FOLLO DISTRIKTSREVISJON IKS Org.nr. 914 022 134 MVA

DELTAKERKOMMUNER: ENEBAKK – FROGN – NESODDEN – OPPEGÅRD – SKI – ÅS

IKT OG BEREDSKAP

Forvaltningsrevisjonsrapport for Oppegård kommune

Foto: Computerworld.

Ski, 2.2.2016

Parkaksen 6, Postboks 3010, 1402 Ski, tlf. 6487 8760, www.follodr.no, revisjonen@follodr.no

Innhold

1 INNLEDNING

1.1 Bakgrunn

Forvaltningsrevisjon er en lovpålagt oppgave for kommunene etter Lov om kommuner og fylkeskommuner av 25.9.1992 med endringer av 12.12.2003 (kommuneloven). Formålet med forvaltningsrevisjon er nedfelt i kommunelovens § 77 nr. 4: "Kontrollutvalget skal påse at kommunens eller fylkeskommunens regnskaper blir revidert på en betryggende måte. Kontrollutvalget skal videre påse at det føres kontroll med at den økonomiske forvaltningen foregår i samsvar med gjeldende bestemmelser og vedtak, og at det blir gjennomført systematisk vurdering av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak og forutsetninger (forvaltningsrevisjon)."

Kontrollutvalget i Oppegård kommune vedtok prosjektplan med formål og problemstillinger for prosjekt *IKT og beredskap* i møte 26.3.2015 (sak 11/15).

1.2 Sammendrag

I denne forvaltningsrevisjonen har vi undersøkt informasjonssikkerhet, IKT-drift og beredskap. *Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune* samsvarer med personopplysningsforskriftens krav til konfidensialitet, integritet og tilgjengelighet. Med noen unntak følger kommunen sine rutinebeskrivelser i praksis. Mål og retningslinjer er utarbeidet, og det er en klar arbeidsdeling i kommunens IKT-arbeid.

1.3 Konklusjoner

Follo distriktsrevisjon IKS konkluderer slik på problemstillingene:

1.3.1 Informasjonssikkerhet

Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune (2007, oppdatert 2015) fastsetter rutiner for å håndtere personopplysningenes konfidensialitet, integritet og tilgjengelighet. Risikovurdering av fagsystemet Gerica for pleie og omsorg er gjennomført, men ikke for andre fagsystemer som behandler personopplysninger. Både personopplysningsforskriften og kommunens sikkerhetshåndbok stiller krav om jevnlig sikkerhetsrevisjon (om lag årlig), men dette er ikke gjennomført.

Avvik vedrørende personopplysninger er ikke meldt til kommunens sikkerhetsansvarlig. Kommunen bør høyne ansattes bevissthet om å melde avvik i samsvar med kommunens rutinebeskrivelse. Kommunen har rutiner for å håndtere og administrere passord og tilgang til IKT-systemene. Kommunens serverrom synes å være tilfredsstillende sikret.

1.3.1 IKT-drift

Oppegård kommune har utarbeidet mål og strategier for sitt IKT-arbeid. *IKT-strategi for Oppegård kommune* (2014) og *Forslag til IKT-Governance i Oppegård kommune* (2015) beskriver rollene som premissgiver, bestiller og leverandør – med tydelig arbeidsdeling. Hvordan man skal gjenoppta normal IKT-drift etter en driftsstans, er beskrevet av tidligere IKT-sjef, men en rutinebeskrivelse foreligger ikke. Kommunens systemer har god kompatibilitet (samspill), etter det revisor erfarer.

1.3.1 Beredskap

Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune bestemmer at beredskapsplaner for IKT skal utarbeides. Dette er ikke gjort; kommunens beredskapsplaner omtaler ikke IKT-beredskap.

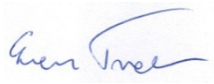
Oppegård kommune gjennomfører generell beredskapsøvelse i kriseledelse om lag annethvert år. De siste fire årene har dette vært papirøvelser, som har blitt evaluert. Bortfall av IKT har ikke inngått i øvelsene.

1.4 Anbefalinger

Follo distriktsrevisjon IKS anbefaler Oppegård kommune å vurdere følgende tiltak:

a. Gjennomføre risikovurdering av alle systemer som håndterer personopplysninger.
b. Gjennomføre sikkerhetsrevisjoner og egenkontroller om lag årlig.
c. Øke ansattes bevissthet om å melde avvik.
d. Utarbeide rutinebeskrivelse for å gjenoppta normal IKT-drift etter en drifsstans.
e. Oppdatere rutinebeskrivelse for backup.
f. Omtale IKT-beredskap i kommunens beredskapsplaner på overordnet nivå og for virksomhetene.
g. Utarbeide rutine for innsending av melding til Datatilsynet om sensitive data.

Steinar Neby
revisjonssjef



Even Tveter
prosjektleder

2 PROSJEKTBESKRIVELSE

2.1 Formål og problemstillinger

Kontrollutvalgets bestilling angir følgende *formål* med forvaltningsrevisjonsprosjektet: "Prosjektet skal kartlegge og vurdere kommunens IKT-drift sentralt og i virksomhetene med fokus på sikkerhet og beredskap".

Kontrollutvalgets bestilling inneholder følgende *problemstillinger*:
"Informasjonssikkerhet

- Har kommunen og virksomhetene tilfredsstillende rutiner for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?
- Hvordan ivaretas sikkerhetsbestemmelsene i personopplysningsforskriften?

IT-drift

- Har kommunen oppdatert mål, retningslinjer og rutiner for IKT-arbeidet?
- Foretas sikkerhetsrevisjon?
- Er det tilfredsstillende arbeidsdeling vedr IKT?
- Har kommunen rutiner for å gjenoppta normal drift etter driftsstans?
- Er kompatibiliteten mellom ulike datasystem i kommunen tilfredsstillende?

Beredskap

- Har kommunen en beredskapsplan for IKT og er denne samordnet med planene i andre deler av kommunen?
- Hvordan er IKT-sikkerheten ivaretatt i virksomhetenes beredskapsplaner?
- I hvilken grad gjennomføres beredskapsøvelser og evaluering av disse?"

2.2 Presiseringer og avgrensninger

Revisor betrakter dette som tre problemstillinger med underproblemstillinger. Følgende bemerkes til de tre problemstillingene:

1. *Informasjonssikkerhet*: De to underproblemstillingene omhandler etter revisors oppfatning samme tema; de er derfor slått sammen. Vi gjennomgår personopplysningsforskriftens viktigste paragrafer. For å vurdere Oppegård kommunes informasjonssikkerhet i praksis, har revisor gjennomgått bruken av fagsystemene Gerica (pleie og omsorg) og SATS (skole).
2. *IKT-drift*: Kulepunktet om sikkerhetsrevisjon omtales under informasjonssikkerhet. Problemstilling nr. 2 og nr. 3 overlapper noe; sikkerhetsrutiner omtales flere steder i rapporten.
3. *Beredskap*: IKT-beredskap berører kommunens overordnete beredskap (kriseledelse) og virksomhetenes beredskap.

Wikipedia opplyser: "Informasjons- og kommunikasjonsteknologi (IKT) er et begrep som omfatter teknologi for innsamling, lagring, behandling, overføring og presentasjon av informasjon. I praksis brukes ofte begrepene datateknikk og kommunikasjonsteknologi. IKT er også ofte omtalt som kun informasjonsteknologi (IT), og tidligere var begrepet elektronisk databehandling (EDB) utbredt."

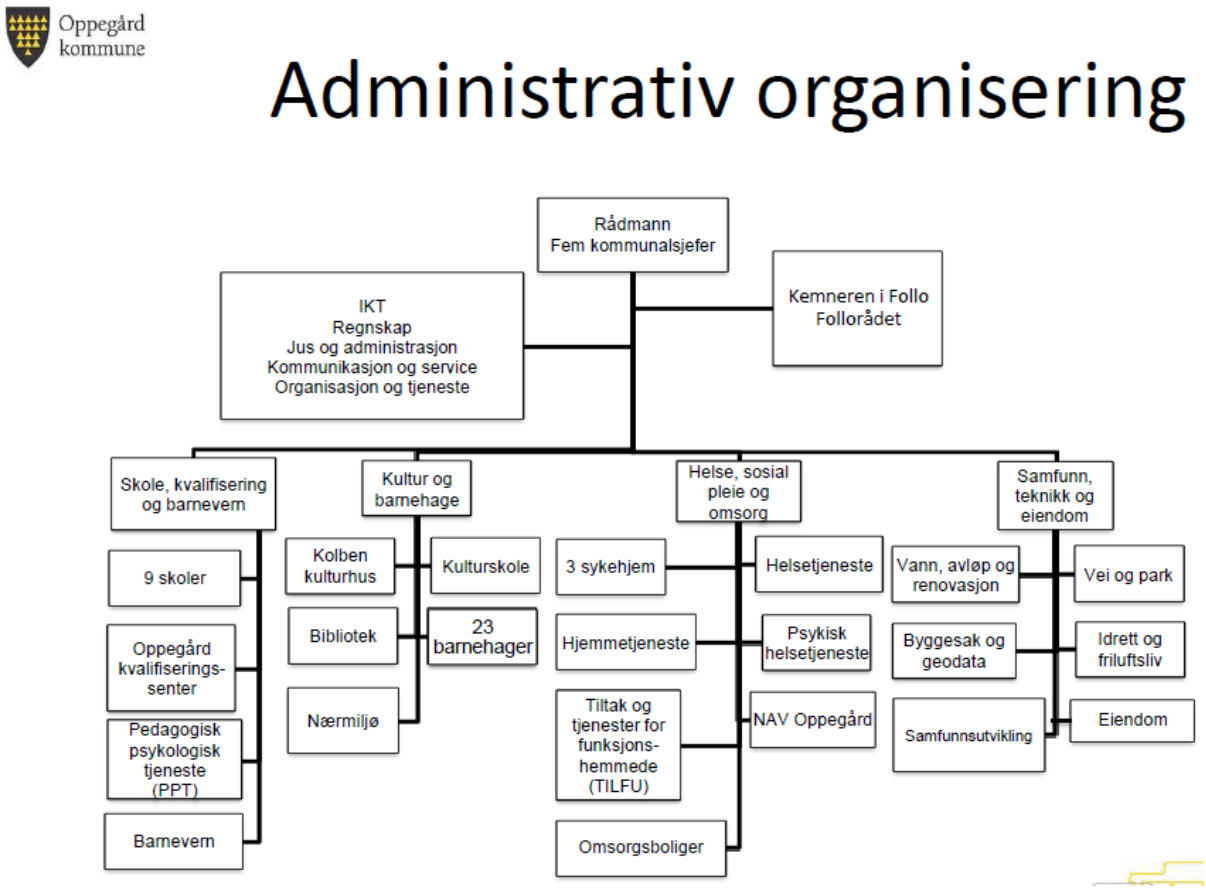
I tråd med kontrollutvalgets bestilling vil vi primært bruke "IKT" i denne rapport. (Referanser til engelsk-språklige kilder kan benytte "IT".) Uttrykket "system" vil ofte si datasystem/ informasjonssystem, det være seg fagsystem (f.eks. Gerica og SATS), operativsystem eller

annen programvare. "Applikasjon" vil si en spesifikk programvare.

2.3 Informasjon om revidert enhet – organisering

Oppegård hadde en befolkningsvekst på 325 innbyggere (+1,2 %) i 2014. Oppegård hadde 26.736 innbyggere 1.7.2015.

Oppegård kommune hadde driftsinntekter på til sammen 1,77 mrd. kr i regnskap 2014. Kommunens personell utfører til sammen 1650 årsverk. Administrativ organisering omfatter rådmann, fem kommunalsjefer og ca. 60 virksomheter:[1]



Revisjonsrapporten benytter uttrykket "skole" som kortform for ni grunnskoler og "pleie og omsorg" for tre sykehjem og Hjemmetjeneste.

2.4 Metode

2.4.1 Metode generelt

Med hjemmel i Kommunelovens § 77 nr. 4 foreligger *Forskrift om revisjon i kommuner og fylkeskommuner mv* (2004), som i § 7 pålegger at forvaltningsrevisjon gjennomføres og rapporteres i henhold til god kommunal revisjonsskikk og anerkjente standarder på området.

[1] Virksomhet er grunnleggende enhet – resultatenhet – i Oppegård kommunes organisasjon. Virksomheters navn skrives med stor forbokstav i denne rapport. Under virksomhet finnes seksjoner.

Styret i Norges Kommunerevisorforbund (NKRF) har fastsatt *Standard for forvaltningsrevisjon* (2011), som er god kommunal revisjonsskikk i forvaltningsrevisjon. Follo distriktsrevisjon IKS følger denne standarden. Noen utdrag fra *Standard for forvaltningsrevisjon*:

4. *Revisjonskriterier* (pkt. 22, 23 og 25): "Revisjonskriterier er de krav, normer og/eller standarder som forvaltningsrevisjonsobjektet skal revideres/vurderes i forhold til. Revisjonskriteriene skal være begrunnet i, og utledet av, autoritative kilder innenfor det reviderte området."
5. *Data/fakta* (pkt. 27): "I valg av metode må revisor sikre dataenes relevans (gyldighet, validitet) i forhold til problemstillingen(e). Datainnsamlingen må gjennomføres på en måte som sikrer dataenes pålitelighet (reliabilitet)."
6. *Vurderinger* (pkt. 31): "Revisor må analysere de innsamlede dataene i forhold til revisjonskriteriene og vurdere om praksis eller tilstand er i tråd med kriteriene."
7. *Konklusjoner* (pkt. 33): "På bakgrunn av vurderinger av dataene opp mot kriteriene skal revisor konkludere i forhold til problemstillingen(e). Dersom revisor finner vesentlige avvik, skal dette komme tydelig til uttrykk i forvaltningsrevisjonsrapporten."
8. *Anbefalinger* (pkt. 34): "Der det er hensiktsmessig bør revisor gi anbefalinger. Anbefalinger må aldri formuleres som pålegg til administrasjonen. Revisor skal også være varsom med å foreslå detaljerte løsninger."
9. *Verifisering og høring/kontradiksjon* (pkt. 45 og 16): "Utføring av forvaltningsrevisjon skal kvalitetssikres." Et rapportutkast sendes til kommunens kontaktperson for prosjektet for verifisering av fakta. Endelig rapport sendes administrasjonssjefen (rådmannen), som "skal gis anledning til å gi uttrykk for sitt syn på de forhold som framgår av rapporten. Høringssvaret skal vedlegges rapporten som går til behandling i kontrollutvalget."

2.4.2 Metode i dette prosjektet

Metoden i forvaltningsrevisjonsprosjektet er i hovedsak intervju og dokumentanalyse. Rådmannen utpekte sikkerhetsansvarlig Espen Hallan til kontaktperson i prosjektet. Revisor har gjennomført bl.a. følgende intervjuer/møter:

- Oppstartsmøte ble avholdt 3.9.2015 med sikkerhetsansvarlig og kommunalsjef stabsfunksjoner Lars Bøhler. Kommunalsjefen er fra høsten 2015 også IKT-sjef.
- Intervju med tidligere IKT-sjef, som høsten 2015 gikk over i annen stilling i Oppegård kommune.
- Intervju med kommunalsjef Helse, sosial, pleie og omsorg, koordinator Hjemmetjeneste og en ansatt som er superbruker (ekspert) på fagsystemet Gerica.
- Intervju med kommunalsjef Skole, kvalifisering og barnevern, administrator for fagsystemet SATS og to ansatte som er superbrukere på fagsystemet.

I dokumentanalysen har revisor gjennomgått *Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune* (2015) og *IKT-strategi for Oppegård kommune* (2014), samt andre dokumenter fremlagt av kommunen (se litteraturliste).

En rød tråd i revisjonsrapporten – fra problemstillinger gjennom fakta til vurderinger og konklusjoner – gir *relevant* informasjon. *Pålitelig* informasjon sikres ved faktainnsamling fra en rekke kilder (metodetriangulering), informanters sjekk av tekstelementer, kommunens verifisering av rapportutkast, samt kvalitetssikring internt i Follo distriktsrevisjon IKS.

Revisjonen takker for godt samarbeid med Oppegård kommune i prosjektet. Rådmannens uttalelse til forvaltningsrevisjonsrapporten er vedlagt.

3 INFORMASJONSSIKKERHET

Problemstilling nr. 1: Informasjonssikkerhet
- Har kommunen og virksomhetene tilfredsstillende rutiner for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?
- Hvordan ivaretas sikkerhetsbestemmelsene i personopplysningsforskriften?

3.1 Revisjonskriterier

Personopplysningslovens § 13 bestemmer at "den behandlingsansvarlige databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger".

Datatilsynets veileder *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer* definerer at begrepet informasjonssikkerhet omfatter sikring av:
- *Konfidensialitet*: beskyttelse mot at uvedkommende får innsyn i opplysningene.
- *Integritet*: beskyttelse mot utilsiktet endring av opplysningene.
- *Tilgjengelighet*: å sørge for at tilstrekkelige og relevante opplysninger er til stede.

Tilfredsstillende informasjonssikkerhet oppnås gjennom systematiske tiltak for kvalitetsstyring og internkontroll i sikkerhetsarbeidet.

Personopplysningsforskriften fastsetter krav til kommunenes informasjonssikkerhet:
- § 2-3 stiller krav om at det skal etableres en sikkerhetsledelse. Videre skal virksomheten etablere sikkerhetsmål og sikkerhetsstrategi der formålet, overordnede føringer, valg og prioriteringer framkommer. Ledelsen skal jevnlig gjennomgå sikkerhetsmål og strategi.
- § 2-4 stiller krav om at det skal føres en oversikt over hvilke personopplysninger som behandles. Sannsynlighet for og konsekvenser av sikkerhetsbrudd skal kartlegges (risikovurdering).
- § 2-5 stiller krav om at det jevnlig gjennomføres sikkerhetsrevisjon. Resultatet av sikkerhetsrevisjonen skal dokumenteres.
- § 2-6 stiller krav om at bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.
- § 2-7 stiller krav om at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.
- § 2-10 stiller krav om fysisk sikring mot uautorisert tilgang til utstyr som brukes for å behandle personopplysninger.
- § 2-11 sier at det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er viktig.
- § 2-12 sier at det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgang er nødvendig.
- § 2-13 sier at det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig.

Datatilsynets kommentar til sikkerhetsbestemmelsene poengterer at ansvar og myndighet

relatert til drift av informasjonssystemet (driftsledelse) og oppfølging av sikkerhetsarbeidet (sikkerhetsledelse) bør klarlegges. Disse *utøvende* og *kontrollerende* funksjonene bør ideelt sett tillegges forskjellige medarbeidere i virksomheten. Sikkerhetsleders arbeidsoppgaver omfatter forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner, kontroll med risikovurdering og avviksbehandling. Datatilsynet anbefaler i *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer* (2000) at sikkerhetsrevisjon foretas om lag årlig.

Revisjonskriterier:

- Kommunen skal ha etablert en sikkerhetsledelse som jevnlig gjennomgår sikkerhetsmål og strategi.
- Kommunen skal ha en klar organisering med etablerte ansvars- og myndighetsforhold.
- Kommunen skal ha oversikt over sine personregistre og gjennomføre risikovurdering av dem.
- Kommunen skal jevnlig – om lag årlig – gjennomføre sikkerhetsrevisjon.
- Kommunen skal ha et avvikssystem for å håndtere sikkerhetsbrudd.
- Kommunen skal ha gjennomført tiltak som:
    - Ivaretar fysisk sikring av IKT-utstyr.
    - Hindrer uautorisert innsyn i personopplysninger.
    - Sikrer tilgang til personopplysninger.
    - Hindrer uautorisert endring av personopplysninger.

3.2 Fakta

3.2.1 Sikkerhetsledelse, sikkerhetsmål og sikkerhetsstrategi

Oppegård kommune utarbeidet i 2007 *Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune*, som ble oppdatert i august 2015. Sikkerhetshåndboken fastsetter at systemet skal evalueres fortløpende og revideres når endrede forhold gjør det naturlig eller nødvendig. Sikkerhetshåndboken (med vedlegg) skal gjennomgås og oppdateres årlig.

"Kommunens målsetting er å yte innbyggerne tjenester med høy kvalitet og samtidig utnytte kommunens ressurser optimalt. Bruk av moderne informasjonsteknologi gjør det mulig å løse kommunens oppgaver best mulig. Samtidig vil bruk av slik teknologi introdusere trusler overfor de opplysninger som behandles. Kommunens overordnede mål med elektronisk behandling av bl.a. personopplysninger er derfor sikker og effektiv saksbehandling.

Kommunen skal ha et bevisst forhold til de risikoer som gjelder ved elektronisk behandling av personopplysninger. Sikkerhetstiltak skal baseres på etablerte og velprøvde løsninger som gir god margin i forhold til sikkerhetsbehovet. Ved behandling av sensitive personopplysninger skal *krav til konfidensialitet ikke vike til fordel for krav til tilgjengelighet.*" (Sikkerhetshåndboken, side 12.)

Kommunens sikkerhetshåndbok bestemmer videre at personopplysninger skal sikres hva gjelder:

- konfidensialitet, slik at opplysningene ikke blir kjent for uvedkommende.
- tilgjengelighet, slik at alle medarbeidere med tjenestlig behov kan utføre pålagte oppgaver, og brukerne av kommunens tjenester gis god informasjon.
- integritet, slik at opplysningene ikke endres utilsiktet ved databehandling.

Utstyr og programvare skal være sikret slik at data ikke kan stjeles eller settes i fare. Uautorisert tilgang skal forhindres med beskyttelsestiltak. Oppegård kommune skal ha tilfredsstillende rutiner og systemer for å ivareta sikkerheten. Systemene skal være tilgjengelig for de personene som har behov og tilgang til dem. Påliteligheten skal være sikker. Det skal være et klart skille mellom åpen og sensitiv informasjon. Alle medarbeidere skal ha tilstrekkelig kunnskap om de systemer de arbeider med.

Sikkerhetshåndboken beskriver følgende organisatoriske nivåer for informasjonssikkerheten (top – down):

- Rådmannen v/kommunalsjef for organisasjonsutvikling.
- Systemeiere (f.eks. kommunalsjef Helse, sosial, pleie og omsorg for Gerica).
- Seksjonsleder IKT.
- Systemadministratorer.
- Øvrige ansatte.

Rådmannen og ledergruppen er øverste administrative organ for informasjonssikkerheten. Deres oppgaver er:

a. Gjennomgang og godkjenning av retningslinjer for informasjonssikkerhet og generelle ansvarsforhold.
b. Overvåking av vesentlige endringer i trusler mot kommunens informasjonsaktiva.
c. Gjennomgang og overvåkning av informasjonssikkerhetshendelser.
d. Godkjenning av større initiativ for å styrke informasjonssikkerheten.

Rådmannen har det overordnete ansvar for sikkerhet i kommunen, herunder eierskap til kommunens IKT-sikkerhetsmål og IKT-sikkerhetspolicy. Rådmannen er ansvarlig for at styringsdokumenter på området er oppdatert og gjenspeiler kommunens sikkerhetspolitikk.

Arbeidet med informasjonssikkerhet inngår som en integrert del av de oppgaver som påhviler kommunens virksomheter og underliggende seksjoner. Lederne på de ulike nivåer skal påse at personopplysninger behandles med tilfredsstillende informasjonssikkerhet.

Systemeier er ansvarlig for at sikkerhetsbestemmelsene i personopplysningslovens § 13 og personopplysningsforskriftens kapittel 2 etterleves. Ansvaret innbefatter at det årlig avsettes tilstrekkelige ressurser, både personalmessig og økonomisk, slik at tilfredsstillende informasjonssikkerhet opprettholdes. Systemeier må etablere klare ansvars- og myndighetsforhold, slik at hvem som har fått delegert hvilke oppgaver er klart.

Det daglige sikkerhetsansvaret er delegert til en dedikert stilling – sikkerhetsansvarlig (50 % stilling) i stabsområdet organisasjon og tjeneste, som rapporterer direkte til rådmannen. Stillingen har følgende arbeidsoppgaver:

- Sikre egen kompetanse og kompetansen til medarbeidere i kommunen med sikkerhetsrelaterte oppgaver.
- Sikre at sikkerhetsbevisstheten blant kommunens ansatte er tilstrekkelig; iverksette tiltak for å oppnå og vedlikeholde sikkerhetsbevissthet.
- Være samlingspunkt for alle sikkerhetsbrudd som rapporteres/oppdages i kommunen; ha ansvar for å melde til Datatilsynet de sikkerhetsbrudd som kan ha innvirkning på kommunens konsesjoner/dispensasjoner etter personopplysningsloven.
- Utarbeide og vedlikeholde kommunens sikkerhetsrutiner. Utforming av disse kan delegeres til operativt sikkerhetspersonell.

- Utarbeide planer for egenkontroll av kommunens sikkerhet.
- Gjennomføre planlagte egenkontroller.
- Overordnet daglig ansvar for dokumentsikkerhet i kommunen.
- Beredskapsplaner - utarbeidet i samarbeid med bl.a. seksjonsleder IKT.
- Katastrofeplaner - utarbeidet i samarbeid med bl.a. seksjonsleder IKT.

Sikkerhetsansvarlig opplyser at overvåking av "trusselbildet" utføres av ham og to ansatte i IKT-seksjonen. Kommunens sikkerhetshåndbok dokumenterer at risikovurderinger gjennomføres. Sikkerhetshåndboken er tilgjengelig på kommunens intranett. Begge kommunalsjefer som revisor har intervjuet, opplyser at de er godt kjent med sikkerhetshåndboken.

Personopplysningsloven bestemmer at virksomhetsleder (eller seksjonsleder under ham) er behandlingsansvarlig. Oppegård kommune tillegger derfor virksomhetslederne det operative ansvaret for kontroll av personopplysninger, noe som presiseres i deres stillingsbeskrivelser. Sikkerhetsansvarlig opplyser at det gjennomføres lite kontroll ovenfra.

3.2.2 Personopplysninger, risikovurdering

IKT-seksjonen fører oversikt over alle kommunens datasystemer som behandler personopplysninger. For pleie- og omsorgssystemet *Gerica* ble risikoanalyse gjennomført 16.11.2015. Fem risikoområder med hendelser beskrives. Hendelsene er vurdert for konsekvens og sannsynlighet på en skala fra 1–5. Konsekvensreduserende tiltak for alle hendelser opplistes.

Kommunalsjef Skole, kvalifisering og barnevern opplyser til revisor at risikoanalyse av systemene som håndterer personopplysninger i skolene, ikke er utført.

Utskrift av sensitive data skal foretas til printere (skrivere) som ikke er alminnelig tilgjengelige. Den enkelte systemeier er ansvarlig for at det avsettes egnede lokaler og utstyr for dette formål. Personale skal være kjent med hvor de skal adressere sine utskrifter.

Meldinger og søknader om håndtering av personopplysninger sendes til Datatilsynet av sikkerhetsansvarlig. Revisors søk i Datatilsynets register viser at Oppegård kommune har innsendt 42 meldinger om oppbevaring av personopplysninger. En skriftlig rutine for dette er ikke fastsatt. Representanter for skole og pleie/omsorg er ikke kjent med hvordan dette gjøres, men forutsetter at meldinger sendes Datatilsynet når det er påkrevd.

3.2.3 Organisering

Sikkerhetshåndboken beskriver ansvarsforhold i kommunen når det gjelder håndtering av personopplysninger (se også kapittel 3.2.1 over). Både representantene fra skole og pleie/omsorg gir uttrykk for at ansvarsforhold og roller er avklart og fornuftige.

I sitt ansettelsesforhold er alle medarbeidere underlagt taushetsplikt i henhold til lov og bestemmelser for fagområdet, samt når det følger av sakens art, jfr. forvaltningsloven og personopplysningsloven. Alle medarbeidere som i sitt arbeid har tilgang til sensitive opplysninger eller informasjon om sikring av slike opplysninger, skal undertegne taushetserklæring, jfr. Oppegård kommunes personalhåndbok. Virksomhetsleder har ansvar for at medarbeiderne informeres om taushetspliktens omfang og varighet, samt om konsekvensene dersom den brytes. Representanter for skole og pleie/omsorg opplyser at taushetserklæring undertegnes av medarbeiderne.

Gjennom et obligatorisk opplæringstilbud gjøres de ansatte kjent med innholdet i sikkerhetshåndboken og hvor den ligger tilgjengelig på intranettet. Opplæring i fagsystemer gis.

Alle sensitive opplysninger som kommunen behandler, ligger på "sikker sone" på kommunens servere. Denne er adskilt fra resten av kommunens nettverk og krever ekstra innlogging

3.2.4 Sikkerhetsrevisjon

Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune pålegger at informasjonssystemenes sikkerhet revideres årlig (12 måneders intervall). Virksomhetslederne skal kontrollere at deres fagsystemer etterlever sikkerhetsstandarder. Gjennomgangen bør dekke følgende sider ved informasjonssystemet:

- Ansvars- og myndighetsforhold.
- Utførelse av arbeidsoppgaver i tilknytting til informasjonssystemet.
- Sikkerhetstiltak, herunder utprøving av tekniske sikkerhetsløsninger og gjennomgang av avvik registrert siden forrige kontroll.
- Risikoanalyse.

Alle ledere i kommunen har ansvar for sikkerhetsrevisjon innenfor sitt ansvarsområde. Den som leder kontrollen, bør ikke selv ha ansvar for den del av virksomheten som kontrolleres. Sikkerhetsrevisjoner kan ledes av sikkerhetsansvarlig. Resultat fra sikkerhetsrevisjon rapporteres til kommunens ledelse. Eventuelle avvik avdekket i sikkerhetsrevisjonen, behandles i samsvar med kommunens system for avvikshåndtering.

Sikkerhetsansvarlig opplyser at han de senere år ikke har gjennomført sikkerhetsrevisjon.

Helsedirektoratet har utgitt *Norm for informasjonssikkerhet* for behandling av personopplysninger. Normen er utarbeidet av organisasjoner i helsesektoren, for å fremme informasjonssikkerhet i den enkelte virksomhet og å bidra til tillit til sektorens behandling av helserelaterte personopplysninger.

Faktaark 6b Sikkerhetsrevisjon sjekkliste for å ivareta kravene i normen, inneholder 208 krav som kommunen må ta stilling til og svare på om de oppfyller. Oppegård kommune har fylt ut sjekklisten og svart ja på alle kravene.

3.2.5 Avvik

Sikkerhåndboken beskriver Oppegård kommunes sikkerhetsarkitektur, som følger Datatilsynets retningslinjer. Sikker sone, der sensitive opplysninger behandles, beskrives i forhold til intern sone og eksternt nettverk. Sikkerhetsbarrierene skal generere alarmer når kritiske hendelser som indikerer mulige sikkerhetsbrudd inntreffer. Alle avvik skal registreres i systemenes hendelseslogg.

Alle sikkerhetsbrudd og sikkerhetsmessige svakheter skal rapporteres til sikkerhetsansvarlig. Skjema i sikkerhetshåndbokens vedlegg I skal benyttes. Sikkerhetsansvarlig skal føre logg over rapporterte hendelser. Han opplyser at avvik ikke er rapport til ham de siste åtte årene, men han utelukker ikke at avvik kan ha skjedd. Mindre brudd håndteres som regel av virksomheten selv eller i kontakt med IKT-seksjonens helpdesk. All aktivitet i Gerica logges; hvem som har vært inne på systemet kan spores.

3.2.6 Fysisk sikring

Sikkerhetshåndboken sier at lokaler og utstyr skal være forsvarlig sikret, med spesiell vekt på rom med utstyr for behandling og lagring av personopplysninger, herunder servere, kommunikasjons- og nettverksenheter. Sikkerhetshåndboken angir hvilke områder som behandler sensitiv informasjon og derfor er definert som fysiske sikkerhetssoner. Kommunens sentrale dataanlegg skal ha adgangskontroll gjennom eget låssystem.

Serverrommet til Oppegård kommune er fysisk sikret ved at man bare kommer seg inn med personlige koder. Uvedkommende har således ikke adgang. Serverrommet har to kjøleanlegg, som bidrar til stabile servere, og automatisk brannslukking. Alle servere har reserveforsyning av strøm fra UPS (batteripakke) og strømaggregat. Dersom ordinær strømforsyning faller ut, starter først UPS og deretter aggregat.

Dokumenter fra SATS skrives ut på printer med sikkerhetskode eller til printere som ikke er alminnelig tilgjengelige. Personalet er kjent med hvor de skal adressere sine utskrifter. På sykehjemmene er alle printere lokalisert inne på vaktrommet, slik at uvedkommende ikke har tilgang. Hjemmetjenestens lokaler er avlåst slik at uvedkommende ikke har tilgang til printere. Pleie og omsorg har rutiner for makulering av dokumenter som inneholder personopplysninger.

3.2.7 Uautorisert innsyn

Sikkerhetshåndboken beskriver hvordan man skal hindre uautorisert innsyn:

Tilgangskontroller
Rutine for autorisasjonstildeling omfatter:

- Autorisasjon av nytilsatte, vikarer og partnere i henhold til tjenestlige behov.
- Endring i autorisasjon ved forandring av oppgaver, herunder sletting av autorisasjon når en medarbeider får nye arbeidsoppgaver eller slutter i virksomheten.
- Kontroll med at tildelte autorisasjoner fungerer etter forutsetningene.

Sikkerhetshåndboken bestemmer at kommunens ansatte gis tilgang til saksområder (personopplysninger) bare i den grad det er nødvendig for å utføre pålagte arbeidsoppgaver.

Fagsystemene har egne passordsystemer som begrenser tilgang og rettigheter til ulike deler av systemet. Tilgang til øverste nivå gis av IKT-seksjonen, mens tilgangene til de ulike delene av fagsystemene administreres av en superbruker etter fullmakt fra systemeier/registeransvarlig. Sikkerhetshåndboken beskriver forholdsregler for bruk av passord på kommunens server. En ansatt/systembrukers rettigheter og tilganger vurderes når det skjer endringer i brukerens arbeidsoppgaver eller ved faglige behov.

Sensitive opplysninger
Informasjonssystemer som inneholder sensitive data, skal være sikret i henhold til Datatilsynets retningslinjer. Datasystemer som inneholder sensitiv informasjon, skal være uttrykkelig identifisert og dokumentert av systemeier/behandlingsansvarlig. Adskilte soner benyttes som et grunnleggende prinsipp i nettverkets sikkerhetsarkitektur.

For å begrense tilgangen til personopplysninger, benyttes Oppegård kommune følgende soner:

- *Sikker sone* behandler sensitive opplysninger. En sikker sone er atskilt fra resten av det interne nettverket, herunder andre sikre soner, samt mot eksterne nettverk.

- *Intern sone* behandler ikke sensitive personopplysninger, men andre opplysninger i virksomheten som ikke skal eksponeres eksternt.

Sikkerhetshåndboken beskriver hvordan sikret sone forholder seg til intern sone og eksternt nettverk. Sikkerhetsbarrierer skal utløse alarm når kritiske hendelser som indikerer sikkerhetsbrudd, inntreffer. Systemene skal ha hendelseslogg som registrerer alle avvik.

Systemendringer
Oppegård kommune benytter hovedsakelig standardsystemer fra leverandører av kommunale informasjonssystemer. For å unngå forringelse av lagret informasjon, skal det være streng kontroll med gjennomføring av endringer i systemene. Systemadministrator skal forvisse seg om at leverandørene har etablert formelle prosedyrer for endringskontroll. Prosedyrene skal sørge for at sikkerhet og kontrollprosedyrer ikke blir kompromittert (tilflyter uvedkommende); programmerere/konsulenter får bare tilgang til de delene av systemet som er nødvendig for arbeidet deres.

Med jevne mellomrom vil det være nødvendig å gjøre endringer i produksjonssystemene. Endringer skal gjennomføres på initiativ fra systemeier i samspill mellom IKT-seksjon, leverandør, behandlingsansvarlig og brukere. Ved oppgraderinger av operativsystem skal prosedyrer sikre at dette ikke får negative konsekvenser for informasjonssystemene.

Gerica
Gerica har "sikkerhetsprofiler" som bestemmer hvilke tilganger de ansatte får til systemet. "Roller" deler dette ytterligere opp. Virksomhetsleder bestemmer hvilken sikkerhetsprofil og rolle den ansatte skal ha. Systemansvarlig utfører tildeling av roller/tilgang. Tilgangsstyringen i Gerica er streng; det skal ikke gis flere tilganger enn nødvendig for å utføre arbeidet. Vikarer som får systemtilgang, gis tidsbegrenset tilgang med sluttdato angitt. Alle tilganger gjennomgås en gang i året.

Ved innsynsbegjæringer fra pårørende eller advokater blir som oftest stabsområde jus og administrasjon rådført. Kun journalansvarlig (virksomhetsleder el.l.) kan gi innsyn.

SATS
Fagsystemet SATS har få tilganger; det er bare rektor, inspektør og en saksbehandler på skolen som har tilgang til systemet. Det kan ikke logges på fra lærer-PC-er på skolen. Ved endring i tilganger sendes melding til IKT-seksjonen, som gir beskjed til systemadministrator i skoleadministrasjonen, som sørger for inn- eller utmelding av systemet. Hun opplyser til revisor at ordningen fungerer bra, og hun har god oversikt over det beskjedne antall brukere ved kommunens grunnskoler

Generell systemtilgang
Alle systembrukere i kommunen skal angis med personens navn; tilgang for "vikar" o.l. brukes ikke lengre. Ved *resett* av passord sendes automatisk melding til brukerens mobiltelefon.

Opplæring
Oppegård kommune gjennomfører hvert år et elektronisk læringsprogram som sendes til alle ansatte. I oktober 2015 handlet det om informasjonssikkerhet. E-læringen innledet slik: "Leksjonene gir deg innblikk i hva du kan gjøre for å bidra til at kommunens håndtering av

informasjon blir både sikrere og bedre". Temaene var:

- Personvern.
- Falske e-postmeldinger og antivirusprogrammer.
- Sikre passord.
- Viktige ting å huske når du bruker e-post!
- Bruk av minnepinner og andre mobile lagringsenheter.
- Sikkerhet på arbeidsplassen.
- Utskrifter og papirhåndtering.
- Sosial manipulering.
- Har du lastet ned programmer fra internett?
- Bruk IKT-portalen og intranettet!

Også Norsk Helsenetts e-læring om informasjonssikkerhet er gjennomført i Oppegård kommune. Representanter fra pleie og omsorg opplyser til revisor at det er sterkt fokus på opplæring i informasjonssikkerhet. En arbeidsgruppe har ansvar for å utarbeide e-læringsprogram for Gerica-brukere. E-læring om lovkrav til dokumentasjon og ivaretakelse av personvern vil bli sendt ut til ansatte.

Samtykke
Både skole og pleie/omsorg innhenter samtykkeerklæringer før opplysninger overføres til andre. Elevers foresatte skal godkjenne all informasjon som overføres fra barneskole til ungdomsskole. Pasienter på sykehjem har avgitt samtykke om hvilke opplysninger som kan overføres til andre behandlere, f.eks. fysioterapeuter.

Rutinebeskrivelse for journalansvarlig beskriver dokumentasjon i Gerica og spørsmål knyttet til taushetsplikt.

3.2.8 Sikring av tilgang til personopplysninger

Sikkerhetshåndboken beskriver tiltak for å sikre ansatte tilgang til informasjonssystemene.

Kontinuitetsplanlegging
For avbruddssituasjoner skal det foreligge dokumenterte og innøvde handlingsplaner for å begrense konsekvensene for virksomheten, og for å normalisere situasjonen innen en akseptabel tid og kostnad. Den system-/registeransvarlige har ansvaret for at det foreligger manuelle rutiner som tas i bruk ved driftsavbrudd.

Sikkerhetshåndboken gjennomgår i et vedlegg informasjonssystemenes sårbarhet. En risikomatrise viser risikofaktorer, der sannsynlighet og konsekvens er estimert. Når produktet av sannsynlighet og konsekvens er høyt, skal tiltak settes inn. To hendelser medfører særlige tiltak: brann i datarom og inkompetanse. Risikofaktorer knyttet til eksterne faktorer beskrives.

Gjenopprettelse av normal drift etter avbrudd eller svikt i kritiske driftsprosesser skal beskrives i *kontinuitetsplan*, som skal spesifisere følgende:

a. Ansvarsforhold identifiseres.
b. Nødprosedyrer for å gjenopprette datasystemer innen tidsfrist fastsettes; eksterne bindinger/kontrakter vies særlig oppmerksomhet.
c. Avtalte nødprosedyrer dokumenteres.
d. Opplæring av de ansatte i nødprosedyrene, inkludert krisehåndtering, fastsettes.
e. Testing og oppdatering av planene fastsettes.

Prioritering av hvilke tjenester som bør settes i drift først og krav til bemanning og reserveløsninger angis. Ved avbrudd i driften av informasjonssystemet etableres alternativer til normal behandling av personopplysningene. Formålet med beredskapsplaner (jf. kapittel 5) er å sikre nødvendig behandling av personopplysninger også ved avbrudd i normal drift, samt at alternativ behandling utføres planmessig.

Sikkerhetskopiering
Sikkerhetskopiering (backup) foretas ved hjelp av en såkalt taperobot. Full backup av databaser og epost-tjenester skjer daglig, mens filsystemene inngår i en inkrementell rutine, det vil si at filer der det er gjort endringer siden siste fullstendige backup, kopieres. I tillegg til taperobot brukes harddisker til sikkerhetskopiering. All backup går først til disk, for så å bli lagt ut på taper. Inaktive taper oppbevares i brannsikkert skap i et annet rom enn dataanlegget.

Prosedyrene for sikkerhetskopiering inngår i IKT-seksjonens interne driftsprosedyrer (*Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune*, punkt 8.1.1). Etter at man la om til virtuelle servere, har man ennå ikke oppdatert prosedyren for backup, ifølge tidligere IKT-sjef. Dette bør komme på plass i nær fremtid.

Driftsprosedyrene inkluderer beskyttelse av dokumenter, datamedia (bånd, disker, kassetter), inn-/utdata og systemdokumentasjon mot ødeleggelse, tyveri og uautorisert tilgang. Representanter fra skole og pleie/omsorg opplyser at oppgradering på systemene fungerer bra. Systemeier bestiller oppgraderinger hos IKT-seksjonen, som utfører oppgraderingen når det passer for systemeier. Større oppgraderinger blir ofte utført av ekstern leverandør.

Skole og pleie/omsorg gir uttrykk for at det er lite nede-tid på deres systemer, og normalt blir dette varslet på forhånd. Sykehjemmene og hjemmetjenesten har utarbeidet rutiner for å opprettholde forsvarlig drift selv om systemet har nede-tid. Skolen har redegjort for hvordan de løser utfordringen med nede-tid; eksamenstiden er den mest sårbare tiden for dem.

3.3 Vurdering

Sikkerhetsledelse, sikkerhetsmål og sikkerhetsstrategi
Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune beskriver kommunens sikkerhetsledelse, sikkerhetsmål og strategier. Organiseringen av sikkerhetsledelsen er tydelig beskrevet med ansvarsforhold og oppgaver. Rådmannen og ledergruppen er øverste administrative organ for informasjonssikkerheten. Kommunen har en sikkerhetsansvarlig, som i organisasjonskartet befinner seg utenfor IKT-seksjonen. Dette tilfredsstiller kravet til at utøvende og kontrollerende ledd i kommunen ikke er det samme. Informanter i skole og pleie/omsorg bekrefter at sikkerhåndbokens bilde av organiseringen samsvarer med faktisk arbeidsdeling. Sikkerhetshåndboken skal oppdateres årlig; det skjedde sist i august 2015.

Personopplysninger, risikovurdering
Sikkerhetshåndboken har i vedlegg en tabell over alle Oppegård kommunes datasystemer som inneholder sensitive opplysninger. Systemeier (virksomhet) oppgis i systemoversikten, som IKT-seksjonen oppdaterer. Etter revisors skjønn har kommunen god oversikt over hvilke systemer som behandler personopplysninger. Kommunen har sendt inn meldinger til Datatilsynet vedrørende håndtering av personopplysninger. Sikkerhetsansvarlig oppgir at han ofte har sendt inn disse meldingene, men skriftlig rutine for innsendingen foreligger ikke.

Personopplysningsforskriftens § 2-4 pålegger behandlingsansvarlig å kartlegge sannsynligheten for og konsekvensen av sikkerhetsbrudd (risikovurdering). Systemeier er behandlingsansvarlig i Oppegård kommune. Pleie og omsorg opplyser at en risikovurdering for behandling av personopplysninger i Gerica ble utarbeidet i 2015. Skole opplyser at risikovurdering av SATS ikke er utarbeidet.

Organisering

Sikkerhetshåndboken redegjør for organiseringen av sikkerhetsarbeidet. Revisors informanter oppgir at det foreligger klare ansvars- og myndighetsforhold. Sikkerhetstiltak for sensitive opplysninger er iverksatt.

Sikkerhetsrevisjon

Personopplysningsforskriftens § 2-5 pålegger jevnlig (om lag årlig) sikkerhetsrevisjon av bruk av informasjonssystemet. Også *Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune* sier at sikkerhetsrevisjon skal gjennomføres årlig. Overordnet ansvar påligger sikkerhetsansvarlig, mens virksomhetslederne skal kontrollere at sikkerhetsprosedyrer utføres i deres fagområder. Sikkerhetsansvarlig opplyser at sikkerhetsrevisjon ikke er fulgt opp systematisk. Pleie og omsorg har gjennomført en egen sikkerhetsrevisjon fastsatt av Helsedirektoratet.

Avvik

Sensitive opplysninger ligger i sikre soner med sikkerhetsbarrierer. Når kritiske hendelser oppstår, utløses alarm som loggføres. Oppegård kommune kan dermed spore sikkerhetsbrudd, f.eks. uautorisert forsøk på å hente ut sensitive opplysninger. Kommunen har rutiner og skjema for avviksrapportering ved misbruk av informasjonssystemet, men sikkerhetsansvarlig har ikke mottatt slik avviksrapport de siste åtte årene. Underrapportering av avvik kan potensielt redusere organisasjonens mulighet til å lære av feil som gjøres. Oppegård kommune bør oppmuntre de ansatte til å registrere avvik og gi eksempler på avvik som skal rapporteres.

Fysisk sikring

Oppegård kommunes serverrom er forsvarlig sikret, slik at uvedkommende ikke kan komme seg inn. Servere har kjøling og nødstrøm, for å sikre stabil drift.

Uautorisert innsyn

Sikkerhetshåndboken beskriver tiltak for å hindre uautorisert innsyn. For både Gerica og SATS har man god kontroll på gitte tilganger. Ingen ansatte har tilgang til systemer de ikke har bruk for i sitt arbeid. Oppegård kommune har også drevet opplæring i håndtering av personopplysninger. Etter revisors skjønn har kommunen effektive rutiner for å unngå uautoriserte innsyn i personopplysninger.

Sikring av tilgang til personopplysninger

Oppegård kommune tar daglig backup av data på servere, noe som sikrer tilgang etter uhell. Rutinebeskrivelsen for backup er imidlertid ikke oppdatert. Informanter i skole og pleie/omsorg oppgir at det har vært lite nede-tid på deres systemer. Samarbeidet med IKT-seksjonen oppgis å fungere meget godt. Dataprogrammer oppdateres i nært samarbeid med IKT-seksjonen og leverandørene. Revisor vurderer at kommunen sikrer ansatte tilgang til de personopplysninger som trengs i deres arbeid.

4 IKT-DRIFT

Problemstilling nr. 2: IKT-drift
- Har kommunen oppdatert mål, retningslinjer og rutiner for IKT-arbeidet?
- Foretas sikkerhetsrevisjon?
- Er det tilfredsstillende arbeidsdeling vedr IKT?
- Har kommunen rutiner for å gjenoppta normal drift etter driftsstans?
- Er kompatibiliteten mellom ulike datasystem i kommunen tilfredsstillende?

4.1 Revisjonskriterier

ISACA (en verdensomspennende forening for IKT-styring og informasjonssikkerhet) har publisert *Grunnleggende retningslinjer for god IT-skikk*. Denne standarden anbefaler at kommuner m.fl. etablerer en IKT-strategi som forankres i kommunens mål og planer, samt at IKT-strategien utmyntes i handlingsplaner og investeringsplaner. God IT-skikk anbefaler at IKT-systemer og sammenhengen mellom dem dokumenteres. En samlet dokumentasjon av kommunens IKT-systemer bør omfatte arbeidsdeling og driftskontinuitet.

God IT-skikk anbefaler at driftsforstyrrelser logges og systemeier informeres ved driftsbrudd. Systemeier skal ha beredskapsplaner som ivaretar kontinuiteten i driften ved alvorlige/katastrofale hendelser. Det bør defineres når en forstyrrelse er så alvorlig at beredskapsplanen iverksettes.

Statskonsults *IKT i det offentlige* anbefaler at IKT-organisasjonen skiller mellom følgende roller:
- *Styringsrollen* omfatter den overordnede strategiske planlegging, koordinering og styring som er nødvendig for å følge opp IKT-virksomheten.
- *Bestillerrollen* ligger hos systemeier, som bestiller funksjonalitet og IKT-løsninger.
- *Leverandørrollen* ligger hos IKT-leverandøren, som skal levere de IKT-løsninger og tjenester som kunden ønsker/spesifiserer, herunder datamaskiner, standard programvare, utviklingsprosjekter/programmeringstjenester, IKT-drift og brukerstøtte. Også IKT-avdelingen har en leverandørrolle internt.

Personopplysningsforskriftens § 2-5 pålegger å gjennomføre sikkerhetsrevisjon av bruk av informasjonssystemet jevnlig (om lag årlig).

Revisjonskriterier:
- IKT-strategi med kommunens mål og planer for IKT-drift skal være utarbeidet.
- Roller i IKT-organisasjonen skal være tydelig definert.
- Planer for driftskontinuitet skal være utarbeidet.
- Sikkerhetsrevisjon skal gjennomføres jevnlig (om lag årlig).

4.2 Fakta

4.2.1 Mål, retningslinjer og rutiner

Basert på *Kommuneplan 2011–2022* har Oppegård kommunestyre vedtatt *IKT-strategi for Oppegård kommune* (2014). IKT-strategien fastsetter Oppegård kommunes overordnete mål

for IKT-bruk slik: "Oppegård kommunene skal aktivt utnytte moderne informasjons- og kommunikasjonsteknologi til å skape effektiv forvaltning, dialog og gode tjenester til innbyggere og næringsliv."

For å realisere statlige pålegg og løse kommunens utfordringer, utpeker IKT-strategien fem satsingsområder:

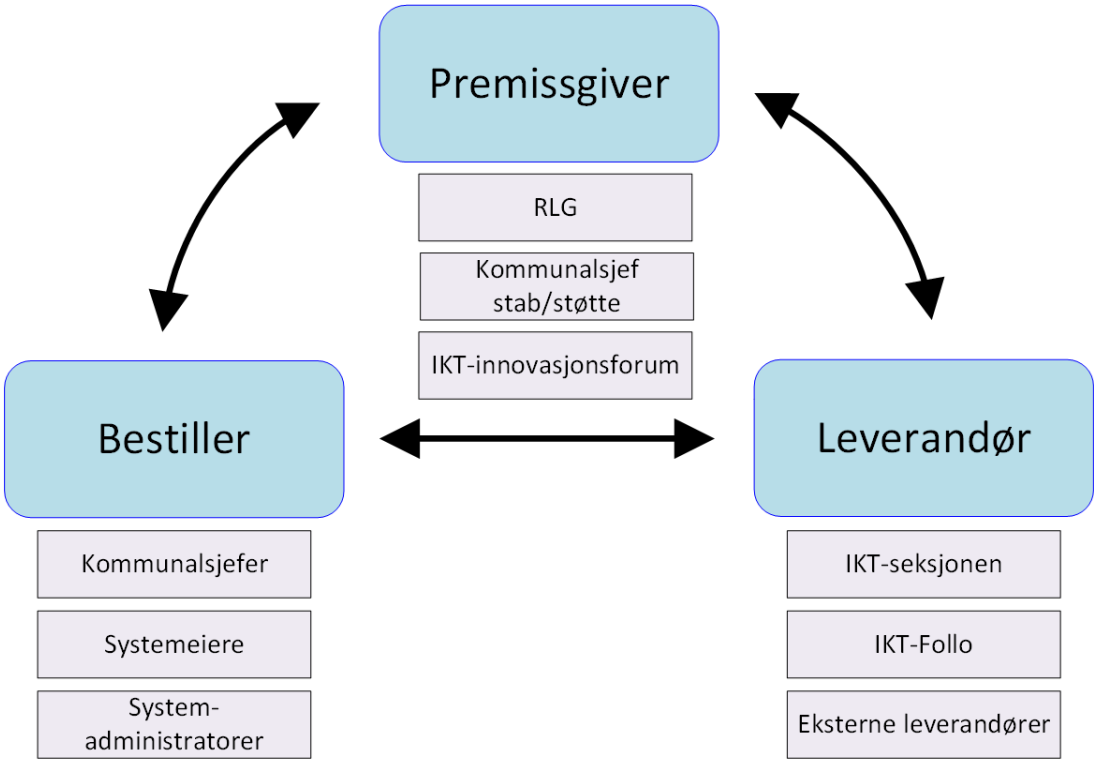
- *Digital forvaltning*: Effektive elektroniske rutiner og systemer for administrative oppgaver; IKT-systemer som sikrer god datakvalitet og gjenbruk av data; forsvarlig dokumenthåndtering og internkontroll i alle fagområder, der relevante opplysninger kan hentes ut til ansatte, parter og publikum; rutiner og systemer som sikrer rasjonell og samordnet IKT-virksomhet; IKT-systemer og utstyr som bidrar til gode og fleksible arbeidsforhold.
- *Velferdsteknologi*: Helhetlig pasientforløp der målet er at pasienten kan bo hjemme så lenge som mulig med trygghetsfremmende teknologiske løsninger; innovative løsninger tilpasset brukernes behov testes ut; ansatte leser og registrerer helseopplysninger mens de er hos pasienten; informasjonsutveksling gjennom Norsk Helsenett; rutiner og systemer som ivaretar sikkerhet og tilgjengelighet døgnet og året rundt (24 – 7).
- *Digital dialog*: Kommunen har gode, brukervennlige digitale løsninger for dialog med innbyggere og brukere; legge til rette for innsyn og flere elektroniske tjenester; ha sikre påloggingsrutiner for tilgang til personopplysninger og innsyn i egne saker; gi innbyggere hjelp til å bruk digitale løsninger.
- *Kompetanse*: Ansatte har tilstrekkelig kompetanse til å bruke IKT-systemene effektivt og kompetanse om lovpålagte krav til personvern, taushetsplikt og informasjonssikkerhet; IKT-personell har god kompetanse innenfor drift, utvikling, opplæring og brukerstøtte; kommunen har bestiller- og prosjektlederkompetanse og kan utnytte innkjøpsprosessen til å fremme innovasjon; god brukerstøtte.
- *IKT-organisering og styring*: Kommunen har en IKT-organisering basert på prinsippene om god IT-styring og kontroll, standarder og felleskomponenter; bruk av "sky-tjenester" baseres på grundige risiko- og sårbarhetsanalyser; databehandleravtaler ved ekstern drift er inngått; IKT-tjenestene ivaretar krav til sikkerhet, tilgjengelighet og kapasitet.

4.2.2 Arbeidsdeling vedrørende IKT

Oppegård kommune har utarbeidet *Forslag til IKT-Governance i Oppegård kommune* (september 2015). IKT-Governance er et begrep som brukes om styring og kontroll av tverrliggende IKT-prosesser, som understøtter alle funksjoner i en organisasjon, det vil si IKT-styring. IKT-Governance/IKT-styring henger tett sammen med virksomhetsstyring.

Forslag til IKT-Governance i Oppegård kommune angir at IKT-styringen skal kjennetegnes av avklart oppgave-, rolle- og ansvarsfordeling mellom delene av den samlede IKT-forvaltningen. Beslutninger bør gjennomføres etter plan, innenfor budsjett og med avtalt kvalitet. IKT-strategien skal knyttes til kommunens øvrige strategier, planer og tiltak. IKT-styringen skal sørge for kostnadseffektiv drift av alle IKT-systemer og infrastruktur, samt bidra til utvikling av kommunen med fokus på innovasjon.

Oppegård kommunes styringsmodell tegnes slik:

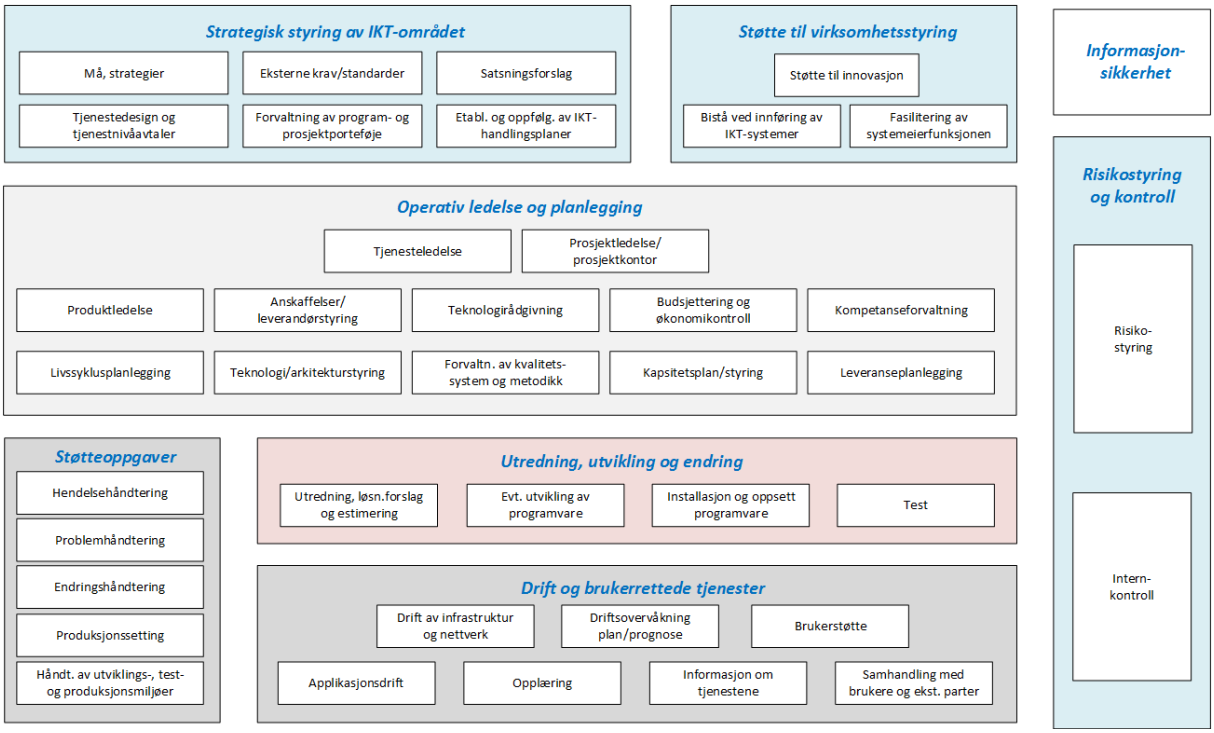


Kilde: *Forslag til IKT-Governance i Oppegård kommune* (2015).

Styringsmodellen innebærer at det samlede ansvaret deles mellom rollene som premissgiver, bestiller og leverandør:

- *Premissgiver* er som regel rådmannens ledergruppe (RLG) med tilhørende stabsfunksjon. Premissgiver har ansvar for strategisk IKT-styring. Kompetanse og kapasitet for dette må besørges.
- *Bestiller* vil normalt si kommunalsjefer og systemeiere/virksomheter. Bestiller er ansvarlig for større IKT-leveranser til sine virksomheter. Bestillerkompetanse, herunder prosjektlederkapasitet, forutsettes styrket.
- *Leverandører* er eksterne utstyrsleverandører, men også IKT-seksjonen, som leverer driftstjenester.

Forslag til IKT-Governance i Oppegård kommune gir oversikt over kommunens IKT-oppgaver:



Kilde: *Forslag til IKT-Governance i Oppegård kommune* (2015).

4.2.3 Gjenoppta normal drift etter driftsstans

Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune fastsetter at kommunen skal ha dokumentert følgende driftsprosedyrer:

- Backup av databaser og filsystemer.
- Kontroll av daglige backup-rutiner.
- Opprettelse av nye servere.
- Betjening av brukerstøttefunksjonen.
- Opprettelse av nye kontoer, avslutning av eksisterende.
- Oppsett av nye arbeidsstasjoner.
- Rutiner for å gjenoppta normaldrift etter driftsstans.
- Rutiner for å ta ned systemer.

Tidligere IKT-sjef har opplyst at kommunen ikke har utarbeidet skriftlige rutiner for å gjenoppta normal drift ved en driftsstans. På forespørsel fra revisor har han redegjort for hvordan IKT-seksjonen vil håndtere driftsstans i to tenkte scenarier:

"Senario 1: Total driftsstans
Her tar vi utgangspunkt i strømstans hvor også UPS og aggregat svikter. Når så strømmen kommer tilbake blir aktivitetene som følger:

Det er to team, Brukerstøtte og Drift, som har hver sine roller her. Brukerstøtte sørger for å informere ledelsen og de ansatte om hva som er skjedd og er tilgjengelig for å svare på henvendelser. Deres oppgave vil også være å sørge for oppdatert informasjon til organisasjonen. De har også en viktig oppgave etter at anlegget er tilbake i full drift. Det er å fange opp eventuelle feil på enkeltsystemer og sørge for at dette blir formidlet til Drift. Hovedfunksjonen til Brukerstøtte er kommunikasjon med og til organisasjonen og eksterne tjenester.

Drift, som er den andre delen, må sørge for at anlegget blir tatt opp i riktig rekkefølge og verifisere de enkelte trinn i denne prosessen. Her har alle innen Drift sine bestemte roller og jobber sammen om få etablert normal drift så fort og sikker som mulig. Drift vil også holde brukerstøtte orientert om fremdriften, slik at de kan gi riktig informasjon til ledelsen og sluttbrukere. Når normal drift er etablert vil det være Brukerstøtte som informerer Drift om følgefeil basert på reaksjoner fra sluttbrukere.

Det er en prioritering på hvilke nett og systemer som skal opp først. 'Sikker Sone' og de tjenester den inneholder er 1. prioritet. (Her finnes bl.a. Pasientjournalsystem.) Dernest kommer Sentralbordet og e-post tjenesten.

Avslutningsvis vil seksjonen sette seg ned og gå gjennom hendelsen for å se om det er tiltak som kan gjøres slik at dette ikke skjer igjen. En rapport/avvik vil oppsummere hele hendelsen med forslag til tiltak som må gjøres for at det ikke skal skje igjen.

Senario 2: Driftsstans enkeltsystem
Her beskrives feil på et system som følge av manglende diskplass og at det ikke er blitt fanget opp av overvåkingssystemene vi har.

En slik hendelse blir stort sett initiert av at flere sluttbruker melder sammenfallende feil. Når Brukerstøtte har registrert dette, sjekker de først overvåkningssystemene for så se om det er noe avvik. Kan de rette feilen selv, blir dette gjort og Drift blir informert. Om de ikke kan rette feilen selv blir den eskalert til Drift. Samtidig blir også berørte brukere og systemadministrator informert om situasjonen.

En i Drift får tildelt oppgaven og vil jobbe med å finne årsaken. Vedkommende trekker på ressurspersoner innen teamet om det er behov for det og sørger for at feilen blir utbedret. Status på fremdrift gis til Brukerstøtte slik at de kan gi denne informasjonen videre. Før systemet settes i full drift vil systemadministrator bli bedt om å sjekke programmet og gi OK.

Avslutningsvis vil seksjonen sette seg ned og gå gjennom hendelsen for å se om det er tiltak som kan gjøres slik at dette ikke skjer igjen. En rapport/avvik vil oppsummere hele hendelsen med forslag til tiltak som må gjøres for at det ikke skal skje igjen.

I begge tilfeller blir behov for ekstern bistand vurdert. Vi har ikke noen responsavtaler, men supportavtaler. Vi har basert oss på redundans i alle ledd så langt det lar seg gjøre. Vi har ekstra servere som kan settes inn om en skulle havarere. I det virtuelle miljøet er det nok kapasitet til at en host/vertsserver kan gå ned. Supportavtalene vi har på servere, nettverksutstyr og lagring er basert på 'neste arbeidsdag'-respons.

Når det gjelder tiden det vil ta før vi er tilbake i drift, kan jeg anslå at senario 1 vil ta fra 6–24 timer og senario 2 fra 2–8 timer. Det kommer an på omfanget av feilen og behovet for ekstern bistand."

4.2.4 Kompatibilitet mellom ulike systemer

Tidligere IKT-sjef opplyser at kommunen har i alt ca. 90 datasystemer. Kommunen foretrekker å bruke anerkjente systemer. Samspillet mellom kommunens systemer oppleves ikke som problemfylt; de kommuniserer godt med hverandre. Ved innkjøp av et system vil kravspesifikasjonene sette krav til samspill med andre systemer. IKT-sjefens generelle inntrykk er at

nyere systemer "snakker" bedre med hverandre. Trenden går dessuten i retning av at data lagres bare på ett sted (høyere gjenbruk av data).

Revisors informanter i skole så vel som pleie/omsorg gir uttrykk for at deres systemer fungerer tilfredsstillende sammen. SATS, som er skolens system for å holde oversikt over personopplysninger m.m., kommuniserer godt med skolens øvrige systemer, f.eks. IKTs Learning og Feide. SATS er et gammelt system som skal byttes ut; anbud er i ferd med å innhentes. Kravspesifikasjonen til nytt system setter krav til brukervennlighet og kompatibilitet med skolens øvrige systemer.

4.3 Vurdering

IKT-strategi for Oppegård kommune (2014) redegjør for kommunens mål, strategi og satsningsområder på IKT-området. IKT-strategien samsvarer etter revisors vurdering med anbefaling for god IT-skikk.

Både personopplysningsforskriften (§ 2-5) og *Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune* (2015) pålegger jevnlig (årlig) sikkerhetsrevisjon. Sikkerhetsansvarlig i Oppegård kommune har ikke gjennomført dette.

Arbeidsdelingen innen IKT-området i Oppegård kommune er tydelig. Det skilles mellom rollene *premissgiver*, *bestiller* og *utfører/leverandør*, slik god IT-skikk anbefaler.

Tidligere IKT-sjef har beskrevet hvordan IKT-seksjonen vil håndtere to scenarier med driftsstans. Revisor har grunn til å tro at IKT-seksjonen vil håndtere driftsstans på en tilfredsstillende måte. *Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune* pålegger utarbeidelse av rutinebeskrivelse for å gjenoppta normal drift ved driftsstans, men dette mangler. Selv om man har rutiner som fungerer i praksis, bør de nedtegnes skriftlig.

Oppegård kommune har som rettesnor å benytte anerkjente IKT-systemer. Revisors informanter i skole og pleie/omsorg opplever at systemene spiller godt sammen (er kompatible).

5 BEREDSKAP

Problemstilling nr. 3: Beredskap
- Har kommunen en beredskapsplan for IKT og er denne samordnet med planene i andre deler av kommunen?
- Hvordan er IKT-sikkerheten ivaretatt i virksomhetenes beredskapsplaner?
- I hvilken grad gjennomføres beredskapsøvelser og evaluering av disse?

5.1 Revisjonskriterier

Grunnleggende retningslinjer for god IT-skikk sier at virksomhetenes risikovurderinger er utgangspunktet for å vurdere IKT-beredskap. "Hva koster det virksomheten å være uten IKT-systemer?" er spørsmålet. IKT-beredskap omfatter planverk, tekniske løsninger og regelmessige øvelser.

Helseberedskapsloven sier følgende i § 2-1 Ansvarsprinsippet: "Den som har ansvaret for en tjeneste, har også ansvaret for nødvendige beredskapsforberedelser og for den utøvende tjeneste, herunder finansiering, under krig og ved kriser og katastrofer i fredstid, med mindre noe annet er bestemt i eller i medhold av lov."

Forskrift om kommunal beredskapsplikt § 7 pålegger: "Kommunens beredskapsplan skal øves hvert annet år. Scenarioene for øvelsene bør hentes fra kommunens helhetlige risiko- og sårbarhetsanalyse." Dette gjelder fremfor alt overordnet beredskapsplan, men også på avdelings- og virksomhetsnivå (resultatenheter) bør øvelser gjennomføres jevnlig. Øvelser gir mulighet for å teste ut om planverk og rutiner fungerer; det er særlig viktig på områder der man ønsker å forbedre seg. Øvelser bør evalueres.

Revisjonskriterier:
- Tekniske løsninger skal være robuste med redundans (overlapping/dublering).
- IKT-beredskap skal omtales i kommunens overordnete beredskapsplan (plan for kriseledelse) og i virksomhetenes beredskapsplaner.
- Beredskapsøvelser skal gjennomføres jevnlig, herunder annethvert år på overordnet nivå (kriseledelse).

5.2 Fakta

5.2.1 Beredskapsplan IKT

Oppegård kommunes overordnede beredskapsplan *Kriseplan for Oppegård kommune* 2013 omtaler ikke IKT. Bortfall av IKT forutsettes å kunne håndteres forsvarlig innenfor kommunens daglige drift. *Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune* beskriver hvilke elementer som skal inngå i beredskapsplaner:
- Ansvar for å utarbeide beredskapsplaner og å iverksette alternativ drift.
- Vurdering av avbruddets virkning på informasjonssystemet og for informasjonssikkerheten.
- Alternativ behandling, herunder beskrivelse av utstyr, program og manuell behandling.
- Verifisering av informasjonssystemet og metode for gjenskaping av normal drift etter korreksjon.

- Øving av beredskapsplaner.

Sikkerhetshåndboken redegjør videre for elementer i kommunens IKT-beredskap:

Vedlikehold av utstyr
Vedlikeholdsavtaler (serviceavtaler) skal tegnes for teknisk sikkerhetsutstyr som er essensielt for datasikkerheten, især for følgende kritiske komponenter:

- UPS (batteripakke) knyttet til kommunens sentrale dataanlegg.
- Dieselaggregat knyttet til kommunens sentrale datarom (serverrom).
- Serviceavtale på kjøleaggregat i det sentrale datarom.

For annet utstyr baserer man seg på nødvendig vedlikehold og utskifting.

Driftsprosedyrer
Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune fastsetter drifts-prosedyrer for backup (jf. kapittel 4.1.3 over).

Programvare

- Kun programvare som er godkjent installert av leder av IKT-seksjonen, kan benyttes på kommunens dataanlegg.
- IKT-seksjonen har ansvar for "brannmur" som beskytter mot nedlasting av skade-lige/ulovlige filer og programvare fra eksterne nettverk. Det er prosedyrer for verifise-ring av informasjon vedrørende ødeleggende programvare.
- IKT-seksjonen vedlikeholder og oppdaterer antivirusprogrammer, som kjøres på regel-messig basis og sjekker filer og programvare som legges inn fra nettet eller andre medier. Alle filer av ukjent eller uautorisert opprinnelse viruskontrolleres.
- Antivirusprogram kontrollerer alle vedlegg til e-post og alt nedlastet materiell. Det skal ikke åpnes vedlegg fra ukjente avsendere eller e-post som åpenbart er spam. Man må ha i minne at de som utvikler virusprogrammer hele tiden ligger foran de som lager beskyttelse.
- Har man vært uheldig og får varsel om virus, skal IKT-seksjonen kontaktes umiddel-bart (sikkerhetshåndbokens punkt 6.3 og 8.1.3).
- Forholdsregler for gjenoppretting etter virusangrep, herunder sikkerhetskopiering av alle data og programvarepakker (sikkerhetshåndbokens kapittel 11).

Sikring
Fullstendig sikkerhetskopiering tas ved hjelp av en taperobot. Det blir tatt daglig backup av databaser og filsystemer.

Oppegård kommune har utarbeidet *Overordnet ROS-analyse av Oppegård kommune* (2011). Risiko- og sårbarhetsanalysen (ROS-analysen) sitt kapittel 3-2 Svikt i infrastruktur IKT gir uttrykk for at kommunen har en god teknisk standard på IKT-drift og sikkerhetsløsninger. Datarommet er fysisk sikret, har både dieselaggregat og UPS (batteripakke) på serverparken, som testes to ganger i året. Ansattes fokus på IKT-sikkerhet og informasjonssikkerhet ansees som relativt høyt.

ROS-analysen vurderte følgende hendelser:

- Alvorlig hendelse som rammer bygning/serverrom fysisk.

- Menneskelig feilhandling.
- Sabotasje, dataangrep.
- Svikt i strømforsyning.
- Teknisk svikt.
- Utro medarbeidere.
- Virus, ondsinnet programvare på nettsteder.

ROS-analysen lister opp en rekke risikoreduserende tiltak:

- Nødstrøm (UPS og aggregat).
- Papirbackup av elektronisk pasientjournal.
- Innføre prosedyre for håndholdte enheter og e-post på mobil.
- Lagre backup på separat lokasjon.
- Følge opp retningslinjer for bruk av sosiale medier i Oppegård kommune.
- Sikre årlig oppdatering av risikovurderinger og prosedyre for informasjonssikkerhet.
- Sørge for økt sikkerhetsbevissthet hos virksomhetsledere og ansatte.
- Teste ut at IKT-systemer i nødsfall kan driftes fra Ski kommune.
- Utarbeide kontinuitetsplaner for kritiske IKT-hendelser.
- Utarbeide enkle sikkerhetsregler som alle ansatte pålegges å følge.
- Vurdere å innføre logging av driftsforstyrrelser og rapportering av sikkerhetsbrudd.
- Øve på utvalgte scenarier.

Tidligere IKT-sjef har gitt tilbakemelding på hvilke tiltak i ROS-analysen som er gjennomført per i dag. Følgende tiltak er ikke gjennomført helt eller delvis: Backup lagres ikke på separat lokasjon. Tiltak for at IKT-systemet kan driftes fra Ski kommune, er ikke gjennomført. Kontinuitetsplaner for kritiske IKT-hendelser er ikke utarbeidet. Logging av driftsforstyrrelser gjøres ikke, men rapportering av sikkerhetsbrudd gjøres gjennom Kvalitetslosen. IKT-seksjonen har ikke gjennomført øvelse, men kommunen gjennomfører øvelse på overordnet nivå annethvert år.

5.2.2 IKT-sikkerhet i virksomhetenes beredskapsplaner

Handlingsplan for alvorlige og ekstreme hendelser for skoler i Oppegård kommune (2014) omtaler ikke IKT spesielt. Heller ikke *Handlingsplan for sykehjemmene* (2013) omtaler IKT.

Representantene fra både skole og pleie/omsorg opplyser at de kan håndtere nede-tid på sine systemer uten at det går utover tjenestetilbudet. For skolene sin del vil nede-tid være mest prekært i eksamenstider. Alle eksamensoppgaver bestilles også på papir, slik at de kan gjennomføres manuelt. Nasjonale prøver trenger man ikke gjennomføre på eksakte datoer. Skolene har også manuelle rutiner for karaktersetting og bytte av skoleår (overgang til neste klassetrinn).

Sykehjemmene og Hjemmetjeneste har en prosedyre for nede-tid i Gerica, som skal sikre at pasienten får nødvendig helsehjelp når fagsystemet er nede. Oppdaterte medisinlister vil alltid foreligge på papir, slik at rett medisin kan utdeles. Lister over hvilke pasienter som skal ha hjemmebesøk, printes også ut på papir. Revisor får opplyst at sykehjemmene og Hjemmetjeneste kan håndtere nede-tid over flere uker. For tre år siden var systemet nede i én uke, noe man oppsummerte at ble håndtert på en god måte. Kommunikasjon med sykehusene kan gjøres telefonisk. Det er manuelle systemer for å dokumentere alt på sykehjemmene og i hjemmesykepleien; data må da legges inn i IKT-systemene når de er oppe og går igjen.

Representantene for pleie og omsorg har opplyst at alle rutinebeskrivelser på området er lagret i Kvalitetslosen. Planen er å systematisere disse bedre slik at det blir lettere å finne fram.

5.2.3 IKT-beredskapsøvelser

Oppegård kommune har ikke gjennomført beredskapsøvelser som handler om bortfall av IKT. Kommunens kriseledelse gjennomfører øvelser om lag annethvert år. Øvelsen i 2011 hadde energibortfall som tema; brudd på vannforsyning var tema i 2013. En øvelse planlagt til 2015 ble utsatt til 2016. Øvelsene har vært i regi av Fylkesmannen i Oslo og Akershus og har vært papirøvelser (skrivebordsøvelser) uten fysiske tiltak. Øvelsene er blitt evaluert av kommunen, som har konkludert med at øvelsene har gitt nyttige erfaringer både organisatorisk og individuelt.

IKT-relaterte øvelser er ikke gjennomført ved skole eller pleie/omsorg. Pleie- og omsorgs-systemet Gerica var, som nevnt, nede i en uke for tre år siden. De manuelle systemene ble tatt i bruk, noe kommunen anså at fungerte godt.

5.3 Vurdering

Kommunens overordnede beredskapsplan *Kriseplan for Oppegård kommune* omtaler ikke IKT spesielt. *Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune* omtaler utarbeiding av beredskapsplaner for IKT; ansvaret ligger på sikkerhets-ansvarlig sammen med seksjonsleder IKT m.fl. Også god IT-skikk tilsier at det er behov for IKT-beredskapsplan. IKT-beredskap bør derfor inngå som en del av Oppegård kommunes beredskapsplaner.

Sikkerhetshåndboken beskriver imidlertid en del elementer som vedrører beredskap. Kommunen har iverksatt tiltak – kjøling og nødstrøm – for å sikre stabiliteten til servere. Avtaler er også på plass for å få levert nødvendige komponenter på kort varsel. Kommunen har ikke utarbeidet tilstrekkelige rutinebeskrivelser for backup og gjenoppretting av normal drift etter en driftsstans. Dette bør prioriteres.

IKT-sikkerhet er ikke omtalt i virksomhetenes beredskapsplaner, hverken hos skole eller pleie/omsorg. Begge har imidlertid manuelle rutiner som gjør at de kan håndtere nede-tid på en tilfredsstillende måte.

Oppegård kommune gjennomfører beredskapsøvelser på overordnet nivå (kriseledelse) annet-hvert år, noe som samsvarer med lovverkets krav. Øvelser i kriseledelse gjennomføres som papirøvelser i regi av fylkesmannen. Det gjennomføres ikke IKT-relaterte beredskapsøvelser i de virksomhetene som revisor har undersøkt. Pleie og omsorg fikk imidlertid trening i manuelle rutiner da deres system var nede, noe som oppgis å ha fungert bra.

6 LITTERATUR

Lov og forskrift

Justis- og beredskapsdepartementet, LOV-2000-04-14-31: *Lov om behandling av personopplysninger* (personopplysningsloven).
Kommunal- og moderniseringsdepartementet, FOR-2000-12-15-1265: *Forskrift om behandling av personopplysninger* (personopplysningsforskriften).
Justis- og beredskapsdepartementet, FOR-2011-08-22-894: *Forskrift om kommunal beredskapsplikt*.

Nasjonale veiledere

Datatilsynet: *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer*, 2000.
Datatilsynet: *En veiledning om internkontroll og informasjonssikkerhet*, 2009.
KS: *Digitaliseringsstrategi 2013-16 for kommuner og fylkeskommuner.*
Statskonsult: *IKT i det offentlige*, 2002.
Helsedirektoratet: *Norm for informasjonssikkerhet*, 2015.

Internasjonale veiledere

Information Systems Audit and Control Association (ISACA), Norway Chapter: *Grunnleggende retningslinjer for god IT-skikk*, ca. 2009.
IT Governance Institute (ITGI): *Control Objectives for Information and Related Technology* (COBIT), 2001.

Oppegård kommunes dokumenter

Sikkerhetshåndbok vedrørende informasjonssikkerhet i Oppegård kommune, 2007, oppdatert august 2015.
IKT-strategi for Oppegård kommune, oktober 2014.
Forslag til IKT-Governance i Oppegård kommune, september 2015.
Kommuneplan 2011–2022.
Overordnet ROS-analyse av Oppegård kommune, 2011.
Handlingsplan for alvorlige og ekstreme hendelser for skoler i Oppegård kommune, 2014.
Handlingsplan for sykehjemmene, 2013.
Kriseplan for Oppegård kommune, 2013

Vedlegg 1: RÅDMANNENS UTTALELSE TIL RAPPORTEN

Oppegård kommune

Follo distriktsrevisjon
Postboks 3010

1402 SKI

Vår ref.:	Deres ref.:	Ark.:	Dato:
Saksbeh.: EH		056 &13	29.01.2016
Saksnr.: 16/411-2			

Svar - forvaltningsrevisjon - IKT og beredskap - uttalelse fra rådmannen til rapporten

Vi vil først takke for en grundig og nyttig gjennomgang av våre systemer. Vi er glade for at distriktsrevisjonens syn er at det vesentligste er på plass. Det er et godt utgangspunkt for utvikling og forbedring på viktige områder.

Rådmannen vil gjerne knytte noen vurderinger til rapportens konklusjoner og anbefalinger.

Kommunen gjør, som nevnt i rapporten, en overordnet risikovurdering av informasjonssikkerheten i den årlige revisjonen av sikkerhetshåndboka. Behovet for en mer inngående analyse vurderes av systemeier med bakgrunn i den overordnede analysen, og i forhold til eventuelt særskilte risikoer eller samsvarskrav (som for eks. nevnte Gerica i forhold til Normen). Behovet for interne sikkerhetsrevisjoner og andre kontrolltiltak har vært vurdert med bakgrunn i den overnevnte revisjonen. Med bakgrunn i rapportens konklusjoner og anbefalte tiltak, er det igangsatt en ny systematisk gjennomgang av tjenestenes avhengighet av systemene, og systemenes sårbarhet. Det er naturlig å vurdere behovet for ytterligere kontrolltiltak med bakgrunn i denne kartleggingen. Dette bør være klart til høstens revisjon av rutinene.

Kommunen har et pågående utviklingsarbeid i organiseringen av IKT driften. I utviklingsprosjektet «Kultur for endring» er et av hovedprosjektene «Forutsigbare IKT tjenester». Kommunens satsning på robusthet er en viktig del av prosjektet. Dette arbeidet er pågående, og tydeligere beskrivelser av kritiske rutiner er en naturlig del av dette. Herunder anbefalingene d og e.

Kommunens beredskapsplanlegging tar utgangspunkt i den overordnede risiko- og sårbarhetsanalysen. Det planlegges forhold til en håndfull dimensjonerende scenarier som kan ha konsekvenser for innbyggerens liv og helse. Bortfall av IKT tjenester gir per i dag ikke slike konsekvenser. Derimot er bortfall av datatilgang en konsekvens i seg selv i noen av scenariene, eksempelvis bortfall av energi. Således er IKT systemer nevnt i den sammenheng. Det er kontinuitet i tjenestene som prioriteres i en kritisk situasjon – ikke IT i seg selv. Tydelig prioritering er grunnleggende i både kriseplanlegging og krisehåndtering. Vi vil alltid måtte vurdere konsekvenser av eventuelle kortvarige og langvarige bortfall i

Postadresse:	Besøksadr.:	Telefon:	Organisasjonsnr.:	postmottak@oppegard.kommune.no
Postboks 510	Rådhuset	66 81 90 90	944 384 081	www.oppegard.kommune.no
1411 Kolbotn	Kolbotnveien 30			

forhold til kvalitet og effektivitet, og kost nytten i ulike forebyggende og skadereduserende tiltak. Som en del av den pågående gjennomgangen av kommunens IKT tjenester, og i forhold til denne rapportens anbefalinger, avstemmer vi nå forholdet mellom tjenestenes avhengighet av enkeltsystemer, og systemenes robusthet (se overnevte kartlegging).

De ansatte har ulike muligheter for å melde om feil, mangler og forbedringsmuligheter i forbindelse med IT-systemene våre. Men vi deler rapportens syn på bevisstheten for viktigheten av dette, og vil vektlegge dette sterkere bl.a i den årlige gjennomgangen med alle ansatte som e-læring (hver høst).

Innmelding av systemer som behandler sensitive data til Datatilsynet, er et ansvar som er delegert til systemeier. Dette ser vi ikke er tydelig nok presisert i våre rutiner, og det vil rettes på i høstens revisjon.

Med hilsen

Anne Skau
Rådmann