rutiner for sikkerhetskopiering av data (backup). I undersøkelsen går det frem at det er utarbeidet skriftlige rutiner for backup [redacted]
- Tilgangsstyring til systemer. Det foreligger skriftlige rutiner for tilgangsstyring til systemer. I kommunen er det IKT-avdelingen som oppretter tilganger til fagsystemene, men det er kommunens fagavdelinger som styrer hvilke data den enkelte bruker skal ha tilgang til i et system. Kommunens fastslåtte prinsipp er at tilganger til systemer og informasjon kun skal gis til brukere etter behov («need to know»).

  Ved pålogging til brukerkonto benyttes det brukernavn og passord (7 tegn bestående av bokstaver, tall og spesialtegn). Når ansettelsesforhold opphører / elever slutter, sperres konto automatisk.
- Bruk av tynnklienter. I undersøkelsen blir det opplyst at kommunen har gått over til å kun benytte tynnklienter. Dette da tynnklienter gir bedre sikkerhet enn tykke klienter og er enklere å håndtere personalmessig i form av sentral styring.
- [redacted] Det fremkommer at kommunen lagrer det meste av sitt materiale på server [redacted] I undersøkelsen blir det tilkjennegitt at utviklingen går mot at stadig mer vil bli lagret i skyløsning. Pr. i dag benytter kommunen

hovedsakelig skyløsning for skoleadministrativt system og for PPT-system. Det går frem at kommunen har inngått databehandleravtaler med leverandører som besitter personopplysninger om elever.

- Nødstrømaggregat for serverrom. Det fremkommer at det er installert nødstrømaggregat for drift av [redacted] serverrom mv. IKT-avdelingen har ikke gjennomført strømbruddøvelse tidligere, men det blir opplyst at en slik øvelse vil bli gjennomført våren 2019. Dette blir beskrevet som et viktig forhold å øve på.

- Supplerende servere. I undersøkelsen går det frem at kommunens datasystem er satt opp med flere supplerende virtuelle servere, slik at en virtuell server overtar automatisk dersom en annen går i stykker. Dette for å sikre beredskap og hindre nedetid.

- Beredskapsordning for sentrale enkeltkomponenter innen IKT. Det blir tilkjennegitt at om følgende enkeltkomponenter går i stykker, vil ikke noe fungere innen kommunens IKT-system:

  [redacted]

  I undersøkelsen går det frem at kommunen har etablert en beredskapsordning med private leverandører knyttet til om noen av ovennevnte komponenter går i stykker. Responstiden for feilretting er avtalt til å være innen fire timer.

- Tiltak mot innbrudd, vannskader, brann o.l. Det blir opplyst at [redacted] serverrom er sikret med flere tiltak, herunder:

  - Det er fastsatt at serverrommet skal være kontinuerlig låst. [redacted]

  - IKT-avdelingen tilkjennegir at serverrommet har murvegger og er uten vannrør. Dette som en sikkerhet mot brann og vannlekkasjer.

- Dersom kjøleanlegget på serverrommet går i stykker, kan serverne bli ødelagte og satt ut av drift. Det blir tilkjennegitt at serverrommet er sikret med automatisk temperaturmåling, og at denne anordningen sender ut varsel på e-post dersom temperaturen i rommet blir for høy.

[redacted]

5.1.2 Revisors vurdering og anbefaling

Revisors vurdering er at Åsnes kommune etterlever ovennevnte revisjonskriterier på en i hovedsak tilfredsstillende måte. Som begrunnelse for dette vil revisor anføre følgende funn:

- I undersøkelsen blir det gitt uttrykk for at kommunen har nedlagt et betydelig arbeid knyttet til informasjonssikkerhet, herunder personvern og generell IKT-sikkerhet. Kommunen nedsatte i 2017 en felles prosjektgruppe til å forberede innføringen av personvernforordningen (GDPR) mv. Som et resultat av prosjektet er det foretatt kartlegging i relasjon til hva hvert av kommunens ca. 70 datasystemer inneholder av personopplysninger, herunder om systemene inneholder sensitive og/eller ikke-sensitive personopplysninger. I denne forbindelse er det utarbeidet en protokoll for hvert datasystem.
- Kommunen har utarbeidet sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet, herunder tilhørende prosedyrer for risikobasert internkontroll mv.
- Den nedsatte prosjektgruppen har, i samarbeid med en rekke ansatte i kommuneadministrasjonen, utarbeidet en del skriftlige rutiner (prosedyrer) relatert til personvernforordningen og generell informasjonssikkerhet. I undersøkelsen går det frem at prosjektgruppen har foretatt en risikovurdering knyttet til hva kommunen har behov for av prosedyrer innen personvern og generell informasjonssikkerhet. Det blir tilkjennegitt at kommunens utarbeidede prosedyrer dekker Datatilsynets rutineangivelse på en risikobasert og tilfredsstillende måte.
- I undersøkelsen går det frem at alle de utarbeidede prosedyrene er gjort gjeldende. De er lagret i kommunens elektroniske kvalitetssystem *Compilo* og ligger åpent for

alle ansatte med tilgang til kommunens datasystemer. Når prosedyrene, herunder prosedyrene for internkontroll, blir lagret i kommunens kvalitetssystem Compilo, utgjør de en integrert del av kommunens helhetlige styringssystem. Compilo er et søkbart system og inneholder både overordnede prosedyrer og styringsdokumenter samt egne mapper for ulike avdelinger og fagområder.

- Kommunens sektor for helse, omsorg og velferd har utarbeidet skriftlige rutiner for kriseløsninger. Sektoren har som ordning å alltid oppbevare papirkopi av pasientenes hovedkort og legemiddelkort. Dette utgjør en sikkerhet dersom det skulle oppstå nedetid for det elektroniske pasientjournalsystemet.

- Kommunen har utarbeidet en prosedyre for beredskapsplanlegging innen IKT. Av prosedyren, som er datert 6. april 2018, går det frem at kommunen skal utarbeide en kriseplan for tilfeller der vesentlige deler av informasjonssystemet faller ut. I undersøkelsen blir det opplyst at kriseplanen så langt ikke er utarbeidet, men at en er i startgropen med å påbegynne dette arbeidet.

  Revisor anbefaler at kommunen følger opp arbeidet med å utarbeide en kriseplan for IKT-området, herunder at planen inneholder tiltak knyttet til å gjennomføre regelmessige øvelser innen området.

- I undersøkelsen går det frem at kommunen har etablert flere tiltak som kan bidra til å sikre driftskontinuitet og til å forebygge alvorlige hendelser innen IKT-området. Dette inkluderer blant annet:

  - Klart definerte roller og arbeidsdeling.
  - Jevnlig oppdatering av operativsystem, programvarer, antivirus-program og brannmur.
  - Rutiner for sikkerhetskopiering av data (backup).
  - Tilgangsstyring til systemer.
  - Tiltak mot innbrudd, vannskader, brann o.l.

[redacted]

Revisor vil anbefale at kommunen vurdere disse tiltakene nærmere.

5.2 Hovedspørsmål II: Om rutiner og systemer for IKT-sikkerhet fungerer

Hovedspørsmål II, jf. punkt 2.2, fokuserer på i hvilken grad fastlagte rutiner og systemer for IKT-sikkerhet fungerer i praksis. Av punkt 9.2 i vedlegg B går det frem at revisor legger til grunn følgende oppsummerte revisjonskriterier for hovedspørsmål II:

- Som en del av internkontrollen må virksomheten sørge for at den gjøres kjent og etterleves blant de ansatte. I denne forbindelse bør de ansatte gis opplæring og innsikt i sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle sikkerhetsrisikoer.

- Det bør, sett i forhold til oppfølging av fastlagte rutiner og systemer for IKT-sikkerhet, være etablert kanaler som sikrer at nødvendig informasjon blir mottatt og fulgt opp. Dette inkluderer iverksettelse av eventuell avviksbehandling.

- Kommunen bør vektlegge at rutinene og systemene for håndtering av IKT-sikkerhet fungerer etter hensikten. Derfor vil det være sentralt å innføre faste rutiner for å forbedre og vedlikeholde internkontrollen, herunder dokumentere erfaring, lære av uønskede hendelser, samt forbedre arbeidsprosessene slik at færrest mulig uønskede hendelser oppstår.

5.2.1 Innhentede data

Av undersøkelsen går det frem at flere ansatte i Åsnes kommune har gjennomført kurs relatert til personvernforordningen (GDPR). I 2018 gjennomførte blant annet 45 ansatte et lokalt/regionalt innføringskurs om emnet. Andre aktører som fagforeninger har også avholdt kurs knyttet til personvernforordningen.

En sentral respondent tilkjennegir at en utfordring kan være å bevisstgjøre mange nok ansatte rundt den nylig iverksatte personvernforordningen (forordningen ble iverksatt som norsk lov fra 20. juli 2018). Derfor har kommunens ledere blitt oppfordret til å ha fokus på temaet i personalmøter. Videre planlegger kommunen å gjennomføre et temamøte om personvern rettet mot kommunens mellomledere våren 2019.

Kommunene i Kongsvingerregionen har nylig opprettet et felles personvernombud. Det blir gitt uttrykk for at personvernombudet vil ha en viktig funksjon med hensyn til å gi råd og veiledning. I og med at personvernombudet skal betjene seks kommuner i

Kongsvingerregionen, kan det også foretas sammenligninger mellom hvordan kommunene har tilpasset seg regelverket (beste praksis).

I undersøkelsen blir det tilkjennegitt at det trolig foreligger forskjellig kjennskap og kunnskap knyttet til personvern og generell IKT-sikkerhet i kommunens ulike avdelinger, hvilket også inkluderer utarbeidede prosedyrer innen området. En bakgrunn for dette opplyses å være at avdelingene må tilpasse seg ulike særlover og krav, foruten at kulturforskjeller og profesjonshensyn kan gjøre seg gjeldende. Eksempelvis foreligger det mange sensitive personopplysninger innen områder som helse, omsorg, sosial, barnevern og oppvekst. Flere respondenter gir uttrykk for at dette også vil ha innvirkning på de ansattes praksis og vektleggelse av personvern og IKT-sikkerhet. Det fremkommer samtidig at den enkelte leder har et sentralt ansvar for å informere egne ansatte om fagområdet, herunder om utarbeidede prosedyrer. Dette er nedfelt som et ledelsesansvar i kommunens prosedyre for sikkerhetsorganisasjon og ansvar.

En utbredt erkjennelse blant respondentene er at den største sikkerhetsrisikoen innenfor IKT er knyttet til menneskelig svikt i hverdagen. Eksempelvis vil det være en alvorlig svikt om sensitiv informasjon blir publisert på internett eller tilgjengeliggjort overfor mange ved en feiltagelse. En annen fare er at e-post kan inneholde vedlegg eller lenker med kryptovirus. Flere respondenter gir uttrykk for at det hadde vært formålstjenlig om alle medarbeidere, som benytter kommunens datasystemer, ble gitt et kort kurs / gjennomgang av kommunens retningslinjer for informasjonssikkerhet/personvern, herunder at de ansatte måtte undertegne på at retningslinjene var forstått og at de forpliktet seg til å følge dem. Dette er også et tiltak som er inntatt i kommunens sikkerhetsstrategi for informasjonssikkerhet, men som ennå ikke er gjennomført. Det opplyses imidlertid at ulike kurstilbud er til vurdering i kommuneadministrasjonen.

I undersøkelsen går det frem at kommunen ikke foretar noen systematisk kontroll av at prosedyrer for informasjonssikkerhet/personvern følges, men at ansatte har plikt til å melde ifra om avvik dersom informasjon ikke blir håndtert i samsvar med lov, forskrift, policy, eller om informasjon kommer på avveie. Dette er nedfelt som et ansvar i kommunens prosedyre for avvikshåndtering innen området.

I Åsnes kommune skal avvik meldes i det elektroniske kvalitetssystemet *Compilo*. Kvalitetssystemet omfatter alle sektorer og avdelinger i kommunen, og det skal meldes avvik knyttet til kategoriene *tjenesteyting, HMS og organisatoriske forhold.* Dette vil også kunne omfatte avvik knyttet til informasjonssikkerhet/personvern. Det blir opplyst at det er registrert få avvik innen området, men at kommunen har avdekket et brudd relatert til snoking i pasientjournal. Dette forholdet resulterte i at vedkommende mottok en reprimande og at saken ble tatt opp med Statens helsetilsyn.

Det fremkommer at kommunen har etablert egne rutiner for revisjon av prosedyrer. I hver prosedyre skal det settes inn en dato for revisjon samt revisjonsansvarlig person. Dette legges inn i det elektroniske kvalitetssystemet Compilo, og revisjonsansvarlig mottar automatisk påminnelse når revisjonsdato nærmer seg. En prosedyre blir ikke godkjent i Compilo med mindre det settes inn en dato for revisjon. Dette er ment som et systematisk verktøy for å forbedre og vedlikeholde internkontrollen.

I Åsnes kommune er det etablert et fast sikkerhetsutvalg for informasjonssikkerhet. Foruten rådmannen består utvalget av fem ansatte fra ulike kommunale avdelinger, heriblant IKT-avdelingen. Sikkerhetsutvalget har en sentral funksjon når det gjelder å forbedre og vedlikeholde internkontrollen, lære av uønskede hendelser, samt forbedre arbeidsprosessene slik at færrest mulig uønskede hendelser oppstår. I undersøkelsen beskrives arbeidet i utvalget som nyttig.

Følgende konkrete oppgaver er tillagt sikkerhetsutvalget:

- Ansvarlig for å revidere kommunens politikk om informasjonssikkerhet.
- Ansvarlig for å overvåke relevante trusler mot kommunens informasjonsverdier og tekniske utstyr.
- Ansvarlig for å overvåke sikkerhetsbrudd.
- Diskusjonsforum i spørsmål som gjelder informasjonssikkerhet/personvern. Dette inkluderer også investeringer i sikkerhetstiltak.

Det skrives referat fra møtene i sikkerhetsutvalget.

***

Revisor har foretatt test av rutine for backup samt observasjon av enkelte fysiske sikringstiltak på [redacted] serverrom. Med bakgrunn i forespørsel fra revisor gjenopprettet IKT-avdelingen en slettet mappe på server ved hjelp av backup. De fysiske sikringstiltakene på serverrommet var som angitt av kommunen (låst dør [redacted] rommet har murvegger og er uten vannrør).

5.2.2 Revisors vurdering og anbefaling

Revisors vurdering er at Åsnes kommune etterlevd ovennevnte revisjonskriterier på en i hovedsak tilfredsstillende måte. Som begrunnelse for dette vil revisor anføre følgende funn:

- Av undersøkelsen går det frem at flere ansatte i Åsnes kommune har gjennomført kurs relatert til personvernforordningen (GDPR). En sentral respondent tilkjennegir at en utfordring kan være å bevisstgjøre mange nok ansatte rundt den nylig iverksatte personvernforordningen. Derfor har kommunens ledere blitt oppfordret til å ha fokus på temaet i personalmøter. Videre planlegger kommunen å gjennomføre et temamøte om personvern rettet mot kommunens mellomledere våren 2019.
- I undersøkelsen blir det tilkjennegitt at det trolig foreligger forskjellig kjennskap og kunnskap knyttet til personvern og generell IKT-sikkerhet i kommunens ulike avdelinger, hvilket også inkluderer utarbeidede prosedyrer innen området. En utbredt erkjennelse blant respondentene er at den største sikkerhetsrisikoen innenfor IKT er knyttet til menneskelig svikt i hverdagen. Flere respondenter gir uttrykk for at det hadde vært formålstjenlig om alle medarbeidere, som benytter kommunens datasystemer, ble gitt et kort kurs / gjennomgang av kommunens retningslinjer for informasjonssikkerhet/personvern, herunder at de ansatte måtte undertegne på at retningslinjene var forstått og at de forpliktet seg til å følge dem. Dette er også et tiltak som er inntatt i kommunens sikkerhetsstrategi for informasjonssikkerhet, men som ennå ikke er gjennomført. Det opplyses imidlertid at ulike kurstilbud er til vurdering i kommuneadministrasjonen.

  Revisor vil anbefale at kommunen følger opp ovennevnte tiltak overfor medarbeiderne i kommunen.
- I Åsnes kommune skal avvik meldes i det elektroniske kvalitetssystemet *Compilo*. Kvalitetssystemet omfatter alle sektorer og avdelinger i kommunen, og det skal

meldes avvik knyttet til kategoriene *tjenesteyting, HMS og organisatoriske forhold.* Dette vil også kunne omfatte avvik knyttet til informasjonssikkerhet/personvern. Det blir opplyst at det er registrert få avvik innen området, men at kommunen har avdekket et brudd relatert til snoking i pasientjournal. Dette forholdet resulterte i at vedkommende mottok en reprimande og at saken ble tatt opp med Statens helsetilsyn.

- Det fremkommer at kommunen har etablert egne rutiner for revisjon av prosedyrer. I hver prosedyre skal det settes inn en dato for revisjon samt revisjonsansvarlig person. Dette legges inn i det elektroniske kvalitetssystemet Compilo, og revisjonsansvarlig mottar automatisk påminnelse når revisjonsdato nærmer seg. En prosedyre blir ikke godkjent i Compilo med mindre det settes inn en dato for revisjon. Dette er ment som et systematisk verktøy for å forbedre og vedlikeholde internkontrollen.
- I Åsnes kommune er det etablert et fast sikkerhetsutvalg for informasjonssikkerhet. Foruten rådmannen består utvalget av fem ansatte fra ulike kommunale avdelinger, heriblant IKT-avdelingen. Sikkerhetsutvalget har en sentral funksjon når det gjelder å forbedre og vedlikeholde internkontrollen, lære av uønskede hendelser, samt forbedre arbeidsprosessene slik at færrest mulig uønskede hendelser oppstår. I undersøkelsen beskrives arbeidet i sikkerhetsutvalget som nyttig. Det skrives referat fra møtene i utvalget.
- Revisor har foretatt test av rutine for backup samt observasjon av enkelte fysiske sikringstiltak på [redacted] serverrom. Med bakgrunn i forespørsel fra revisor gjenopprettet IKT-avdelingen en slettet mappe på server ved hjelp av backup. De fysiske sikringstiltakene på serverrommet var som angitt av kommunen (låst dør [redacted] rommet har murvegger og er uten vannrør).

5.3 Revisors konklusjon og samlede anbefalinger

Problemstillingen gjør seg gjeldende i følgende hovedspørsmål:

I. I hvilken grad har kommunen etablert tilfredsstillende rutiner og systemer for å ivareta krav til IKT-sikkerhet?

   a. Personvern

   b. Kriseløsninger, sikkerhetskopiering av data (backup) mv.

II. I hvilken grad fungerer fastlagte rutiner og systemer for IKT-sikkerhet i praksis?

Med bakgrunn i vurderingene som er foretatt i punkt 5.2.1 og i punkt 5.2.2, er revisors samlede konklusjon at Åsnes kommunes praksis innen det reviderte området i hovedsak synes å fungere tilfredsstillende. Revisor fremmer samtidig som nevnt, enkelte anbefalinger:

- Kommunen har utarbeidet en prosedyre for beredskapsplanlegging innen IKT. Av prosedyren, som er datert 6. april 2018, går det frem at kommunen skal utarbeide en kriseplan for tilfeller der vesentlige deler av informasjonssystemet faller ut. I undersøkelsen blir det opplyst at kriseplanen så langt ikke er utarbeidet, men at en er i startgropen med å påbegynne dette arbeidet.

  Revisor anbefaler at kommunen følger opp arbeidet med å utarbeide en kriseplan for IKT-området, herunder at planen inneholder tiltak knyttet til å gjennomføre regelmessige øvelser innen området.

  [redacted]

  Revisor vil anbefale at kommunen vurdere disse tiltakene nærmere.

- I undersøkelsen blir det tilkjennegitt at det trolig foreligger forskjellig kjennskap og kunnskap knyttet til personvern og generell IKT-sikkerhet i kommunens ulike avdelinger, hvilket også inkluderer utarbeidede prosedyrer innen området. En utbredt erkjennelse blant respondentene er at den største sikkerhetsrisikoen innenfor IKT er knyttet til menneskelig svikt i hverdagen. Flere respondenter gir uttrykk for at det hadde vært formålstjenlig om alle medarbeidere, som benytter kommunens datasystemer, ble gitt et kort kurs / gjennomgang av kommunens

retningslinjer for informasjonssikkerhet/personvern, herunder at de ansatte måtte undertegne på at retningslinjene var forstått og at de forpliktet seg til å følge dem. Dette er også et tiltak som er inntatt i kommunens sikkerhetsstrategi for informasjonssikkerhet, men som ennå ikke er gjennomført. Det opplyses imidlertid at ulike kurstilbud er til vurdering i kommuneadministrasjonen.

Revisor vil anbefale at kommunen følger opp ovennevnte tiltak overfor medarbeiderne i kommunen.

6 Rådmannens uttalelse til rapporten

ÅSNES KOMMUNE

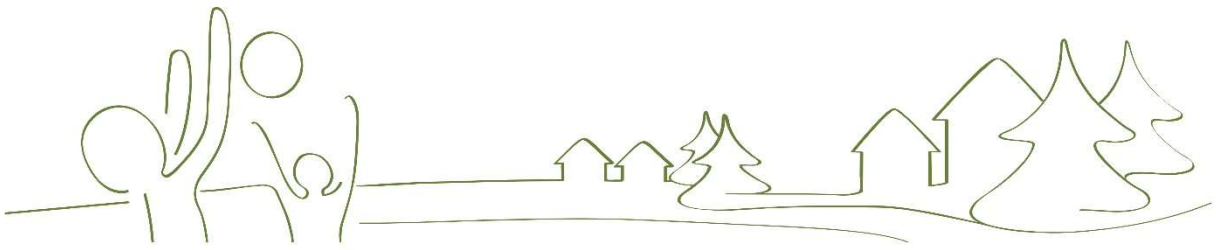
Rådmannens uttalelse rapport – forvaltningsrevisjon – IKT-sikkerhet i Åsnes kommune

Rådmannen har lest rapporten knyttet mot forvaltningsrevisjon – IKT-sikkerhet i Åsnes kommune.

Rådmannen har ikke funnet feil i selve rapporten. I all hovedsak er de funn som er gjort gjenkjennbare og i tråd med hvordan rådmannen vurderer at de faktiske forholdene er.

Flisa den 24. april 2019

Stein Halvorsen
rådmann



7 Kilder

Andersen, Jon Aarum (1995): *Ledelse og ledelsesteorier. Om hvilke svar ledelsesforskningen kan gi.* Oslo: Bedriftsøkonomens forlag.

Andersen, Kari Merete, Bodhild Laastad, Stein Ove Songstad og Anna Ølnes (2006): *Veileder i forvaltningsrevisjon.* Oslo: Norges Kommunerevisorforbund.

COSO (2005): *Helhetlig risikostyring - et integrert rammeverk. Oslo: Norges Interne Revisorers Forening.*

Datatilsynet (2009): En veiledning om internkontroll og informasjonssikkerhet. Oslo: Datatilsynet.

Datatilsynet (2018): Veileder. Internkontroll og informasjonssikkerhet. Oslo: Datatilsynet.

Direktoratet for forvaltning og IKT (2016): *Internkontroll i praksis – informasjons-sikkerhet. Grunnleggende innføring.* Oslo: Direktoratet for forvaltning og IKT.

E-forvaltningsforskriften (2004).

Eriksen, Frits A., Ole Kr. Rogndokken og Stein Ove Songstad (2000)*: Veileder forvaltningsrevisjon.* Oslo: Norges kommunerevisorforbund.

Forskrift om kontrollutvalg i kommuner og fylkeskommuner (2004).

Holme, Idar Magne og Bernt Krohn Solvang (1996): *Metodevalg og metodebruk.* 3. utgave. Oslo: Tano.

ISACA (2009): *Grunnleggende retningslinjer for god IT-skikk.* Oslo: ISACA Norway Chapter.

Jacobsen, Dag Ingvar (2005): *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode.* 2. utgave. Kristiansand: Høyskoleforlaget.

Kjelleberg, Francesco og Marit Reitan (1995): *Studiet av offentlig politikk. En innføring.* Oslo: Tano.

Kommunal- og regionaldepartementet (2009): *85 tilrådingar for styrkt eigenkontroll i kommunane.* Oslo: Kommunal- og regionaldepartementet.

Kommuneloven (1992).

Larsen, Ann Kristin (2007): *En enklere metode. Veiledning i samfunnsvitenskapelig forskningsmetode.* Bergen: Fagbokforlaget.

Norges Kommunerevisorforbund (2011): *RSK 001. Standard for forvaltningsrevisjon.* Oslo: Norges Kommunerevisorforbund.

Odelstingsproposisjon nr. 70 (2002–2003): *Om lov om endringer i lov 25. september 1992 nr. 107 om kommuner og fylkeskommuner m.m. (kommunal revisjon).* Oslo: Kommunal- og regionaldepartementet.

Offerdal, Audun (2005): «Iverksettingsteori – resultatene blir sjelden som planlagt». I Baldersheim, Harald og Lawrence E. Rose (red.): *Det kommunale laboratorium.* 2. utgave. Bergen: Fagbokforlaget.

Personvernforordningen (2018).

Pressman, Jeffrey L. og Aaron Wildavsky (1973): *Implementation. How great expectations in Washington are dashed in Oakland. Or, why it's amazing that federal programs work at all. This being a saga of the economic development administration. As told by two sympathetic observers who seek to build morals on a foundation of ruined hopes.* Berkeley, Calif.: California University Press.

Ryen, Anne (2002): *Det kvalitative intervjuet. Fra vitenskapsteori til feltarbeid.* Bergen: Fagbokforlaget.

Thagaard, Tove (1998): *Systematikk og innlevelse*. Bergen: Fagbokforlaget.

Thorsvik, Jan (1985): «Hvorfor mislykkes offentlig politikk?». I Bleiklie, Ivar m.fl. (red.): *Politikkens forvaltning. Festskrift til Knut Dahl Jacobsen på 60-årsdagen 14. desember 1985*. Bergen: Universitetsforlaget.

Winter, Søren (2001): «Implementeringsforskningen og dens relation til evaluering». I Dahler-Larsen, Peter og Hanne Kathrine Krogstrup (red.): *Tendenser i evaluering.* Odense: Odense Universitetsforlag.

8 Vedlegg A: Sammenfatning av problemstillinger, revisjonskriterier og metode

Mens revisjonskriteriene utvelges med bakgrunn i problemstillingen og danner grunnlaget for hva de innhentede dataene skal vurderes opp mot, danner metoden grunnlaget for hvordan de nødvendige dataene skal kunne hentes inn. Det kan fastslås at forvaltningsrevisjon er en dynamisk prosess (Andersen, K.M. m.fl.: 2006).

Problemstillinger	Revisjonskriterier	Metode
Problemstillingen gjør seg gjeldende i følgende hovedspørsmål: I. I hvilken grad har kommunen etablert tilfredsstillende rutiner og systemer for å ivareta krav til IKT-sikkerhet? a. Personvern b. Kriseløsninger, sikkerhetskopiering av data (backup) mv. II. I hvilken grad fungerer fastlagte rutiner og systemer for IKT-sikkerhet i praksis?	Kilder til revisjonskriterier: • Personvernforordningen (2018). • Kommuneloven (1992). • Odelstingsproposisjon nr. 70 (2002–2003). • E-forvaltningsforskriften (2004). • ISACA (2009): *Grunnleggende retningslinjer for god IT-skikk.* • *COSO (2005): Helhetlig risikostyring - et integrert rammeverk.* • Kommunaldepartementet (2009): *85 tilrådingar for styrkt eigenkontroll.* • Datatilsynet (2009): *En veiledning om internkontroll og informasjonssikkerhet.* • Datatilsynet (2018): *Veileder. Internkontroll og informasjonssikkerhet.* • Direktoratet for forvaltning og IKT (2016): *Internkontroll i praksis – informasjons-sikkerhet. Grunnleggende innføring.* • Implementeringsteori.	Kvalitative intervjuer Tester og observasjon

9 Vedlegg B: Utledede revisjonskriterier

I det følgende utledes revisors revisjonskriterier i relasjon til problemstillingene, jf. punkt 2.2.

9.1 Hovedspørsmål I: Rutiner og systemer for å ivareta IKT-sikkerhet

Understående revisjonskriterier relaterer seg til hovedspørsmål I, jf. punkt 2.2. Hovedspørsmålet fokuserer på i hvilken grad kommunen har etablert tilfredsstillende rutiner og systemer for å ivareta krav til IKT-sikkerhet. I denne forbindelse omfatter dette:

a. Personvern

a. Kriseløsninger, sikkerhetskopiering av data (backup) mv.

Som et overordnet krav til kommunen, fastslår kommuneloven § 23 nr. 2 at administrasjonen skal være gjenstand for *betryggende kontroll*. Dette forutsetter at det er etablert en tilstrekkelig internkontroll i hele kommunens organisasjon, herunder i forbindelse med anvendelse av informasjons- og kommunikasjonsteknologi (IKT). Revisor legger til grunn at det er sentralt med god internkontroll innen IKT-området, da kommunen er avhengig av IKT-tjenester for å fungere i det daglige, foruten at IKT-området også er forbundet med betydelige personvernhensyn. Som et ledd i dette arbeidet vil det normalt være sentralt å dokumentere og systematisere internkontrollen. I 2009 gav Kommunaldepartementet ut en veileder med 85 tilrådinger for styrket egenkontroll i kommunene. Følgende fremgår av tilråding nr. 16 og tilråding nr. 18:

> Tilråding nr. 16: Kommunene bør basere seg **mindre på uformell kontroll**. En **formalisering** vil gjøre kommunene mindre sårbare ved skifte av personell, endringer i omgivelsene og habilitetsproblematikk, og vil øke det organisatoriske minnet. (Revisors utheving).
>
> Tilråding nr. 18: Kommunene bør i sammenheng med behovet for økt formalisering av internkontrollen **dokumentere** internkontrollen i større grad. (Revisors utheving).

Etablering av rutiner og systemer vil være et virkemiddel for å systematisere og dokumentere internkontrollen. I odelstingsproposisjon nr. 70 (2002–2003), som omhandler diverse endringer i kommuneloven, heter det blant annet som en utdyping til lovens § 23 nr. 2, at:

> Det er i tråd med allment aksepterte ledelsesprinsipper at en leder av en virksomhet etablerer **rutiner og systemer** som blant annet skal bidra til å sikre at organisasjonen når de mål som er satt. (Revisors utheving).

***

Behandling av informasjon er både en kjerneaktivitet og viktig støtteaktivitet i norske kommuner (Direktoratet for forvaltning og IKT: 2016). Effektiv og pålitelig informasjonsbehandling er avgjørende for at virksomheten skal nå sine mål. Informasjonssikkerhet[4], herunder IKT-sikkerhet, knytter seg til å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte (Datatilsynet: 2018). Dette omfatter å sikre:

- Konfidensialitet - at informasjonen ikke blir kjent for uvedkommende.
- Integritet - at informasjonen ikke blir endret utilsiktet eller av uvedkommende.
- Tilgjengelighet - at informasjonen er tilgjengelig for autoriserte ved behov.
- Robusthet - at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser.

Brudd på konfidensialitet, integritet, tilgjengelighet eller robusthet kan få konsekvenser for både virksomheten selv, innbyggerne og andre offentlige og private virksomheter (Direktoratet for forvaltning og IKT: 2016). Det kan for eksempel medføre:

- Feil beslutninger.
- Brudd på rettigheter og rettssikkerhet.
- Omdømmetap og økonomiske tap for innbyggere, næringsliv og virksomheten selv.
- Ødeleggende livssituasjon.
- Effektivitetstap for virksomheten selv og andre.
- Tap av liv og helse.

[4] Informasjonssikkerhet omfatter både muntlig, papirbasert og digital behandling av informasjon. Denne forvaltningsrevisjonen er primært avgrenset til digital behandling av informasjon, nærmere bestemt IKT-sikkerhet.

I e-forvaltningsforskriften § 15 første ledd stilles det krav om at offentlige forvaltningsorgan, herunder kommuner, skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten. Dette benevnes som sikkerhetsmål og sikkerhetsstrategi og skal danne grunnlaget for forvaltningsorganets internkontroll innen informasjonssikkerhetsområdet. Av annet ledd i sistnevnte paragraf går det frem at den nevnte internkontrollen bør utgjøre en integrert del av virksomhetens helhetlige styringssystem. Omfang og innretning på internkontrollen skal videre være tilpasset risiko, jf. e-forvaltningsforskriften § 15 tredje ledd.

Personvernforordningens artikkel 24 stiller krav til internkontroll i form av egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med personvernforordningen. Dette innebærer en forholdsmessighet hvor en ser på behandlingens art, omfang, formål og sammenheng, samt risikoene for fysiske personers rettigheter og friheter, og ut fra det gjennomfører egnede tekniske og organisatoriske tiltak. Ved innføring av internkontroll bør virksomheten først identifisere hvilke personopplysninger som behandles, og deretter gjennomføre en risikovurdering for å avklare føringer for internkontrollen (Datatilsynet: 2018). Dette som en del av internkontrollens styrende elementer, hvilket igjen vil gi grunnlag for å utarbeide de rutinene det er behov for.

Internkontrollens gjennomførende elementer inneholder rutinene som skal brukes av de ansatte i deres arbeidssituasjon. Virksomheten må utarbeide de nødvendige rutinene for at behandlingen skal gjennomføres i forsvarlige former. Datatilsynet (2018) anfører at det kan være hensiktsmessig å utarbeide rutiner innen følgende områder for håndtering av personopplysninger:

- Iverksettelse og opphør av behandling.
- Informasjon (rettferdig og gjennomsiktig behandling, personvernforordningens artikkel 12, 13 og 14).
- Innhenting og kontroll av samtykke (personvernforordningens artikkel 7 og 8).
- Den registrertes rett til innsyn (personvernforordningens artikkel 15).
- Dataportabilitet (personvernforordningens artikkel 20).

- Den registrertes rett til å få korrigert og slettet personopplysninger (personvernforordningens artikkel 16, 17 og 19).
- Begrensning av behandling (personvernforordningens artikkel 18 og 19).
- Den registrertes rett til å protestere (personvernforordningens artikkel 21).
- Særskilte regler for automatiserte avgjørelser (personvernforordningens artikkel 22).
- Utlevering av personopplysninger til andre.
- Overføring til tredjestater (personvernforordningens artikkel 44-49).

En risikovurdering vil vise om alle rutinene overfor er relevante, samt hvorvidt det er behov for andre rutiner i tillegg.

ISACA[5] har publisert *Grunnleggende retningslinjer for god IT-skikk* (2009). Av denne standarden går det frem at IKT-kriseløsninger blant annet innebærer behov for planverk, tekniske løsninger samt regelmessige øvelser. Det foreligger en rekke tiltak som kan bidra til driftskontinuitet og til å forebygge alvorlige hendelser. Blant annet vil dette innbefatte å sikre:

- Klart definerte roller og arbeidsdeling.
- Jevnlig oppdatering av operativsystem, programvarer, antivirusprogram og brannmur.
- Rutiner for sikkerhetskopiering av data (backup).
- Tilgangsstyring til systemer.
- Tiltak mot innbrudd, vannskader, brann o.l.

Med bakgrunn i ovennevnte legges følgende oppsummerte revisjonskriterier til grunn:

- Kommunen har beskrevet mål og strategi for IKT-sikkerhet i virksomheten. Dette benevnes som sikkerhetsmål og sikkerhetsstrategi og skal danne grunnlaget for forvaltningsorganets internkontroll innen området. Omfang og innretning på internkontrollen skal være tilpasset risiko og bør utgjøre en integrert del av virksomhetens helhetlige styringssystem.

[5] En verdensomspennende forening for IKT-styring og informasjonssikkerhet.

- Kommunen har gjennomført en risikovurdering og utarbeidet nødvendige skriftlige rutiner for håndtering av personopplysninger.
- Kommunen har fokus på kriseløsninger innen IKT-området. Dette innebærer behov for planverk, tekniske løsninger samt regelmessige øvelser. Det er etablert tiltak som kan bidra til driftskontinuitet og til å forebygge alvorlige hendelser innen IKT-området. Blant annet vil dette innbefatte å sikre:
    - Klart definerte roller og arbeidsdeling.
    - Jevnlig oppdatering av operativsystem, programvarer, antivirus-program og brannmur.
    - Rutiner for sikkerhetskopiering av data (backup).
    - Tilgangsstyring til systemer.
    - Tiltak mot innbrudd, vannskader, brann o.l.

9.2 Hovedspørsmål II: Om rutiner og systemer for IKT-sikkerhet fungerer

Understående revisjonskriterier relaterer seg til hovedspørsmål II, jf. punkt 2.2. Hovedspørsmålet fokuserer på i hvilken grad fastlagte rutiner og systemer for IKT-sikkerhet fungerer i praksis. Følgelig er spørsmålet knyttet til implementering, da implementering retter søkelyset på hva som skjer, om noe, etter at det er fastlagt en ordning for et område (Offerdal: 2005).

At implementeringen ikke alltid går som planlagt, finnes det mange eksempler på (Pressman og Wildavsky: 1973, Kjellberg og Reitan: 1995, Winter: 2001). En ting er selve vedtaket, en annen ting er hvordan det settes ut i livet (Offerdal: 2005). Det er mange forhold som kan forklare hvorfor implementeringen ikke alltid går som planlagt. Uklare mål, knapphet på tid, manglende økonomi og utilstrekkelige personalressurser, er eksempler på vanlige forklaringsfaktorer (Thorsvik: 1985, Offerdal: 2005).

Som en del av internkontrollen må virksomheten sørge for at den gjøres kjent og etterleves blant de ansatte (Datatilsynet: 2009). I denne forbindelse bør de ansatte gis opplæring og innsikt i sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle sikkerhetsrisikoer (Ibid.).

I følge anerkjente normer for internkontroll, slik som COSO-rammeverket (2005), vil et siktemål med internkontroll være å fokusere på om aktiviteter og resultater leveres i tråd med fastsatte mål og intensjoner. Det bør derfor, sett i forhold til oppfølging av fastlagte rutiner og systemer for IKT-sikkerhet, være etablert kanaler som sikrer at nødvendig informasjon bli mottatt og fulgt opp. Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på øvrig IKT-sikkerhet, skal virksomheten iverksette avviksbehandling (Datatilsynet: 2009). Formålet med avviksbehandling er å lukke avviket så rasket som mulig, gjenopprette normaltilstand og hindre gjentagelse.

Virksomheten bør vektlegge at rutinene og systemene for håndtering av IKT-sikkerhet fungerer etter hensikten (Ibid.). Derfor vil det være sentralt å innføre faste rutiner for å forbedre og vedlikeholde internkontrollen, herunder dokumentere erfaring, lære av uønskede hendelser, samt forbedre arbeidsprosessene slik at færrest mulig uønskede hendelser oppstår. Eksempelvis kan det som et tiltak gjennomføres faste møter hvor styringssystemet for IKT-sikkerhet er tema, inklusiv gjennomgang av avvik og forslag til forbedring.

Med bakgrunn i ovennevnte legges følgende oppsummerte revisjonskriterier til grunn:

- Som en del av internkontrollen må virksomheten sørge for at den gjøres kjent og etterleves blant de ansatte. I denne forbindelse bør de ansatte gis opplæring og innsikt i sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle sikkerhetsrisikoer.
- Det bør, sett i forhold til oppfølging av fastlagte rutiner og systemer for IKT-sikkerhet, være etablert kanaler som sikrer at nødvendig informasjon blir mottatt og fulgt opp. Dette inkluderer iverksettelse av eventuell avviksbehandling.
- Kommunen bør vektlegge at rutinene og systemene for håndtering av IKT-sikkerhet fungerer etter hensikten. Derfor vil det være sentralt å innføre faste rutiner for å forbedre og vedlikeholde internkontrollen, herunder dokumentere erfaring, lære av uønskede hendelser, samt forbedre arbeidsprosessene slik at færrest mulig uønskede hendelser oppstår.

10 Vedlegg C: Reliabilitet og validitet

10.1 Reliabilitet og validitet

Reliabilitet og validitet er sentrale begreper i kvalitetssikringen av undersøkelser. I det følgende angis sider ved undersøkelsens reliabilitet og validitet.

10.1.1 Reliabilitet

En undersøkelses reliabilitet bestemmes av hvordan målingene er gjort og hvor nøyaktig en er i den videre behandlingen av dataene (Holme og Solvang: 1996). For å sikre undersøkelsens reliabilitet er det viktig å være nøye i nedtegnelsen av dataene. Derfor deltar det to representanter ifra revisjonen under intervjuene. Mens den ene foretar selve intervjuutspørringen fokuserer den andre på å nedtegne dataene korrekt. På denne måten søkes det å sikre en forsvarlig gjengivelse av dataene. For å sikre at respondentene «kjenner seg igjen» i de nedtegnede intervjudataene forelegges de sine respektive intervjureferater til verifisering.

Jacobsen (2005) fremhever at respondentene kan bli utsatt for en undersøkelseseffekt. Det er ikke uvanlig at en undersøkelsessituasjon kan oppfattes som kunstig og unaturlig. Dette kan få intervjuobjektene til å opptre noe annerledes enn de ellers ville ha gjort. For eksempel kan enkelte bli reserverte med å svare på kritiske spørsmål. For å forhindre noe av dette forsøkes det i størst mulig grad å anonymisere respondentenes svar.

For at intervjusituasjonen skal oppleves så naturlig som mulig vektlegges det at intervjuene skal foregå på et rolig sted og at respondentene skal få snakke relativt fritt. En fordel med de kvalitative intervjuene er nettopp muligheten til å snakke relativt fritt. Imidlertid er det nødvendig med en viss struktur på intervjuene. Det er derfor utviklet en intervjuguide med de sentrale temaene og spørsmålene for undersøkelsen (jf. vedlegg D). Dermed unngås det i større grad at sentrale spørsmål kan utebli, foruten at det også forenkler analysearbeidet. Når det stilles spørsmål om bestemte temaer, blir det enklere å kategorisere og tolke dataene ut ifra dette. Hvilke spørsmål som stilles til hver enkelt respondent vil imidlertid variere noe. Dette kommer av deres ulike posisjoner og roller (jf. punkt 4.2). Fleksibilitet er som Thagaard (1998) fremhever, viktig for å knytte spørsmålene til den enkelte respondents forutsetninger.

Videre har det vært fokus på å sikre at rapportens opplysninger stemmer overens med mottatte opplysninger. Derfor har forvaltningsrevisjonsrapporten blitt underlagt intern kvalitetssikring i henhold til Hedmark Revisjon sine rutiner for intern kvalitetskontroll av forvaltningsrevisjonsprosjekter. Rapportens grunnlag har i denne forbindelse blitt kontrollert flere ganger.

10.1.2 Validitet

Validiteten sier noe om hvor gyldige eller relevante dataene er for det en søker å undersøke (Eriksen m.fl.: 2000).

En fordel med den kvalitative intervjuundersøkelsen er at den sikrer høy begrepsvaliditet, hvilket omhandler at en faktisk måler det en søker å måle. Det er nemlig intervjuobjektene som i stor grad definerer hva som er den «riktige» forståelsen av fenomenet (Jacobsen: 2005). Det kvalitative intervjuet påtvinger ikke respondentene faste svaralternativer som et kvantitativt spørreskjema. Ved å stille utdypende spørsmål kan man således styrke muligheten for å avklare eventuelle misforståelser (Larsen: 2007). For å forenkle analyse- og kategoriseringsarbeidet har det imidlertid blitt valgt å strukturere intervjuene noe (jf. punkt 10.1.1). Intervjuene «flyter således ikke helt fritt».

Den kvalitative metoden vektlegger detaljer, nyanserikdom og det unike ved hver enkelt respondent (Jacobsen: 2005). En styrke ved metoden er at den er egnet til å oppnå nærhet og dybde på et avgrenset område (Ryen: 2002). En svakhet med metoden er imidlertid at den kan være lite egnet til generalisering. Inneværende intervjuundersøkelse er ikke basert på generaliserbare data, idet et representativt utvalg ville ha krevd et større og mer tilfeldig utvalg. Revisor anser imidlertid den valgte metodebruk som velegnet til å kunne fremskaffe nyanserte data i relasjon til problemstillingens komplekse karakter (jf. punkt 4.1), hvilket igjen muliggjør at det kan reises aktuelle spørsmål i relasjon til IKT-sikkerhet i Åsnes kommune. I relasjon til problemstillingen er det foretatt test av rutine for backup samt observasjon av fysiske sikringstiltak på [redacted] serverrom. Hensikten har vært å supplere deler av intervjudataene.

For å styrke undersøkelsens validitet har det videre blitt trukket inn sentral litteratur og regelverk som berører forvaltningsrevisjonens problemområde (jf. kapittel 3 og

litteraturlisten). Dette har dannet basis for utledelsen av revisjonskriteriene (jf. vedlegg B) og vil bidra til at det gis større visshet om at undersøkelsen er relevant.

11 Vedlegg D: Intervjuguide

Innledning

-Presentasjon av møtedeltakerne.

-Orientering om hva forvaltningsrevisjon er i sitt vesen.

-Orientering om bakgrunnen for prosjektet samt om prosjektets tidsplan. Det orienteres samtidig om at det skrives et referat fra intervjuet som sendes respondenten for godkjenning i etterkant.

-Ev. spørsmål ifra møtedeltakerne.

Hoveddel

-Organisering og ansvarsfordeling knyttet til IKT-sikkerhet i kommunen.

-Presentasjon av problemstillinger.

Hovedspørsmål I

Hovedspørsmål I fokuserer på i hvilken grad kommunen har etablert tilfredsstillende rutiner og systemer for å ivareta krav til IKT-sikkerhet. I denne forbindelse omfatter dette:

a. Personvern
b. Kriseløsninger, sikkerhetskopiering av data (backup) mv.

-Informasjonssikkerhet, herunder IKT-sikkerhet, knytter seg til å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte (Datatilsynet: 2018). Dette omfatter å sikre:

- Konfidensialitet - at informasjonen ikke blir kjent for uvedkommende.
- Integritet - at informasjonen ikke blir endret utilsiktet eller av uvedkommende.
- Tilgjengelighet - at informasjonen er tilgjengelig for autoriserte ved behov.
- Robusthet - at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser.

-I e-forvaltningsforskriften § 15 første ledd stilles det krav om at offentlige forvaltningsorgan, herunder kommuner, skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten. Dette benevnes som sikkerhetsmål og sikkerhetsstrategi og skal danne grunnlaget for forvaltningsorganets internkontroll innen informasjonssikkerhetsområdet. Omfang og innretning på internkontrollen skal være tilpasset risiko og bør utgjøre en integrert del av virksomhetens helhetlige styringssystem.

-Personvernforordningens artikkel 24 stiller krav til internkontroll i form av egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med personvernforordningen. Ved innføring av internkontroll bør virksomheten først identifisere hvilke personopplysninger som behandles, og deretter gjennomføre en risikovurdering for å avklare føringer for internkontrollen (Datatilsynet: 2018).

-Internkontrollens gjennomførende elementer inneholder rutinene som skal brukes av de ansatte i deres arbeidssituasjon. Virksomheten må utarbeide de nødvendige rutinene for at behandlingen skal gjennomføres i forsvarlige former. Datatilsynet (2018) anfører at det kan være hensiktsmessig å utarbeide rutiner innen følgende områder for håndtering av personopplysninger:

- Iverksettelse og opphør av behandling.
- Informasjon (rettferdig og gjennomsiktig behandling, personvernforordningens artikkel 12, 13 og 14).
- Innhenting og kontroll av samtykke (personvernforordningens artikkel 7 og 8).
- Den registrertes rett til innsyn (personvernforordningens artikkel 15).
- Dataportabilitet (personvernforordningens artikkel 20).
- Den registrertes rett til å få korrigert og slettet personopplysninger (personvernforordningens artikkel 16, 17 og 19).
- Begrensning av behandling (personvernforordningens artikkel 18 og 19).
- Den registrertes rett til å protestere (personvernforordningens artikkel 21).
- Særskilte regler for automatiserte avgjørelser (personvernforordningens artikkel 22).
- Utlevering av personopplysninger til andre.

- Overføring til tredjestater (personvernforordningens artikkel 44-49).

En risikovurdering vil vise om alle rutinene overfor er relevante, samt hvorvidt det er behov for andre rutiner i tillegg.

-Kommunen har fokus på kriseløsninger innen IKT-området. Dette innebærer behov for planverk og tekniske løsninger samt regelmessige øvelser.

-Kommunen har etablert tiltak som kan bidra til driftskontinuitet og til å forebygge alvorlige hendelser innen IKT-området. Blant annet vil dette innbefatte å sikre:

- Klart definerte roller og arbeidsdeling. Antall ansatte med utvidede rettigheter bør begrenses.
- Jevnlig oppdatering av operativsystem, programvarer, antivirus-program og brannmur.
- Rutiner for sikkerhetskopiering av data (backup).
- Adgangskontroll til systemer.
- Tiltak mot innbrudd, vannskader, brann o.l.

Hovedspørsmål II

Hovedspørsmål II fokuserer på i hvilken grad fastlagte rutiner og systemer for IKT-sikkerhet fungerer i praksis. Følgelig er spørsmålet knyttet til implementering, da implementering retter søkelyset på hva som skjer, om noe, etter at det er fastlagt en ordning for et område (Offerdal: 2005).

- Som en del av internkontrollen må virksomheten sørge for at den *gjøres kjent og etterleves blant de ansatte* (Datatilsynet: 2009). I denne forbindelse bør de ansatte gis opplæring og innsikt i sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle sikkerhetsrisikoer (Ibid.).

-I følge anerkjente normer for internkontroll, slik som COSO-rammeverket (2005), vil et siktemål med internkontroll være å fokusere på om aktiviteter og resultater leveres i tråd med fastsatte mål og intensjoner. Det bør derfor, sett i forhold til oppfølging av fastlagte rutiner og systemer for IKT-sikkerhet, være etablert kanaler som sikrer at nødvendig

informasjon bli mottatt og fulgt opp. Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på øvrig IKT-sikkerhet, skal virksomheten iverksette avviksbehandling (Datatilsynet: 2009).

- Kommunen bør vektlegge at rutinene og systemene for håndtering av IKT-sikkerhet brukes og fungerer etter hensikten. Derfor vil det være sentralt å innføre faste rutiner for å forbedre og vedlikeholde internkontrollen, herunder dokumentere erfaring, lære av uønskede hendelser, samt forbedre arbeidsprosessene slik at færrest mulig uønskede hendelser oppstår. Eksempelvis kan det som et tiltak gjennomføres faste møter hvor styringssystemet for IKT-sikkerhet er tema, inklusiv gjennomgang av avvik og forslag til forbedring.

-Tester og observasjoner for å kontrollere om etablerte rutiner er gjennomført og fungere i praksis.

***

-Risikoforhold/suksesskriterier/forbedringspotensial knyttet til problemområdet.

-Ev. spørsmål ifra møtedeltakerne.

Avslutning

-Kort oppsummering.

-Ev. spørsmål ifra møtedeltakerne.

-Etterspørre relevante dokumenter innen området. Reglement, rutiner o.l. knyttet til IKT-sikkerhet i kommunen

-Takke for samtalen – ser frem til videre samarbeid og tar kontakt ved behov.

12 Vedlegg E: Overordnede prosedyrer

Åsnes kommune har utarbeidet flere overordnede prosedyre relatert til personvernforordningen og generell informasjonssikkerhet. Disse prosedyrene omfatter hele kommuneorganisasjonen og er inndelt i kategoriene *styrende, gjennomførende, daglige* og *kontrollerende.*

Styrende prosedyrer

- Ansvarsmatrise informasjonssikkerhet- GDPR
- Bruk av personopplysninger / Behandlinger
- Fagsystemer - Oversikt over behandlinger
- Fastsetting av akseptabel Risiko
- Internkontroll system (informasjonssikkerhet)
- Prosedyre for etablering av personvernrådgiver/-ombud
- Prosedyre for å opprette databehandleravtale
- Sikkerhetsmål for behandling av personopplysninger
- Sikkerhetsorganisasjon og ansvar
- Sikkerhetsstrategi for informasjonssikkerhet

Gjennomførende prosedyrer

- Databehandleravtale – SLA-avtale
- Henvendelse om innsyn
- Informasjon til den registrerte
- Informasjonsplikt ved behandling av personopplysninger
- Opprettelse av nye brukere på kommunens datasystemer
- Prosedyre for beredskapsplanlegging
- Prosedyre for bruk av bærbart datautstyr
- Prosedyre for etablering av nødprosedyrer ved manuell drift
- Prosedyre for fysisk sikring av områder og utstyr
- Prosedyre for håndtering av flyttbare lagringsmedium
- Prosedyre for innhenting av taushetserklæring fra politikere
- Prosedyre for konfigurasjonsendringer

- Prosedyre for lagring av hendelsesregistre
- Prosedyre for nødrettstilgang
- Prosedyre for oppbevaring av personopplysninger
- Prosedyre for opplæring av ledere og medarbeidere GDPR
- Prosedyre for retting og sletting av personopplysninger
- Prosedyre for taushetserklæring- eksterne aktører
- Prosedyre for taushetsplikt
- Prosedyre for tilknytning via fjernaksess
- Prosedyre for å hindre destruktiv programvare

Daglige prosedyrer

- Daglig informasjonssikkerhet
- Innhenting av tillatelse fra den registrerte - personvernerklæring
- Personvern og informasjonssikkerhet - den ansattes plikter

Kontrollerende prosedyrer

- Informasjon til de registrerte
- Ledelsens gjennomgang informasjonssikkerhet / GDPR
- Prosedyre for anmodninger om innsyn i personopplysninger
- Prosedyre for anmodninger om korrigering av personopplysninger
- Prosedyre for anmodninger om sletting av personopplysninger
- Prosedyre for avvikshåndtering (GDR) Informasjonssikkerhet
- Prosedyre for avviksmelding til Datatilsynet
- Prosedyre for behandling av personopplysninger
- Prosedyre for egenkontroll
- Prosedyre for innsamling av personopplysninger
- Prosedyre for oppfølging av risikovurderinger
- Prosedyre for oppstart av ny behandlingsaktivitet
- Prosedyre for risikovurderinger
- Prosedyre for sikkerhetsrevisjon
- Prosedyre for sletting av personopplysninger
- Prosedyre for varsling til den registrerte om sikkerhetsbrudd

- Protokoll MAL
- Protokoll for behandling