IT-sikkerhet

Forvaltningsrevisjonsrapport
Haugesund kommune

Mai 2021

www.kpmg.no

Forord

Etter vedtak i kontrollutvalget i Haugesund kommune 17.11.20 har KPMG gjennomført en forvaltningsrevisjon rettet mot IT-sikkerhet. Denne rapporten er svar på kontrollutvalgets bestilling.

Oppbygging av rapporten

Våre konklusjoner og anbefalinger fremgår av rapportens sammendrag. Kapittel 1 er en innledning til rapporten. Her blir formål, problemstillinger og metode presentert. I kapittel 2 gir vi en utvidet bakgrunn for prosjektet og IT-sikkerhet mer generelt, med en omtale av utfordringsbildet. I kapittel 3 viser vi hvordan arbeidet med IT-sikkerhet i Haugesund kommune er organisert. I kapittel 4 besvarer vi problemstillinger knyttet til systemer, rutiner og prosedyrer knyttet til IT-sikkerhet. I kapittel 5 besvarer vi problemstillinger knyttet til beredskap og bevissthet. I kapittel 6 presenterer vi våre anbefalinger. I kapittel 7 er kommunedirektørens uttalelse til rapporten tatt inn.

Vi vil takke kommunen for all den gode hjelpen vi har fått i arbeidet med forvaltningsrevisjonen.

Sammendrag

Formålet med forvaltningsrevisjonen er å kartlegge hvordan Haugesund kommune arbeider med IT-sikkerhet gjennom etablerte rutiner, prosedyrer og rammer. Videre er det et formål å kartlegge og vurdere hvordan kommunens arbeid innen IT-sikkerhet og digitale beredskap er tilstrekkelig for å kunne håndtere uønskede digitale hendelser. For å svare på dette er det stilt opp to hovedproblemstillinger i forvaltningsrevisjonen. Dette er et kort sammendrag av våre konklusjoner og anbefalinger.

Problemstilling 1: Hvordan arbeider Haugesund kommune med IT-sikkerhet?

Haugesund kommune har utarbeidet og benytter en rekke systemer, rutiner og prosedyrer knyttet til informasjonssikkerhet. Samtidig viser våre undersøkelser at ikke alle styrende dokumenter er godt nok operasjonalisert i kommunen. Det har blant annet blitt avdekket at flere av målsettingene i kommunens «sikkerhetsmål- og strategi» ikke er utarbeidet eller implementert.

Det er videre utarbeidet en rekke rutiner for å ivareta kravene i personopplysningsloven. Personvernombudet er godt kjent, og tilsendte databehandleravtaler er i tråd med personopplysningslovens bestemmelser. En generell observasjon er imidlertid at det ved enkelte tilfeller går lang tid mellom oppdatering av rutiner.

Haugesund kommune har nylig innført tofaktorautentisering, noe som bedrer tilgangskontrollen til sentrale systemer. Dette er innført for alle kommunens ansatte med unntak av elever og politikere. Selv om disse brukergruppene ikke er omfattet av sikringstiltaket foreligger det andre kontrollmekanismer for politikere.

Vi ser det som positivt at krav til IT-sikkerhet har blitt inkludert i hele livsløpet fra anskaffelse til avhending i forespørsler til IT-leverandører. Samtidig ser vi et forbedringspotensial i at disse kravene og IKT-enhetens involvering i IKT-anskaffelser kunne vært tydeliggjort i rutiner for anskaffelser. Det kan også være hensiktsmessig å gjennomføre risikovurderinger utover DPIA ved visse anskaffelser.

Haugesund kommune håndterer avvik gjennom avviksrapporteringssystem Risk Manager. Hovedansvaret for oppfølging av avvik er videre lagt til de ulike tjenesteledere. Det er også vårt inntrykk at avvik knyttet til personvern og informasjonssikkerhet er tillagt ekstra kontrollmekanismer ved at personvernombudet og leder for arbeidsgruppen i personvern og informasjonssikkerhet har jevnlige gjennomganger av registrerte avvik og sender ut påminnelser til tjenesteledere om oppfølging. Samtidig viser revisjonen at forståelsen for avvik i kommunen varierer blant ansatte. Varierende forståelser kan, etter vår vurdering, medføre risiko og usikkerhet knyttet til om avvik faktisk meldes og håndteres på en enhetlig måte.

Det største forbedringspotensialet ligger imidlertid i bedre og mer systematisk arbeid med kartlegging av uønskede hendelser og beredskapsplaner. Etter vår vurdering er det risiko knyttet til at det ikke er gjennomført systematiske kartlegginger av trusselbildet og risikovurderinger knyttet til sannsynlighet for og konsekvenser av IT-relatert hendelser, samt at det ikke finnes spesifikke beredskapsplaner innenfor IKT-området. Behovet for slike analyser og planer er i dag særdeles aktuelt, og omfanget av dataangrep mot offentlig sektor i starten av 2021 understreker dette klart og tydelig.

Problemstilling 2: I hvilken grad er kommunens arbeid med IT-sikkerhet tilstrekkelig for å kunne håndtere uønskede digitale hendelser?

Våre undersøkelser avdekker at Haugesund kommune ikke har gjennomført beredskapsøvelser knyttet direkte til IT-bortfall, eller uønskede digitale hendelser generelt. Dette fremstår som en svakhet, da øvelser vil bidra til bevisstgjøring og kompetanseheving blant kommunens ansatte generelt, og spesielt de med ansvar for beredskap relatert til IT-sikkerhet. Øvelser vil også bidra direkte til å identifisere svakheter i rutiner, rolle- og ansvarsforhold. Gitt risikobildet på feltet, er vår vurdering at Haugesund kommune bør være beredt for fullstendig eller delvis bortfall av IT-systemer generelt og sektorvis. Revisjonen viser i tillegg at arbeidet med digital beredskap frem til nyere tid har fremstått som reaktivt, i den grad at kommunen har reagert på og håndtert hendelser som har oppstått fremfor å

forebygge gjennom beredskapsplanlegging, øvelser og evaluering. Selv om det enda ikke er utarbeidet slike beredskapsplaner eller vært gjennomført øvelser innen tema, observerer vi at kommunen nå i større grad jobber proaktiv med IT-sikkerhet, og blant annet valget om å melde seg inn i kommune-csirt er et eksempel på dette.

I tillegg til beredskapsøvelser innenfor IT-sikkerhet, kan kompetansehevende tiltak også bestå av andre opplæringstilbud og kurs. Våre undersøkelser viser at Haugesund kommune har tatt i bruk slike opplæringstiltak for å øke kompetansen til ledere, tillitsvalgte og ansatte i kommunen innen personvern og informasjonssikkerhet. Vår vurdering er at kursserien som har vært benyttet er godt kjent og refereres til blant samtlige informanter som et godt tiltak for å øke forståelsen knyttet til en omfattende og kompleks tematikk. Regelverket knyttet til informasjonssikkerhet og personvern er omfattende og til dels komplisert, og det er derfor positivt at revisjonen viser at de ansatte er kjent med og benytter nøkkelpersoner og kontaktpunkter i kommunen.

Til tross for at vi anbefaler mer systematisk arbeid med opplæring og kompetanseheving for alle kommunens ansatte fremstår det ikke som om kommunens ansatte selv føler seg utrygge på rutiner og håndtering knyttet til IT-sikkerhet.

Anbefalinger

Vi anbefaler at Haugesund kommune prioriterer følgende:

- Haugesund kommune bør etablere et system for systematiske og jevnlige gjennomganger av rutiner, systemer og prosedyrer knyttet til informasjonssikkerhet. Dette for å sikre at det helhetlige arbeidet er oppdatert og koordinert.
- [redacted]
- IT-sikkerhet bør inngå som et sentralt element i den pågående rulleringen av ROS-analysen, med spesiell vekt på å kartlegge mindre og mer alvorlige uønskede IT-relaterte hendelser
- Beredskapsgruppen bør utrede hvordan IT-sikkerhet påvirker de forskjellige virksomhetsområdene, og koble IKT-enheten på arbeidet med beredskapsplaner
- Haugesund kommune bør fullføre innmeldingen i Kommune-Csirt og utrede hvordan deres rådgivnings- og øvrige tjenester kan styrke kommunens arbeid med IT-sikkerhet
- Det bør gjennomføres beredskapsøvelser knyttet til bortfall av IT-systemer i alle virksomheter, med sikte på å kartlegge backup-rutiner og muligheter for å opprettholde kritiske tjenester
- Kommunen bør utarbeide og/eller ferdigstille opplæringsprogram i IT-sikkerhet for ansatte
- Kommunen bør benytte seg av muligheten for å gjennomføre kurs om generell informasjons- og datasikkerhet i KS læring eller andre leverandører, og vurdere behovet for ytterligere kurs og opplæring for tidligere ansatte basert på erfaringene fra opplæringsprogrammet for nyansatte
- Kommunen bør, ved implementering av nytt avvik- og kvalitetssystem, gi tilstrekkelig opplæring i system og rutiner for avviksrapportering. En generell opplæring i hva som er avvik relatert til personvern og informasjonssikkerhet vil også være hensiktsmessig.
- Haugesund kommune bør tydeliggjøre når IKT-enheten skal inngå ved anskaffelser av nye systemer, og kommunisere dette ut til de ulike tjenesteområdene

Innhold

1. Innledning

1.1 Bakgrunn og formål

Kontrollutvalget i Haugesund kommune vedtok i møtet 17.11.20 i sak 37/20 å bestille forvaltningsrevisjon om "IT-sikkerhet" fra KPMG.

Formålet med forvaltningsrevisjonen har vært å kartlegge rutiner, prosedyrer og rammer for arbeidet med IT-sikkerhet i Haugesund kommune. Videre har det vært et formål å kartlegge og vurdere i hvilken grad kommunens digitale beredskap er tilstrekkelig for å kunne håndtere uønskede digitale hendelser.

Forvaltningsrevisjonen har hatt som målsetting å være forbedringsorientert, ved å gi anbefalinger om tiltak ved avdekte avvik eller mulige forbedringsområder.

1.2 Problemstillinger

Grunnlaget for forvaltningsrevisjonen er to overordnede problemstillinger med tilhørende delspørsmål. Disse gjengis her, og de har vært førende for utledning av revisjonskriteriene og all datainnsamling.

1. Hvordan arbeider Haugesund kommune med IT-sikkerhet?

a) Hvilke systemer, rutiner og prosedyrer har kommunen for å ivareta krav til informasjonssikkerhet?
   I. Har kommunen etablert tilgangskontroll for sine systemer?
   II. Har kommunen prosedyrer for kassering av gammelt utstyr og programvare?
   III. Har kommunen rutiner for personvern i tråd med personopplysningsloven?
b) Har kommunen oppdatert sin helhetlige risiko- og sårbarhetsanalyse og hvordan omtales risiko knyttet til informasjons- og kommunikasjonsteknologi her?
c) I hvilken grad gjennomføres det analyser og risikovurderinger ved anskaffelse av nye systemer?
d) Hvordan håndteres avvik?
e) Har kommunen rutiner for å gjennoppta normal drift etter driftsstans på kritiske områder?
f) Har kommunen en beredskapsplan for IKT og hvordan er denne samordnet med andre planer?

2. I hvilken grad er kommunens arbeid med IT-sikkerhet tilstrekkelig for å kunne håndtere uønskede digitale hendelser?

a) I hvilken grad gjennomføres beredskapsøvelser innenfor hendelser knyttet til IKT?
b) I hvilken grad er ansatte gjort kjent med planverk, ansvar og rutiner for håndtering?
c) I hvilken grad gis opplæring til ansatte om informasjonssikkerhet?
d) Opplever de som har ansvar for oppgaver dersom hendelser oppstår, trygghet i forbindelse med rutiner og håndtering?

1.3 Revisjonskriterier

Revisjonskriterier er de krav og normer som tilstand og/eller praksis i kommunen måles mot. Revisjonskriterier må være aktuelle, relevante og gyldige for kommunen. Kilder for å utlede revisjonskriterier har vært:

- ✓ Lov om kommuner og fylkeskommuner
- ✓ Personopplysningsloven
- ✓ eForvaltningsforskriften
- ✓ Sivilbeskyttelsesloven
- ✓ Forskrift om kommunal beredskapsplikt
- ✓ NSMs grunnprinsipper
- ✓ NOU 2018:14 – IKT-sikkerhet i alle ledd
- ✓ Digitaliseringsdirektoratets veileder i planlegging og gjennomføring av IKT-øvelser
- ✓ Digitaliseringsdirektoratets veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet

Revisjonskriterier er nærmere gjort rede for i vedlegg 2.

1.4 Metode

Forvaltningsrevisjonen er gjennomført i samsvar med kravene i RSK001 Standard for forvaltningsrevisjon[1].

For å svare på problemstillingene er følgende teknikker brukt for å samle inn data:

- ✓ Dokumentinnsamling og -analyse
- ✓ Intervjuer

Til grunn for rapporten ligger en gjennomgang og analyse av sentrale dokumenter opp mot revisjonskriteriene. Liste over mottatt dokumentasjon er å finne i vedlegg 1.

Det er gjennomført intervjuer med 11 personer i Haugesund kommune:

- ✓ Kommunedirektør
- ✓ Kommunaldirektør (Administrasjon og service)
- ✓ Enhets- og virksomhetsledere eller stedfortredere (IKT, Skole, Helse og Bygg og vedlikehold)
- ✓ Personvernombud
- ✓ Beredskapskoordinator
- ✓ Ansattrepresentanter (hovedtillitsvalgte for to fagforeninger)
- ✓ Leder for arbeidsgruppen i personvern og informasjonssikkerhet

Intervjuene har vært en sentral informasjonskilde. Utvalget av personer er basert på forventet informasjonsverdi, personenes erfaring og formelt ansvar i forhold til forvaltningsrevisjonens formål og problemstillinger. Formålet med intervjuene har vært å få utfyllende og supplerende informasjon til dokumentasjonen vi har mottatt fra kommunen. Data fra intervjuene er verifisert av respondentene, dvs. at respondentene har fått anledning til å lese igjennom referatene og gjøre eventuelle korrigeringer.

Datainnsamlingen ble avsluttet 2. mars 2021.

Rapport er sendt kommunedirektøren til uttalelse den 07.04.2021 med høringsfrist den 23.04.2021.

[1] Utgitt av Norges Kommunerevisorforbund.

2. Utfordringsbildet

Norge er et av de mest digitaliserte landene i verden. Digital utvikling gir en rekke gevinster som samfunnet som helhet og den enkelte innbygger kan nyte godt av. Digitaliseringsstrategi for offentlig sektor 2019-2025 definerer mål og innsatsområder for digitaliseringsarbeid i offentlig sektor i tidsperioden fram til 2025[2]. Hovedmålet er å oppnå en enklere hverdag for innbyggere og næringsliv.

Digitalisering fører imidlertid også til utfordringer knyttet til informasjonsteknologi (IT) (også omtalt som informasjons- og kommunikasjonsteknologi, eller *IKT*). IT-sikkerhet omhandler et bredt spekter av fenomener som kan være alt fra at IT-systemer ikke fungerer som de skal og helt- eller delvis faller bort. Dette kan skyldes en rekke forhold, som feilbruk, bortfall av strøm, manglende oppdateringer, fiendtlige angrep, osv. Tjenestene som omtales inkluderer alle systemene som Haugesund kommune selv har ansvar for og bruker i sin virksomhet. Personvern og datasikkerhet inngår også i forvaltningsrevisjonen, siden manglende integritet og beskyttelse av IT-systemer kan føre til at personopplysninger kommer på avveie. I intervjuene har vi spurt om hvordan informantene selv forstår begrepet IT-sikkerhet, og vi har funnet at alle i stor grad har den samme forståelsen for begrepet. Alle legger en bred forståelse for IT-sikkerhet til grunn.

Samtidig som offentlig sektor skal digitaliseres ytterligere opplever kommunene nye utfordringer, farer og trusler. Statistisk sentralbyrå gjennomfører en årlig innhenting av statistikk over offentlig sektors bruk av IKT. Statistikken omfatter statlige virksomheter, kommuner og fylkeskommuner. Blant kommunene rapporteres det om følgende IKT-sikkerhetsproblemer det siste året:

- ✓ 52,9% har opplevd forsøk på identitetstyveri (phishing)
- ✓ 20,3% at IKT-utstyr har kommet på avveie
- ✓ 19,7% sammenbrudd i forbindelsen til internett eller andre eksterne nettverk
- ✓ 10,2% uautorisert tilgang til systemer eller data
- ✓ 4,6% virusangrep, «ormer» eller lignende som resulterte i tap av data eller arbeidstid

Kommunene rapporterer om flere hindringer i arbeidet med å utvikle digitale tjenester. Over fire av ti kommuner nevnte følgende områder som hindringer:

- ✓ Mangel på felles standarder for datautveksling
- ✓ Mangel på felles offentlige løsninger og infrastruktur
- ✓ Utfordringer med å integrere eksisterende IT- og fagsystemer med digital forvaltning
- ✓ Vanskelig å frigjøre ressurser til utvikling
- ✓ Avhengig av utvikling hos andre virksomheter
- ✓ Manglende kompetanse i virksomheten
- ✓ IKT-utgifter høyere enn forventet
- ✓ Vanskelig å rekruttere IKT-spesialister

2.1.1 Dataangrep i kommune-Norge

I løpet av sommeren og høsten 2020, har det vært registrert flere tilsiktede dataangrep mot virksomheter og ansatte i kommune-Norge. Blant annet ble det i august kjent at enkelte av tjenestene til Sykehuset Innlandet HF var blitt rammet av et angrep gjennom internett hvor man fryktet at det var hentet ut personsensitiv informasjon[3]. I tillegg meldte Driftsselskapet Hedmark IKT tidlig september om at det hadde blitt sendt ut infiserte e-poster til om lag 10.000 ansatte i sju kommuner i Innlandet

[2] https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2653874/?ch=1

[3] https://sykehuset-innlandet.no/om-oss/aktuelt/nyheter/dataangrep-mot-sykehuset-innlandet-hf

fylke[4]. Angrepene illustrerer at sikring av informasjons- og kommunikasjonsteknologi har blitt en sentral del av beredskaps- og sikkerhetsarbeidet i kommunene.

I januar 2021 ble Østre Toten kommune rammet av et stort dataangrep der data ble kryptert og sikkerhetskopier ble slettet. Angrepet førte blant annet til at arbeid i ulike tjenester måtte utføres manuelt da datasystemer var utilgjengelige. Sensitive personopplysninger kan også være på avveie.

2.1.2 Personvern og sikkerhet

I etterkant av at personopplysningsloven trådte i kraft i 2018 har håndtering av personopplysninger og IKT-sikkerhet fått økt oppmerksomhet. Datatilsynet har uttrykt sin bekymring rundt kommuners og fylkeskommuners evne til å håndtere IT-sikkerhet i skoler[5]. Flere tilsyn gjennomført av Datatilsynet har avdekket feil i kommuners håndtering av IT-sikkerhet og personvern. I løpet av 2019 og 2020 har flere kommuner og offentlige virksomheter blitt ilagt overtredelsesgebyr med bakgrunn i brudd på personopplysningsloven:

- ✓ Indre Østfold kommune - brudd på konfidensialitet
- ✓ Bergen kommune – mangelfull sikring av vedvarende konfidensialitet
- ✓ Rælingen kommune – manglende risikovurderinger, personvernkonsekvensvurderinger, testing og mangelfull sikkerhet
- ✓ Oslo kommune - sårbarheter uten tiltak, manglende sikkerhet og mangelfull sikkerhetstesting
- ✓ Oslo kommune – informasjonssikkerhet ved lagring av pasientopplysninger
- ✓ Bergen kommune – mangelfull personopplysningssikkerhet

2.1.3 Hjemmekontor

Koronapandemien har siden nedstengingen i mars 2020 medført en rask og stor økning i bruken av hjemmekontor i det norske samfunnet. En undersøkelse utført av Næringslivets sikkerhetsråd avdekket at nærmere tre av ti virksomheter innenfor offentlig administrasjon opplevde at IT-sikkerheten deres var svekket i løpet av de første ukene med hjemmekontor under koronakrisen[6].

[4] https://www.nrk.no/innlandet/10.000-kommuneansatte-rammet-av-dataangrep-1.15143964

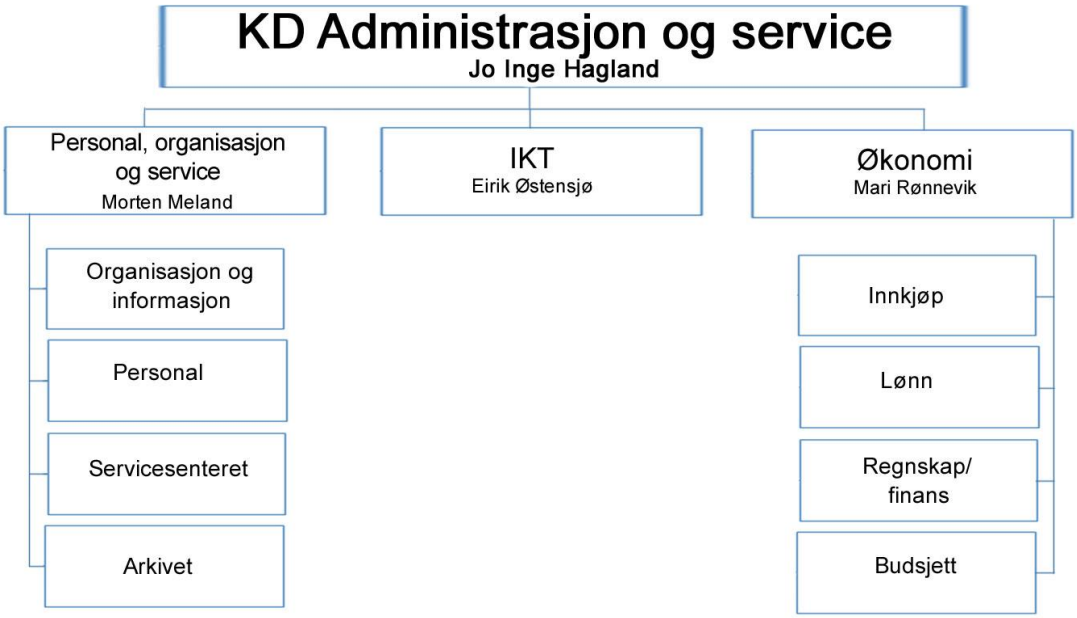
[5] Datatilsynet slår alarm om IT-sikkerhet i skolene – E24

[6] https://norsis.no/stor-undersokelse-hjemmekontor-svekket-it-sikkerheten-mest-i-det-offentlige/

3. Organisering av arbeidet med IT-sikkerhet i Haugesund kommune

Haugesund kommune har etablert en IKT-enhet med ansvar for data- og telekommunikasjon i kommunen. Enheten leverer også tjenester til kommunale foretak, interkommunale selskap og andre organisasjoner. Målsettingen for IKT er å drifte Haugesund kommune sine data-, kommunikasjons- og telesystem på en kostnadseffektiv og rasjonell måte, med fokus på stabilitet og driftssikkerhet. IKT-enheten skal også ivareta innkjøp av utstyr, holde seg til gjeldende lovverk og rutiner for datasikkerhet, samt fungere som rådgiver innen IKT-spørsmål. IKT-enheten er organisert under kommunaldirektør for administrasjon og service.

Figur 1 Organisasjonskart over tjenesteområde administrasjon og service i Haugesund kommune



I Haugesund er det også etablert en egen arbeidsgruppe for personvern med representanter for alle tjenesteområdene i Haugesund kommune. Av mottatt dokumentasjon fremkommer det at gruppen arbeider med overordnede dokumenter i kommunen og sender ut oppgaver til virksomheter ved behov. I rutiner utarbeidet av arbeidsgruppen fremgår det samtidig at det i flere tilfeller er delegert den enkelte enhetsleder å implementere og utarbeide gjeldende rutiner for informasjonssikkerhet i egen enhet.

4. IT-sikkerhet: Systemer, rutiner og prosedyrer

4.1 Revisjonskriterier

I kapittel 4 vil vi besvare problemstilling 1 *Hvordan arbeider Haugesund kommune med IT-sikkerhet?* med underproblemstilling 1 a) hvilke systemer, rutiner og prosedyrer har kommunen for å ivareta krav til informasjonssikkerhet? med delspørsmål, samt 2 b) har kommunen oppdatert sin helhetlige risiko- og sårbarhetsanalyse og hvordan omtales risiko knyttet til informasjons- og kommunikasjonsteknologi her?, 2 c) i hvilken grad gjennomføres det analyser og risikovurderinger ved anskaffelse av nye systemer? 2 d) hvordan håndteres avvik, 2 e) har kommunen rutiner for å gjenoppta normal drift etter driftsstans på kritiske områder? og 2 f) har kommunen en beredskapsplan for IKT og hvordan er denne samordnet med andre planer?

Revisjonskriterier er utledet fra eForvaltningsforskriften, personopplysningsloven, forskrift om kommunal beredskapsplikt og veiledere fra digitaliseringsdirektoratet.

- ✓ Kommunen skal ha implementert egnede tiltak slik at uvedkommende ikke har tilgang til personopplysninger og taushetsbelagt informasjon
- ✓ Kommunen skal ha prosedyrer for behandling av personopplysninger i tråd med krav i personopplysningsloven
- ✓ Kommunen skal ha etablert rutiner for å håndtere brudd og avvik på personopplysningssikkerheten
- ✓ Kommunen skal kartlegge og vurdere sannsynligheten for uønskede digitale hendelser
- ✓ Kommunen bør ha en beredskapsplan for IKT som er samordnet med kommunens helhetlige beredskapsplan
- ✓ Kommunen bør ha utviklet planverk for hendelseshåndtering og gjenoppretting ved driftsstans på sentrale IKT-systemer.
- ✓ Kommunen bør ha etablert krav som ivaretar IKT-sikkerhet i hele livsløpet fra anskaffelse til avhending av IKT-produkter og -tjenester

For detaljert beskrivelse av revisjonskriteriene som er benyttet se vedlegg 2

Kapittelet er strukturert på følgende måte:

- ✓ Rutiner, retningslinjer og andre styrende dokumenter for informasjons- og IT-sikkerhet
- ✓ Tilgangskontroll
- ✓ Prosedyrer for behandling av personopplysninger
- ✓ Avvikshåndtering
- ✓ Kartlegging av risiko- og sårbarhet innen IKT
- ✓ Anskaffelser og kassering av systemer, utstyr og programvare
- ✓ Beredskapsplaner IKT
- ✓ Driftsstans

4.2 Fakta

4.2.1 Rutiner, retningslinjer og prosedyrer for informasjonssikkerhet

Haugesund kommune har flere rutiner, retningslinjer og andre styrende dokumenter som legger føringer for arbeidet med personvern og informasjonssikkerhet. Nedenfor gjengis kort rutinene som er blitt oversendt i forbindelse med forvaltningsrevisjonen.

Rutine / prosedyre	Hensikt	Sist oppdatert/ godkjent
Sikkerhetsmål- og strategi	[redacted] dokument for informasjonssikkerhet, og presenterer definerte sikkerhetsmål og strategi i kommunen. Av dokumentet kommer det frem at det overordnede formålet med kommunens behandling av personopplysninger er sikker og effektiv saksbehandling. Delen om strategi viser til organiseringen av sikkerheten i kommunen og legger frem ansvar og retningslinjer for å ivareta informasjonssikkerhet.	[redacted]
Personvernerklæring	Det er utarbeidet en personvernerklæring som har til hensikt å gi innbyggere og andre brukere av kommunens tjenester, informasjon om hvordan kommunen behandler personopplysninger som kommunen innhenter, og hvilke rettigheter de registrerte har. Selv om det trekkes frem at Rådmannen er behandlingsansvarlig for kommunens behandling av personopplysninger er det daglige ansvaret delegert til virksomhetsleder og enhetsleder for den aktuelle behandlingen. Disse er igjen ansvarlig for at personopplysningsloven følges. I henhold til personvernerklæringen må det foreligge samtykke i de tilfeller hvor det ikke foreligger lovhjemmel for den aktuelle behandlingen.	Ukjent
Informasjon til kommunens innbyggere og ansatte om behandling av personopplysninger	Vi er blitt oversendt et utdrag fra kommunens hjemmeside som er styrende for kommunens arbeid med personvern. Informasjonsdelen er rettet mot kommunens innbyggere og beskriver grunnlaget for, og gir eksempler av, hvilke behandlinger kommunen foretar seg.	Publisert i 2018
Innsyn etter offentleglova	Hensikten med rutinen er å sikre at innsynskrav blir ivaretatt i henhold til gjeldende lov og forskrifter. Det fremkommer av rutinen at det påligger Arkiv og den enkelte Enheten å påse at krav om innsyn blir fulgt opp, og eventuelt sikre at avslag på innsyn hjemles i gjeldende lovkrav.	Sist godkjent i 2017
Rutiner for innsyn i personopplysninger	Haugesund kommune har under utarbeidelse en rutine for innsyn i personopplysninger. Hensikten med denne rutinen er å sikre at den registrertes rett til innsyn i personopplysninger om seg selv blir ivaretatt i henhold til personopplysningslovens (GDPR) artikkel 15. Det vises til at virksomhetsleder, enhetsleder eller den enkelte saksbehandler har ansvaret knyttet til saksbehandlingen av innsynskravet. Dette inkluderer hvordan man skal gå frem for å svare ut innsynskravet avhengig av om en virksomhet behandler personopplysninger om den enkelte eller ikke. I henhold til rutinen skal det gis opplysninger om formålet med behandlingen, innsyn i hvilke opplysninger	Under utarbeidelse

	som behandles og retten til å be om retting og sletting av personopplysningene som behandles.	
Taushetsplikt	Hensikten med rutinen er å sikre at personvernet ivaretas på en tilfredsstillende måte, samt å sikre at det blir orientert om aktuelt lov- og regelverk og skrevet under på individuell avtale om taushetsplikt i henhold til gjeldende lov og regelverk. Taushetsplikten gjelder for alle kommunens ansatte, inkludert øvrige personer som utfører oppdrag på vegne av kommunen. I rutinen beskrives ansvar knyttet til informasjonsdeling om taushetsplikten og oppfølging av administrative oppgaver knyttet til oppbevaring og arkivering av signerte taushetserklæringer. Rutinen inkluderer også prosedyre for brudd på taushetsplikten (avvikshåndtering).	Sist godkjent i 2013
Melde avvik – informasjonssikkerhet og personvern	Hensikten med denne rutinen er å sikre at avvik som angår personvernet og informasjonssikkerhet blir meldt og håndtert iht. personopplysningsloven. Det vises til den enkeltes ansvar dersom man avdekker brudd på personvernet og informasjonssikkerhet.	Sist godkjent i 2019
Rutine for retting og sletting av helseopplysninger/ journalopplysninger	Rutinen skal sikre at pasienters rettigheter knyttet til retting og sletting av helse- og journalopplysninger i helseregistre blir ivaretatt i henhold til gjeldende lover og forskrifter. I rutinen beskrives både ansvar knyttet til ulike roller og hvordan den praktiske utførelsen skal forekomme når en beslutning er tatt.	Sist godkjent i 2020
Sjekkliste for gjennomføring av tiltak for nyansatte medarbeidere i Haugesund kommune	Sjekklisten beskriver tiltak som skal foretas i forbindelse md nyansettelser. Blant annet påpekes det at innføring i Risk Manager og signering av taushetserklæring skal foretas første arbeidsdag.	Ukjent
Opphør av ansettelsesforhold – oppsigelse fra arbeidstaker	Hensikten med rutinen er å sikre at ansatte som slutter blir ivaretatt i henhold til gjeldende lover, forskrifter og arbeidsavtale og at lønn opphører tilsvarende. I følge rutinen skal blant annet enhetsleder sende melding til IKT om opphør i stilling. Det henvises også til ulike skjema (sjekkliste ved opphør av arbeidsforhold og sluttintervju) ligger i Risk Manager.	Sist godkjent i 2007

Som det fremkommer av tabellen har Haugesund kommune rutiner på en rekke områder, for eksempel når det gjelder innsyn i personopplysninger, nyansettelser og redigering og sletting av helseopplysninger. En tilbakemelding i intervju er likevel at det eksisterer et forbedringspotensial hva gjelder systematisk arbeid med oppdatering, samt å sikre at rutinene er innarbeidet i kommunens ulike tjenesteområder. Dette ser imidlertid ikke ut til å ha ført til alvorlige uønskede hendelser, og det påpekes av de involverte at det oppleves som at arbeidet på området er tilfredsstillende.

Intervjuene avdekker at svært få etterlyser, eller har vært bevisste på, manglende rutiner eller behovet for bedre eller mer oppdaterte rutiner. Det kommer imidlertid frem at dette i stor grad kan skyldes at arbeidet med informasjonssikkerhet i relativt liten grad er formalisert, noe som medfører at rutiner og prosedyrer på mange områder ikke bør *endres*, men at det er behov for at de utarbeides. Det er tydelig at arbeidet som gjøres av de ansvarlige på feltet oppleves som tilfredsstillende på svært mange områder, men at det samtidig er lite kjennskap til rutiner, retningslinjer og prosedyrer. Årsaken til at arbeidet oppleves som tilfredsstillende oppgis mellom annet til å være at kommunen har en velfungerende og godt kjent IKT-enhet, og et godt kjent personvernombud. Samtlige av informantene forteller om kjennskap til disse, og at de kontaktes ved behov for bistand og at bistanden i all hovedsak oppleves som god.

4.2.2 Tiltak for å hindre uvedkommende tilgang til personopplysninger og taushetsbelagt informasjon

Haugesund kommune har etablert [redacted] som kommunens overordnede styrende dokument for informasjonssikkerhet. Tiltak for å hindre uvedkommende tilgang til informasjon nevnes spesifikt i dette dokumentet og fremgår i flere av sikkerhetsmålene som Haugesund kommune har etablert. Sikkerhetsmålene inkluderer blant annet definerte mål for fysisk sikkerhet og tilgang til systemer og informasjon.

Sikkerhetsmålene skal oppnås ved gjennomføring av tiltak definert i Sikkerhetsstrategien. I Sikkerhetsstrategien defineres organisering og ansvar for sikkerhetsarbeidet, IKT-reglement, krav til fysisk sikkerhet, tilgang til systemer, dokumentsikkerhet med mer. [redacted]

Videre har Haugesund satt overordnede krav for behandling av personopplysninger som skal legges til grunn for etablering av sikkerhetstiltak. Konfidensialitet er også inkludert i sikkerhetsstrategien for å sikre ivaretagelse av taushetsplikt og hindre at uvedkommende får kjennskap til opplysninger. Det er etablert en sjekkliste for nyansatte som viser at IKT-enheten er involvert i brukeradministrasjon og tildeling av nødvendige tilganger.

Haugesund kommune har etablert en rutine for innsyn etter offentlighetsloven. Rutinen inneholder krav som skal ivareta taushetsplikten i saker der det bes om innsyn etter offentlighetsloven. Dette inkluderer krav til at taushetsbelagte opplysninger skal unntas fra offentligheten og hvordan det håndteres etter offentlighetsloven.

Våre informanter trekker frem to-faktorautentisering som det viktigste og best kjente tiltaket for å styrke adgangskontroll til kommunens IT-systemer. [redacted]

To-faktorautentisering oppfattes som et spesielt viktig tiltak for å øke IT-sikkerheten, noe som også understøttes av råd fra NSM i etterkant av Østre Toten-angrepet. [redacted]

I tillegg har kommunen selv avdekket mangler knyttet til bruk av rutiner for bruker- og tilgangsstyring, og spesielt gjelder dette mangler der ansatte har sagt opp mens brukerkontoer ikke har blitt avsluttet, o.l. Vi har blitt tilsendt rutine for «opphør i ansettelsesforhold – oppsigelse fra arbeidstaker», hvor det fremkommer at enhetsleder skal sende melding til IKT om opphør i stilling. Under faktaverifikasjon ble vi gjort klar over at selv om kommunen har rutiner for dette er det en sårbarhet knyttet til at rutinene ikke alltid følges av ledere. Kommunen har nylig gått til anskaffelse av et nytt system for identitetskontroll knyttet til brukeradministrasjon [redacted] Dette skal integreres i HR-systemet, og føre til bedre muligheter for oppfølging og automatisk oppretting og lukking av brukerkontroll ved tilsettinger og opphør av arbeidsforhold enn med dagens løsning med et sentralt brukerregister. Avtale er inngått, men systemet var ikke operativt ved revisjonstidspunktet.

4.2.3 Prosedyrer for behandling av personopplysninger

Behandling av personopplysninger er inkludert i Haugesund kommunes Sikkerhetsmål- og strategi som er kommunens overordnede styrende dokument for informasjonssikkerhet.

Som tabellen innledningsvis i dette kapittelet viser har kommunen etablert flere rutiner innen personvern og informasjonssikkerhet hvorav enkelte av rutinene er nyetablerte. Haugesund kommune er også i ferd med å etablere Rutine for innsyn i personopplysninger (rutinen var ikke godkjent på tidspunkt for forvaltningsrevisjonen). Rutinen skal etablere at registrertes rett til innsyn i personopplysninger om seg selv blir ivaretatt i henhold til personvernforordningen (GDPR) artikkel 15. Av samtale med nøkkelpersoner i kommunen kommer det frem at rutinen også er tiltenkt å inneholde retningslinjer for sletting av personopplysninger.

Haugesund kommune har etablert «Rutine for retting og sletting av helseopplysninger/journalopplysninger» for å sikre at pasienters rettigheter knyttet til retting og sletting av helse- og journalopplysninger i helseregistre ivaretas. Personopplysningslovens artikkel 16 og 17 er inkludert som relevante lovkrav.

I følge Personopplysningslovens artikkel 28 skal behandling utført av en databehandler være underlagt en avtale eller et annet rettslig dokument. Her skal gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte, samt den behandlingsansvarliges rettigheter og plikter fastsettes. Vi har blitt forelagt mal for databehandleravtale, samt syv utfylte versjoner. Vår gjennomgang av alle tilsendte databehandleravtaler – samt mal – viser at samtlige inkluderer overnevnte krav skissert i personopplysningslovens artikkel 28 3. ledd.

Det er etablert en behandlingsprotokoll som kartlegger kommunens behandling av personopplysninger. Av intervju fremgår det at denne har blitt overført til systemet Draft-it, og benyttes eksempelvis for å gjennomføre DPIA (Data Protection Impact Assessments[7]). Det fremgår av oversendt dokumentasjon at Haugesund kommune alltid skal vurdere behovet for å gjennomføre en DPIA for behandling av personopplysninger, blant annet i forbindelse med innkjøp av nye systemer. Vi har blitt tilsendt et eksempel på dette. DPIA ved anskaffelser av nye systemer omtales videre i kapittel 4.2.6.

Prosedyrene for håndtering av personopplysninger fremstår som både kjent og anvendt av de relevante ansvarshavende i kommunen. Vi er òg blitt forelagt en rutine for håndtering av avvik knyttet til personvern og informasjonssikkerhet, denne diskuteres videre i neste seksjon. Personvernombudet har en rådgivende rolle i arbeidet med å sikre personopplysninger, og kommunedirektøren har det overordnede ansvaret for sikkerheten. Personvernombudet virker å være godt kjent blant kommunens ansatte, og ledere på forskjellige nivåer omtaler personvernombudets arbeid som både viktig og godt. I tillegg er det opprettet en arbeidsgruppe for personvern og informasjonssikkerhet som møtes for å diskutere personvernrelaterte problemstillinger. Alle sektorer har en representant inn i personverngruppa, men visse sektorer dekker flere områder (for eksempel oppvekst, som har skole, barnevern, m.m.) noe som kan føre til visse utfordringer, siden de forskjellige områdene har kompliserte og særskilte behov og utfordringer knyttet til personvern. Det kan dermed være vanskelig for en representant for hele sektoren å ha tilstrekkelig oversikt over personvern for alle områdene i sektoren.

I de forskjellige virksomhetene brukes forskjellige systemer for håndtering av personopplysninger (for eksempel Visma i skolene og Gerica i helse- og omsorgssektoren), og IKT-enheten har ansvar for databehandleravtaler med alle leverandører av slike systemer. En rekke informanter beskriver også at det er godt kjent at det skal gjennomføres risikovurderinger (DPIA) i forkant av anskaffelser av IT-systemer, og det fremstår som om dette i all hovedsak etterfølges.

4.2.4 Avvikshåndtering

Avvik, spesielt innen personvern og informasjonssikkerhet, skal rapporteres til Datatilsynet innen 72 timer etter at avviket er oppdaget (med mindre bruddet ikke vil føre til skade for fysiske personers sikkerhet). Siden 2020 har personvernombudet og leder for arbeidsgruppen for personvern og informasjonssikkerhet hatt jevnlige møter hvor de har foretatt gjennomganger av innmeldte avvik med

[7] Vurdering av personvernkonsekvenser

tanke på videre varsling av Datatilsynet innen satte tidsfrister. Tilbakemeldinger i intervju tyder på at det har forekommet tilfeller hvor personvernombudet i kommunen har meldt avvik til Datatilsynet.

Haugesund kommune har etablert en spesifikk rutine for avvikshåndtering innen området informasjonssikkerhet og personvern. Rutinen inneholder krav til registrering, informering og lukking av brudd og avvik relatert til personvern og informasjonssikkerhet. Håndtering av innkommende avvik behandles av ledere innenfor de ulike tjenesteområdene som er delegert ansvar for informasjonssikkerhet og personvern innen sin enhet/virksomhet. Avvik med alvorlighetsgrad for personvernet og sannsynlighet for at bruddet vil medføre en risiko for de registrerte sine rettigheter og friheter blir meldt videre til Datatilsynet av Personvernombudet.

Avvik registreres i verktøyet Risk Manager. I tidsperioden 01.01.2019 – 25.01.2021 har 104 avvik innen området «Informasjonssikkerhet og personvern» blitt registrert i systemet. 83 av de registrerte avvikene har status «lukket», 5 har status «avvist», 4 har status «Nytt» og 12 «Til behandling».

Haugesund kommune har inkludert krav til avvikshåndtering i [redacted]. Det skal være tatt i bruk systematiske læreprosesser ved uønskede hendelser slik at sannsynlighet for tilsvarende eller gjentatte hendelser reduseres. Ansvar for oppfølging og beslutning av korrigerende tiltak er definert avhengig av hvilken kategori hendelsen tilhører.

Intervjuene bekrefter at de omtalte rutinene er kjent og i stor grad brukes. De ansatte i kommunen har ofte både rådgivere/ansvarlige for personvern i egen sektor, i tillegg til at alle vi har snakket med som har lederansvar er godt kjent med personvernombudet og hvor brudd og avvik skal meldes inn.

Tilbakemeldinger i flere av intervjuene viser imidlertid at kommunens ansatte har forskjellige oppfatninger om hva som er avvik, og hvordan avvik meldes. Inntrykket er at bevissthet og kompetanse blant de ansatte i kommunens virksomheter på dette feltet er noe fragmentert, og varierer mellom ulike sektorer i kommunen. Det er også observert store forskjeller mellom sektorer og ansattgrupper når det gjelder hva som anses som avvik og meldes inn. Det fremkommer også at avvik ofte ikke håndteres på en måte som de ansatte opplever som formålstjenlig dersom formålet med avvikssystemet er kvalitetsforbedring og læring.

Vi har avdekket store forskjeller knyttet til oppfatninger om avvik, og oppfølging av dette, mellom sektorer som for eksempel skole og helse- og omsorg. Flere i kommunens ledelse har også påpekt at det er behov for en bevisstgjøring rundt funksjonen til, og formålet med, avvikssystemet.

Intervjuene viser også at mange oppfatter avvikssystemet Risk Manager som tungvint og gammeldags, og at manglende brukervennlighet *kan* føre til høyere risiko for at avvik ikke meldes og behandles på en optimal måte. Andre informanter påpeker at utfordringene knyttet til avvikshåndtering i større grad skyldes manglende omforent forståelse og rutiner for melding og håndtering av avvik i kommunen, og at intet system vil endre det faktum. Haugesund kommune har nylig besluttet å gå til anskaffelse av nytt avvikshåndteringssystem (i samarbeid med andre kommuner på Haugalandet), og vi har derfor valgt å ikke fokusere spesielt på utfordringene knyttet til den utgående tekniske løsningen.

4.2.5 Kartlegging og vurdering av sannsynlighet for uønskede digitale hendelser

Haugesund kommune har utarbeidet en helhetlig risiko- og sårbarhetsanalyse (ROS-analyse) som er et krav i henhold til lov om kommunal beredskapsplikt. ROS-analysen var sist oppdatert i 2017, men vi er informert om at det på tidspunktet for revisjonen pågår en rullering (oppdatering) av analysen. IKT-enheten har vært involvert i arbeidet med ROS-analysen.

Uønskede digitale hendelser er direkte inkludert som del av tre hendelser i ROS-analysen:

- ✓ Brudd på informasjonssikkerhet
- ✓ Nedetid data og telefoni
- ✓ Tap av data

Det fremgår av analysen hvordan de definerte risiko- og sårbarhetsfaktorene kan påvirke hverandre.

ROS-analysen har også definert tiltak som må være på plass for å sikre data og systemer, samt etablering av rutiner og rammeverk. Vi har ikke fått oversendt rutinene som nevnes for bortfall av data- og teletrafikk. Videre er det etablert krav til sikkerhetskopiering av data og lagring på en separat lokasjon i henhold til etablert plan.

Sikkerhetsmål er definert for uønskede hendelser. Målene inkluderer at det skal være mulig å spore digitale hendelser, samt at det skal være tatt i bruk rutiner for å håndtere uønskede hendelser.

Det fremgår av oversendt dokumentasjon og intervjuer at kartleggingen av uønskede digitale hendelser i stor grad gjøres gjennom kommunens arbeid med helhetlig ROS-analyse.

Det fremkommer av intervjudata at uønskede hendelser knyttet til IT-sikkerhet ikke er kartlagt i tilstrekkelig grad i Haugesund kommune. Dette fremstår som et av de viktigste forbedringspunktene avdekket i denne revisjonen. Temaet er tett knyttet til diskusjonene om risikovurderinger, beredskapsplan og beredskapsøvelser nedenfor (se seksjon 4.2.6, 4.2.8 og 5.2.1). Våre informanter forteller at de i svært liten grad kjenner til slike kartlegginger, og det fremkommer tydelig at informantene også selv anser dette som en svakhet. Sentrale personer forteller at man ikke har hatt en systematisk og strukturert tilnærming til identifisering og kartlegging av svakheter og potensielle uønskede hendelser.

Flere informanter uttrykker at de «regner med at IKT-avdelingen gjør slike ting», men vår revisjon har avdekket at manglende kjennskap til slike kartlegginger i stor grad skyldes at det faktisk ikke er gjennomført. Flere omtaler løse planer om å gjennomføre kartlegginger og tester, men dette har altså ikke materialisert seg i større kartleggingsarbeid. Her påpekes det også at koronapandemien har vært et mulig hinder for denne type proaktivt arbeid i løpet av det siste året. Arbeid knyttet til uønskede hendelser omtales som noe «ad-hoc» (ref. to-faktorautentisering etter Østre Toten-hendelsen), og ingen omtaler konkrete rutiner eller kartlegginger knyttet til uønskede hendelser som kjente og/eller tilfredsstillende. Det påpekes av flere at dette bør inngå som en sentral del av arbeidet med ny ROS-analyse, og at man bør gå bredere ut enn man har gjort frem til nå. Samtlige informanter understreker at det er *viktig* for kommunens IT-sikkerhet at kartleggingen av uønskede hendelser og sannsynligheten for slike gjennomføres på en god måte.

I forbindelse med kartlegging og vurdering av sannsynlighet for uønskede hendelser kommer flere informanter inn på Haugesund kommunes pågående innmelding i Kommune-Csirt. Dette er et nasjonalt senter for kommuner og fylkeskommuner, og formålet er å støtte disse med relevant informasjon om sårbarheter, samt at de tilbyr rådgivningstjenester. Informantene mener også at Kommune-Csirt vil kunne gjennomføre penetrasjonstester o.l. for å teste sikkerheten til kommunens systemer. Medlemskap i Kommune-Csirt vil dermed kunne være en viktig kilde til informasjon og støtte i kartlegging og vurdering av sannsynlighet for uønskede hendelser.

4.2.6 Risikovurderinger ved anskaffelse av nye systemer

Av oversendt dokumentasjon fremgår det at det alltid skal gjøres en vurdering av behov for gjennomføring av DPIA før nye systemer anskaffes. Vi har fått oversendt et eksempel på gjennomført DPIA i forbindelse med en anskaffelse. En tilbakemelding i intervju er at kommunen i stor grad foretar fullstendige DPIA som et føre-var tiltak, ettersom prosessen enda oppleves som relativt ny. I intervjuene framstår det som uklart hvilke andre risikovurderinger som gjennomføres i anskaffelsesprosesser. Vi har ikke blitt gjort kjent med etablerte krav og rutiner for risikovurderinger ved anskaffelser utover DPIA.

Det er gitt tilbakemelding om at det er varierende hvor langt de ulike tjenesteområdene har kommet i forbindelse med gjennomføring av DPIA. Inntrykket er at sektorer som helse har kommet lengst, selv om det nå også i større grad gjennomføres DPIA i tjenesteområdet oppvekst. Det er identifisert et behov for å etablere rutiner for å fange opp denne problematikken, og det henvises blant annet til at et IKT-reglement eller innkjøpsreglement kan være gode alternativer.

I økonomireglementet for kommunen står det skrevet at det skal foreligge rutiner for innkjøp, samt at relevante fagpersoner skal trekkes inn i utarbeidelse av konkurransedokumenter for å oppnå best mulig resultat i anskaffelsesprosessen. Vi er blitt sendt rutine for anskaffelsesprosess i Haugesund kommune som beskriver ulike trinn som skal ivaretas i prosessen. Det henvises ikke eksplisitt til at aktuelle fagpersoner skal trekkes inn ved anskaffelsesprosesser, og det uttrykkes i intervju at det har vært noe varierende praksis knyttet til om IKT blir involvert ved anskaffelser av nye systemer. Likevel er inntrykket at praksisen har blitt noe tydeligere og at det er etablert en forståelse i de ulike sektorene i kommunen om at IKT-enheten skal involveres i forbindelse med anskaffelser innen IKT-området. IKT-enheten påpeker også selv at de har uttrykt et sterkt ønske om å være delaktig i alle anskaffelser, selv om disse håndteres av innkjøpsavdelingen. Her uttrykkes det også et ønske om en revurdering av rutinene for anskaffelser, siden det per nå er noe uklar ordlyd i rutinene og IKT-enheten ved visse tilfeller har blitt utelatt fra anskaffelsesprosesser de selv mener de burde ha vært involvert i.

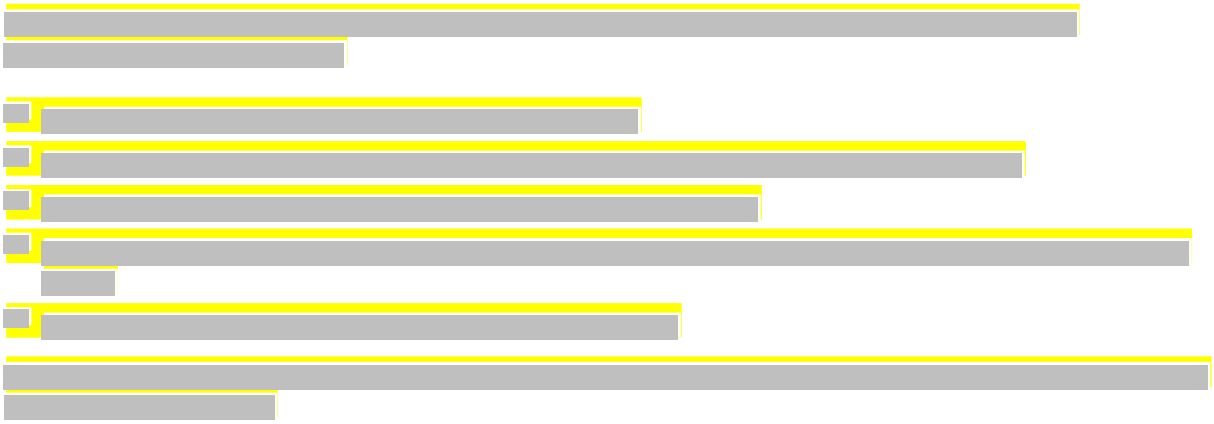
4.2.7 Rutiner for kassering av gammelt utstyr og programvare

Det er ikke etablert en egen rutine for kassering av gammelt utstyr, men i intervjuene framgår det at krav til sikker avhending av datautstyr er inkludert i anskaffelsesprosesser og innkjøpsavtaler ved at kommunen stiller krav til sine leverandører. Vi har blitt oversendt et eksempel på en anskaffelsesprosess som skisserer krav til sikker avhending av datautstyr. Kassering av utstyr og sikker sletting fremgår ved to av tildelingskriteriene:

- ✓ Sikker innsamling (retur) og sikker sletting er omtalt, herunder står det skrevet at leverandør må skissere hvordan den søker å tilrettelegge for å oppnå kravet
- ✓ Ombruk, kassering og re-/oppsirkulering fremgår som et annet tildelingskriterium. Kravet settes i sammenheng med et ønske om å minimere miljøbelastning.

Dette innebærer at rutiner for kassering av utstyr inngår under rutiner for anskaffelser, og rutiner for kassering eksisterer dermed i alle tilfeller der rutiner for anskaffelser blir fulgt. Det første tildelingskriteriet omhandler IT-sikkerhet i forbindelse med innsamling av utstyr og sletting av data. Sistnevnte kriterium omhandler i større grad de miljømessige aspektene ved kassering, og IT-sikkerhet er tilstrekkelig dekket gjennom det første kriteriet. Dette fordrer imidlertid at kommunen aktivt vektlegger og vurderer dette tildelingskriteriet ved anskaffelser.

4.2.8 Beredskapsplan for IKT



Vi er blitt oversendt beredskapsplaner på overordnet nivå samt fra ulike sektorer i kommunen. Tabellen nedenfor henviser til hvordan hendelser relatert til IKT er implementert i de respektive planene.

Beredskapsplan	Tiltakskort og andre identifiserte funksjoner relatert til IKT hendelser
Overordna beredskapsplan for Haugesund kommune	• Viser til avhengighet av data- og teletrafikk og behov for manuelle rutiner ved bortfall av systemer • Viser til at det er tiltakskort innen svikt i infrastruktur for strøm, data og tele. Vi er blitt oversendt tiltakskort for strømforsyning som nevner manglende tilgang til datasystem som konsekvens. • Overordnet beredskapsplan viser til at IKT-sjef er blant fagpersonene som kan tiltre beredskapsledelsen ved behov. Det fremkommer òg at denne personen skal ha opplæring i kommunal kriseberedskap
Helseberedskapsplan for Haugesund kommune	• Helseberedskapsplanen er samordnet med kommunens overordnede plan ved å legge til grunn hendelser som analysen viste var kommunens største sårbarhet, blant disse hendelsene er bortfall av data- og telekommunikasjon • Svikt i teknisk materiell, samt infrastruktur som elektrisitet-, telefoni- og vannforsyning er identifisert som hendelser som kan føre til redusert kapasitet • Kontaktlisten for IKT-ansvarlig ser ut til å være utdatert • Inneholder tiltakskort for «forsyningssvikt (strøm, telefon og data)»
Beredskapsplan for vann i Haugesund kommune	• Bortfall av, eller hendelser relatert til IKT, er ikke omtalt
Beredskapsplan NAV Haugesund	• Inneholder tiltakskort for «brudd på internett forbindelse» • Inneholder rollebeskrivelse for operativ leder IKT
Beredskapsplan psykisk helse og rus	• Inneholder tiltakskort for 9 tjenestegrupper innen «Forsyningssvikt IKT: fagsystem, Outlook, telefoni og adgangskontroll».

Som vi allerede har beskrevet er Haugesund kommunes arbeid med kartlegging av uønskede IT-relaterte hendelser mangelfull, og dette er et helt sentralt element i god beredskap og anvendelige og nyttige beredskapsplaner relatert til IT-sikkerhet. Svært få informanter har konkret kjennskap til beredskapsplaner knyttet til IT-hendelser, og også her ser det ut til å råde en oppfatning – blant de som ikke har ansvar for det – om at dette finnes og er utarbeidet av de med ansvar for feltet. Dette viser igjen at tilliten til styringslinjer, delegeringsreglementer og de *personene* som har ansvar er høy i kommunen. Det er imidlertid viktig å understreke at det finnes relativt begrenset omtale av hendelser knyttet til IT-sikkerhet i de dokumentene som er fremlagt. Flere uttrykker også en viss bekymring for at

de ikke vet hvordan de skulle håndtert en situasjon med bortfall av IT-systemer i sine virksomheter, og etterlyser og påpeker betydningen av at slike planer er både oppdaterte og kjente.

Et tema som også har kommet opp i intervjuene er at IT-miljøet ikke er direkte representert i beredskapsteamet, men at de er indirekte representert via Administrasjon og service. Dette teamet har ansvar for å jobbe med ROS-analyser og planer for sine sektorer, og det blir av noen påpekt at det kunne være hensiktsmessig om IT-erfaring og kompetanse i enda større grad ble en del av dette arbeidet. Dette begrunnes blant annet i at IT-sikkerhet er relevant for alle sektorer, og det derfor er viktig at analyser og planer blir utarbeidet i tråd med innsikt i utfordringsbildet og kunnskap om sårbarhet og løsninger.

Planer for beredskap er også knyttet til bruken av øvelser for å teste og forbedre beredskap. Dette kommer vi tilbake til i kapittel 5.2.1.

4.2.9 Driftsstans på kritiske områder

Vi har blitt oversendt et dokument som inneholder beredskapsrutiner for hendelser relatert til IKT-drift, sist oppdatert januar 2021. Det fremkommer av dokumentet at rutinene gjelder for situasjoner når Haugesund kommune er satt i kriseberedskap. Følgende hendelser beskrives i planverket:

- ✓ Strømbrudd
- ✓ Nettverksfeil
- ✓ Evakuering
- ✓ Feil på kjøleanlegg
- ✓ Feil på telefoni
- ✓ Feil / stopp av SAN
- ✓ Feil på UPS

Det er òg etablert E-post-varslingsrutiner som ligger lagret på Rutinen inneholder en brukermanual for hvordan man skal varsle for planlagt nedetid, samt akutte hendelser. Det vises også til hvilke systemer som betraktes som viktige, lokasjoner, samt hardware som benyttes. Vi er og blitt oversendt eksempler på e-post varsling fra IKT til ulike tjenesteområder ved nedetid på systemer, samt driftsmeldinger knyttet til samme tematikk kategorisert etter «info», «advarsel» og «kritisk». Av driftsmeldingene fremgår det at kun to meldinger er kategorisert som kritisk – disse omfatter nettverksproblemer.

Tilbakemeldinger i intervjuene tyder på at kommunen har opplevd hendelser hvor systemer har vært satt ut av drift over en kortere periode. Eksempler som nevnes er utfall av strømkurser i datarom, bortfall i e-post i lengre perioder ved to tilfeller, og skole-PCer som har sluttet å fungere. Dette betegnes som mindre alvorlige hendelser av informantene, og de beskriver selv at de var i stand til å håndtere problemene *og* at de har ført til læring og mindre sannsynlighet for at det samme skjer igjen. Det har også vært flere tilfeller av virus, noe som blant annet medførte at ble utilgjengelig.

4.3 Vurderinger

Haugesund kommune har en rekke systemer, rutiner og prosedyrer knyttet til informasjonssikkerhet på plass. Kommunen har utarbeidet et tydelig overordnet styrende dokument innen informasjonssikkerhet og personvern som setter mål innen området. Samtidig har vi avdekket noen forbedringsområder. Blant annet fremgår det av våre undersøkelser at flere av målsettingene i kommunens overordnede styrende dokumenter for informasjonssikkerhet og personvern hverken er utarbeidet eller implementert. Med dette refererer vi spesielt til IKT-reglementet og beredskapsplan for IKT.

Det er videre etablert flere rutiner for å etterleve kravene i personvernlovgivningen, og det har siden før EUs personvernforordning ble en del av norsk lovverk blitt utført arbeid på området av en kommunal arbeidsgruppe for personvern og informasjonssikkerhet. Videre eksisterer protokoll for behandling av personopplysninger, og databehandleravtaler er etablert med leverandører. Rollen til personvernombudet er kjent i organisasjonen. Vi observerer også at det jevnlig rapporteres avvik innen området Informasjonssikkerhet og personvern. Vi ser det som positivt at det er igangsatt et arbeid med å forbedre rutiner innen bruker- og tilgangsstyring.

Samtidig har vi gjort en vurdering av at det ved enkelte tilfeller går lang tid mellom oppdatering av rutiner. Vi har heller ikke vært i stand til å finne rutiner knyttet til sletting av personopplysninger på et overordnet nivå for kommunen, og tema er i mindre grad omtalt i rutinen som er under utarbeidelse. Selv om sletting òg reguleres av databehandleravtalene, er kravet til sletting i personopplysningsloven såpass strengt at det etter vår oppfatning bør gis tydelig føringer for hvordan man kan ivareta disse kravene.

Vi oppfatter at det er etablert i kommunen at IKT-enheten skal involveres i anskaffelser av IKT-produkter og tjenester. Det er formalisert visse krav til ivaretagelse av sikkerhet ved avhending av utstyr i kommunens sikkerhetsmål og -strategi. Videre ser vi at gjennomføring av DPIA ved anskaffelser er etablert. Vi ser det som positivt at krav til IT-sikkerhet har blitt inkludert i hele livsløpet fra anskaffelse til avhending i en nylig forespørsel til IT-leverandører. Samtidig ser vi et forbedringspunkt i at disse kravene og IKT-enhetens involvering i IKT-anskaffelser kunne vært tydeliggjort i rutiner for anskaffelser. Det kan også være gunstig å gjennomføre risikovurderinger utover DPIA ved anskaffelser der det er hensiktsmessig. Vi har ikke blitt gjort kjent med at gjennomføring av slike risikovurderinger gjennomføres i dag.

Haugesund kommune håndterer avvik gjennom avviksrapporteringssystem Risk Manager. Hovedansvaret for oppfølging av avvik er lagt til de ulike tjenesteledere. Det er vårt inntrykk at avvik knyttet til personvern og informasjonssikkerhet er tillagt ekstra kontrollmekanismer ved at personvernombudet og leder for arbeidsgruppen i personvern og informasjonssikkerhet har jevnlige gjennomganger av registrerte avvik og sender ut påminnelser til tjenesteledere om oppfølging. Vi har likevel observert at det er noe fragmentert og varierende praksis knyttet til avviksrapporteringen. Noe av dette kan forklares ved at det i utgangspunktet er ulike oppfatninger knyttet til hva som er et avvik innen informasjonssikkerhet og personvern. Varierende forståelser kan, etter vår vurdering, medføre risiko og usikkerhet knyttet til om avvik faktisk meldes på en helhetlig måte. Inntrykket er òg at det fremstår som sannsynlig at det forekommer tilfeller med underrapportering i visse sektorer. Vår vurdering er at varierende praksis i forbindelse med rapportering av avvik viser et behov for systematisk opplæring og bevisstgjøring.

Det fremstår som spesielt viktig å skape en helhetlig oppfatning om hva avvik er og hva som er formålet med å melde avvik. Det er spesielt viktig å etablere en forståelse hos ansatte og ledere på alle nivåer om at dette er et *kvalitetssystem* som er grunnlaget for å forbedre virksomheten, og ikke primært å telle feil og mangler. Dette innebærer at det etableres en felles forståelse om at avvik både er feil og mangler, men også forbedringsmuligheter, og at de som har ansvar for å følge opp avviksmeldinger håndterer det deretter. Vår vurdering er at opplæring bør være sentralt ved implementering av det nye avvik- og kvalitetssystemet kommunen nå har gått til anskaffelse av.

Det største forbedringspotensialet ligger i bedre og mer systematisk arbeid med kartlegging av uønskede hendelser og beredskapsplaner. Etter vår vurdering er det sårbart at det ikke er [redacted] og risikovurderinger knyttet til sannsynlighet for og konsekvenser av IT-relatert hendelser. Behovet for slike analyser er i dag særdeles aktuelt, og omfanget av dataangrep mot offentlig sektor i starten av 2021 understreker dette klart og tydelig. Det fremstår som viktig at IKT-enheten involveres aktivt i alle delene av dette arbeidet, og vi anbefaler

også at Haugesund kommune ser til andre kommuner og Kommune-Csirt for deling av beste praksis på området samt konkret rådgivning knyttet til risikovurderinger og beredskapsplaner.

Vi har i tillegg gjort en vurdering om at kommunen bør planlegge for delvis eller fullstendig bortfall av IT-systemer. Det har, som sagt, bare i løpet av kort tid vært en rekke uønskede digitale hendelser rettet mot offentlig sektor, og herunder kommune-Norge. Det vil trolig alltid finnes en restrisiko relatert til IKT-hendelser – noe som taler for at det bør etableres beredskap, samt at denne burde dimensjoneres for å takle uønskede hendelser. Kommunen har opplevd tilfeller med driftsstans på systemer i perioder. Det har blitt utarbeidet beredskapsrutiner for enkelte IT-relaterte hendelser. Vår vurdering er at dette arbeidet bør forsterkes og inkludere mulige hendelser på flere områder.

5. IT-sikkerhet: Beredskap og bevissthet

5.1 Revisjonskriterier

I kapittel 5 besvarer vi problemstilling 2: *I hvilken grad er kommunens arbeid med IT-sikkerhet tilstrekkelig for å kunne håndtere uønskede digitale hendelser?* med underproblemstilling 2 a) i hvilken grad gjennomføres beredskapsøvelser innenfor hendelser knyttet til IKT?, 2 b) i hvilken grad er ansatte gjort kjent med planverk, ansvar og rutiner for håndtering? 2 c) i hvilken grad gis opplæring til ansatte om informasjonssikkerhet? og 2 d) opplever de som har ansvar for oppgaver dersom hendelser oppstår, trygghet i forbindelse med rutiner og håndtering?

Revisjonskriteriene er utledet fra forskrift om kommunal beredskapsplikt og Digitaliseringsdirektoratet sin veileder i planlegging og gjennomføring av IKT-øvelser og veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet, samt NOU 2018: 14 IKT-sikkerhet i alle ledd.

- ✓ Haugesund kommunens bør ha gjennomført øvelser relatert til IKT-sikkerhet.
- ✓ Haugesund kommunen bør ha et system for opplæring som sikrer at alle ansatte har en forståelse for hva informasjonssikkerhet er, og hvilket ansvar de har i forbindelse med dette.
- ✓ Medarbeidere bør være kjent med planer og tiltak for hendelseshåndtering.

For detaljert beskrivelse av revisjonskriteriene som er benyttet se vedlegg 2

5.2 Fakta

5.2.1 Beredskapsøvelser og andre tester knyttet til IKT

Forvaltningsrevisor har etterspurt dokumentasjon om beredskapsøvelser i kommunen, spesielt de som innebærer eller har inkludert aspekter av IKT. [redacted]

[redacted]. En tilbakemelding er at det har vært gjennomført øvelse knyttet til atomberedskap, hvor informasjons- og kommunikasjonsteknologi har vært inkludert i samhandlingen mellom aktører. [redacted]

IKT-enheten har en sentral rolle i planlegging og gjennomføring av øvelser knyttet til IT-sikkerhet, og dette er et ansvar enheten selv og andre sentrale aktører er enige om plasseringen av. Som tidligere nevnt, i forbindelse med beredskapsplaner, ser mange en positiv utvikling i IKT-enhetens kapasitet, og representanter for enheten vektlegger selv at det over tid har vært et sterkt ønske å arbeide langt mer proaktivt med kartlegging og øvelser. Økte ressurser over tid har nå ført til en situasjon der enheten selv opplever at det er mulig å arbeide på denne måten fremover.

Flere omtaler hendelser av varierende alvorlighetsgrad (gjerne kortere driftsstanser og nedetid på systemer) som en form for «øvelse». Samtidig er vår forståelse at [redacted] uønskede hendelser i liten grad kan forstås som et alternativ til å øve på potensielle uønskede hendelser før de inntreffer.

Det fremgår tydelig av intervjuene at øvelser knyttet til IT-sikkerhet både er ønsket og nødvendig. Mangel på slike øvelser fører til en viss usikkerhet knyttet til mulighetene for å håndtere alvorlige uønskede hendelser, og flere informanter mener at kommunen ikke ville vært i stand til å håndtere en hendelse der sentrale IT-systemer falt bort, og trekker paralleller til hendelsen i Østre Toten. Noen omtaler øvelser som generelt nyttige for læring, mens andre igjen peker på at slike øvelser ville tydeliggjøre hvorvidt kommunen har backup-systemer og rutiner på plass. Det fremstår som sannsynlig at mange av kommunens tjenester – inkludert helse- og omsorgstjenester – ikke er

tilstrekkelig forberedt på et bortfall av sentrale IT-systemer, og konsekvensene av en større hendelse vil potensielt være svært store. Noen omtaler at beredskapsplanene for helse-, omsorgs- og sosialtjenester for eksempel omtaler bortfall av journalsystemer, men ansatte i tjenestene har i liten grad kjennskap til hvilke rutiner som er knyttet til dette, og påpeker at det er viktig at slike planer og rutiner er kjent for de ansatte dersom de skal ha maksimal effekt.

Øvelser knyttet til IT-sikkerhet kan være det som omtales som «skrivebordsøvelser», og IKT-avdelingen fremstår som en sentral aktør i planlegging og gjennomføring av slike øvelser. IKT-avdeling anser også selv dette som en del av sitt ansvarsområde, og det omtales som både mulig og ønskelig å gjennomføre slike øvelser uten at dette krever betydelig økning i ressurser eller andre former for tiltak.

Et sentralt formål med øvelser er å forbedre ferdigheter og kompetanse, i tillegg til å evaluere og forbedre sikkerhetstiltak og beredskapsplaner. Ettersom IKT-relaterte øvelser ikke har funnet sted, kan vi heller ikke konkludere med hva som hadde vært potensielle gevinster ved å gjennomføre øvelser av ulikt slag rettet mot digitale hendelser.

5.2.2 Opplæring og kompetanse

Et av de definerte sikkerhetsmålene i Haugesunds kommune overordnede styrende dokument for informasjonssikkerhet er at kommunen skal sikre at medarbeidere som bruker kommunens informasjonssystemer har en tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov og krav.

I gjennomføringen av forvaltningsrevisjonen er vi gjort kjent med at det har blitt arrangert e-læringskurs for ledere, tillitsvalgte og ansatte i kommunen i 2018 og 2019 med GDPR som tema. E-læringskurset, som først ble sendt ut til ledere og tillitsvalgte i 2018, besto av 13 leksjoner som inneholdt opplæring om personvern, personopplysninger og databehandling. Kurset ble sendt ut i forbindelse med at personvernforordningen ble en del av norsk lovgivning 20. juli 2018, og hensikten var å etablere grunnleggende kunnskap om forordningens innhold og dens praktiske og juridiske betydning. Det var i tillegg en hensikt med kurset at kommunens ansatte skulle bli oppmerksom på nødvendige tiltak og aktiviteter for å etterleve det nye lovverket. Kursinnholdet viser at følgende tema var inkludert i opplæringen:

- ✓ Velkommen til introduksjonskurs om personvern
- ✓ Hva er personopplysninger og databehandling
- ✓ Behandling av personopplysninger krever et lovlig formål
- ✓ Behandling av personopplysninger: hvem er involvert?
- ✓ Har vi databehandleravtaler på plass?
- ✓ Innbyggerne får nye personvernrettigheter
- ✓ Personvernerklæring, informasjon og åpenhet
- ✓ Når avvik oppstår, må vi rapportere
- ✓ Personvern: risiko, konsekvenser og tiltak
- ✓ Vi må prioritere personvern i alle tjenester og løsninger
- ✓ Anonymisering og pseudonymisering
- ✓ Er skolen klar for nye personvernregler?
- ✓ Helse: er vår avdeling klar for de nye personvernreglene?

For øvrig ble kurset sendt ut til alle kommunens ansatte ca. et år etter at det ble sendt ut til alle ledere og tillitsvalgte.

Våre informanter omtaler nærmest utelukkende det omtalte e-læringskurset når de blir spurt om de kjenner til opplæringstiltak knyttet til IT-sikkerhet. Dette indikerer riktig nok at kurset blir husket, men det viser også at det ikke finnes andre kjente universelle opplæringstiltak knyttet til temaet i kommunal regi. Videre er det gitt tilbakemeldinger i intervjuene om at kursene i all hovedsak oppfattes som

positivt. Mange vektlegger også at kursene er lite omfattende, går raskt å gjennomføre, og at det er noe begrenset hvor mye læring de kan bidra til. Mange beskriver kurset som noe man bare må trykke seg gjennom. Kursene omtales som obligatoriske, og dette knyttes spesielt til mulighetene kommunen har for å spore hvem som har tatt kurset, hvor lang tid de bruker på hver modul, osv. KS læring brukes som plattform for kursene, og det er her mulig for kommunen å gjennomføre flere kurs som er tilgjengelig på denne plattformen.

Flere virksomheter har også hatt kurs/fått tilbud om å delta på kurs om GDPR med personvernombudet. Det siste året har opplæring naturlig nok blitt gitt digitalt, men også før dette var det omtalte GDPR-kurset utarbeidet som et rent digitalt kurs. En av informantene gir tilbakemelding om at man mister en viss læringseffekt når man ikke samles fysisk for opplæring og kurs. Dette fremkommer imidlertid ikke i noen andre intervjuer, og de aller fleste anser digitale møter og samhandling som hensiktsmessig og effektivt.

Utover GDPR-kurset omtaler noen informanter forskjellige type kurs som de oppfatter som delvis relevante for IT-sikkerhet, som for eksempel kurs i Teams, Outlook, o.l. Vi anser her ikke slike kurs som direkte knyttet til IT-sikkerhet.

Én informant påpeker at Haugesund kommune har mye god informasjon om IT-sikkerhet på sitt intranett. Dette er imidlertid ikke informasjon som omtales av andre, og det fremstår ikke som om denne informasjonen er godt kjent eller ofte brukt av de ansatte. Vi er i midlertidig gjort kjent med at IKT-enheten for tiden arbeider med videoer og informasjon om IT-sikkerhet som er tiltenkt nyansatte i kommunen.

Informantene er noe delt i synet på behovet for mer omfattende og systematisk opplæring knyttet til IT-sikkerhet. Det overordnede inntrykket etter intervjuer og dokumentgjennomgang er imidlertid at det fremstår som hensiktsmessig med mer omfattende og helhetlig arbeid med opplæring knyttet til IT-sikkerhet. Temaer som informantene nevner er generell informasjons og datasikkerhet (hvordan sikre at andre ikke får tilgang til enheter og informasjon), sikker bruk av og håndtering av e-post (bruk av blindkopi, lagring, sletting, arkivering, osv.), og sektorspesifikke temaer (for eksempel håndtering av elevers brukernavn og passord).

5.2.3 Trygghet og kjennskap til planverk og rutiner for håndtering av uønskede hendelser

Personene med ansvar for ulike aspekter ved kommunens IT-sikkerhet uttrykker i all hovedsak at de er komfortable med kommunens arbeid med IT-sikkerhet. De oppfatter at de har relativt klare roller og oversikt over hvem som har ansvar for hva. I tillegg er det stor tillit til og en positiv oppfatning av arbeidet IKT-enheten gjør, og dette fremstår som den sentrale kilden til trygghet hos de som har overordnet ansvar for områder knyttet til IT-sikkerhet. Når det gjelder kommunens rutiner og systematiske arbeid med IT-sikkerhet er de fleste åpne på at kommunen har et stykke igjen å gå, men at arbeidet som gjøres allikevel er relativt godt.

Revisjonen viser at det ikke arbeides systematisk med bevisstgjøring rundt planverk og rutiner, og flere informanter uttrykker som vi har vært inne på at dette er en svakhet, som også gir grobunn for utrygghet. Dette gjelder både rutiner for personvern o.l., men også hvordan for eksempel bortfall av IT-systemer i helsetjenestene skal håndteres. Informanter i flere sektorer har som nevnt tidligere en tro på at planer eksisterer, en tro som i visse tilfeller er ubegrunnet. Men også der troen er begrunnet er det svært viktig at planer og rutiner gjøres kjent for de ansatte, slik at de raskt kan tas i bruk og følges ved behov.

Det samme bildet avtegner seg i intervjuer med informanter som ikke er i lederposisjoner. De aller fleste opplever relativt stor grad av trygghet når det gjelder IT-sikkerhet, men også her er dette i hovedsak basert på en tillit til at de med ansvar for IT-sikkerhet gjør det de skal. Få informanter besitter selv nødvendig kjennskap til lover, regler, rutiner og prosedyrer til at de på selvstendig grunnlag føler seg trygge på hvordan de skulle agere dersom uønskede hendelser oppstår. Men, de aller fleste er klare på hvordan de ville gått frem og hvem de hadde henvendt seg til ved behov.

5.3 Vurderinger

Arbeidet med digital beredskap henger tett sammen med vurderingen av hvorvidt det gjennomføres kartlegginger av uønskede hendelser (ROS-analyse), samt kommunens beredskapsplaner. I dette kapittelet har vi fokusert mer på hvorvidt det gjennomføres øvelser og annen aktivitet som styrker den faktiske beredskapen og bidrar til læring blant ansatte og ledere.

. I de tilfeller hvor IKT har vært del av andre øvelser er det vårt inntrykk at digitale systemer (som eksempelvis Teams og andre samhandlingsverktøy) har vært benyttet i kommunikasjon mellom involverte aktører.

IKT-sikkerhet og bevissthet knyttet til dette har fått mye oppmerksomhet de senere årene. Av Lysne-utvalget påpekes det blant annet at manglende øvelser kan bidra til å forsterke uklare rolle- og ansvarsforhold i hendelseshåndteringen. I tillegg trekkes det frem at øvelser gir gode forutsetninger for å avdekke sårbarheter, samt bedrer forutsetningene for å håndtere hendelser som måtte oppstå. Slik sett kan beredskapsøvelser anses både som kompetansehevende tiltak, samt gir mulighet til å evaluere og etterprøve om etablert planverk og rutiner er tilstrekkelig og hensiktsmessig utformet. Siden Haugesund ikke har en egen beredskapsplan for IKT, vil sistnevnte være avhengig av at dette først kommer på plass for å kunne vurdere hensiktsmessigheten til planverket gjennom øvelser.

Gitt digitaliseringens hastighet, og stadige endringer i risikobilde er vår vurdering at Haugesund kommune bør planlegge for fullstendig eller delvis bortfall av IKT-systemer, og øve på dette både på overordnet nivå, samt innad i de ulike tjenesteområdene.

Inntrykket generelt er at arbeidet med digital beredskap har vært reaktivt frem til nyere tid. IT-sikkerhetsarbeidet handlet i større grad om å reagere på og håndtere hendelser som oppsto. Gjennom intervju og faktaverifikasjon har vi fått inntrykk av at arbeidet beveger seg mer i en proaktiv retning, og at det er i større grad er fokus på å arbeide i tråd med en føre-var tankegang – som blant annet innmeldingen i Kommune-csirt er et eksempel på. Vi gir likevel en vurdering om at mangler knyttet til beredskapsplaner, øvelser og inkluderingen av digitale hendelser i ROS-analyser indikerer at noe av arbeidet enn så lenge kan karakteriseres som reaktivt. Ved mer systematisk kartlegging, planlegging og andre forebyggende mekanismer mener vi kommunen kan stå bedre rustet om en eventuell hendelse skulle inntreffe. En slik proaktiv tilnærming innebærer at uønskede hendelser kartlegges, planer utarbeides på bakgrunn av analyser, og at øvelser gjennomføres regelmessig for å sikre at backup-systemer og rutiner for å håndtere hendelsene både er på plass og fungerer i praksis.

I tillegg til beredskapsøvelser innenfor IT-sikkerhet, kan kompetansehevende tiltak også bestå av andre opplæringstilbud og kurs. Våre undersøkelser viser at Haugesund kommune har tatt i bruk slike opplæringstiltak for å øke kompetansen til ledere, tillitsvalgte og ansatte i kommunen innen personvern og informasjonssikkerhet. Vår vurdering er at kursserien som har vært benyttet er godt kjent og refereres til blant samtlige informanter som et godt tiltak for å øke forståelsen knyttet til en omfattende og kompleks tematikk.

Det er imidlertid viktig for Haugesund kommune å være klar over at ikke alle kommunens ansatte har egne datamaskiner eller regelmessig bruker kommunens e-post. Dette gjelder spesielt ansatte som ikke har kontorarbeid, og kun unntaksvis bruker IT-utstyr i sitt arbeid. Helse- og omsorgssektoren er her et konkret eksempel, og kommunen må ta hensyn til dette når de legger opp til informasjon om og eventuelt og gjennomføring av kurs digitalt. Dersom det er obligatoriske kurs som oppfattes som viktige for kommunens sikkerhet bør det også legges opp til at de ansatte kan ta disse kursene i arbeidstiden. Dette blir igjen spesielt relevant for de som ikke normalt har tilgang på eller bruker datamaskiner i løpet av sin arbeidsdag.

Regelverket knyttet til informasjonssikkerhet og personvern er omfattende og til dels kompliserte - og det er positivt at de ansatte er kjent med nøkkelpersoner og kontaktpunkter i kommunen. Til tross for at vi anbefaler mer systematisk arbeid med opplæring og kompetanseheving for alle kommunens ansatte fremstår det altså ikke som om kommunens ansatte selv føler seg utrygge på rutiner og håndtering knyttet til IT-sikkerhet.

Vi har videre gjort en vurdering av at opplæringstiltak og kurskategorier rettet mer spesifikt mot IT-sikkerhet er mer fraværende. Utover informasjonen som nå utarbeides av IKT-enheten har det ikke vært gjennomført spesielle opplæringstiltak rettet mot samtlige av kommunens ansatte om potensielle farer og trusler som kan oppstå som følge av bruk av digitale systemer. Selv den med lavest stillingsprosent kan utgjøre en risiko for kommunens systemer – noe som taler for at kompetanse og kunnskap bør opparbeides blant alle kommunens medarbeidere.

Vår overordnede vurdering knyttet til dette kapittelet er at trygghet i stor grad vil avhenge av opplæring, kompetanse og kjennskap til ansvar og rutiner. Selv om vår undersøkelse viser at flere av informantene opplever trygghet i egne arbeidsoppgaver og ansvar, er inntrykket at det er noe mer utydelig hvordan en uønsket digital hendelse ville vært håndtert foruten om å varsle videre i linjen opp til IKT-enhet. Det er vår oppfatning og vurdering at trygghet til ansvar og rutiner ville blitt tydeliggjort gjennom mer systematiske læringsprosesser, eksempelvis ved å gjennomføre øvelser, tester eller kurs og andre opplæringstiltak som kan forbedre ferdigheter og kompetanse. Spesielt opplæringstiltak og kurs bør i tillegg rettes mot alle ansatte for å bygge tilstrekkelige barrierer mot uønskede digitale hendelser.

6. Anbefalinger

KPMG vil her komme med anbefalinger på områdene der det i forvaltningsrevisjonen er funnet avvik eller forbedringspotensial.

Revisjonen viser at Haugesund kommune ikke har vært utsatt for alvorlige uønskede hendelser, og at kommunen arbeider godt med en rekke aspekter knyttet til IT-sikkerhet. Det fremstår som positivt at det er god kjennskap til personer med ansvar for å gi råd, følge opp og implementere rutiner og prosedyrer i kommunen. Informantene uttrykker også stor tillit til disse personene, og vurderer det arbeidet som gjøres, for eksempel i IKT-enheten og av personvernombudet, som godt. Dette skaper trygghet blant kommunens ansatte. Vi har også funnet indikasjoner på at de ansatte i kommunen opplever at det er lov å gjøre feil, og at feil rapporteres og utnyttes i læringsprosesser i mange tilfeller.

Vi har imidlertid avdekket svakheter knyttet til institusjonaliseringen av arbeidet med IT-sikkerhet, avvikshåndtering, risikovurderinger og kartlegging, beredskapsplaner og bruk av øvelser på uønskede hendelser relatert til IT-sikkerhet. Vi har et klart inntrykk av at disse spørsmålene nå vies oppmerksomhet i kommunens arbeid.

Våre anbefalinger er at Haugesund kommune prioriterer følgende:

- Haugesund kommune bør etablere et system for systematiske og jevnlige gjennomganger av rutiner, systemer og prosedyrer knyttet til IT-sikkerhet. Dette for å sikre at det helhetlige arbeidet er oppdatert og koordinert.

- IT-sikkerhet bør inngå som et sentralt element i den pågående rulleringen av ROS-analysen, med spesiell vekt på å kartlegge mindre og mer alvorlige uønskede IT-relaterte hendelser

- Beredskapsgruppen bør utrede hvordan IT-sikkerhet påvirker de forskjellige virksomhetsområdene, og koble IKT-enheten på arbeidet med beredskapsplaner

- Haugesund kommune bør fullføre innmeldingen i Kommune-Csirt og utrede hvordan deres rådgivnings- og øvrige tjenester kan styrke kommunens arbeid med IT-sikkerhet

- Det bør gjennomføres beredskapsøvelser knyttet til bortfall av IT-systemer i alle virksomheter, med sikte på å kartlegge backup-rutiner og muligheter for å opprettholde kritiske tjenester

- Kommunen bør utarbeide og/eller ferdigstille opplæringsprogram i IT-sikkerhet for ansatte

- Kommunen bør benytte seg av muligheten for å gjennomføre kurs om generell informasjons- og datasikkerhet i KS læring eller andre leverandører, og vurdere behovet for ytterligere kurs og opplæring for tidligere ansatte basert på erfaringene fra opplæringsprogrammet for nyansatte

- Kommunen bør, ved implementering av nytt avvik- og kvalitetssystem, gi tilstrekkelig opplæring i system og rutiner for avviksrapportering. En generell opplæring i hva som er avvik relatert til personvern og informasjonssikkerhet vil også være hensiktsmessig.

- Haugesund kommune bør tydeliggjøre når IKT-enheten skal inngå ved anskaffelser av nye systemer, og kommunisere dette ut til de ulike tjenesteområdene

7. Uttalelse fra kommunedirektøren

Uttalelse fra kommunedirektøren

Kommunedirektøren vil bemerke at forvaltningsrevisjonsrapport fra KPMG om IT-sikkerhet er nyttig og grundig. Haugesund kommunen ønsker å bruke anbefalingene for å videreutvikle og forbedre kommunens IT-sikkerhet.

Revisjonen anbefaler at Haugesund kommune prioriterer følgende:

- Haugesund kommune bør etablere et system for systematiske og jevnlige gjennomganger av rutiner, systemer og prosedyrer knyttet til IT-sikkerhet. Dette for å sikre at det helhetlige arbeidet er oppdatert og koordinert.

Kommunens avviks- og kvalitetssystem er verktøyet kommunen skal benytte for å sikre at rutiner, systemer og prosedyrer knyttet til arbeidet med IT-sikkerhet jevnlig blir oppdatert og koordinert. Kommunedirektøren ser at dette ikke er gjort i tilstrekkelig grad og vil sørge for at dette blir utført. Se også svar nedenfor om anskaffelse av nytt avviks- og kvalitetssystem.

[redacted]

Haugesund kommune skal i løpet av 2021 utarbeide egen beredskapsplan for IKT. Se også svar nedenfor om ROS-analyser og beredskap.

- IT-sikkerhet bør inngå som et sentralt element i den pågående rulleringen av ROS-analysen, med spesiell vekt på å kartlegge mindre og mer alvorlige uønskede IT-relaterte hendelser

Samtlige ROS-analyser for Haugesund kommune oppdateres og skal være ferdig behandlet i løpet av høsten 2021. I den forbindelse vil kommunen oppdatere analysen med mindre og mer alvorlige uønskede IT-relaterte hendelser. Kommunen vil også i samarbeidet med Kommune-Csirt be om råd om hvilke områder kommunen bør ha et særlig søkelys på. ROS-analysen vil i tillegg gi et grunnlag for å oppdatere beredskapsplaner og øvelser i beredskapsarbeid.

- Beredskapsgruppen bør utrede hvordan IT-sikkerhet påvirker de forskjellige virksomhetsområdene, og koble IKT-enheten på arbeidet med beredskapsplaner

Kommunedirektøren merker seg denne anbefalingen og vil ta med seg i arbeidet med oppdatering og utarbeidelse av nye beredskapsplaner.

- Haugesund kommune bør fullføre innmeldingen i Kommune-Csirt og utrede hvordan deres rådgivnings- og øvrige tjenester kan styrke kommunens arbeid med IT-sikkerhet

Haugesund kommune har fullført innmeldingen og er medlem i Kommune-Csirt.

- Det bør gjennomføres beredskapsøvelser knyttet til bortfall av IT-systemer i alle virksomheter, med sikte på å kartlegge backup-rutiner og muligheter for å opprettholde kritiske tjenester

Kommunedirektøren merker seg denne anbefalingen og vil ta det med seg i planleggingen av nye øvelser.

- Kommunen bør utarbeide og/eller ferdigstille opplæringsprogram i IT-sikkerhet for ansatte
- Kommunen bør benytte seg av muligheten for å gjennomføre kurs om generell informasjons- og datasikkerhet i KS læring eller andre leverandører, og vurdere behovet for ytterligere kurs og opplæring for tidligere ansatte basert på erfaringene fra opplæringsprogrammet for nyansatte

Kommunedirektøren merker seg begge anbefalingen om opplæring i IT-sikkerhet og vil fortsette arbeidet med å utvikle opplæringsprogram innen IT-sikkerhet og personvern (GDPR). Kommunedirektøren følger anbefalingen om å gi bedre opplæring i IT-sikkerhet til ikke bare å omfatte nyansatte. Slike kurs og e-læringskurs er under utvikling og vil være obligatoriske for alle ansatte. Opplæring av ansatte er en nødvendig for å få til en god sikkerhetskultur.

- Kommunen bør, ved implementering av nytt avvik- og kvalitetssystem, gi tilstrekkelig opplæring i system og rutiner for avviksrapportering. En generell opplæring i hva som er avvik relatert til personvern og informasjonssikkerhet vil også være hensiktsmessig.

Prosessen med å anskaffe et nytte system er startet. Avviksregistrering og kvalitetssystem er sentrale komponenter i kommunens internkontroll, og er nødvendig i arbeidet med å bedre IT-sikkerheten. Ved innføring av et nytt avvik- og kvalitetssystem vil opplæring bli vektlagt. Det er viktig at alle ansatte er bevisst funksjonen til, og formålet med et avvikssystem, herunder avvik relatert til personvern og informasjonssikkerhet.

- Haugesund kommune bør tydeliggjøre når IKT-enheten skal inngå ved anskaffelser av nye systemer, og kommunisere dette ut til de ulike tjenesteområdene

Kommunedirektøren ser at organisasjonen må bli mer oppmerksom på når IKT-enheten skal inngå ved anskaffelser, og slik sørge for at sikkerheten i leveranser av IT-systemer o.l. blir ivaretatt. Kommunedirektøren vil presisere og oppdatere kommunens innkjøpsreglement og rutiner på dette området.

Med hilsen

Ole Bernt Thorbjørnsen
Kommunedirektør

Dokumentet er godkjent elektronisk

Vedlegg 1 Dokumentliste

Rutiner og styrende dokumenter

[redacted]

- ✓ Personvernerklæring Haugesund kommune
- ✓ Rutiner for innsyn i personopplysninger
- ✓ Rutine for taushetsplikt
- ✓ Rutine for å melde avvik innen informasjonssikkerhet og personvern

[redacted]

- ✓ Rutine for innsyn etter offentleglova
- ✓ IKT rutiner i forbindelse med nyansettelser (NAV)
- ✓ IKT rutiner i forbindelse med permisjon i ansettelsesforhold (NAV)
- ✓ Sjekkliste for nyansatte
- ✓ Rutine for redigering og sletting av helseopplysninger
- ✓ Rutine for oppsigelse fra arbeidstaker
- ✓ Informasjon om brukerskjema – retningslinjer for ny bruker, endring av bruker og sletting av bruker
- ✓ Anskaffelsesrutine
- ✓ Økonomireglementet

[redacted]

Planer, analyser og protokoller

[redacted]

- ✓ DPIA DigiHelse
- ✓ Protokoll over behandling av personopplysninger 2018
- ✓ Eksempel på innkjøpsavtale
- ✓ Analyseskjema – helhetlig risiko- og sårbarhetsanalyse

Kurs og opplæring

- ✓ Informasjon og kursinnhold GDPR

Rapporter

- ✓ Årsrapport personvern 2020
- ✓ Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon 6.0
- ✓ Oversikt meldte avvik GDPR 2019-2021

Databehandleravtaler

- ✓ Mal for databehandleravtale
- ✓ Databehandleravtale ACOS
- ✓ Databehandleravtale Fit Outcomes
- ✓ Databehandleravtale Lindorff
- ✓ Databehandleravtale NAV
- ✓ Databehandleravtale Sem og Stenersen Prokom AS – Bookup
- ✓ Databehandleravtale Skolelab
- ✓ Databehandleravtale Trygg Trafikk Nettskolen

Annet

Vedlegg 2 Revisjonskriterier

Lov om kommuner og fylkeskommuner (kommuneloven)

Loven gjelder virksomheten i kommunene, og legger grunnlaget for hvilke plikter, myndighet og muligheter kommunene har i utøvelse av virksomheten.

Eforvaltningsforskriften

Forskriftens formål er blant annet å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Gjennom forskriften reguleres flere aspekter som er relevant for informasjonssikkerhet i kommunal forvaltning. Etter §15, *Internkontroll på informasjonssikkerhetsområdet,* skal 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.

Lov om behandling av personopplysninger (Personopplysningsloven)

Ny lov om behandling av personopplysninger trådte i kraft 20.juli 2018 og gjorde EUs personvernforordning (GDPR) til norsk lov. Regelverket stiller strenge krav til alle private og offentlige virksomheter ved behandling av personopplysninger, herunder også kommunene. Formålet med forordningen er blant annet å sikre vern av fysiske personer i forbindelse med behandlinger av personopplysninger. Med behandling siktes det til enhver bruk av personopplysninger, inkludert elektronisk databehandling og ikke-elektronisk behandling hvor personopplysningene skal inngå eller inngår i et register.

NSMs grunnprinsipper

Nasjonal sikkerhetsmyndighet (NSM) har utviklet et sett med grunnleggende prinsipper for IKT-sikkerhet med formål om å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. De er et utvalg av de prinsippene og tiltakene som NSM mener er mest relevante for norske virksomheter. Utvelgelsen er gjort i samarbeid med norske offentlige og private virksomheter. Ved å implementere de anbefalte tiltakene vil virksomheter etablere et godt forsvar mot cybertrusler, men det er ingen garanti for at de ikke blir rammet.

Selv om NSM anbefaler alle virksomheter å følge prinsippene betyr ikke det at virksomheten oppfyller sikkerhetsloven ved å følge dem. Men grunnprinsippene kan være en nyttig, første byggestein for IKT-systemer som er eller kan bli underlagt sikkerhetsloven.

Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (Sivilbeskyttelsesloven)

Lovens formål er å beskytte liv, helse, miljø, materielle verdier og kritisk infrastruktur ved bruk av ikke-militær makt når riket er i krig, når krig truer, når rikets selvstendighet er i fare, og ved uønskede hendelser i fredstid.

Etter §14 *Kommunal beredskapsplikt – risiko- og sårbarhetsanalyse,* plikter kommunen å kartlegge hvilke uønskede hendelser som kan inntreffe i kommunen, vurdere sannsynligheten for at disse hendelsene inntreffer og hvordan de i så fall kan påvirke kunnen. Resultatene fra arbeidet skal vurderes og sammenstilles i en helhetlig risiko- og sårbarhetsanalyse. Videre sier §15, *Kommunal beredskapsplikt – beredskapsplan for kommunen*, at det med utgangspunkt i risiko- og sårbarhetsanalyse skal kommunen utarbeide en beredskapsplan som skal inneholde en oversikt over hvilke tiltak kommunen har forberedt for å håndtere uønskede hendelser. Beredskapsplanen skal

minimum inneholde en plan for kommunens kriseledelse, varslingslister, ressursoversikt, evakueringsplan og plan for informasjon til befolkningen og media.

Forskrift om kommunal beredskapsplikt

Forskriftens formål er å sikre at kommunen ivaretar befolkningens sikkerhet og trygghet. Kommunen skal jobbe systematisk og helhetlig med samfunnssikkerhetsarbeidet på tvers av sektorer i kommunen, med sikte på å redusere risiko for tap av liv eller skade på helse, miljø og materielle verdier. Plikten omfatter kommunen som myndighet innenfor sitt geografiske område, som virksomhet og som pådriver overfor andre aktører

Kommuner er pålagt gjennom krav i sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt, å utarbeide en beredskapsplan basert på den helhetlige risiko- og sårbarhetsanalysen. Kommunens beredskapsplan skal integrere øvrige beredskapsplaner i kommunen. Selv om det stilles få eksplisitte krav til IKT sikkerhet for kommunene i forskrift om kommunal beredskapsplikt ligger slike krav implisitt til forskriften ved at kommunens ROS-analyse (som beredskapsplanen skal utarbeides på bakgrunn av) skal omfatte særlige utfordringer knyttet til kritiske samfunnsfunksjoner og tap av kritisk infrastruktur, samt kommunens evne til å opprettholde sin virksomhet når den utsettes for en uønsket hendelse. Som nasjonalt fagmiljø for IKT-sikkerhet har Av prinsipp 4.1 fremkommer det at virksomheter bør forberede seg på å håndtere hendelser, slik at uønskede hendelser kan oppdages raskt, kontrolles, skaden minimeres og hendelsesårsaken fjernes effektivt. Dette inkluderer gjenopprettelse av integriteten til systemer og nettverk.

NOU 2018: 14 IKT-sikkerhet i alle ledd

Utredningen beskriver utfordringer knyttet til IKT-sikkerhet i samfunnet. Vurderingene i utredningen er benyttet som bakgrunnsmateriale i forbindelse med forvaltningsrevisjonen.

Digitaliseringsdirektoratet sin veileder i planlegging og gjennomføring av IKT-øvelser

Veilederen tar for seg hvordan man kan planlegge og gjennomføre øvelser med tema informasjonssikkerhet. Den beskriver formål med øvelser, ulike øvelsesformer, valg av scenario, øvelsesdirektor, dreiebok, gjennomføring av øvelsen, evaluering av øvelsen og kobling til ledelsessystem. Veilederen er benyttet som bakgrunnsmateriale i forvaltningsrevisjonen.

Digitaliseringsdirektoratets veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet

Veilederen omhandler arbeid med utvikling av kompetanse og kultur knyttet til digital sikkerhet. Av veilederen kommer det frem at formålet med opplæringsprogram er å bidra til at ansatte får nødvendig opplæring for å kunne utføre sine daglige oppgaver på en sikker måte, og som bidrar til at sikkerhetskulturen utvikler seg i ønsket retning.