FORVALTNINGSREVISJONSRAPPORT

SARPSBORG KOMMUNE
ROLVSØY, 26. MAI 2020

IT-sikkerhet

Planer og rutiner for IT-sikkerhet og iverksatte sikkerhetstiltak

Delrapport 1 av 2

Innhold

Prosjektmandat

Østre Viken kommunerevisjon IKS skal i henhold til kommuneloven[1] utføre forvaltningsrevisjon. Etter loven innebærer forvaltningsrevisjon å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Østre Viken kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med god kommunal revisjonsskikk. God kommunal revisjonsskikk er å følge RSK 001; Standard for forvaltningsrevisjon, utarbeidet av Norges kommunerevisorforbund (NKRF). Dette innebærer blant annet at rapporten skal skille klart mellom hva som er innsamlet data og hva som er revisjonens vurderinger. Det skal være en tydelig sammenheng mellom problemstillinger, faktaopplysninger[2], vurderinger, konklusjoner og eventuelle anbefalinger.

Prosjektet er gjennomført på bakgrunn av plan for forvaltningsrevisjon 2018-2019, vedtatt i bystyret i Sarpsborg kommune 1. mars 2018, sak 11/18 og videreført i plan for forvaltningsrevisjon 2020-2021, vedtatt i bystyret 27. februar 2020, sak 2/20.

Etter kommuneloven skal vi rapportere resultatet av revisjonen til kontrollutvalget i kommunen. Prosjektet er gjennomført i tidsrommet desember 2019 - april 2020. Vi gjennomførte oppstartsmøtet med kommuneadministrasjonen 3. desember 2019. I oppstartsmøtet mottok vi også innspill fra administrasjonen som vi har tatt hensyn til i gjennomføringen av prosjektet.

Vi har kvalitetssikret faktagrunnlaget underveis gjennom verifisering av intervjuer og referater fra systemgjennomgang. I tillegg er rapportens faktautkast i sin helhet verifisert av kommunen, slik at eventuelle feil eller misforståelser er rettet opp.

Grunnet Corona-tiltakene i Norge og forsinkelser i deler av prosjektet, ble rapporten delt i to delrapporter. Denne rapporten er delrapport 1 og omhandler planer og rutiner for IT-sikkerhet og iverksatte sikkerhetstiltak. Delrapport 2 omhandler sikkerhetskultur. Delrapport 2 vil bli utarbeidet etter gjennomført spørreundersøkelse med ansatte i kommunen. Revisjonen har gjennomført høringsmøte med administrasjonen på delrapport 1 i videokonferanse 6. mai 2020. I etterkant av møtet er rapporten sendt på offisiell høring i kommunen. Kommunedirektørens uttalelse fremgår av kapittel 4.

Prosjektet er gjennomført av forvaltningsrevisor Unn Elisabeth West med bistand fra forvaltningsrevisor Sten Morten Henningsmoen og regnskapsrevisor Anita Marie Torp. Revisorenes habilitet og uavhengighet er vurdert opp mot kommunen og undersøkte virksomheter, og revisjonen finner de habile til å utføre prosjektet. Det er også gjennomført en testing av kommunens IT-sikkerhet. Testingen er gjennomført av Netsecurity AS.

Vi takker kontaktpersonen og andre som har deltatt, for et godt samarbeid i gjennomføringen av prosjektet.

Østre Viken Kommunerevisjon IKS
Rolvsøy, 26. mai 2020

Lene Brudal
oppdragsansvarlig revisor

Unn Elisabeth West
forvaltningsrevisor

[1] Kommuneloven kapittel 23 jfr. § 23-3 og kapittel 24, jfr. § 24-2.

[2] Fakta er en gjengivelse av informasjonen vi har fått tilgang til gjennom datainnsamlingen.

Sammendrag

Med økt digitalisering følger også økte krav til tilgjengelighet av viktige IKT-systemer. Dette er helt sentrale faktorer når nye, sikre digitale løsninger skal planlegges og implementeres. I forbindelse med digitalisering av kommunens løsninger er det derfor avgjørende å sikre informasjonen slik at den ikke kommer på avveie. Østre Viken kommunerevisjon har i dette prosjektet gjennomført en forvaltningsrevisjon for å vurdere om kommunen har etablert planer og rutiner som kan ivareta kommunens IT-sikkerhet på en tilfredsstillende måte og om kommunen har implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon.

I denne delen av prosjektet har vi blant annet undersøkt om kommunen har etablert sikkerhetsmål og –strategi, prosedyrer og rutiner for sikring av kommunens nettverk og systemer. Vi har også vurdert om kommunen gjennomfører risikovurderinger, har internkontroll, gjennomfører sikkerhetsrevisjoner og har effektiv rapportering til toppledelsen. I del to av prosjektet vil det bli gjort undersøkelser av sikkerhetskulturen i kommunen.

Revisjonens gjennomføring
Revisjonen har tatt utgangspunkt i utvalgte deler av personvernregelverket, eForvaltningsforskriften, norm for e-helse, NSM ti grunnkrav for IT-sikkerhet, samt veiledere og strategier på området. I dette prosjektet har vi benyttet data fra ulike kilder, og brukt ulike metoder for innsamling av data, for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet. Date er hentet inn gjennom analyse av dokumenter oversendt fra kommunen, intervjuer med ansatte og ledere i organisasjonen, gjennomgang av systemer for overvåking og IT-sikkerhet, gjennomgang av kommunens kvalitetssystem RiskManager. Det er også gjennomført en test av kommunens IT-sikkerhet. Testen er utført av et eksternt firma, Netsecurity. I rapporten er det er klart skille mellom faktaopplysninger, innhentet etter de ulike metodene som nevnt over og revisjonens vurderinger av faktainformasjonen. Da revisjonskriteriene og faktabeskrivelsen knyttet til de to problemstillingene i stor grad er overlappende har vi valgt å presentere problemstillingene samlet.

Revisjonens funn og konklusjoner
Sarpsborg kommune er en organisasjon som prioriterer IT-sikkerhetsarbeidet. Det er vår konklusjon at kommunen i stor grad har etablert planer og rutiner som ivaretar kommunens IT-sikkerhet på en tilfredsstillende måte. Kommunen har også implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon. Det er imidlertid noen områder hvor vi vurderer at kommunen har et forbedringspotensial.

Revisjonens anbefaler at Sarpsborg kommune bør:

- gjennomgå planer og rutiner knyttet til arbeidet med IT-sikkerhet, og oppdatere disse etter dagens organisering, ansvar og funksjoner
- sørge for en felles forståelse i organisasjonen av hvordan risikovurderinger skal gjennomføres og dokumenteres
- etablere rutiner for passordbruk og –bytte, som i større grad ivaretar IT-sikkerheten
- vurdere å etablere en rutine/sjekkliste for håndtering av uforutsette IT-hendelser
- oppdatere internrevisjonsgrunnlaget til gjeldende regelverk og vurdere å inkludere kontrollmiljøet i større grad
- vurdere om gjennomgående funn etter flere gjennomførte internrevisjoner, i større grad bør etableres som en problemstilling/avvik på et overordnet organisatorisk nivå
- sørge for å ha en øvet sikkerhetsorganisasjon med tanke på IKT-hendelser

1 Gjennomføring av prosjektet

Denne revisjonen er gjennomført før og under perioden med Corona-tiltak i Norge. Største delen av faktainnsamlingen, som testing av kommunens IT-sikkerhet, innhenting av dokumentasjon, intervjuer og systemgjennomgang var på plass før coronatiltakene trådte i kraft 13. mars 2020. Spørreundersøkelsen var ikke sendt ut, og dermed utsatt. For å sikre fremdrift i prosjektet har revisjonen i samråd med kontrollutvalgssekretariatet og kommunens kontaktperson derfor besluttet å utarbeide en rapport som består av to deler. Del 1 omhandler problemstilling 1 – Planer og rutiner for IT-sikkerhet og problemstilling 2 - Iverksetting av sikkerhetstiltak, mens delrapport 2 vi ta for seg problemstilling 3 – sikkerhetskultur. Rapportens del 1 er fullført i henhold til fremdriftsplanen. Rapportens del 2 gjennomføres etter at Coronatiltakene er avsluttet eller redusert.

Prosjektet bygger på risiko- og vesentlighetsvurdering, nærmere beskrevet i prosjektplanen datert 5. desember 2019. Her fremgår blant annet følgende om risiko på området: *«Den pågående digitaliseringen av samfunnet blir drevet fremover og gjort mulig av teknologiutvikling. Digitaliseringen gjør at stadig flere arbeidsprosesser utføres eller støttes av digitale verktøy. Kunnskap om, eller muligheten for å gjennomføre, manuelle rutiner forsvinner. Med økt digitalisering følger også økte krav til tilgjengelighet av viktige IKT-systemer. Dette er helt sentrale faktorer når nye, sikre digitale løsninger skal planlegges og implementeres. Ny teknologi kan gjøre det mulig å lage sikrere løsninger, men kan også medføre økt kompleksitet, introduksjon av nye sårbarheter og økt behov for sikkerhetskompetanse.*

NSM opplyser i sin årsrapport at de erfarer at økte muligheter innen teknisk sikring ikke alltid utnyttes og at mangelfullt teknisk vedlikehold av systemer, eksempelvis manglende sikkerhetsoppdateringer, skaper unødvendige sårbarheter.
[...]
I forbindelse med digitalisering av kommunens løsninger er det derfor avgjørende å sikre informasjonen slik at den ikke kommer på avveie. For eksempel ved hjelp av tilgangsstyring, kryptering, osv. Personopplysningsloven § 13 med den tilhørende forskriften kapittel 2 oppstiller i dag krav til kommunenes sikring av informasjon (informasjonssikkerhet).
[…]
Datatilsynets tilsyn med kommuner i 2016 viste vesentlige avvik knyttet til informasjonssikkerhet, noe som indikerer at det kan være god grunn til å også se nærmere på dette i Sarpsborg. Eksempelvis ble det avdekket at virksomheter ikke har tilstrekkelig fokus på å ivareta personvernet og på å oppfylle pliktene i personopplysningsloven knyttet til internkontroll og informasjonssikkerhet. Datatilsynet vurderer det som viktig for virksomhetene å ha et akseptabelt nivå på internkontroll og informasjonssikkerhet før store digitaliseringsprosesser starter opp.»

1.1 Problemstillinger og avgrensning

- Er det etablert planer og rutiner som kan ivareta kommunens IT-sikkerhet på en tilfredsstillende måte?

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

Det er en klar sammenheng mellom IT-sikkerhet og personvern, spesielt knyttet til kommunal tjenesteyting. Det er imidlertid to ulike innganger når en skal vurdere de to områdene. Dette prosjektet

omhandler IT-sikkerheten og er avgrenset mot personvern, som vil bli et eget forvaltningsprosjekt på et senere tidspunkt.

I takt med den digitale utviklingen har IT-sikkerhet blitt et stadig viktigere tema. Det er viktig at kommunen har planer og rutiner for å håndtere IT-sikkerhetsmessige situasjoner, som virusangrep og lignende. I dette prosjektet har vi vurdert kommunens planer og rutiner relatert til IKT-sikkerhet og dataangrep, herunder kommunens arbeid med risikovurderinger på området. Vi har også sett på hvilke sikkerhetstiltak kommunen i praksis har satt i verk for å sikre seg mot uønskede hendelser. Vi har derfor undersøkt hvordan kommunen har innrettet seg for å fange opp trusler og angrep, og vi har gjennomført tester mot kommunens systemer gjennom bruk av ekstern leverandør av IT-sikkerhetstjenester. Vi har også undersøkt om kommunen har implementert rutiner og prosedyrer knyttet til IT-sikkerhet, om kommunen følger opp etterlevelse av disse (internkontroll), og om det er etablert en god sikkerhetskultur i organisasjonen. Som nevnt innledningsvis vil sikkerhetskulturen omtales i egen rapport – delrapport 2.

Både revisjonskriterier og faktagrunnlag er delvis overlappende for problemstilling 1 og 2 slik at vi i denne rapporten har valgt å presentere problemstillingene samlet i kapittel 2.

1.2 Revisjonskriterier

I henhold til standard for forvaltningsrevisjon må revisor fastsette revisjonskriterier for forvaltningsrevisjonen. Revisjonskriterier er en samlebetegnelse for krav og forventninger som blir brukt til å vurdere ulike sider av kommunens virksomhet og tjenester. Revisjonskriterier fastsettes vanligvis med basis i en eller flere av følgende kilder: lovverk, politiske vedtak og føringer, kommunens egne retningslinjer, anerkjent teori på området og andre sammenlignbare virksomheters løsninger og resultater.

I denne rapporten er følgende kilder benyttet til å utlede revisjonskriteriene:

- *Kommuneloven*
- *Personvernforordningen – GDPR*
- *Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)*
- *Digitaliseringsdirektoratets veiledere til informasjonssikkerhet*
- *Direktoratet for e-helses Norm for informasjonssikkerhet og personvern i helse- og omsorgs-tjenesten*
- *Nasjonal strategi for digital sikkerhet 05/2019*
- *ISO/IEC 27001 (Information technology)*

Revisjonskriteriene fremkommer i kapitlene 2.1 og 3.1, utledningen av revisjonskriteriene fremkommer i vedlegg 1. Revisjonskriteriene er også oversendt kommunen i forkant av prosjektet.

1.3 Revisjonsmetoder

I henhold til god revisjonsskikk skal praksis eller tilstand innen det reviderte området beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner. I dette prosjektet har vi benyttet data fra ulike kilder, og brukt ulike metoder for innsamling av data, for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet.

Utfordringer og begrensninger i rapportens faktagrunnlag beskrives nedenfor sammen med beskrivelsen av de ulike metodene som er benyttet. Vi tar også hensyn til metodens begrensninger i vurderingene.

I dette prosjektet er informasjonen hentet inn gjennom bruk av følgende metoder:
- Dokumentanalyse
- Intervjuer
- Spørreundersøkelse – *denne er ikke grunnlag for delrapport 1, men kommer inn i delrapport 2*
- Testing av IT-sikkerheten
- Systemgjennomgang

Dokumentanalyse
Vi har gjennomgått sentrale dokumenter på området. Dokumentene ble oversendt fra kommunen og mottatt innen fristen, som var 10. januar 2020. Fullstendig oversikt over dokumentene fremgår i kapittel 6.

Intervjuer
Det er totalt gjennomført 15 intervjuer:
- Fagansvarlig informasjonssikkerhet
- Personvernombud
- Direktør for kommuneområde Teknologi og endring
- Beredskapskoordinator
- 2 rådgivere virksomhet forvaltning og utvikling - kommuneområde Helse og velferd
- 2 rådgivere stab - kommuneområde Oppvekst
- Avdelingsleder IT-drift og IT-brukerservice
- 5 ansatte på IT-avdelingen
- Controller

Alle referatene fra intervjuene er verifisert. Det betyr at den som er intervjuet, har lest gjennom referatet fra intervjuet og bekreftet at referatet er i overenstemmelse med det som ble sagt under intervjuet, og rettet opp eventuelle misforståelser eller lagt til eventuelle mangler. Der vi har konkludert, bygger vurderingene alltid på skriftlig dokumentasjon eller informasjon fra flere kilder.

Testing av systemet – rekognosering og phishing
På oppdrag fra revisjonen har selskapet Netsecurity gjennomført en rekognosering av kommunens system. Dette er en simulering av hvordan en målrettet angriper kan angripe kommunens systemer og organisasjon. En rekognosering har som mål å identifisere eventuelle datalekkasjer, sensitive systemer som ikke bør være på nett og andre forhold som kan utgjøre en risiko for at uvedkommende kan komme seg inn i kommunens systemer. Dette kan gi et godt bilde av hvilken risiko som eksisterer i organisasjonen. En rekognoseringsrapport danner gjerne grunnlaget for penetrasjonstesting, der man simulerer hvordan en målrettet angriper vil angripe systemene. Revisjonen har kun fått gjennomført en rekognosering, for å avdekke mulige svakheter i kommunens systemer. Det er ikke gjort tester av systemet som sådan utover dette.

Det ble også gjennomført en phishing-test mot 750 brukere. Målet var å teste risikoen hos sluttbrukerne ved et målrettet angrep. Testingen ble gjennomført den 25. februar 2020. E-postene ble sent kl. 12:06, og alle e-postene var utsendt i løpet av de neste minuttene.

Deler av resultatene fremkommer i denne rapporten. På grunn av konfidensialiteten vil ikke resultatene i sin helhet fremgå her. Kommunen får egen informasjon om detaljerte funn fra undersøkelsen.

Systemgjennomgang
Vi hadde en gjennomgang av IT-avdelingenes systemer for kontroll og sikring av kommunens IT-systemer, 3. februar 2020. To ansatte fra IT-avdelingen deltok i gjennomgangen, deriblant leder IT-drift

og –brukerservice. Vi hadde også en gjennomgang av Risk Manager på IT-sikkerhetsområdet, 13. februar 2020. Personvernombudet deltok på denne gjennomgangen. Det ble skrevet et notat etter begge gjennomgangene. Notatene er verifisert av de som deltok på gjennomgangene fra kommunen.

Om kommunen

Sarpsborg kommune har 4 410 ansatte per 1. januar 2020. Kommunen er organisert ved at kommunedirektøren har ett team og seks kommuneområder.

Figur: Organisasjonskart Sarpsborg kommune

2 Planer, rutiner og sikkerhetstiltak

2.1 Revisjonskriterier

Elektronisk kommunikasjon med og i forvaltningen omfattes av de alminnelige reglene i forvaltningsloven. Forvaltningsloven er hjemmelslov for eForvaltningsforskriften. Det fremkommer i veileder til eForvaltningsforskriften at denne gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen.

Informasjonssikkerhet er et ledelsesansvar. Mål og strategi for informasjonssikkerhet (sikkerhetsmål og sikkerhetsstrategi) er ledelsens viktigste redskap i styringen av informasjonssikkerheten innenfor forvaltningsorganets ansvarsområde. Videre bør mål og strategi inngå som grunnlaget i internkontrollen.

Forvaltningsorganets internkontroll skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen på informasjonssikkerhetsområdet bør være en integrert del av virksomhetens helhetlige styringssystem. Fordi forvaltningsorganer vanligvis behandler personopplysninger, vil personopplysningsregelverket også være sentralt i arbeidet med informasjonssikkerheten.

I Nasjonal strategi for digital sikkerhet står det at å ivareta digital sikkerhet først og fremst er et virksomhetsansvar. Virksomhetsledere er ansvarlig for å foreta risikovurderinger, og på bakgrunn av dette gjennomføre tilstrekkelige tiltak. Samfunnet er avhengig av at kritiske samfunnsfunksjoner opprettholdes, og det forutsettes at de digitale infrastrukturene som understøtter dem virker overalt og hele tiden.

Norm for e-helse ble lansert allerede i september 2006, og den har blitt endret flere ganger i takt med endringer i annet lovverk. Normen viser til at god informasjonssikkerhet og godt personvern er en forutsetning for digitalisering. Sektoren må bygge og forvalte robust teknologi, organisasjon og sikkerhetskultur.

Kommunen må sette i verk planlagte sikkerhetstiltak for å sikre seg mot uønskede hendelser, fange opp trusler og angrep. Det er viktig at ledelsen og forvaltningsorganet for øvrig har tilstrekkelig styring og kontroll med det som gjøres i forvaltningsorganet for å ivareta informasjonssikkerheten.

Revisjonskriterier:

- Kommunen har beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).
- Kommunens sikkerhetsmål og –strategi har tydelige krav og forventninger til sikkerheten.
- Kommunens sikkerhetsstrategi og internkontroll inkluderer relevante krav som er fastsatt i annen lov, forskrift eller instruks.
- Kommunen har etabler tydelig ansvarfordeling i risikostyringen.

- Kommunen gjennomfører risikovurderinger på informasjonssikkerhetsområdet.
- Kommunens prosess for risikostyring er en del av en helhetlig styringsstruktur og er kjent i virksomheten.
- Kommunen har, med bakgrunn i risikoene forbundet med de ulike behandlingene etablert et egnet sikkerhetsnivå knyttet til IT-sikkerheten.
- Kommunen har gjennomført en kartlegging av verdikjeder, informasjonsverdier, utstyr og brukertilganger.

- Kommunen har oversikt over alt IKT-utstyr.
- Kommunen har kontroll på nettverk og komponenter.
- Kommunen har prosedyrer for og sørger for sikker konfigurasjon.
- Kommunen har en oversikt over type leverandører.
- Kommunen stiller krav til produkter og leverandører slik at sikkerheten er ivaretatt i hele produktets eller tjenestens levetid.
- Kommunen sørger for god e-post og Websikkerhet.

- Kommunen har informert sine ansatte om hvilke sikkerhetstjenester og -produkter de skal benytte under tjeneste for organet, og hvorledes de skal gå frem for å anskaffe nødvendig utstyr og data, inkludert passord, PIN-koder mv.
- Kommunen har prosedyrer for bruk av informasjonssystemene.
- Kommunen har en prosedyre for tilgangskontroll og autorisering.
- Kommunen har etablert prosedyrer for oppbevaring og bruk av passord/PIN-koder o.l., dekrypteringsnøkkel og signaturfremstillingsdata.

- Kommunen har sørget for at det er etablert klare ansvarsforhold mellom avsender, mottaker og eventuell meldingsformidler ved sending av meldinger med helse- og personopplysninger.
- Kommunen sørger for sikker overføringskryptering ende-til-ende for helse- og personopplysninger.

- Kommunen har prosedyrer for avviksregistrering.
- Kommunen har en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet.
- Kommunens internkontrollen er en integrert del av virksomhetens helhetlige styringssystem.
- Kommunens internkontroll (styring og kontroll) på informasjonssikkerhetsområdet er basert på kommunens sikkerhetsmål og sikkerhetsstrategi.
- Kommunens internkontroll har et omfang og en innretning som er tilpasset risikoen på informasjonssikkerhetsområdet.
- Kommunen har planer for gjennomføring av sikkerhetsrevisjoner.
- Kommunen gjennomfører sikkerhetsrevisjoner jevnlig og følger opp resultatene av disse.
- Kommunen har etablert effektive rapporteringslinjer til toppledelse.
- Ledelsens gjennomgang skal være minimum årlig og dekke bl.a. avvikshendelser og eventuelle korreksjoner i styringssystemet.

- Kommunen har etablert en beredskapsplan for ulike typer hendelser.
- Kommunen gjennomfører øvelser som tester planverket.

2.2 Revisors undersøkelse

Mål, strategi og organisering

I dokumentet *Sikkerhetsorganisering i Sarpsborg kommune*, datert 11.08.2015 fremkommer det hvordan kommunen har organisert arbeidet med informasjonssikkerheten og hvem som har ansvar på ulike områder. Vi har fått oversendt et revidert utkast til *Sikkerhetsorganisering* i Sarpsborg kommune, som er utarbeidet med bakgrunn i dagens organisering. Dette dokumentet er ennå ikke godkjent. Det fremkommer at kommunen i arbeidet med informasjonssikkerheten blant annet har et personvernombud og en fagansvarlig informasjonssikkerhet. Det sektorovergripende arbeidet er plassert i kommuneområde teknologi og endring, som består av fem avdelinger:

- Innbyggerdialog (servicetorg og kommunikasjonsrådgivere)
- Porteføljestyring
- Informasjonsforvaltning
- IKT-brukerservice
- IKT drift

I tillegg har kommunen delegert oppgaver knyttet til arbeidet med informasjonssikkerhet til ulike lederfunksjoner i organisasjonen. Fagansvarlig informasjonssikkerhet har overordnet operativt ansvar for informasjonssikkerheten, personvernombudet er ansvarlig for å informere og gi råd om de forpliktelsene virksomheten har etter personvernlovgivningen, og IKT-driftsleder er overordnet operativt ansvarlig for drift av informasjonssystemene. Stillingen fagansvarlig informasjonssikkerhet ble opprettet høsten 2019.

Fagansvarlig informasjonssikkerhet og personvernombudet er plassert i staben, mens avdelingsleder IKT drift er organisert i linjen. Det kommer frem av intervjuene at det er vesentlig at fagansvarlig informasjonssikkerhet og avdelingsleder IKT-drift ikke er plassert i samme avdeling i virksomheten. Fagansvarlig informasjonssikkerhet og avdelingsleder IKT drift rapporterer begge direkte til direktør KTE.

Fagansvarlig informasjonssikkerhet skal informere direktør KTE om sikkerheten på de ulike områdene etc, men det er opp til hver enkelt leder/ansatt om det blir jobbet på området. Det er til en viss grad opp til den enkelte leder å prioritere IT-sikkerhet. Mange ledere har lagt oppgaver knyttet til informasjonssikkerhet og personvern inn i årshjul, og har det som fast tema f.eks. på personalmøter i løpet av året, men dette er ikke gjennomgående praksis hos alle.

I *Funksjonsbeskrivelse fagansvarlig informasjonssikkerhet,* udatert, fremkommer det blant annet at fagansvarlig informasjonssikkerhet er kommunedirektørens rådgiver for informasjonssikkerhet i kommunen og at stillingen fordrer god forståelse for IKT-relaterte risikoer, og andre typer informasjonssikkerhetsrisikoer. Dette inkluderer å selv være oppdatert og holde organisasjonen løpende oppdatert på trusselbildet og sårbarheter. Det kommer frem i intervjuene at fagansvarlig informasjonssikkerhet også har som oppgave å være brobygger mellom IKT-sikkerheten og arbeidet med personvernet.

Det kommer frem av intervjuene at det har vært krevende å opprette en kommuneområdeovergripende rolle innen informasjonssikkerheten, fordi det ikke er like mye som er regulert på IT-sikkerhetsområdet i regelverket, slik det er på personvernområdet. Personvernombudsrollen er tydelig definert gjennom GDPR.

I intervjuene sier personvernombudet at den som har ombudsrollen ikke bør ha sikkerhetsansvaret samtidig. Det er derfor kommunen har opprettet to stillinger, der den ene har ombudsrollen og den

andre har fagansvaret for informasjonssikkerheten. Det kommer frem av samtalene med ansatte ved IT-avdelingen at de opplever å jobbe mer med sikkerheten nå som det er ansatt en egen fagansvarlig for informasjonssikkerhet. De vi intervjuet sier at de opplever at kommunen prioriterer arbeidet med sikkerhet, og mener kommunen er opptatt av å lykkes på dette området og derfor bruker mer ressurser på området enn mange andre sammenlignbare kommuner.

Kommunen gjennomførte et GDPR complianceprosjekt / implementeringsprosjekt i 2018. Etter det ble en del av styringsdokumentene revidert. Tidligere var blant annet kommunens sikkerhetsmål/-strategi på ti sider, etter dette prosjektet ble dokumentet justert ned til en side. Dokumentet *Sikkerhetsmål og sikkerhetsstrategi* er datert 26.03.2019. Det fremkommer at dette dokumentet gjelder for alle ansatte og folkevalgte i kommunen. Dokumentet beskriver hva som er målene på ulike områder i sikkerhetsarbeidet og hva som er kravene/forventningene for at disse målene skal kunne nås. Kravene som er definert er formulert på et overordnet nivå. Kommunen har også utarbeidet et målbilde for informasjonssikkerhet og personvern. Her fremkommer kommunens innsatsområder og delmål for ivaretakelse av informasjonssikkerheten. Det foreligger også et utkast til målbilde for kommeområde teknologi og endring (KTE), som sier noe om kommunens mål knyttet til digitalisering og samhandling mellom tjenester, samt ivaretakelse av informasjonssikkerheten. Det er også utarbeidet en *Digitaliseringsstrategi for Sarpsborg kommune*, vedtatt 06.06.2017, hvor det er formulert overordnede mål og strategi på området. Det er foretatt en vurdering av status per juni 2017, og det er formulert tiltak som skal gjennomføres i perioden 2017 til 2021.

Det kommer frem av intervjuene at IT-avdelingen benytter NSMs[3] ti grunnprinsipper i arbeidet med IT-sikkerhet. NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og underliggende tiltak, som skal beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenester mot uautorisert tilgang, skade eller misbruk.

I dokumentet *Retningslinjer for kvalitetssystem*, datert 20.10.2017 står det at kommunen har innført kvalitetssystemet RiskManager. Systemet består av flere moduler, blant annet dokumenthåndtering, avviksregistrering og risikovurderinger. Det kommer frem av intervjuene at ikke alt er helt på plass når det gjelder arbeidet på sikkerhetsområdet per i dag og noe begrunnes i kvalitetssystemet RiskManager. Flere opplever RiskManager som uoversiktlig, med svært mange dokumenter og dårlig sortering, og det kan være vanskelig for ansatte å orientere seg i systemet. Kommunen ønsker å forenkle dette og gjøre det mer tilgjengelig. Fagansvarlig informasjonssikkerhet vil få ansvaret for å få dette på plass. Det kommer frem av intervjuene at sikkerhetsarbeidet oppleves å bli både prioritert og tatt på alvor blandt kommunens ledere.

Risikostyring, gjennomføring av risikovurderinger og egnet sikkerhetsnivå

I intervjuet med fagansvarlig informasjonssikkerhet fremkommer det at de enkelte avdelingene og virksomhetene i kommunen er ansvarlig for å vurdere sin del av risikoområdene, vurdere bruken av sine systemer, prosesser, hvor de lagrer data og vurdere om ansatte har tilstrekkelig forståelse for reglementet.

I dokumentet *Rutiner for gjennomføring av risikovurderinger informasjonssikkerhet,* datert 01.03.2015 fremkommer det at Risikovurderinger skal gjennomføres og dokumenteres minimum en gang i året, før nye behandlinger av personopplysninger og ved endringer som kan påvirke informasjonssikkerheten. Risikovurderingene skal gi kommunen oversikt over mulige uønskede hendelser, gi informasjon om sannsynlighet og konsekvens for uønskede hendelser og en oversikt over restrisiko og eventuelle nødvendige tiltak. Det fremkommer at rutinen gjelder for alle medarbeidere i kommunen. Det er den

[3] Nasjonal sikkerhetsmyndighet

enkelte virksomhetsleder som har ansvaret for at rutinen etterleves innenfor sin virksomhet. Det foreligger også en *Rutine for håndtering av risiko, personopplysninger*, datert 28.05.2013. Rutinen beskriver hvordan risiko for personopplysninger som avdekkes i risikovurderinger skal håndteres.

I gjennomgangen av IT-avdelingens sikkerhetssystemer 03.02.2020 blir det sagt at kommunen har skriftlige rutiner på når og hvem som skal gjøre risikovurderinger på de ulike områdene, og at dette ligger i RiskManager. Det blir videre sagt at for IT-avdelingens vedkommende er det en selvfølge å tenke sikkerhet ved innføring av nye systemer. IT-avdelingen har fokus på det tekniske nivået når det gjelder risikovurdering, om porter er sikre og lignende. Det ble for noen år siden utarbeidet en oversikt over de ulike rollene, og hvilket ansvar som ligger i de ulike rollene. Det kommer frem av intervjuene med ansatte på IT-avdelingen, at de ikke har ansvar for dataene som ligger innenfor et system, annet enn at de oppbevares og sikkerhetskopieres og ligger trygt.

Det kommer frem av intervjuene at ansatte ikke opplever det som enkelt å finne frem i RiskManager. Noen av de vi snakket med mener at de ikke har tilgang til RiskManager.

Deler av helseområdet hadde tidligere egne prosedyrer på risikovurderinger. I den senere tid er noen av disse flyttet opp til nivå 1, felles prosedyrer, i RiskManager. Dette for at kommunen bør ha samme prosedyrer på de områdene der de nå har de samme kravene. Dette er en av konsekvensene som kommer av tydeligere føringer på risikovurdering, også på andre områder enn helse.

Det kommer frem på systemgjennomgangen at kommunen har drøftet forskjeller og sammenhenger mellom DPIA og risikovurderinger for digitale system/program. Risikovurderinger av et system/program vil ta for seg ulike sider ved systemet og mer enn det som handler om sikring av personopplysninger. Mens risikovurderinger tar utgangspunkt i informasjonsverdiene som skal beskyttes, tar en DPIA utgangspunkt i rettighetene og frihetene til personene som er registrert i systemet, og ser på hva som kan true disse rettighetene.

I en gjennomgang av IT-avdelingens sikkerhetssystemer kommer det frem at IT-avdelingen har fokus på at alle nye systemer blir risikovurdert. Kommunen har imidlertid også systemer som har vært der over flere år, og her gjennomføres det kun risikovurderinger når det anses at det er behov for det. Det kommer frem av samtalene med ansatte på IT-avdelingen at de gamle systemene jobbet mer eller mindre i et lukket miljø hos kommunen, mens de nye som regel er skysystemer. Som eksempel har kommunen i risikovurderingen av Office 365 tatt utgangspunkt i en risikovurdering gjort av Bærum kommune, og bygget videre på denne. Det ble gjort en vurdering av hva som er relevant å ta med for Sarpsborg kommune, men mye er veldig likt, som rammeverk mv. Kommunens begrunnelse for dette er at Bærum er dyktige og grundige på dette området, og kommunesektoren er god på informasjonsdeling.

I intervjuene sier ansatte på IT-avdelingen at de har blitt gode på å gjøre ROS-analyser. De har egne rutiner og system for å håndtere endringer. De har også et eget verktøy for det, *Pureservice.* Standardendringer gjøres fortløpende. Større endringer tas opp i CAB[4], der blir endringene gjennomgått og evt. besluttet gjennomført. Hvis endringer feiler sørger IT-avdelingen for at de kan reversere endringene på en enkel måte.

Det kommer også frem av intervjuene at kommunen også har gammel maskinvare og programvare som ikke er oppdatert fra leverandørens side. Dette blir vurdert til å kunne være en sikkerhetsrisiko. Det kommer frem av intervjuene at ansatte ikke kjenner til at det har blitt gjennomført dokumenterte risikovurderinger på dette området, men at sikkerhetsrisikoen har blitt diskutert internt.

[4] change advisory board

I gjennomgangen av systemet RiskManager kommer det frem at kommunen har gjennomført risikovurderinger i noen år. I begynnelsen var de mest opptatt av at risikovurderingene ble gjennomført og dokumentert, men ikke så mye i hvilke form de fremsto. Det har medført at mange av risikovurderingene er dokumentert i Word dokumenter som er lagret i Risk Manager, og dermed ikke i Risikomodulen til systemet. Det kommer frem av samtaler med personvernombudet at Risikovurderinger som er lagt i et Word dokument er mer krevende å følge opp ved endringer, enn risikovurderinger i modulen. Det er også mer komplisert å vurdere om risikovurderingene og eventuelle tiltak for å redusere risikoen er fulgt opp eller utsatt. Det ble også bekreftet i kommunens internrevisjon at Risk Manager ikke alltid ble brukt til å dokumentere risikovurderinger.

I intervjuene med ansatte fremkommer det at avdeling forvaltning og utvikling ikke bruker modulen for risikovurdering i RiskManager, men at de har et eget skjema for dette.

De som jobber med informasjonssikkerheten i kommunen sier i intervjuene at de har et arbeid å gjøre i kommunen, når det kommer til å få alle ansatte til å forstå trusselbildet og sårbarheten på sikkerhetsområdet. Kommunen er mer bevisst og oppmerksom på risikoaspektet nå enn tidligere.
De som jobber med sikkerheten i kommunen har fått 1,5 timer på ledelsens gjennomgang i år. Fokus vil være det å forstå risiko og kommunisere det. Nye systemer og tjenester kommer raskt, og det er et press på å komme raskt i gang. Kommunens innføring av en ny app for aktivitetsstøtte er et eksempel på dette.

Det kommer frem av intervjuene med IT-avdelingen at i det videre arbeidet med å styrke sikkerheten i kommunen er det nødvendig å få brukerne av IT-systemene/de ansatte med på laget. De er den største usikkerhetsfaktoren. Kommunen viser til hendelsen hos Helse Sør-Øst hvor angrepet skjedde gjennom mulighet for opplasting av et bilde. Også ved Vigilo-hendelsen i Bergen og Fredrikstad var det også bare en liten bryter som kunne slås av og på. Når kommunen innførte intranett i 2014 kunne man gjøre søk på tvers av systemer og man kunne da få treff på saker som ikke var skjermet i kommunens arkivsystem. Dette er nok et eksempel på at man må ha kontroll før man setter i gang med nye systemer.

I intervjuene blir det sagt at kommunen er på god vei til å få et egnet sikkerhetsnivå sett opp mot regelverk og normer på området. Fagansvarlig sier at på den tekniske delen av systemet er de trygge på at de har et godt sikkerhetsnivå. Arbeidet med sikkerheten er basert på Datatilsynets anbefalinger. Det mangler imidlertid noe, men det grunnleggende er på plass. Som tidligere nevnt er de mer bekymret for at nye systemer, app'er med mer, ofte iverksettes for fort. Det medfører at en ikke har tid til å vurdere kritiske områder i forkant, som for eksempel; kontroll på at data kan gjenopprettes, god nok backup, logging ved hendelser, gode nok sikringstiltak osv..

Det er også en utfordring å få virksomhetene til å jobbe proaktivt med risikovurderinger. Som eksempel blir det vist til at en av virksomhetene har ment at de har gjort en risikovurdering da de tok i bruk et nytt program/app. Det viste seg at risikovurderingen bestod i at de hadde snakket om det, men det ble ikke skrevet ned og dermed ikke dokumentert.

Fagansvarlig informasjonssikkerhet sier at kommunen jobber med å balansere risiko opp mot påtrykk om endringer. Alle som skal sette i gang nye behandlinger får en sjekkliste, som sier noe om hva som må gjøres/sikres før de kan sette i gang. De som jobber med informasjonssikkerheten sier at det imidlertid ikke er tilstrekkelig forståelse i organisasjonen, for når i prosessen en gjør hvilke vurderinger. Det blir gjort mange risikovurdering, men i mange tilfeller setter en i gang behandlingene før

risikovurderingene er gjennomført. Det er viktig å finne ut av hvem som tok beslutningen om å sette i gang behandlingene når slikt skjer.

I intervjuene med ansatte på i IT-avdelingen kommer det frem at mye av fokuset på IT-sikkerhet nå, er litt selvfølgelig for de som jobber på IT-området. For den vanlige bruker er det ofte ikke like naturlig. Man må ofte ha opplevd en hendelse selv for å ta det alvorlig. Det kommer frem i intervjuene at de som jobber på informasjonssikkerhetsområdet opplever at toppledelsen tar dette på alvor, og at de sjelden møter motstand i dette arbeidet.

Det kommer frem av intervjuene at det er ulikt fra kommuneområde til kommuneområde hvordan kommunikasjonen er om IT-sikkerheten. Barnevernområdet har dette med sikkerhet i ryggmargen, det har også helseområdet med sine rutiner. I andre kommuneområder er det ulike utfordringer. Det vises blant annet til at skole- og barnehageområdet har fått begrenset med drahjelp fra sentrale myndigheter og andre leverandører, samtidig som det stadig innføres nye systemer. Det er i liten grad etablert felles retningslinjer og verktøy for å ivareta risikoen på en god nok måte på oppvekstområdet. Kommunen opplever imidlertid bedring på området, selv om risikoen på noen områder fremdeles er litt for høy.

I intervjuene med ansatte på oppvekstområdet fremkommer det at det er gjort risikovurderinger på noen områder innen skole, blant annet ved innføring av Vigilo. Det er dessverre mye som mangler av risikovurderinger når det gjelder skolene. Dette arbeidet har i stor grad blitt skjøvet ut til den enkelte virksomhet, og administrasjonen har i liten grad deltatt i dette arbeidet.

[Avsnitt unntatt offentlighet, jf. offl. § 24 tredje ledd.]

Et annet risikoområde på skole er å få på plass en erstatning for systemet *Sikker arbeidsflyt*. Vigilo skulle ha levert funksjonalitet for det, men den er ikke ferdig. Kommunen har derfor benyttet minnepinner til blant annet dokumenter knyttet til spesialundervisning. Disse skal være låst ned i arkivskapet på skolene. Ny løsning i Vigilo skulle komme på plass 9. mars.

Ansatte på IT-avdelingen sier i intervjuene at de mener kommunen har et rimelig godt nivå på IT-sikkerheten. De har heller ikke opplevd noen episoder slik som for eksempel i Bergen. De mener imidlertid at de har et stykke arbeid som gjenstår, når det gjelder prosedyrer, dokumentasjon etc. Det fremkommer også av intervjuene med ansatte på IT-avdelingen at de opplever at kommunens ansatte ikke alltid tar sikkerhetsinformasjon som kommer fra IT-avdelingen like alvorlig. De opplever at det ofte blir oppfattet som at sikkerhetsarbeidet er noe som IT kun har en egeninteresse i. De ansatte er mest opptatt av at systemene skal fungere og at det er lett tilgjengelig overalt. Det er derfor viktig og nødvendig at sikkerhetsarbeidet blir forankret et annet sted i organisasjonen for at det skal få innvirkning på sikkerhetskulturen.

I intervjuene fremkommer det at kommunen per i dag ikke har gjennomført en kartlegging av verdikjedene ved innhenting, behandling, lagring etc. av data. Personvernombudet sier at skal man skal lykkes med reelle risikovurderinger, må arbeidet på dette området spisses ut mot virksomhetene.

Kommunen har ikke gått gjennom hele arbeidsprosessen per i dag, men at det kan være nyttig å gjennomføre en slik kartlegging, dels for å bli klar over nye risikoområder og for å få hjelp til å gjøre prioriteringer. I intervjuene kommer det imidlertid også frem at kommunen jobber med et nytt helhetlig overordnet strategidokument, som ivaretar hele verdikjeden inkludert sikkerhet, kultur og GDPR.

Netsecurity fant i sin gjennomgang at kommunen har etablert flere sikkerhetstiltak. Det var ingen umiddelbare funn som måtte gjøres noe med. Netsecurity hadde enkelte områder hvor det burde iverksettes tiltak. Det ble eksempelvis gjort funn knyttet til passord på avveie. Rapport fra rekognoseringen i sin helhet følger som vedlegg til rapporten (unntatt offentlighet).

IKT-utstyr, konfigurasjon, nettverk, leverandører og systemer, samt e-post-sikkerhet

I gjennomgangen av IT-avdelingens sikkerhetssystemer fremkommer det at kommunen har et system som gir visuell oversikt over alle kommunens digitale løsninger. Eksempelvis blir det vist frem en oversikt, som synliggjør de servere som kommunen per i dag har. Klikker en på denne oversikten kan en få opp liste som viser alle serverne, med alle egenskaper og detaljer for hver server. Dette kan brukes til oppdateringer, oppgraderinger og vurdering av ressursbehov. Alt ligger som virtuelle maskiner og ikke fysiske servere. Man kan også se tidslinje og logger for hver server. Systemet viser når sertifikater går ut, hvor mange som ikke har vært logget inn de siste tre måneder og mer. I intervjuene fremkommer det at IT-avdelingen har oversikt over alle PC'er, serverparken, alle applikasjoner og alt av mobilt utstyr. Kommunen bruker ConfigManager, som gir inventaroversikt over alt av alt utstyr - alle PC'er, iPad'er og servere.

I en gjennomgang av IT-avdelingens sikkerhetssystemer fremkommer det at IT-avdelingen har et overvåkingssystem som overvåker kommunens infrastruktur og viser hendelser i infrastrukturen. Alle hendelser loggføres. Kommunen har flere overvåkingssystem som viser tilstanden til utstyr og tjenester, f.eks. om diskene begynner å gå fulle, om det er stort minneforbruk eller unormal nettverkstrafikk. Det er satt opp flere overvåkingsskjermer i driftsavdelingen hvor en løpende kan følge med på status, samt at blir det sendt e-postvarsling dersom det oppstår kritiske hendelser.

Det fremkommer av samtaler med ansatte på avdelingen at IT-avdelingen har som mål å reagere på hendelser og rette opp feil, før sluttbrukeren merker at det er en feil. De har en vaktordning på de mest risikoutsatte områdene, der konsekvensen for en feil i systemet er størst. Disse er sentralisert og alle slike henvendelser går via vaktordningene til IT-avdelingen. IT-avdelingen kan dermed bli kontaktet utenom arbeidstid dersom noe oppstår.

Det kommer frem av intervjuene med ansatte på IT-avdelingen at de har mange ansatte med lang erfaring. Når det skjer en hendelse, for eksempel da de hadde et angrep på Citrix i år, blir tiltak raskt iverksatt basert på erfaring. Det foreligger ikke skriftliggjorte rutiner for dette, men de skriver protokoll etter hendelsen. På spørsmål om det ikke er en risiko å ikke har prosedyrer på dette området, svarer ansatte at det nok kunne vært hensiktsmessig å ha en sjekkliste med oversikt over hvem som gjør hva når osv.

I testen som ble gjennomført av kommunens sikkerhetssystemer, i form av en phishing-mail, kommer det frem at IT-avdelingen reagerte på varsling om phishingen, ved å informere i interne kommunikasjonskanaler og gjennomføre tiltak som blokkering av domenet i brannmur. Det fremkommer også at Phishing-mailen ble videresendt frem og tilbake internt på IT-avdelingen, før noen kom frem til at de burde informere om phishing-mailen internt i kommunen. Informasjonen ble så lagt ut etter at dette ble besluttet.

Figuren viser andelen som ga fra seg passord, besøkte siden uten å gi fra seg passord og andelen som ikke ble påvirket.

[Figur og avsnitt unntatt offentlighet, jf. offl. § 24 tredje ledd.]

Kommunen har etablert *Retningslinjer for bruk av kontorstøtteverktøy og lagring av dokumenter*, datert 13.05.2014. Her fremkommer det i pkt. 11 informasjon om at ansatte skal gjøre en vurdering av om mottatte e-poster er sikre, dersom den vurderes til ikke å være sikker, skal den slettes umiddelbart. Det står ingenting om at det skal meldes videre.

IT-drift har et eget oppslagsverk som er tilgangsstyrt fra IT-avdelingen og kommunen har en egen server som drifter dette. Her har de oversikt over alle sine systemer, hvordan de fungerer, og vanlige hendelser. Her fremgår også informasjon om hvilken database og server systemene benytter. Her skal all informasjon som er nødvendig for å drifte systemene ligge. Støttesystemer ligger også her. Et annet system kommunen har viser om backupen fungerer som den skal. Vedlikeholdet ivaretas også i dette systemet. IT-avdelingen gjennomfører jevnlig sikkerhetsoppdateringer etter intern rutine.

Det kommer frem av intervjuene at kommunen også oppdaterer konfigureringer kontinuerlig. Prosedyren er at dette gjøres månedlig og mange av konfigurasjonene er automatisert. Noen konfigurasjoner gjøres manuelt, blant annet på grunn av risiko for at noe går feil ved oppdateringen. Kommunen har systemer for å installere sikkerhetsoppdateringer. Kommunen har etablert et råd for å fange opp andre sårbarheter. Kommunen har også avtale med HelseCert, og får rapporter derfra når det er oppdaget nye trusler. I intervjuene kommer det frem at medlemskapet hos HelseCERT gir gode vurderinger og følger tett opp kritiske sårbarheter. De er igjen linket mot NorCERT[5]. Dette er en ordning som kommunen synes fungerer bra, og de får fortløpende informasjon om sårbarheter av betydning.

[5]Norwegian Computer Emergency Response Team - en funksjon i Nasjonalt cybersikkerhetssenter

Det kommer frem i intervjuene at kommunens ledergruppe har vedtatt at ansatte kun skal ha en pc hver. Det er imidlertid noen unntak. Noen ansatte har mer enn en PC. De har da som regel en hjemme-PC og en på kontoret. PC-en på kontoret blir tatt vare på når det gjelder oppgraderinger og sikring, men den som alltid står hjemme hos den ansatte blir ikke tatt vare på i samme grad. Det henger blant annet sammen med løsningen som var på maskinen da maskinen ble kjøpt. I det nye systemet vil dette være løst. Det kommer frem at denne risikoen kan løses ved at de ansatte tar med hjemme-PC til IT-avdelingen for oppdatering og sikring. På spørsmål om det finnes en oversikt over alle PC-ene som eventuelt er hjemme-PC for ansatte, er svaret at det ikke finnes en fullstendig liste på dette. IT-avdelingen har imidlertid sikkerhetstiltak dersom den ansatte ikke har logget seg inn på 60 eller 90 dager, som fører til at kontoene blir sperret. Da slutter PC'en å fungere. Det kommer frem at det finnes mange veldig gamle PC'er som er kommunens eiendom der ute, og noen er opp til 12 år gamle. Dersom disse PC-ene ikke har blitt slettet fra systemet og brukes til å logge inn på fagsystemer, skjer det som oftest via Citrix. Citrix har god beskyttelse, det er derfor ikke en veldig stor eksponering.

Kommunen har ulike antivirusprogram på alle servere, klienter, skyer, e-post osv. Kommunen sørger for at alle brannmurer blir oppdatert dersom det oppdages nye trusler i andre land og områder. Antivirusprogrammet kommuniserer med denne brannmuren, og blir med dette også oppdatert kontinuerlig.

Systemansvarlig for det enkelte fagsystem har ansvaret for å følge opp det enkelte systemet. Det ligger logger i hvert fagsystem. For eksempel på helseområdet, logger Gerica alle sine brukere med hva, hvor og når. IT har ingen brukere med administratortilgang til kommunens fagsystemer.

I intervjuene med ansatte på helseområdet fremkommer det at når det gjelder Gerica, hvor kommunen håndterer sensitive opplysninger, oppdaterer IKT systemet. Noen ganger gjøres oppdateringer med bistand fra leverandør. I det siste har kommunen ofte kjøpt denne tjenesten, fordi det blir stadig mer omfattende, og fordi det er en risiko i forbindelse med oppdateringer. Kommunen har avtaler som regulerer håndteringen av disse oppdateringene.

I oversendt dokumentasjon foreligger en oversikt over de fagsystemene som benyttes i kommunen, hvem som er leverandøren av systemet og hvem i kommunen som er delegert systemeier, forvalter og driftsansvarlig.

I intervjuene vises det til at det må skilles på leverandører av systemer til kommunen og leverandører av IT-tjenester. Når det gjelder leverandører av utstyr og programvare, er det IT-drift som følger opp dette gjennom utstyrets/programvarens levetid. Leverandører av IT-tjenester blir regulert gjennom databehandler avtaler. Databehandleravtalene skal sikre at personopplysninger blir behandlet i samsvar med regelverket og skal sette en klar ramme for hvordan databehandleren kan behandle opplysninger på vegne av kommunen. Kommunen har etablert databehandleravtaler og oversikt over leverandører, og at leverandørene er i henhold flere krav.

I en beskrivelse fra kommunen om *Nettverk og samarbeidspartnere* på IT-sikkerhet, mottatt 10.01.2019, angir kommunen at de samarbeider på flere arenaer innen IT-sikkerhet. IT-avdelingen har løpende samarbeid med ulike leverandører på det systemtekniske området. Kommunen deltar i ulike nettverk som Digi Viken Øst[6], KiNS[7] og HelseCERT[8]. Kommunen deltar også i Østfold-nettverk for personvernombud og har opprettet et eget GDPR-nettverk internt. Kommunen har et eget team på

[6] Samarbeid mellom flere østfoldkommuner for samhandling og digital utvikling
[7] Foreningen kommunal informasjonssikkerhet
[8] Helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet

kommuneområde Helse og velferd, som arbeider med digitalisering og IT-løsninger i helsesektoren. Det fremkommer videre at nettverk for informasjonssikkerhet per i dag er sammenfallende med personvernnettverket i kommunen, ledet av personvernombudet. Etter opprettelse av egen rådgiverstilling som fagansvarlig informasjonssikkerhet, vil dette nettverket etterhvert bli utvidet med mer dedikerte informasjonssikkerhetsrelaterte oppgaver.

Det kommer frem i intervjuene at kommunen har laget en applikasjonsoversikt. De har oversikt over antall PC'er og annet utstyr. Det blir sagt i intervjuene at kommunen har for mange applikasjoner i spill, med stor spredning. Dette jobber de systematisk med, blant annet med en porteføljestyring. De ønsker å få ned antall applikasjoner/leverandører og jobber med dette sammen med andre kommuner i Viken (DigiViken).

Tilgangskontroll og autorisering

Det kommer frem av systemgjennomgangen i RiskManager at ansatte har tilgang til dokumentene og prosedyrene som gjelder deres eget arbeidsområde. Under området *Informasjonssikkerhet* ligger det flere prosedyrer og rutiner som skal bidra til å øke sikkerheten på området. Dette området har alle ansatte tilgang til.

I Risk Manager foreligger det en oversikt over viktige dokumenter for nye medarbeidere. Brosjyren «*Min elektroniske arbeidsplass»* gir blant annet informasjon om hvorfor informasjonssikkerhet er nødvendig og hvordan ansatte skal ivareta fysisk og elektronisk sikkerhet, tilgangsrettigheter og passord. Den informerer også om at ansatte skal være oppmerksomme på virus og annen skadelig programvare, om innkjøp, tilkobling og avhending av utstyr. Videre at kun datautstyr som er godkjent og konfigurert av IT-avdelingen skal kobles til kommunens nettverk, og at det ikke er tillatt å laste ned og installere programvare til eget bruk eller låne ut egen brukeridentitet til andre eller å avsløre eget eller andres passord. Ved endring av passord skal kommunens gjeldende regler for dette følges.

Kommunen har oversendt dokumentet *Brukerdokumentasjon ansattmelding*, datert 25.04.2014. Her kommer det frem at *Ansattmelding* er et program for å sentralisere alle meldinger vedrørende administrasjon av ansatte og deres stillinger, generelle datatilganger, telefoni, nøkkelkort med mer. Systemet henter også informasjon fra Visma HR. *Ansattmelding* er et system der IT-avdelingen og ledere kan administrere ulike tilganger for ansatte i sin virksomhet, ved nyansettelser, når ansatte slutter eller endrer stillingsinnhold i kommunen. Blant annet generell datatilgang, Visma Enterprise, mobil- og kontortelefon, tilgang til Infotorget, fjerntilgang, sak- og arkivsystemet med mer.

I samtale med ansatte i IT-avdelingen sies det at når noen slutter i kommunen, legges kontoen i karantene før den slettes etter en viss tid. Det er systemet som styrer dette. Når det kommer inn en melding om at en ansatt slutter, deaktiveres brukerkontoen slik at den ansatte ikke kan logge inn. I noen tilfeller er det behov for å hente ut informasjon fra brukerkontoen til den som har sluttet, derfor slettes den ikke før etter en viss tid. Ved behov for å hente ut informasjon innhenter man tillatelse fra brukeren. I noen tilfeller foreligger det også rettslig krav om å hente ut informasjon. Det er prosedyrer på dette. Det kommer frem av intervjuene med ansatte på helseområdet at de i den månedlige egenkontrollen også sjekker om tilganger er fjernet for ansatte som har sluttet.

Kommunen har en samlet tilgangsoversikt over alle tilganger som har blitt gitt i kommunen. Det blir sagt i intervjuene at dette burde vært en del av et felles management system i fremtiden. Det blir opplyst om at kommunen har blitt strengere når det gjelder å gi tilganger til kritiske systemer/sensitive opplysninger. Rettighetene til de ansatte er begrenset til spesielle fagområder.

Det kommer frem i intervjuene at når det skal gis tilganger til nyansatte, blir disse først registrert i HR-systemet, da går det melding om at personen blir opprettet i AD – digital ident. Avdelingen personen blir plassert inn i har en del rettigheter. Godkjenningen til å få tilgang til fagapplikasjoner, avhenger av hvilken avdeling/virksomhet personen er ansatt i. Når personen er registrert i applikasjonen er det systemeier som styrer hvilke tilganger den ansatte har innen i applikasjonen. Policy er at alt som er sensitivt av informasjon skal inn i fagsystemene. Det gis tilgang til nettverk, infrastruktur etc. basert på tjenstlig behov.

Det kommer frem av intervjuene at kommunen tidligere hadde et eget IT-nett med servere og PC-er, der alt var i ett nett. De er nå i prosess for å få til separate nett på flere områder, noe som gjør systemet mindre sårbart.

[Avsnitt unntatt offentlighet, offl. § 24 tredje ledd]

Kommunen har tofaktor-autentisering på all tilgang som skjer utenfra; fra hjemmekontorer og all annen tilgang via Internett. Det er også innført tofaktor-autentisering på tilgang til skytjenester som kommunen bruker, f.eks. Office365.

Videre kommer det frem av intervjuene med ansatte på oppvekstområdet at det er ulike løsninger som har to-faktorinnlogging, for eksempel PAS[9]. På andre områder er det FEIDE[10]-innlogging, eller andre proprietære løsninger.

Kommunen jobber med å bytte ut alle PC'er, som ikke lenger kan oppdateres. Det blir sagt i intervjuene at det oppleves som noe utfordrende å få til en forståelse for at dette er nødvendig for IT-sikkerheten. Samtidig blir det sagt at det nå er et mye større fokus på informasjonssikkerheten, enn det var for noen år siden.

[Avsnitt unntatt offentlighet, offl. § 24 tredje ledd]

[9] Prøveadministrasjonssystemet fra Utdanningsdirektoratet
[10] Felles Elektronisk IDEntitet

Når det gjelder tilganger til fagsystemer, for eksempel Vigilo har lærerne kun tilgang til sin(e) klasse(r). Dersom en elev for eksempel får tak i innloggingsinformasjonen til en lærer vil skadeomfanget være avgrenset til denne lærerens tilgangsgruppe. For å få tilgang til all informasjon på en skole eller i kommunen må man gjennom en overordnet konto. Kommunen jobber nå med å få på plass to-faktor autentisering også for lærer-innlogging. Foreldre kan også logge seg inn i systemet, og bruker minid eller andre godkjente sikkerhetsløsninger. Sokrates, det andre fagsystemet som skolen bruker, er også beskyttet av to-faktor autentisering.

I intervjuene med ansatte på IT-avdelingen fremkommer det at de ikke har tilgang til dataene i de ulike fagsystemene, og de har heller ikke brukertilgang til systemene. IT ansatte har ikke tilgang til å opprette eller slette brukere, det er det systemeier som er ansvarlig for. IT-drift skal sørge for at data ikke går tapt, ta backup osv.

I intervjuene fremkommer det at kommunen også sørger for sikker pålogging ved kun å ha autoriserte PC'er i kommunens nettverk. Det vil si at all pålogging skjer med brukernavn og passord. Det er kun registrerte brukere i AD som har tilgang i kommunens interne nett og systemer. På skytjenester er det to-faktor autentisering. For hjemmekontor brukes VPN-forbindelse og to-faktor autentisering. Kommunen har fysisk tilgangssikring til datarom.

[Avsnitt unntatt offentlighet, offl. § 24 tredje ledd]

I intervjuene med ansatte på oppvekstområdet blir det sagt at de viktigste områdene knyttet til IT-sikkerhet i skolen, er at ansatte kjenner og følger rutiner rundt bruk av PC og forvaltning av passord. Det er også viktig at ansatte kan låse PC'en og at en ikke blir observert når en skriver inn passordet etc.

Sikring av helse- og personopplysninger.

Det kommer frem av intervjuene at det på helse og velferdsområdet er svært mange prosedyrer og rutiner knyttet til informasjonssikkerhet. Helse var tidligere ute enn andre områder og har vært mye styrt og hjulpet på dette området fra overordnede departementer og direktorater. Kommuneområde helse og velferd har fulgt norm for e-helse en god stund. På helseområdet er det to systemansvarlige for systemet Gerica. Det jobbes mye med velferdsteknologi og innovativ arbeidsmetodikk. Kommunen har fokus på dette, fordi prognosene blant annet viser stor mangel på sykepleiere i årene som kommer. Arbeidet med velferdsteknologi startet kommunen med i 2009. De startet med medisineringsstøtte, deretter kom E-senior. Kommunen har digitale trygghetsalarmer, avstandsoppfølging via iPad, GPS-sporing med mer. Kommunen jobber nå med utviklingen av digitalt tilsyn.

I intervjuene fremkommer det at de som jobber med sikkerhet og forvaltning av Gerica har møte med direktør kommuneområde helse og velferd hver 14. dag. De opplever at det er stor interesse for området fra ledelsens side, og at de gjennom disse møtene får mer tyngde i formidlingen ut til ansatte.

Det kommer frem av norm for e-helse at ny lovgivning, teknologisk utvikling og store enkelthendelser med mye oppmerksomhet, har ført til en økt oppmerksomhet rundt personvern og informasjonssikkerhet i helse- og omsorgssektoren. Som en følge av dette har kommunen fått et økt behov for oppdatert veiledning og en modernisert og oppdatert Norm for informasjonssikkerhet og personvern i helse- og

omsorgssektoren (Normen). Normen justeres fortløpende opp mot nye overordnede regelverk eller generelle normer som gjelder for alle virksomhetsområder. Som tidligere nevnt har dette ført til at helseområdet i kommunen nå har fjernet noen av sine egne sikkerhetsinstrukser og mål, og har sluttet seg til kommunens felles sikkerhetsinstruks og -mål. Felles instrukser og prosedyrer på informasjonssikkerhetsområdet er å finne på nivå 1 i Risk Manager. Instrukser og prosedyrer på informasjonssikkerhetsområdet som gjelder det enkelte virksomhetsområdet er å finne på nivå 2.

Helse og velferdssektoren har i mange år hatt fokus på informasjonssikkerheten. I rapporten *Elektronisk pasientjournal i omsorgstjenesten - Status, utfordringer og behov*, utarbeidet av Helsedirektoratet oktober 2014 fremkommer det at Gerica ble utviklet for å understøtte søknadsprosessen, saksbehandling og fakturering. Systemet ble videreutviklet ut fra behov meldt fra tjenesten, i første omgang med hovedfokus på hjemmetjenesten og videre på nasjonale prosjekter for elektronisk meldingsutveksling. Informasjon overføres over Norsk Helsenett[11].

Kommunen har oversendt dokumentet *Sikkerhetssamtale og revisjon Norsk Helsenett 2014* hvor det fremgår vurderinger av om kommunen utgjør en risiko for Norsk Helsenett. I dokumentet fremkommer det at kommunen har etablert eget gjestenett, at kommunen følger opp innmeldte avvik og at ansatte på helse- og sosialområdet kjenner normen for e-helse. Dokumentet konkluderer med at kommunen ikke tilfører helsenettet økt risiko gjennom sin tilkobling. Det kommer også frem av intervjuene at alt på helseområdet er kryptert fra ende til ende ved SSL, VPN etc. All data i transport er sikret mot avlytting.

I 2017 og 2018 er det gjennomført internrevisjoner på virksomheter innen helse og sosialområdet i kommunen. I revisjonen fra 2018 fremkommer det at ansatte synes det er vanskelig å finne fram til den relevante informasjonen om informasjonssikkerhet, i blant annet RiskManager og på Sarpedia.

Avvik, internkontroll og rapportering

I dokumentet *Retningslinjer for kvalitetssystem* står det at i avviksmodulen til RiskManager, skal alle avvik som oppdages registreres. Ledere på alle nivåer kan her følge med på omfanget og få oversikt over meldte avvik. Registrering av avvik skal gi virksomhetene og organisasjonen et grunnlag for å vurdere om oppgavene utføres slik de skal.

Kommunen har en *Prosedyre for avviksbehandling*, datert 20.10.2017. Her fremkommer det at alle ansatte er ansvarlige for å rapportere avvik innenfor sitt ansvars-/arbeidsområde. Det fremgår også at avvik som er avdekket etter en internrevisjon eller et tilsyn også skal registreres i avvikssystemet. Det fremgår videre at kommuneledelsen får fremlagt rapport på oppfølging av registrerte avvik fire ganger i året.

I *Brosjyre for informasjonssikkerhet i Sarpsborg kommune*, 10.09.2015 og «*Min elektroniske arbeidsplass»* fremkommer det også at «*alle sikkerhetshendelser skal rapporteres til nærmeste overordnede eller til IKT-drift. Alle slike rapporter vil seriøst bli fulgt opp for å forhindre og/eller begrense eventuelle skader. Dersom en hendelse er et brudd på lov, prosedyre eller reglement skal det registreres som avvik i RiskManager*».

Det var en økning i antall totalt meldte avvik fra 2017 til 2018 (fra 40 til 80). Det var en forventning om en ytterligere økning fra 2018 til 2019, men i 2019 var det en svak nedgang (fra 80 til 74). Personvernombudet sier at det er vanskelig å gi et klart svar på hvorfor det var en svak nedgang i 2019.

[11] Norsk Helsenett utvikler, forvalter og drifter nasjonale e-helseløsninger og infrastruktur, og sørger for sikker samhandling i helsesektoren.

Kommunen har også *Prosedyre for håndtering av alvorlige sikkerhetsbrudd*, datert 19.06.2019, som omhandler brudd på personvernregelverket, melding til parter og til Datatilsynet.

Det kommer frem i intervjuene at det å melde avvik bør være et innarbeidet system i kommunen. Direktør for KTE sier imidlertid han tror at det er noe underrapportering og ønsker at alle avvik blir registrert. Av de avvikene som er meldt inn er ca. 50 % reelle avvik. Det oppleves som en utfordring at RiskManager er noe utdatert og at systemet derfor gir få analysemuligheter og kvalitative oversikter. Det kommer frem av intervjuene at alle avvikene som blir meldt inn, også blir fulgt opp.

I systemgjennomgangen fremkommer det at kommunen benytter en eldre versjon av RiskManager. I samtaler med personvernombudet kommer det frem at systemet mangler noen funksjoner, som kunne sikret bedre oppfølging av blant annet avvik. Avviksmeldingene går kun til virksomhetsleder, som eier avviket på et overordnet nivå. Det hadde vært ønskelig at bla personvernombudet og fagansvarlig informasjonssikkerhet fikk melding når det ble meldt et avvik. Kommunen er i prosess med å finne et nytt system for kvalitetsstyring.

Det kommer frem i intervjuene at de som jobber med informasjonssikkerheten har stusset over nedgangen i antall rapporterte avvik. Kommunen har jobbet mye med å få ansatte til å registrere avvik generelt. Nedgangen i antall meldte avvik kan begrunnes i flere ting, som tidspress, dobbeltkommunikasjon fra ledere og manglende kultur for å melde avvik i noen virksomheter. De ser at det særlig i oppvekstsektoren er få meldte avvik. Dette er derfor et område de vil jobbe mer med internt i kommunen. Blant annet vil det bli tema på kommunedirektørens virksomhetsledersamlinger, som de gjennomfører fire ganger i året.

I intervjuene med ansatte på helseområdet fremkommer det at de har et innarbeidet system for å melde avvik. Det blir også meldt flest avvik på helse, fordi det er en kultur for å melde avvik. Det blir sagt i intervjuene at det å melde avvik ikke oppfattes som angiveri, men at det er for å få gjort ting riktig. Det å ha tydelige definisjoner på normen for e-helse og når det skal meldes avvik på det området, har de diskutert. Det kan av og til være vanskelig med tydelige felles definisjoner, men terskelen er ikke høy for å melde avvik på helseområdet. De fleste avvikene er imidlertid på selve utføringen av tjenestene.

I intervjuene med ansatte i IT-avdelingen fremkommer det at det ikke er meldt så mange avvik på IT-sikkerheten. IT-avdelingen har lukket flere innmeldte avvik, som i prinsippet ikke er å definere som avvik. Det fremkommer at det antagelig er en underrapportering på avvik fra IT-avdelingen.

Det kommer også frem av intervjuene at hittil meldte sikkerhetsavvik viser at de fleste avvikene er eid av andre deler av virksomheten. I intervjuene blir det sagt at IT-avdelingen er mer en bidragsyter med data, enn håndterer av avvik og at det teknisk sett handler mest om systemene fungerer eller ikke. Utover det vil det for eksempel være Microsoft som er ansvarlig for sikkerhetshull.

Det fremkommer av dokumentasjon at kvalitetssystemet fungerer som kommunens daglige internkontrollsystem, og skal oppfylle de kravene som blant annet stilles internt og i lov og forskrift. Virksomhetsleder/avdelingsleder har ansvar for kvalitets- og internkontrollsystemet for sin egen virksomhet/avdeling, og for å påse at prosedyrene innenfor egen virksomhet etterleves. De har også ansvar for at internkontrolldokumenter legges inn og oppdateres i kvalitetssystemet RiskManager.

I intervjuene sier direktør KTE at han mener at kommunen har god kontroll på arbeidet på sikkerhetsområdet. Han ser imidlertid at det fremdeles er en jobb å gjøre på dette området. Kommunen har et veldig fokus på det og de opplever at de blir hørt og prioritert i virksomheten. De jobber nå med å bygge sikkerhetskulturen. Han sier at må-kravene er godt ivaretatt.

Det de savner er et ordentlig management system på sikkerhetsområdet, der rutiner og rapporteringer på området kan samles. Fagansvarlig informasjonssikkerhet sier at det har vært en forskjell mellom stat og kommunen når det gjelder prioritering av IT-/informasjonssikkerhet. Digitaliseringsdirektoratet (tidligere Difi[12]) har gitt mange av premissene for statlig sektor på IT-sikkerhetsområdet. Selv om direktoratet har sagt at føringene kan være aktuelle for kommunene også, så står kommunene friere og må selv prioritere hvordan de vil jobbe med dette området. Det er få lover og forskrifter på området, men det er en del normer.

I dokumentet *Rutine for egenkontroll, informasjonssikkerhet*, datert 11.08.2015 fremkommer det at egenkontrollen er ment å sikre at sikkerhetsmål og strategier, organisering og sikkerhetsbestemmelser, samt forsvarlig behandling av personopplysninger blir etterlevd. Egenkontrollen skal også danne grunnlag for forbedring av informasjonssikkerheten. Det er virksomhetsleder/avdelingsleder som er ansvarlig for at egenkontrollen gjennomføres årlig. I rutinen står det at «*avvik fra denne rutinen skal håndteres og varsles i henhold til avviksrutine»*. Sikkerhetsansvarlig i kommunen har ansvar for at virksomhetene dokumenterer resultatene fra egenkontrollen. Egenkontrollen er hjemlet i personopplysningsforskriften[13].

Egenkontrollen er basert på en egen sjekkliste, *Sjekkliste for egenkontroll av informasjonssikkerhet ved enhet (navn)*, sist revidert 02.01.2020. Elementer i sjekklisten er blant annet om ansatte har fått utdelt folderen «*Min elektroniske arbeidsplass*», om ansatte har fått nødvendig IKT-opplæring, om enheten har rutiner for å sikre at alle medarbeidere har riktige tilganger til IKT-systemene, at medarbeidere som slutter eller endrer stilling ikke lenger har tilgang til fagsystemer og om enheten har gjennomført risikovurderinger av informasjonssikkerhet det siste året. Det kommer frem i intervjuene at noe informasjon fra egenkontrollene brukes i kommunens internrevisjoner, men dette er ikke systematisk. Egenkontrollene skal gjennomføres årlig og senest november hvert år. Ansatte som jobber med informasjonssikkerheten i kommunen sier at det er en viss feilmargin i egenkontrollene. Det er flere som antakelig svarer det de tror leder og andre ønsker å høre.

I intervjuene med ansatte som jobber med e-helse kommer det frem at på helseområdet gjennomføres det månedlige egenkontroller. Det er virksomhetene som skal gjennomføre denne egenkontrollen. Resultatene av disse kontrollene leveres inn to ganger per år. Resultatene blir formidlet på ledelsens gjennomgang. Egenkontrollen består i et skjema i Excel på 20-25 punkter, som virksomhetene skal gå gjennom. Det blir utarbeidet rapporter på bakgrunn av resultatene fra egenkontrollene. Dette er en egenkontroll spesielt laget for helseområdet og er et annet type skjema enn det som brukes på andre områder i kommunen.

Dokumentet IKT-reglement, udatert, er en del av *Sjekkliste for egenkontroll av informasjonssikkerhet*. I dokumentet fremkommer det at ledere skal rapportere en gang pr år på om medarbeiderne har signert IKT-reglementet. Signering av IKT-reglementet gjøres ved å gjennomføre E-læringskurset «*IKT-reglementet*» som ligger i Læringsportalen. Dokumentet beskriver videre fremgangsmåten for lederne.

Det kommer frem av dokumentasjonen at internrevisjonsrapportene viser til regelverket som ligger til grunn for revisjonen. Følgende regelverk nevnes; lov om behandling av personopplysninger (personopplysningsloven) forskrift om behandling av personopplysninger (personopplysningsforskriften), Kommuneloven §§ 20.2, 23.2 og rammeverk som Sarpsborg kommunes styringssystem for informasjonssikkerhet.

[12] Direktoratet for forvaltning og IKT

[13] Revisjonen legger til at personopplysningsforskriften ble opphevet i 2018.

Sarpsborg kommunes internrevisjoner er basert på COSO[14]-modellen. Det fremkommer av internrevisjonsrapporter at revisjonene vurderer noen områder på IT-sikkerheten i virksomhetene. Utgangspunktet for revisjonene er vern av personopplysninger, og i mindre grad kommunens IT-sikkerhet som sådan, samtidig som disse områdene naturlig nok må sees i sammenheng. På de fleste områdene som blir vurdert i revisjonene, er bruken av ulike digitale verktøy et element. Revisjonene vurderer blant annet virksomhetenes fysiske sikring, sikring av dokumenter som er lagret digitalt, bruk av minnepinner, ansattes IKT-kompetanse, virksomhetenes prosedyrer og risikovurderinger, samt avviksmeldinger.

Plan for internrevisjon utarbeides hvert år, både på bakgrunn av risikovurderinger og med en tanke om at de fleste virksomheter i kommunen skal være gjenstand for kontroll. Utvalg til internrevisjoner er basert på en fordeling på kommuneområdene. I tillegg gir direktørene, og de som jobber på sikkerhetsområdet innspill basert på risiko. I et møte i forkant av de årlige revisjonene blir den enkelte virksomhet vurdert ut fra hva som er deres risikoområder. Personvernombudet sier i intervjuene at utvalg til revisjonene har endret seg litt over tid. Kommunen har en tanke om at det bør gjennomføres internkontroller i alle kommunens virksomheter, men personvernforordningen er mer tydelig på at man skal jobbe risikobasert. Internkontrollene er innrettet på en sånn måte at de tar for seg ulike områder innen sikkerhetsarbeidet. Utgangspunktet for revisjonene er om virksomhetene håndterer personopplysninger i tråd med regelverket. Derfor er både informasjonssikkerhet og IKT-sikkerhet en del av internkontrollene. I kontrollene etterspørres ofte virksomhetenes sikkerhetskultur. Det fremkommer av intervjuene at i internkontrollene som gjennomføres blir ansatte ute i virksomhetene også spurt om de kjenner til kommunens sikkerhetsmål og –strategi. Kommunens controller legger til at internrevisjonene handler mye om hvordan ansatte i kommunen registrerer og behandler informasjon, spesielt informasjon om kommunenes brukere.

Det kommer frem av intervjuene at kommunen jevnlig har gjennomført internrevisjoner siden 2016. Vi har mottatt åtte rapporter fra gjennomførte internrevisjoner i Sarpsborg kommune. Revisjonene er gjennomført i perioden 2017 til 2019. Revisjonene er gjennomført ved ulike virksomheter i kommunen.

De som jobber med sikkerhetsområdet svarer litt ulikt på hvor mange internrevisjoner kommunen gjennomfører i året. Noen sier 2 til 3, andre 3 til 4 og noen 4 til 5. Det er en gruppe på 3-4 fagpersoner som gjennomfører revisjonene. Fagansvarlig informasjonssikkerhet og personvernombudet er deltakere på disse revisjonene, sammen med kommunens controller og rådgiver KTE. Den siste internrevisjonen som ble gjennomført, ble gjennomført med IT-avdelingen, og rapporten er nylig ferdigstilt. Det kommer frem av intervjuene at det er kommuneledelsen som velger ut virksomheter til revisjon på grunnlag av innspill på ledelsens gjennomgang.

De som gjennomfører internrevisjonene er opptatt av at disse revisjonene ikke skal oppleves som at de er ute etter å «ta» noen, men at de kan hjelpe i til i virksomhetenes forbedringsarbeid. Det fremkommer av intervjuene at når revisjonen er gjennomført utarbeides det en rapport. Rapportene inneholder blant annet funn og tiltak til oppfølging. Dette blir sendt til den reviderte virksomheten/avdelingen. Funn fra revisjonen blir forankret i kommunens ledergruppe. Ansvaret for å følge opp videre ligger hos kommunens controller. På neste internrevisjon blir det sjekket ut om tiltakene er fulgt opp.

Funn fra internrevisjonene blir registrert som avvik på den enkelte virksomhet i RiskManager. Der legges det inn tiltak som skal til for å lukke avviket også. Det utarbeides tiltak på flere nivå både for den enkelte virksomhet, for ledernivået osv. Der revisjonen viser at det er nødvendig med mer overordnede

[14] Committee of Sponsoring Organisations of the Treadway Commission

tiltak, blir dette lagt til kommunedirektørens stab. Tiltakene legges på det nivået det er nødvendig å iverksette tiltak på. Revisjonene gjøres på vegne av kommunedirektøren. Direktøren for det området som blir revidert mottar alltid kopi av rapportene og blir alltid informert. Resultatene fra internrevisjonene brukes til læring for andre virksomheter også.

Det fremkommer i samtlige rapporter at det er en relativt stor andel ansatte som ikke kjenner til brosjyren *«Min elektroniske arbeidsplass»* og at noen ansatte ennå ikke har gjennomført obligatorisk opplæring i IKT-reglementet. I tre av enhetene som var gjenstand for internrevisjon i 2018 sier henholdsvis 43 %, 63 % og 4,6 % av medarbeiderne at de som har mottatt denne. I ledelsens gjennomgang fremkommer det en rapportering fra enhetene i kommunen der hele 82 % av medarbeiderne har fått utdelt folderen *«Min elektroniske arbeidsplass»*.

I den forrige revisjonen som ble gjort på IKT ble det gitt 13 anbefalinger. 12 av 13 gikk på rutiner ellers i organisasjonen, det var kun én anbefaling som var IT-teknisk og det var knyttet til to-faktor innlogging.

I Rutine for ledelsens gjennomgang, informasjonssikkerhet, datert 11.08.2015 fremkommer det at ledelsens gjennomgang skal utføres en gang per år. Ledelsens gjennomgang skal blant annet vurdere resultater og konklusjoner fra risikovurderinger og egenkontroll, avvik og hendelser, behov for oppdateringer og endringer av rutiner og prosedyrer og gi forslag til forbedringstiltak. Temaene som var gjenstand for ledelsens gjennomgang i 2018 var trusselbildet/hendelser i 2018, sikkerhetsmål, -strategi og –organisering, status om GDPR -arbeidet, personvernombudets rolle, interne revisjoner av informasjonssikkerhet i 2018, status fra virksomhetene 2018 og tiltak framover.

Beredskapsplan og -øvelse

I *Beredskapsplan Sarpsborg kommune*, vedtatt 29.06.2012 (og revidert årlig) fremkommer det at kommunen skal gjennomføre årlige øvelser, hvor man øver ulike deler av kommunens krisehåndteringsorganisasjon og sikrer at beredskapsplanen er funksjonelt utformet og kjent for alle som bør kjenne til innholdet i den. Videre står det at ROS-analysen[15] skal danne grunnlaget for utforming av beredskapsplan. Planen har flere delplaner deriblant Delplan IKT. Det er direktør KTE som er ansvarlig for denne. Planen ble sist oppdatert 9.01.2020. Planen viser beredskapsmessige forhold på IKT området, og inkluderer varslingsliste for IKT- personell under uønskede hendelser og ressursoversikt på IKT- området. I planen er det definert hva som er representative uønskede hendelser innen IKT, og det er definert hvilke aktiviteter som skal iverksettes ved hver evt. uønsket hendelse.

Helhetlig ROS-analyse Sarpsborg kommune 2019 ble vedtatt i bystyret 26.09.2019. Analysen er gjennomført av Norconsult. Analysen er avgrenset til temaet samfunnssikkerhet. Elementer i ROS-analysen som er sentrale i denne revisjonen er *Alvorlige tilsiktede og utilsiktede IKT-hendelser*, samt svikt i ekomtjenester. Her fremkommer det en vurdering av kommunens sårbarhet og forslag til tiltak.

Det kommer frem av intervjuet at i arbeidet med beredskapen i kommunen, har IT-sikkerhet/cyber-security blitt løftet til øverste nivå i beredskapsplanene. Det er laget egne scenarier der kommunen også har fått tydeliggjort IT-sikkerhetsutfordringer.

I intervjuene kommer det frem at kommunen ikke har gjennomført øvelser som tester planverket på IT-området per i dag. Det er gjennomført noen øvelser i småskala. Blant annet hadde kommunen noen studenter til å kjøre test mot ledelsen. Det fremkommer at noen kommuneområder er bedre til å øve IT-sikkerhet enn andre. Det sies imidlertid i intervjuene at delplanene i liten grad har vært gjenstand for øvelser og at IT-sikkerhet er et område de burde ha øvd på. Det kommer frem av intervjuene at det er et

[15] Risiko- og sårbarhetsanalysen

ønske fra de som jobber innen IT-sikkerheten at kommunen i større grad burde ha en øvet sikkerhetsorganisasjon.

2.3 Revisors vurderinger

Mål, strategi og organisering

Digitaliseringsdirektoratet sier i sin veileder til informasjonssikkerhet at offentlige virksomheter i henhold til eForvaltningsforskriften skal etablere mål og strategi for informasjonssikkerhet.

Det er vår vurdering at kommunen har etablert mål og strategi for informasjonssikkerheten. Vi legger blant annet til grunn at dokumentene *Sikkerhetsmål og sikkerhetsstrategi, Utkast til målbilde for kommuneområde teknologi og endring (KTE)* og *Digitaliseringsstrategi for Sarpsborg kommune* gir overordnede føringer for informasjonssikkerheten, samt stiller krav og forventninger til måloppnåelse og regeletterlevelse på området.

Videre finner vi at kommunen har utarbeidet retningslinjer for hvordan sikkerhetsarbeidet skal organiseres og gjennomføres. Gjeldende retningslinje er ikke oppdatert i henhold til dagens organisering, men utkast til nye retningslinjer ivaretar ansvar og organisering på en tydelig og avklart måte i tråd med dagens organisering.

Risikostyring, gjennomføring av risikovurderinger og egnet sikkerhetsnivå

Det er flere kritiske områder i kommunen som er avhengig av god sikkerhet, som å opprettholde liv og helse, og tilgang på blant annet strøm og vann. Den digitale utviklingen på mange områder skjer imidlertid raskt, og for å kunne møte denne utviklingen er det en forutsetning at sikringstiltak er på plass. Det fremkommer av den fremlagte dokumentasjonen at risikovurderinger skal gjennomføres og dokumenteres minimum en gang i året, både før nye behandlinger av personopplysninger igangsettes og ved endringer som kan påvirke informasjonssikkerheten. Det er den enkelte virksomhetsleder, som er delegert ansvaret for at rutinen etterleves innenfor sin virksomhet. Det er vår vurdering at kommunen har etablert tydelig ansvarsfordeling i risikostyringen, og at risiko følges opp på ulike nivåer i kommunen.

Av kvalitetssystemet og intervjuene ser vi at kommunen har gjennomført risikovurderinger i noen år. Det er derfor vår vurdering at kommunen gjennomfører risikovurderinger på informasjonssikkerhetsområdet. Det er imidlertid litt lite systematikk i hvordan dokumentasjonen på gjennomførte risikovurderinger er lagret. Noen vurderinger fremkommer i Word dokumenter i Risk Manager, andre i kvalitetssystemets risikomodul og deler av helseområdet bruker eget skjema for risikovurderinger. Det fører til at det kan være utfordrende å få en god oversikt over de risikovurderingene som er gjennomført og tilsvarende også mer krevende å følge opp.

Det er også vår vurdering at risikovurderingsbegrepet ikke er entydig definert i alle virksomheter. Vi ser det som positivt at kommunen selv har identifisert dette som et forbedringsområde, sammen med det å etablere en oversiktlig registrering av de risikovurderinger og tiltak som gjøres i alle deler av virksomheten.

På grunnlag av intervjuene og dokumentasjon er det vår vurdering at kommunens prosess for risikostyring er en del av en helhetlig styringsstruktur og er kjent i virksomheten, men at prosessen ikke alltid blir fulgt. Kommunen gjennomfører tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, men som det kommer frem av intervjuene er det imidlertid arbeid som gjenstår på dette området. Slik revisjonen vurderer fakta handler det om å få en større forståelse i organisasjonen for de prosesser som må til i forkant av innføringen av nye systemer og app'er slik at kommunen er rustet til å gjennomføre risikovurderinger og iverksette sikringstiltak knyttet til systemene før de tas i bruk. I tillegg gjenstår det arbeid med å få etablert en sikkerhetskultur som har innsikt og forståelse for sikkerhetsarbeidet på området og de prosesser som må gjennomføres. En vurdering av

sikkerhetskulturen i kommunen vil fremkomme i delrapport 2 til denne forvaltningsrevisjonen. Kommunen er imidlertid bevisst på at sikkerhetskulturen er avgjørende for IT-sikkerheten, og således er det vår foreløpige vurdering at kommunen er på god vei til å få et egnet sikkerhetsnivå sett opp mot regelverk og normer på området.

Foreløpig har kommunen ikke fullført en kartlegging av verdikjedene ved innhenting, behandling, lagring etc. av data, jf. grunnkravene fra NSM. Kommunen jobber imidlertid med et nytt helhetlig overordnet strategidokument, som skal ivareta hele verdikjeden inkludert sikkerhet, kultur og GDPR. Vi er enige med kommunen i at det kan være nyttig å gjennomgå og kartlegge arbeidsprosesser for å avdekke nye risikoområder og for å få hjelp til å gjøre prioriteringer, og det er positivt at kommunen er i gang med dette.

IKT-utstyr, konfigurasjon, nettverk, leverandører og systemer, samt e-post-sikkerhet

På bakgrunn gjennomgangen av IT-avdelingens sikkerhetssystemer og intervjuene er det vår vurdering at kommunen gjennom bruk av funksjoner i sine systemer har nødvendig oversikt over sitt IKT-utstyr. Kommunens ledergruppe har bestemt at ansatte kun skal ha en pc hver. Noen har imidlertid to. Slik vi vurderer fakta foreligger det en risiko for at disse pc'ene ikke i like stor grad blir ivaretatt med tanke på oppgradering og sikring, men uten at sikkerhetsrisikoen fremstår som så stor grunnet andre sikkerhetstiltak.

Det er vår vurdering at kommunen har kontroll på sine nettverk og komponenter. Vi legger til grunn kommunens overvåkingssystem, e-post varslinger ved kritiske hendelser, vaktordning på de mest risikoutsatte områdene osv. IT-avdelingen gjennomfører også jevnlig sikkerhetsoppdateringer etter intern rutine. Kommunen har også prosedyre for å oppdatere konfigureringer månedlig. Flere konfigurasjoner er automatisert og noen er manuelle. Det er vår vurdering at kommunen sørger for sikker konfigurasjon, og er bevisst på risikoutsatte områder.

På bakgrunn av gjennomgangen med IT-avdelingens sikkerhetssystemer og intervjuene er det vår vurdering at kommunen også har oversikt over de ulike leverandørene og stiller krav til dem og produktene. IT-drift følger opp leverandører av systemer til kommunen og ved kjøp av ulike IT-tjenester ivaretas sikkerheten gjennom å inngå databehandleravtaler med leverandørene.

Kommunen har ansatte på IT-avdelingen med lang erfaring, og det fremkommer at rutinene for håndtering av hendelser er erfaringsbasert og ikke nødvendigvis skriftliggjort. I testen av kommunens sikkerhetssystemer, i form av en phishing-mail, kommer det frem at kommunens håndtering av hendelsen ble beskrevet som veldig god. IT-avdelingen reagerte raskt og effektivt ved å informere i interne kommunikasjonskanaler og gjennomføre tiltak som blokkering av domenet i brannmur. Det fremkommer imidlertid også at Phishing-mailen ble videresendt litt frem og tilbake internt på IT-avdelingen, før noen kom frem til at de burde advare mot phishing-mailen internt i kommunen. Det er derfor vår vurdering at kommunen med fordel kan etablere en sjekkliste for aktiviteter og tiltak ved uforutsette hendelser på IT-området. Dette for å reagere enda raskere på slike hendelser og sikre at hendelser følges opp uavhengig av hvem som er på jobb på tidspunkt for hendelsen.

I Retningslinjer for bruk av kontorstøtteverktøy og lagring av dokumenter fremkommer det informasjon om at ansatte skal gjøre en vurdering av om mottatt e-poster er sikre, og dersom den vurderes til ikke å være sikker, skal den slettes umiddelbart. Det er vår vurdering at det her også burde vært nevnt hva og hvor den ansatte skal rapportere om slike hendelser. [Resten av avsnittet unntatt offentlighet, offl. § 24 tredje ledd]

Kommunen anser brosjyren *«Min elektronisk arbeidsplass»* som et viktig element i kommunens arbeid med IT/IKT-sikkerhet, ved at den inngår som en sentral del i internrevisjonene. Når da internrevisjonene avdekker at alle virksomheter som er kontrollert siden 2017, har en stor andel ansatte som ikke kjenner kommunens brosjyre, er det vår vurdering at avvik og tiltak knyttet til dette burde vært løftet til overordnet nivå i kommunen for alle virksomheter. Samtidig stiller vi spørsmål ved at avvik på dette området ikke også fremkommer i kommunens egenkontroller. Det er etter vår vurdering sentralt å jobbe mer målrettet og tilpasse informasjon ut til den enkelte bruker av systemene og gi tidligere informasjon til virksomhetsledere om viktigheten av å følge opp overfor egne ansatte, og derigjennom også kunne redusere feilmarginen i egenkontrollene.

Tilgangskontroll og autorisering

Fakta viser at kommunen har prosedyrer for tilgangskontroll. Vi legger til grunn opplysninger fra intervjuer og dokumentet *Brukerdokumentasjon ansattmelding,* som gir føringer for å gi tilganger til ulike portaler og systemer. Noen tilganger og autoriseringer er knyttet til den avdeling/virksomhet der den ansatte arbeider og andre tilganger er individuelle og etter arbeidsrelatert behov. Det er vår vurdering at kommunen har etablert tilfredsstillende prosedyrer for tilgangskontroll og autorisering som styrer hvem i organisasjonen som skal gi de ulike tilgangene, at tilgangene er begrenset til behov, samt at brukerkonto blir deaktivert når den ansatte slutter slik at det ikke lenger er mulig å logge inn.

Kommunen har også etablert prosedyrer for bruk av informasjonssystemene. Vi legger til grunn kommunens *IKT-reglement*, kommunens brosjyre «*Min elektroniske arbeidsplass*» og *Retningslinjer for bruk av kontorstøtte verktøy og lagring av dokumenter* osv. som blant annet gir informasjon om hvorfor informasjonssikkerhet er nødvendig og hvordan ansatte skal ivareta fysisk og elektronisk sikkerhet, tilgangsrettigheter og passord.

[Avsnitt unntatt offentlighet, offl. § 24 tredje ledd]

Sikring av helse- og personopplysninger

Det er en forutsetning at virksomheten har oversikt over og kontroll på alt eget utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger. Dette gjelder også utstyr ved avdelingskontor, hjemmekontor og mobilt utstyr. Det fremkommer i intervjuene at Helse og

velferdsområdet har hatt fokus på sikring av helse- og personopplysninger og har jobbet etter norm for e-helse i mange år. På helseområdet har mye av utviklingen av sikringstiltak, systemer og standarder blitt iverksatt av sentrale myndigheter. Det er vår vurdering at dette har gitt helseområdet et forsprang i arbeidet med sikring av personopplysninger i forhold til andre virksomheter i kommunen.
Det er vår vurdering at kommunen ved bruk av Gerica og overføring av informasjon over Norsk Helsenett, sørger for at det er etablert klare ansvarsforhold ved sending av meldinger med helse- og personopplysninger. Kommunen sørger for sikker overføringskryptering ende-til-ende for helse- og personopplysninger på kommuneområde Helse og velferd.

Det er vår vurdering at det er en rask utvikling i samfunnet både på digitalisering, sikkerhetsarbeidet og endring og etablering av regelverk knyttet til sikringen av personopplysninger mm. Vi ser det som positivt at kommunen nå samkjører noen av de overordnede rutinene i organisasjonen som er felles for flere virksomheter.

Avvik, internkontroll og rapportering

Kommunen har en *Prosedyre for avviksbehandling* hvor det fremkommer at alle ansatte er ansvarlige for å rapportere avvik innenfor sitt ansvars-/arbeidsområde, og at avvik skal registreres i kvalitetssystemet. Funn etter gjennomført internrevisjon skal også registreres som avvik. Det er vår vurdering at kommunen ivaretar kravet om å ha en prosedyre for avviksregistrering.

Det er også vår vurdering at det ikke alltid er klarhet i begrepsbruken i de ulike rutinene og prosedyrene. Det kan ha bakgrunn i at arbeidet på informasjonssikkerhetsområdet har blitt utviklet over tid og på enkelte områder er delvis overlappende. Det gjelder bruk av ulike begreper som informasjonssikkerhet, datasikkerhet, IT-sikkerhet, sikkerhetsarbeid osv. Det er vår vurdering at dette også er noe som er drøftet i kommunen, og at de som jobber med personvern, IT-sikkerhet og informasjonssikkert i kommunen har en felles forståelse av. Samtidig er det vår vurdering at kommunen med fordel kan rydde i begrepsbruken i sine rutiner, prosedyrer og systemer på dette området. Det vil gjøre det enklere for ansatte å forstå hva som er etterspurt på ulike områder, og lettere å kunne finne frem i prosedyrer og rutiner i Risk Manager. Eksempelvis *Prosedyre for håndtering av alvorlige sikkerhetsbrudd*. Bruk av begrepet sikkerhetsbrudd kan gjenspeile flere områder, også IT-sikkerheten som sådan. Begrepet informasjonssikkerhet omhandler også flere aspekter, som personvern og IT-sikkerhet osv.

Digitaliseringsdirektoratet sier i sin veileder til informasjonssikkerhet at offentlige virksomheter i henhold til eForvaltningsforskriften skal etablere et tilfredsstillende system for internkontroll. Det er vår vurdering at kommunen har etablert en internkontroll som baserer seg på rutiner og prosedyrer som er å finne i kommunens kvalitetssystem, melding av avvik, en årlig egenkontroll gjennomført av virksomhetsledere og internrevisjon. Det er vår vurdering at internkontrollen gjennom internrevisjoner og egenkontroller er en del av virksomhetens helhetlige styringssystem ved at resultatene meldes som avvik og følges opp i kvalitetssystemet både på overordnet- og virksomhetsnivå, samt som en del av ledelsens gjennomgang.

Kommunens internrevisjon bygger på de grunnleggende prinsippene i COSO-modellen. Det er vår vurdering at kommunens internrevisjon er basert på en modell som er anerkjent og egnet til å revidere etter. Etter revisjonens oppfatning gjennomføres internrevisjoner jevnlig. Dette er sikret gjennom årlige planer og følges opp gjennom avvikssystemet, samt ledelsens årlige gjennomgang. Utgangspunktet for revisjonene er i stor grad personvernregelverket. Det er vår vurdering at dette også ivaretar vurderinger av IT-sikkerheten på flere områder, men at vurderingene av IT-sikkerheten med fordel kan fremheves i revisjonene/rapportene.

Rapportene etter gjennomførte internrevisjoner viser til at den blant annet tar utgangspunkt i forskrift om behandling av personopplysninger (personopplysningsforskriften). Vi presiserer at personopplysningsforskriften, slik den fremstilles i rapportene, er opphevet og ikke lenger er aktuell for kommunen å revidere etter. Denne ble endret samtidig som personvernforordningen trådte i kraft i 2018.

Det kommer frem i intervjuene at melding av antall avvik er svært varierende fra virksomhet til virksomhet. Det kommer også frem av internrevisjonsrapportene at det er ulik kultur for å melde avvik. Det er derfor en mistanke om underrapportering på avvik i kommunen. I COSO-modellen er kontrollmiljøet en faktor som skal vurderes. Vi savner i den forbindelse at kommunen gjør en tydeligere vurdering av kontrollmiljøet, for å vurdere om det er klima i den enkelte virksomhet for å kunne gi tilbakemeldinger og melde avvik når det er behov for det.

Egenkontrollen som gjennomføres regelmessig på alle områder i virksomheten er etter vår vurdering en sentral del av kommunens internkontroll. Sjekklisten for egenkontroll har et enkelt oppsett, noe vi også mener er viktig for gjennomføringen, men kontrollen bygger da i liten grad på anerkjente internkontrollmodeller.

Det er også vår vurdering at kommunen må oppdatere flere av sine rutiner, slik at disse er sammenhengende, hjemlet i gjeldende regelverk og bruker riktig tittel på de som er ansvarlige i henhold til dagens organisering og stillingstitler. Dette gjelder blant annet *Rutine for egenkontroll, informasjonssikkerhet.*

Det er videre vår vurdering at kommunens internkontroll (styring og kontroll) på informasjonssikkerhetsområdet er basert på kommunens sikkerhetsmål og sikkerhetsstrategi, og har et omfang og en innretning som er tilpasset risikoen på informasjonssikkerhetsområdet.

Det er vår vurdering at kommunen også har etablert effektive rapporteringslinjer til toppledelsen. Fagansvarlig informasjonssikkerhet er plassert i stab KTE og direktør KTE har klare rapporteringslinjer til toppledelsen.

Beredskapsplan og -øvelse

Kommunen har etablert en beredskapsplan for ulike typer hendelser i *Beredskapsplan Sarpsborg kommune.* Her fremkommer det at kommunen skal gjennomføre årlige øvelser, hvor man øver ulike deler av kommunens krisehåndteringsorganisasjon. Det er laget egne scenarier der kommunen også har fått tydeliggjort IT-sikkerhetsutfordringer. Kommunens ROS-analyse danner grunnlaget for utforming av beredskapsplan. Det er vår vurdering at beredskapsplanen også ivaretar IT-sikkerheten gjennom *Delplan IKT*.

Av intervjuene fremkommer det at kommunen ikke har gjennomført øvelser som tester planverket på IT-området per i dag, at delplanene i liten grad har vært gjenstand for øvelser og at IT-sikkerhet er et område de burde ha øvd på. Det er gjennomført noen mindre interne øvelser. Det er imidlertid vår vurdering at kommunen i større grad burde ha en øvet sikkerhetsorganisasjon, og i større grad inkludere IT-sikkerheten i sine beredskapsøvelser eller gjennomføre egne øvelser på IKT-hendelser.

2.4 Konklusjon og anbefalinger

Sarpsborg kommune er en organisasjon som prioriterer sikkerhetsarbeidet. Det er vår konklusjon at kommunen i stor grad har etablert planer og rutiner som ivaretar kommunens IT-sikkerhet på en tilfredsstillende måte, og implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til

informasjon. Kommunen gjennomfører en rekke kontrollaktiviteter på IT-sikkerhetsområdet, både preventive, oppdagende, manuelle og ledelsesbaserte kontroller.

Vi ser at noen av planene og rutinene per i dag ikke er oppdatert til dagens organisering og noen ikke etter gjeldende regelverk. Kommunen er imidlertid i gang med å rette opp i dette og etablere nye planer og rutiner på flere områder. Kommunen har gjennomført risikovurderinger i lengere tid. Det å gjennomføre risikovurderinger er imidlertid ikke likt forstått av alle i organisasjonen, og det er ikke alltid sørget for at risikovurderingene er gjennomført før innføringen av nye systemer og app'er iverksettes. Dokumentasjonen på gjennomførte risikovurderinger er heller ikke systematisert i tilstrekkelig grad. Vi ser det som positivt at kommunen selv har kommet frem til denne konklusjonen og nå jobber med dette.

Kommunen har i all hovedsak kontroll på sitt IT-utstyr, sine nettverk og komponenter, og gjennomfører sikker konfigurasjon. Kommunen stiller også krav til leverandører og systemer slik at sikkerheten skal være ivaretatt.

[Avsnitt unntatt offentlighet, offl. § 24 tredje ledd]

Kommunen har etablert en internkontroll og gjennomfører internrevisjoner/sikkerhetsrevisjoner som er tilpasset risikoen på området. Det er også etablert effektive rapporteringslinjer til toppledelsen. Internrevisjonen, som en del av internkontrollen er etablert etter anerkjent standard. Det samme er ikke tilfellet for egenkontrollen. I tillegg mener vi at kommunen i større grad kan følge opp kontrollmiljøet som en del av internkontrollen. Det ser også ut til at der internrevisjonene viser gjennomgående avvik i flere virksomheter blir det i liten grad gjort vurderinger av om dette er en problemstilling som bør meldes som avvik på et høyere nivå i organisasjonen.

Videre har vi funnet at kommunen har etablert beredskapsplaner som ivaretar IT-sikkerheten, men at disse i liten grad er øvet i organisasjonen. I testen av kommunens IT-sikkerhet viste kommunen en veldig god håndtering av hendelsen, men det er ikke etablert skriftlige rutiner/sjekkliste for håndtering av slike hendelser.

Revisjonen anbefaler at kommunen bør:

- gjennomgå planer og rutiner knyttet til arbeidet med IT-sikkerhet, og oppdatere disse etter dagens organisering, ansvar og funksjoner
- sørge for en felles forståelse i organisasjonen av hvordan risikovurderinger skal gjennomføres og dokumenteres
- etablere rutiner for passordbruk og –bytte, som i større grad ivaretar IT-sikkerheten
- vurdere å etablere en rutine/sjekkliste for håndtering av uforutsette IT-hendelser
- oppdatere internrevisjonsgrunnlaget til gjeldende regelverk og vurdere å inkludere kontrollmiljøet i større grad
- vurdere om gjennomgående funn etter flere gjennomførte internrevisjoner, i større grad bør etableres som en problemstilling/avvik på et overordnet organisatorisk nivå
- sørge for å ha en øvet sikkerhetsorganisasjon med tanke på IKT-hendelser

3 Kommunedirektørens uttalelse[16]

Sarpsborg kommune

Unntatt offentlighet
OFL §5

ØSTRE VIKEN KOMMUNEREVISJON IKS
Råkollveien 103
1664 ROLVSØY

Deres ref.:	Vår ref.:	Dato:
	19/12318-13	26.05.2020

Kommunedirektørens uttalelse revisjonsrapport IT-sikkerhet

Kommunedirektøren mener Østre Viken Kommunerevisjon IKS har gjennomført en grundig og god revisjon. Det er positivt at kontrollutvalget ønsket en revisjon på dette området og at også kommunerevisjonen understreker viktigheten av at kommunen har god informasjonssikkerhet. Revisjonskriteriene samsvarer godt med de mål kommunen har hatt for sin forvaltning av digitale verdier og sikring av IKT-systemer.

Kommunedirektøren merker seg at revisjonen innledningsvis også fremhever dette ved å påpeke at god informasjonssikkerhet og trygge IKT-systemer er helt sentralt og avgjørende når flere og nye tjenester digitaliseres. Kommunen har jobbet systematisk med dette i lengre tid, og prioritert innsats på dette området for å møte fremtiden på en trygg og god måte. Kommunedirektøren merker seg revisjonens funn og konklusjoner som innledningsvis oppsummer:

> *«Sarpsborg kommune er en organisasjon som prioriterer IT-sikkerhetsarbeidet. Det er vår konklusjon at kommunen i stor grad har etablert planer og rutiner som ivaretar kommunens IT-sikkerhet på en tilfredsstillende måte. Kommunen har også implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon.»*

Kommunedirektøren er enig i revisjonens liste på syv anbefalte tiltak og har følgende kommentarer.

Revisjonen anbefaler at kommunen bør:

- gjennomgå planer og rutiner knyttet til arbeidet med IT-sikkerhet, og oppdatere disse etter dagens organisering, ansvar og funksjoner

Svar: Planer og rutiner er oppdatert i henhold til dagens organisering og vil bli vurdert ved den årlige gjennomgangen i kommunedirektørens ledergruppe.

- sørge for en felles forståelse i organisasjonen av hvordan risikovurderinger skal gjennomføres og dokumenteres

[16] Deler av uttalelsen er unntatt offentlighet, offl. § 24 tredje ledd.

Svar: Kommune har påbegynt et arbeid med anskaffelse av nytt kvalitetssystem. I forbindelse med dette prosjektet vil kommunedirektørens stille krav til hvordan risikovurderinger skal gjennomføres og dokumenteres.

- vurdere å etablere en rutine/sjekkliste for håndtering av uforutsette IT-hendelser

Svar: Kommunen ser nytteverdi i å etablere et tiltakskort for håndtering av større, kritiske IT-hendelser. Pr. i dag håndteres slike hendelser ved å samle alle relevante fagpersoner i et type Incident Response Team, uten at prosessene og oppgavene på forhånd er dokumentert. Tiltakskort og etablering av rutiner og sjekklister vil være nyttig for dette arbeidet. Dette iverksettes innen utgangen av 2020.

- oppdatere internrevisjonsgrunnlaget til gjeldende regelverk og vurdere å inkludere kontrollmiljøet i større grad

Svar: Dette er tatt til etterretning, og vil være en naturlig del av forestående prosjekt med oppgradering og fornyelse av kommunens kvalitetssystem.

- vurdere om gjennomgående funn etter flere gjennomførte internrevisjoner, i større grad bør etableres som en problemstilling/avvik på et overordnet organisatorisk nivå

Svar: Kommunen ser positivt på innspillet, som vil bidra til ytterligere læring og forbedring etter interne sikkerhetsrevisjoner.

- sørge for å ha en øvet sikkerhetsorganisasjon med tanke på IKT-hendelser

Svar: Gjennomføring av skrivebordsøvelser for å øve involverte ledere og medarbeidere i håndtering av IKT-hendelser har vært diskutert ved flere anledninger tidligere. Vi ser positivt på at revisjonen peker på dette forbedringstiltaket, og vil ta sikte på å gjennomføre første øvelse i løpet av de kommende 12 månedene

Med hilsen

Unni Elisabeth Skaar
Kommunedirektør

Dette brevet er signert elektronisk

4 Dokumentliste og kildehenvisninger

Dokumenter fra Sarpsborg kommune

- Organisasjonskart
- Sikkerhetsorganisering i Sarpsborg kommune
- Sikkerhetsorganisering i Sarpsborg kommune - utkast v. 2020
- Funksjonsbeskrivelse personvernombud
- Funksjonsbeskrivelse fagansvarlig informasjonssikkerhet v 2009
- IKT-reglementet - Rapportering for ledere
- Rutine for egenkontroll
- Rutine for ledelsens gjennomgang
- Sjekkliste egenkontroll informasjonssikkerhet
- Nettverk og samarbeidspartnere på IT-sikkerhet
- Digitaliseringsstrategi for Sarpsborg kommune
- Målbilde informasjonssikkerhet og personvern
- Sikkerhetsmål og sikkerhetsstrategi for Sarpsborg kommune
- Internrevisjon informasjonssikkerhet Enhet omsorgstjenester Borgen 2017
- Ledelsens gjennomgang for 2015
- Ledelsens gjennomgang for 2016
- Ledelsens gjennomgang for 2017
- Ledelsens gjennomgang for 2018
- Rapport internrevisjon Enhet Helsehuset Sarpsborg 2018
- Rapport Internrevisjon informasjonssikkerhet Enhet HR 2017
- Rapport Internrevisjon informasjonssikkerhet Enhet kemner 2018
- Rapport internrevisjon informasjonssikkerhet Fossen barnehager 2018
- Rapport internrevisjon Lande barneskole 2019
- Rapport internrevisjon Sarpsborg brannvesen 2019
- Sikkerhetssamtale og revisjon Norsk Helsenett 2014
- Sluttrapport internrevisjon Virksomhet forvaltning og utvikling 2019
- Målbilde for teknologi og endring v08
- Fagsystemer i Sarpsborg kommune
- Retningslinje for kvalitetssystem
- Prosedyre for avviksbehandling
- Prosedyre for håndtering av alvorlige sikkerhetsbrudd
- Rutine for gjennomføring av risikovurderinger informasjonssikkerhet
- Nivå for akseptabel risiko, personopplysninger
- Rutine for håndtering av risiko, personopplysninger - på høring
- Beredskapsplan Sarpsborg kommune
- Delplan IKT
- Helhetlig ROS-analyse Sarpsborg kommune 2019 - vedtatt i bystyret 260919
- IKT-reglement.pdf
- Opplæring og kompetanseheving innen IT-sikkerhet for ansatte
- Arbeidsreglement
- Ansettelsesprosedyre - 01 Sjekkliste - før tiltredelse
- Ansettelsesprosedyre - 02 Sjekkliste - første uke
- Ansettelsesprosedyre - 03 Sjekkliste - første måned
- Ansettelsesprosedyre - 04 Sjekkliste - første år
- Min elektroniske arbeidsplass, Brosjyre om informasjonssikkerhet.pdf
- Retningslinjer for bruk av kontorstøtteverktøy og lagring av dokumenter
- Gerica - Sikkerhetsinstruks for bruker

- Gerica - Sikkerhetsinstruks bruker skjema
- Brukerdokumentasjon ansattmelding.docx
- Om annen relevant dokumentasjon – beskrivelse fra kommunen

Regelverk

- *Kommuneloven*
- *Personvernforordningen – GDPR*
- *Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)*

Veiledere og standarder

- *Digitaliseringsdirektoratets veiledere til informasjonssikkerhet*
- *Direktoratet for e-helses Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten*
- *ISO/IEC 27001 (Information technology)*

- *Nasjonal strategi for digital sikkerhet 05/2019*

5 Vedlegg

1. Utledning av revisjonskriterier
2. Anonymisert rapport fra NetSecurity – *Recon report Sarpsborg kommune*
3. Anonymisert rapport fra NetSecurity – *Phishing report Sarpsborg kommune*

Vedlegg 1 - Utledning av revisjonskriterier

Personvernforordningens regler om informasjonssikkerhet følger av artikkel 32. Bestemmelsen fastslår at både den behandlingsansvarlige og databehandleren plikter å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen», eForvaltningsforskriften skal legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger.

Digitaliseringsdirektoratet sier i sin veileder til informasjonssikkerhet at offentlige virksomheter skal i henhold til eForvaltningsforskriften §15 etablere mål og strategi for informasjonssikkerhet og et tilfredsstillende system for internkontroll.

Sikkerhetsmålene bør beskrive både formål med informasjonsbehandlingen i forvaltningsorganet og overordnede føringer for informasjonsbehandling og bruk av IKT. Disse føringene vil naturlig uttrykkes som mål med vekt på konfidensialitet, integritet og tilgjengelighet i virksomhetens informasjonsbehandling og bruk av IKT. Sikkerhetsstrategien omfatter sentrale valg og prioriteringer i sikkerhetsarbeidet. Sikkerhetsstrategien består naturlig av to hoveddeler:

1. Retningslinjer for hvordan sikkerhetsarbeidet skal organiseres og gjennomføres
2. Retningslinjer for relevante tiltaksområder.

De siste bør etableres etter risikovurderinger i internkontrollarbeidet.

Sikkerhetsloven skal bidra til å sikre Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser mot sikkerhetstruende virksomhet

Digitaliseringsdirektoratet sier i sin veileder om informasjonssikkerhet at offentlige virksomheter i utgangspunktet har få eller ingen skjermingsverdig verdier iht. sikkerhetsloven, og må i liten grad forholde seg til regelverket.

Alle offentlige virksomheter må imidlertid ha tilstrekkelig oversikt for å være i stand til gjøre gode vurderinger, og kunne identifisere skjermingsverdig informasjon og skjermingsverdige informasjonssystemer. Alle virksomheter bør også vurdere om de i gitte situasjoner må være i stand til å motta og håndtere sikkerhetsgradert informasjon, eksempelvis i en krisesituasjon. Disse virksomhetene må legge til rette for at klarert personell kan motta og håndtere gradert informasjon.

Det kommer frem av samtale med informasjonssikkerhetsansvarlig i Sarpsborg kommune at de ikke har skjermingsverdige verdier per i dag. Sikkerhetsloven vil derfor ikke inngå i denne revisjonen.

En stadig større deler av kommunikasjonen i helse- og omsorgssektoren foregår elektronisk. De utfordringer dette medfører for personvernet førte til at det ble utarbeidet omforente regler for trygg og sikker informasjonsutveksling mellom aktørene i sektoren. Direktoratet for e-helse har utarbeidet en bransjenorm for å bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet. Normen stiller krav om detaljer og tar opp i seg gjeldende regelverk. I tillegg supplerer den gjeldende regelverk på noen områder.

Normen skal legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger.

De delene av normen som bygger på bestemmelsene i personvernlovgivningen/GDPR og som blant annet omhandler ansvar og organisering av personvernet, dataansvarliges ansvar, personvernombud og protokoll, vil undersøkes i en eventuell revisjon på personvernregelverket.

Hoveddelen av den nye kommuneloven trådte i kraft fra og med det konstituerende møtet i det enkelte kommunestyret og fylkestinget ved oppstart av valgperioden 2019–2023. Noen bestemmelser trådte i kraft 1. jan 2020. Kommuneloven § 25-1 vil tre i kraft senere. Kommunal- og moderniseringsdepartementet har sendt forslag til endringer av internkontrollbestemmelser i en rekke lover og forskrifter på ulike sektorer på høring. Endringene er en konsekvens av at reglene om internkontroll med kommuneplikter i hovedsak skal følge av den nye kommuneloven og ikke av særlovgivningen.

Personvernforordningen (GDPR)

Artikkel 32. Sikkerhet ved behandlingen

«1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

- *a) pseudonymisering og kryptering av personopplysninger,*
- *b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,*
- *c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,*
- *d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.*

2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

3. Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i artikkel 42 kan brukes som en faktor for å påvise at kravene i nr. 1 i denne artikkel er oppfylt.

4. Den behandlingsansvarlige og databehandleren skal treffe tiltak for å sikre at enhver fysisk person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, behandler nevnte opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at vedkommende gjør dette.»

eForvaltningsforskriften

§ 5. *Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen*
Når et forvaltningsorgan legger til rette for bruk av elektronisk kommunikasjon for mottak av opplysninger som på forvaltningens hånd kan være underlagt taushetsplikt, eller som kan være underlagt krav til sikring etter reglene om behandling av personopplysninger eller tilsvarende regler, skal risiko for uberettiget innsyn i opplysningene være forebygget på tilfredsstillende måte
……...

§ 15.Internkontroll på informasjonssikkerhetsområdet
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.

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Omfang og innretning på internkontrollen skal være tilpasset risiko

§ 17. Informasjon om bruk av sikkerhetstjenester mv.
Et forvaltningsorgan skal gi sine ansatte anvisning på hvilke sikkerhetstjenester og -produkter de skal benytte under tjeneste for organet, og hvorledes de skal gå frem for å anskaffe nødvendig utstyr og data, herunder signaturfremstillingsdata og dekrypteringsnøkkel med tilhørende sertifikat samt passord og PIN-koder mv……..

§ 20. Forvaltningsansattes bruk av forvaltningsorganets informasjonssystem
Forvaltningsansatte skal følge instruksene arbeidsgiver har fastsatt om bruk og sikring av virksomhetens informasjonssystemer, herunder om kontroll med materiale som skal lastes ned eller installeres på den ansattes arbeidsstasjon, og forvaltningsorganets sikkerhetsstrategi for øvrig, jf. § 15.

§ 21. Informasjon
Forvaltningsorganet skal sørge for at enhver, i den utstrekning det er nødvendig, får tilsvarende informasjon som nevnt i § 17 og § 19 tredje ledd i forbindelse med anskaffelse av sertifikat eller, hvis det ikke er mulig, ved første gangs bruk av slike tjenester ved kommunikasjon med et forvaltningsorgan. Forvaltningsorganet skal på samme måte informere publikum om at håndtering av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel skal skje i henhold til § 22 og § 25.

§ 22. Krav til oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel
Innehaver av signaturfremstillingsdata skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre.
Innehaver skal aldri forlate arbeidsstasjon og lignende uten å sikre at signaturfremstillingsdata ikke er tilgjengelige for andre. Innehaver skal sikre:

a) at signaturfremstillingsdata fjernes fra arbeidsstasjonen dersom dataene er lagret i smartkort eller i en annen enhet som lett kan fjernes, og
b) at den aktuelle arbeidsoperasjonen er avsluttet og eventuelle lagrede eller behandlede signaturfremstillingsdata er deaktivert, eller
c) at signaturfremstillingsdata på annen måte er sikret mot misbruk.

Innehaver av signaturfremstillingsdata skal ikke overlate disse til andre eller gi andre tilgang til dem. Skal noen handle på vegne av en annen skal dette skje med fullmektigens egne signaturfremstillingsdata.

Bestemmelsene om oppbevaring og bruk av signaturfremstillingsdata gjelder tilsvarende for bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel.

§ 25. Varslingsplikt ved tap eller mistanke om misbruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel
Innehaver av signaturfremstillingsdata skal straks varsle sertifikatutsteder eller den som ellers er utpekt til å motta varsel, dersom det oppstår mistanke om at signaturfremstillingsdata er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt. Det samme gjelder for bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel.

Nasjonal strategi for digital sikkerhet

Som en del av Nasjonal strategi for digital sikkerhet, lagt frem på lanseringskonferanse i januar 2019, er det utarbeidet anbefalte tiltak for bedret digital sikkerhet. Tiltakene er todelt. Den første delen er rettet mot sentrale tiltak, og den andre delen har 10 anbefalte tiltak rettet mot virksomheter i offentlig og privat sektor. Det fremkommer av dokumentet at virksomheter må gjennomføre nødvendige tiltak for å sikre IKT-systemene, og at NSMs grunnprinsipper for IKT-sikkerhet beskriver tiltak som alle virksomheter bør implementere for god grunnsikring. Anbefalte tiltak for virksomheter er:

- **Ledelse**. Det bør etableres aktiviteter for sikkerhetsstyring, hvor det er tydelige krav og forventninger til sikkerhet.

- **Risikostyring**. Etabler prosess for risikostyring som er en del av en helhetlig styringsstruktur, prosessen må være kjent i virksomheten. Etabler tydelig ansvar og effektive rapporteringslinjer til toppledelse og styre.
- **Kartlegg verdikjeder, informasjonsverdier, utstyr og brukertilganger**. Lag en oversikt over virksomhetens sentrale mål, hvilke verdier og verdikjeder som inngår, hvor viktige data lagres og hvem som har tilgang til disse dataene.
- **Inkluder digital sikkerhet i virksomhetskulturen**. Virksomheter må sørge for at ansatte har nødvendig informasjon, kunnskap og ferdigheter til å opprettholde ønsket sikkerhetsnivå. Kartlegg virksomhetens sikkerhetskultur og identifiser hva som kan forbedres. Fastsett ønsket kultur og gjennomfør tilpasset, årlige treningsprogram for å fremme god sikkerhetskultur.
- **Leverandørkontroll**. Det må stilles krav til produkter og leverandører slik at sikkerheten er ivaretatt i hele produktets eller tjenestens levetid. Sats på god bestillerkompetanse og gjør en risikovurdering som forankres hos ledelsen.
- **Sikker konfigurasjon**. Konfigureringen må oppdateres kontinuerlig, i takt med endringer i teknologi, bruksmønster og trusselbilde. Oppgrader program- og maskinvare. Fjern unødvendig kompleksitet og ubrukt funksjonalitet. Blokker kjøring av ikke-autoriserte programmer.
- **Kontroll på nettverk og systemkomponenter**. Virksomheten må innføre tiltak for beskyttelse mot skadevare, overvåkning og analyse av IKT-systemet og håndtering av endringer. Installer sikkerhetsoppdateringer så raskt som mulig. Beskytt trådløse nettverk med sterke sikkerhetsmekanismer. Planlegg og dokumenter endringer. Slå på logging og gjennomgå viktige logger jevnlig.
- **E-post og websikkerhet**. Virksomheten bør ha kontroll på informasjonsflyten som går til og fra eget nettverk, samt innad i eget nettverk. Bruk kun siste versjon av nettlesere. Beskytt e-post med DMARC[17]. Krypter viktig informasjon når det lagres på bærbare medier og når det sendes over nettet.
- **Tilgangskontroll**. Virksomheten må ha kontroll på kontoer, kontrollere bruk av administrative privilegier, sørge for sikker pålogging og jevnlig gjennomgå tilgangsrettigheter. Fysisk tilgang til nettverk og informasjonssystemer, inkludert datarom, bør tilgangsstyres på lik linje med logiske tilganger. Endre standard passord og ikke tildel sluttbrukere administratorrettigheter. Bruk 2-faktor autentisering, eller som et minimum, sterke passord.
- **Hendelsesberedskap**. Etabler en beredskapsplan for ulike typer hendelser og gjennomfør øvelser som tester planverket.

Norm for informasjonssikkerhet – e-helse

Styringssystem

Det stilles krav til et styringssystem som en del av virksomhetens internkontrollsystem. Styringssystemet bør inneholde en styrende, en gjennomførende og en kontrollerende del.

Den styrende delen bør blant annet inneholde

- Informasjonsikerhetsmål
- Sikkerhetsinstruks

Den gjennomførende delen bør inneholde

- Oversikt over type leverandører
- Konfigurasjonskart over informasjonssystemene og tekniske beskrivelse av konfigurasjonen
- Prosedyrer for godkjenning av alle konfigurasjonsendringer i informasjonssystemene.
- Prosedyrer og regler for bruk av informasjonssystemene

[17] Domain based Message Authentication, Reporting and Conformance. Mekanisme som sjekker om innkommende e-post faktisk kommer fra domenet det påstår at det kommer fra (autentisering av avsender).

- Prosedyrer for drift av informasjonssystemene
- Dokumentasjon av sikkerhetstiltak – organisatoriske, fysiske og tekniske
- Prosedyrer ved bruk av databehandlere, leverandører av kommunikasjonstjenester, utstyr eller programvare og andre leverandører

Den kontrollerende delen bør inneholde

- Planer for gjennomføring av sikkerhetsrevisjoner
- Prosedyre for oppfølging av resultater fra disse sikkerhetsrevisjoner. Sikkerhetsrevisjoner skal gjennomføres jevnlig
- Planer for ledelsens gjennomgang og prosedyre for oppfølging av handlingsplaner besluttet av ledelsen. Ledelsens gjennomgang skal være minimum årlig og dekke bl.a. avvikshendelser og eventuelle korreksjoner i styringssystemet
- Prosedyrer for avvikshåndtering ved bl.a. brudd på prosedyrer

Videre stilles det krav til risikostyring knyttet til kravene i GDPR om konfidensialitet, integritet, tilgjengelighet, og i tillegg robusthet.

I robusthet ligger:
Det skal finnes egnede tekniske og organisatoriske tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting av personopplysningssikkerheten og informasjonssikkerheten for øvrig.

Oversikt over IKT-utstyr

Virksomheten skal ha oversikt over alt IKT-utstyr. Denne oversikten skal inkludere stasjonære og bærbare datamaskiner, mobiltelefoner og annet kommunikasjonsutstyr, servere, nettverksutstyr (rutere, svitsjer, brannmurer, osv.), skrivere, lagringsnettverk, apper, IP-telefoner mv.

I større virksomheter bør følgende tiltak gjennomføres:

- Utarbeide oversikt over maskin- og programvare som vedlikeholdes med automatiske verktøy
- Inventarsystemet for programvare bør spore versjon av det underliggende operativsystemet samt programmer som er installert på dem

Risikovurdering

Før behandling av helse- og personopplysninger igangsettes skal det gjennomføres risikovurderinger for å kartlegge risikoområder og klarlegge sannsynlighet for og konsekvens av uønskede hendelser. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten. I tillegg skal virksomhetens ledelse jevnlig gjennomføre risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten Dataansvarlig og databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som står i forhold til risikoen. Ved vurdering av hvilke tiltak som skal iverksettes, skal det tas hensyn til informasjonsbehandlingens art og sammenhengen den utføres i, omfang, formål, den tekniske utviklingen og gjennomføringskostnadene for tiltakene.

Normen har listet opp ni kriterier som kan benyttes for å avgjøre om en behandling vil kreve en vurdering av personvernkonsekvenser (jf GDPR).

1. Er behandlingen en evaluering eller poengvurdering?
2. **Omfatter den automatiserte avgjørelser?**
3. **Innebærer den systematisk overvåking?**
4. Involverer den sensitive personopplysninger?
5. Dreier det seg om en behandling av personopplysninger i stor skala?
6. Vil to eller flere datasett sammenstilles?
7. Omfatter den personopplysninger om registrerte med særskilt beskyttelsesbehov?
8. **Tar den i bruk ny teknologi eller brukes eksisterende teknologi til nye formål?**

9. Vil konteksten for behandlingen begrense muligheten de registrerte har til å utøve sine rettigheter?

Taushetsplikt

For å sikre konfidensialitet for helse- og personopplysninger skal virksomhetens leder sikre at alt personell som gis tilgang har taushetsplikt, og at de er bevisst taushetspliktens innhold og omfang, for alle helse- og personopplysninger samt for annen informasjon med betydning for informasjonssikkerheten. Det skal som minimum:

- Beskrives konsekvenser ved brudd på taushetsplikten.
- Beskrives konsekvenser ved å tilegne seg eller forsøke å tilegne seg opplysninger man ikke har tjenstlig behov for (ulovlig tilegnelse).
- Beskrives konsekvenser ved å endre/forsøk på å endre opplysninger man ikke har autorisasjon til å endre. Brudd på taushetsplikten og/eller ulovlig tilegnelse skal som konsekvens minimum medføre en advarsel for den som begår bruddet, og bruddet skal behandles iht. avviksprosedyre. Ved alvorlige eller gjentatte brudd på taushetsplikten må konsekvenser for ansettelsesforholdet vurderes. Brudd på taushetsplikten og/eller ulovlig tilegnelse er forbudt og varsling av tilsynsmyndighetene og anmeldelse må vurderes.

Informasjonssikkerhet

Sentrale sikkerhetstiltak som skal gjennomføres av virksomheter som behandler helse- og personopplysninger omfatter både dataansvarlige og databehandlere. Alle sikkerhetstiltak skal være egnede, og velges basert på risikovurderinger.

- Det skal settes vilkår og betingelser til ansatte om
    - Sikkerhetsinstruksen
    - Taushetserklæring
    - Virksomhetens sanksjonsmuligheter ved brudd

Virksomheten skal iverksette tiltak som gjør at ansatte:

- har tilstrekkelig kunnskap til å utnytte systemene for sin rolle og til å ivareta informasjonssikkerheten.
- behandler helse- og personopplysninger etter gjeldende regelverk, Normen og virksomhetens rutiner

Kompetansebygging må skje kontinuerlig og være tilpasset de ulike roller og brukergrupper.

Når et ansettelsesforhold opphører må det sikres at den som har vært ansatt leverer tilbake til arbeidsgiver alle medier (herunder digitalt, papir, osv.) som kan inneholde personopplysninger som denne har fått tilgang til i egenskap av å være ansatt i helse- og omsorgssektoren.

Tilgangsstyring

Databehandler skal innenfor rammen av taushetsplikt sørge for at

- kun autorisert personell har tilgang til nødvendige helseopplysninger. Det må etableres en autentisering som sikrer identifisering av autorisert bruker.
- Det er en regulering av privat bruk av virksomhetens informasjonssystemer.
- Det iverksettes kontrollerende tiltak.

Tilgangsstyring skal etableres for alle behandlingsrettede helseregistre (inkl. elektronisk pasientjournal (EPJ)) og fagsystemer.

Autorisering

Det skal etableres prosedyre for tildeling og administrasjon av tilgangsrettigheter.

Dataansvarlig skal sørge for at det oppettes et autorisasjonsregister.

Ved tilgang til helseopplysninger mellom virksomheter skal helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet. Pasienten/brukeren kreve at tilgang til egne helseopplysninger sperres for helsepersonell fra andre virksomheter enn der opplysningene er nedtegnet.

Flere personer skal ikke benytte samme autentiseringskriteria.

Gjennomgang og kontroll av tilgangsstyring, herunder tildelte autorisasjoner, skal foretas av den enkelte leder ved endringer i organisering eller flytting av ansatte. Gjennomgangen skal gjøres minimum årlig.

Brukerutstyr (PC og printere - stasjonære)

Sikkerhetstiltak skal hindre at personer som ikke er autoriserte får tilgang til helse- og personopplysninger – enten ved adgangsregulert kontroll av lokaler med utstyr, eller ved at utstyret sikres mot misbruk og skjermer, utskrifter mv. skjermes mot uautorisert innsyn.

Driftsutstyr (servere og nettverksutstyr)

Sikkerhetstiltak skal hindre at annet enn autorisert personell får adgang til slikt utstyr.

Mobilt utstyr og hjemmekontor

For slikt utstyr kan man ikke sikre lokaler, utstyret må derfor sikres. Det skal gjennomføres risikovurdering av de løsninger som benyttes. Det skal etableres administrative prosedyrer for bruk av mobilt utstyr og hjemmekontor.

All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer sikres ved kryptering iht. «NSM Cryptographic Requirements Version 3.1»1.

Kryptering

Tekniske tiltak skal iverksettes slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres.

Sikker IT-drift

Konfigurasjonskontroll
Det er en forutsetning at virksomheten har oversikt over og kontroll på alt eget utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger. Dette gjelder også utstyr ved avdelingskontor og hjemmekontor og mobilt utstyr.

Konfigurasjonen skal sikre at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt.

Konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, skal ikke settes i drift før følgende tiltak er gjennomført:

- Risikovurdering som viser at nivå for akseptabel risiko oppfylles
- Test som sikrer at forventede funksjoner er ivaretatt
- Implementering som sikrer mot uforutsette hendelser
- Ny konfigurasjon er dokumentert
- Konfigurasjonsendringer er godkjent av virksomhetens leder eller den ledelsen bemyndiger

Konfigurasjonskontroll skal reguleres gjennom avtale ved:

- Bruk av databehandler.
- Bruk av fjernaksess for vedlikehold og oppdateringer.

Alle endringer i organisasjonen, informasjonssystemene og systemer som har innvirkning på informasjonssikkerheten skal forankres på relevant ledernivå. Virksomheten skal utarbeide prosedyrer for endringsledelse.

Sikkerhetskopiering

Virksomhetens ledelse skal for øvrig sørge for sikkerhetskopiering av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk.

Logging

- Loggene skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd.
- Det skal etableres prosedyrer for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke.
- Det skal etableres prosedyrer for ved behov å kunne sammenholde loggene med autorisasjonsregister.
- Dersom brudd avdekkes skal personalmessige reaksjoner iverksettes.
- Dersom personalmessige reaksjoner ikke har nødvendig effekt over tid, dvs. det er gjentatt tilgang av flere personer som ikke er autorisert, skal nødvendige tekniske tiltak iverksettes.
- Loggene og autorisasjonsregister skal sikres mot endring og sletting av uautorisert personell.

For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres logg over følgende:

- Autorisert bruk av informasjonssystemene skal registreres.
- Sikkerhetsbarrierene skal registrere sikkerhetsrelevante hendelser, bl.a. forsøk på uautorisert bruk av informasjonssystemet.
- Nettverksoperativsystemer skal registrere alle forsøk på uautorisert bruk.
- Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk.
- Bruk av selvautorisering til behandlingsrettet helseregister skal registreres.
- Loggene skal sikres mot endring og sletting av uautorisert personell.

Følgende skal som minimum registreres i loggene:

- entydig identifikator for den autoriserte brukeren
- rollen den autoriserte brukeren har ved tilgangen
- virksomhetstilhørighet
- organisatorisk tilhørighet til den som er autorisert
- type opplysninger det er gitt tilgang til
- hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer
- grunnlaget for tilgangen
- tidspunkt og varighet for tilgangen

Ved bruk av tilgang til helseopplysninger mellom virksomheter skal i tillegg følgende logges hos virksomhetene:

- person og organisatorisk tilhørighet til den som har hentet frem helseopplysningene
- hvorfor helseopplysningene er hentet frem
- hvilke tidsperioder vedkommende har hentet frem helseopplysningene

Alle logger skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med autorisasjonsregister.

Styring og håndtering av tekniske sårbarheter

Styring og håndtering av tekniske sårbarheter skal følge prosedyrene for endingsstyring. Virksomheten skal ha prosedyrer for å skaffe seg informasjon om tekniske sårbarheter i utstyr og programvare.

Utgangspunktet for styring og håndtering er:

- Oversikt over IKT-utstyr
- Programvare: programvaren, leverandør, versjonsnumre, hvilken versjon som er installert hvor og hvem som har ansvaret for programvaren

Det skal etableres prosedyrer og operative tiltak som ivaretar:

- Ansvaret for: overvåkning, risikovurdering, korrigering og koordinering
- Hvordan virksomheten skal reagere og varsle om sårbarheter
- Prioritering og etablering av tidslinje for korrigering
- Alle korrigeringer bør testes før de implementeres

Sikkerhetsrevisjon av informasjonssystemer

Virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner. Det skal foreligge en godkjent plan for sikkerhetsrevisjoner.

Sikkerhetsrevisjonen skal som minimum omfatte vurderinger av:

- Plassering av ansvar og organisering av sikkerhetsarbeidet
- Kvalitet på sikkerhetsmål og sikkerhetsstrategi
- Overholdelse av prosedyrer for bruk av informasjonssystemer og helse- og personopplysninger
- Resultat av opplæring
- Forvaltning og bruk av helse- og personopplysninger
- Tilgang til helse- og personopplysninger og tiltak mot uautorisert innsyn
- Testing, analysering og vurdering av hvor effektive de tekniske og organisatoriske sikkerhetstiltak er
- Ivaretakelse av informasjonssikkerhet hos kommunikasjonspartnere, databehandlere og leverandører

Resultatene og konklusjonene fra sikkerhetsrevisjonene skal dokumenteres. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemene som ikke er forutsatt, skal dette behandles som avvik.

<u>Kommunikasjonssikkerhet</u>

Styring av nettverkssikkerhet
Nettverkssikkerhet er et sentralt tiltak for å sikre behandling av helse- og personopplysninger. Virksomheten skal tydelig definere hvilke krav som gjelder for nettverkssikkerheten, og tiltakene som iverksettes skal være basert på en risikovurdering.

Sikring av nettjenester
Ved tilkobling til nett utenfor virksomheten skal det etableres tekniske tiltak som ivaretar at:

- Kun eksplisitt angitt tillatt trafikk kan passere, annet stoppes
- Minst to uavhengige, tekniske tiltak skal iverksettes slik at personer utenfor virksomheten ikke skal kunne få uautorisert tilgang til og/eller kunne endre eller slette helse- og personopplysninger.

- Trafikk kan ikke passere direkte utenfra og inn; all slik ekstern trafikk må initieres fra virksomhetens systemer.
- Logging iverksettes for å kontrollere at regler ikke brytes; ved brudd stenges kanalen inntil ny sikker løsning finnes.

Meldingsformidling

Det må etableres klare ansvarsforhold mellom avsender, mottaker og eventuell meldingsformidler og ansvarsforholdene skal fremgå av avtalene mellom virksomhetene og meldingsformidler. Alle avtaler skal være skriftlige.

Avsender er ansvarlig for:

- Egen tilkoblingssikring som hindrer utilsiktet tilgjengeliggjøring og inntrenging.
- Tjenesten skal ikke kunne formidle program som inneholder virus e.l.
- Sikker overføringskryptering ende-til-ende.
- Rett adressering.
- Ved behov skal meldingen eller e-posten være signert på en slik måte at virksomheten ikke kan benekte å ha sendt den.
- Avviksrapportering i forbindelse med feilsending.
- Melding eller e-post avleveres i avtalt format.

Mottaker er ansvarlig for:

- Egen tilkoblingssikring som hindrer utilsiktet tilgjengeliggjøring og inntrenging.
- Ivareta overføringskryptering ende-til-ende.
- Ved behov skal mottaket registreres slik at mottaker ikke kan benekte å ha mottatt meldingen eller e-posten.
- Avviksrapportering i forbindelse med feil, dvs. mottak av melding eller e-post som ikke er adressert til virksomheten.
- Melding eller e-post mottas i avtalt format.

Meldingsformidler er ansvarlig for:

- Melding eller e-post kun avleveres til adressaten.
- Melding eller e-post skal ikke endres eller destrueres under transport fra avsender til mottaker.
- Melding eller e-post skal ikke kunne leses av andre enn avsender og mottaker.
- Melding eller e-post skal avleveres innen avtalte tidsfrister fra avsendelse.
- Avviksrapportering i forbindelse med alle ovenstående punkter.

E-post, SMS og sosialmedier
Virksomheten skal iverksette tiltak for å forhindre at helseopplysninger tilgjengeliggjøres ved hjelp av e-post, SMS eller andre ukrypterte kanaler.

- Virksomheten skal forsikre seg om ved tekniske tiltak og organisatoriske tiltak at epost ikke inneholder identifiserbare helseopplysninger.
- Logging skal iverksettes for å kontrollere at regler ikke brytes. Regelbrudd skal håndteres som avvik og personalmessige konsekvenser skal vurderes.

Tilkobling til Internett
Virksomheten skal iverksette tiltak:

- Tekniske tiltak som sikrer at Internett-tjenesten er logisk atskilt fra der helse- og personopplysninger behandles.
- Logging iverksettes for å kontrollere at regler ikke brytes. Regelbrudd skal håndteres som avvik og personalmessige konsekvenser skal vurderes.

Digital kommunikasjon med pasienter/bruker

Ved digital kommunikasjon med pasienten er virksomheten ansvarlig for at:

- Pasienten/brukeren entydig identifiseres.
- Tekniske tiltak iverksettes slik at all kommunikasjon krypteres.
- Det ikke skal kunne kommuniseres samtidig med andre parter enn den angitte pasient/brukeren.
- Helse- og personopplysninger ikke stilles til rådighet på en slik måte at pasient/bruker er avhengig av å lagre opplysningene på eget utstyr for å gjøre seg kjent med informasjonen.

Leverandørforhold og avtaler
I dette punktet omtales kun de avtalemessige forhold som angår informasjonssikkerhet.

Under er listet eksempler på kommunikasjonsparter hvor det utveksles identifiserbare helseog personopplysninger, og/eller parter som har/får adgang til utstyr og/eller programvare hvor slike opplysninger behandles. Det skal inngås skriftlige avtaler med disse, dersom ikke annet er angitt. Avtalene skal inkludere forpliktelser om at partene skal oppfylle de krav og tiltak som følger av den til enhver tid gjeldende Norm for informasjonssikkerhet, samt regulering av sanksjoner ved brudd på Normen og avtalen for øvrig.

- Leverandør av kommunikasjonstjenester, f.eks. Norsk Helsenett. For virksomheter innen sektoren som ved tilknytningsavtale med Norsk Helsenett har forpliktet seg til å tilfredsstille kravene i dette dokument, er ingen særskilt avtale om informasjonssikkerhet nødvendig for kommunikasjon via helsenettet.
- Databehandlere, som utfører behandling av helse- og personopplysninger på vegne av virksomheten.
- Leverandører av utstyr og/eller programvare som må ha adgang for vedlikehold, feilretting, oppdatering, ved hjelp av online tilkobling og/eller fysisk oppmøte.
- Sikkerhetsleverandører.

Valg av databehandler
Databehandler har et selvstendig ansvar for informasjonssikkerhet og for ivaretakelse av den registrertes personvern.

Den dataansvarlige kan bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven.

Leverandører
Virksomheten skal for å ivareta konfidensialitet, integritet og tilgjengelighet for helse- og personopplysninger forsikre seg om at:

- leverandøren etterlever Normen med tanke på dataansvarliges plikter vedrørende sikkerhetsrevisjoner og avviksbehandling.
- leverandørens utstyr som benyttes ved online oppkobling ved hjelp av kommunikasjonsnett eller medbrakt utstyr som knyttes til virksomhetens utstyr, ikke har ondsinnet programvare som inneholder virus e.l. og at utstyret er sikret mot adgang fra uvedkommende.
- leverandøren kun skal få adgang etter særskilt tillatelse fra virksomheten i hvert enkelt tilfelle, og kun adgang til de enheter hvor det er behov.
- all adgang skal skje under overvåking fra virksomhetens personale.
- tilgjengelighet til helse- og personopplysninger så vidt mulig skal opprettholdes når leverandøren utfører arbeid på virksomhetens utstyr/programvare, slik at virksomhetens oppgavebehandling ivaretas.

Sikkerhetsleverandører
Den dataansvarlige skal etablere nødvendige sikkerhetstiltak. Et alternativ til egen etablering av sikkerhetstiltak kan være å få utført sikkerhetsoppgaver hos en leverandør hvor fordeling av oppgaver mellom virksomheten og leverandøren til sammen skal tilfredsstille kravene i Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Med sikkerhetsleverandøren skal det inngås avtale om gjennomføring av konkrete sikkerhetsoppgaver.

Tilgang til helseopplysninger mellom virksomheter
Det kan etableres tilgang til helseopplysninger mellom virksomheter. Med tilgang menes at helsepersonell i en virksomhet gis adgang til direkte elektronisk å hente frem helseopplysninger om pasienter/brukere registrert ved en annen virksomhet.

Håndtering av informasjonssikkerhetsbrudd

Virksomhetens ledelse, eller det organ ledelsen bemyndiger, skal behandle avvik med det formål å gjenopprette normal tilstand, fjerne årsaken til avviket og å hindre gjentagelse.

Avvikshåndteringen iverksettes ved sikkerhetsbrudd og/eller når behandling av helse- og personopplysninger er utført i strid med gjeldende regelverk, retningslinjer eller prosedyrer.

Avvikshåndtering kan også iverksettes ved tilfeller av manglende eller uhensiktsmessige prosedyrer.

Alle ansatte er ansvarlig for å rapportere oppdagede avvik

- Det skal samles inn fakta om hendelsesforløpet
- Det skal foreslås tiltak for å gjenopprette normal tilstand og forhindre gjentagelse.
- Tiltak og plan på det nivå som er gjennomførbart skal vedtas.
- Tiltaket iverksettes
- Det sendes statusrapport til virksomhetens ledelse
- Ved gjentatte avvik skal det gjennomføres ny risikovurdering.

IKT-beredskap

Manglende tilgjengelighet til helse- og personopplysninger kan medføre skader både for virksomheten og for virksomhetens brukere. Virksomheten må derfor sørge for at nødvendige helse- og personopplysninger er tilgjengelige også ved stopp i hele eller deler av det elektroniske informasjonssystemet.

Virksomheten må foreta en kartlegging av de enkelte informasjonssystemer med henblikk på kritikalitet.

Revisjonskriteriene punktvis oppsummert

PROBLEMSTILLING 1
Er det etablert planer og rutiner som ivaretar kommunens IT-sikkerhet på en tilfredsstillende måte?

1. Kommunen har beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi) eforv.forskr. § 15

2. Kommunens sikkerhetsmål og –strategi har tydelige krav og forventninger til sikkerheten. Jf. NSMs grunnprinsipper for IKT-sikkerhet.

3. Kommunens sikkerhetsstrategi og internkontroll inkluderer relevante krav som er fastsatt i annen lov, forskrift eller instruks. eforv.forskr. § 15

4. Kommunen har etabler tydelig ansvarfordeling i risikostyringen Jf. NSMs grunnprinsipper for IKT-sikkerhet.

5. Kommunen har oversikt over alt IKT-utstyr, jf norm for e-helse

6. Kommunen har en prosedyre for tilgangskontroll og autorisering, Jf. NSMs grunnprinsipper for IKT-sikkerhet og norm for e-helse

7. Kommunen har etablert prosedyrer for oppbevaring og bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel, signaturfremstillingsdata.

8. Kommunen har gjennomført en kartlegging av verdikjeder, informasjonsverdier, utstyr og brukertilganger Jf. NSMs grunnprinsipper for IKT-sikkerhet.

9. Kommunen har sørget for at det er etablert klare ansvarsforhold mellom avsender, mottaker og eventuell meldingsformidler ved sending av meldinger med helse- og personopplysninger. Norm for e-helse

10. Kommunen sørger for sikker overføringskryptering ende-til-ende for helse- og personopplysninger. Norm for e-helse

11. Kommunen har prosedyrer for avviksregistrering, norm for e-helse

12. Kommunen har prosedyrer for bruk av informasjonssystemene, norm for e-helse

13. Kommunen har en oversikt over type leverandører, norm for e-helse

14. Kommunen stiller krav til produkter og leverandører slik at sikkerheten er ivaretatt i hele produktets eller tjenestens levetid Jf. NSMs grunnprinsipper for IKT-sikkerhet

15. Kommunen har etablert en beredskapsplan for ulike typer hendelser Jf. NSMs grunnprinsipper for IKT-sikkerhet

16. Kommunen gjennomfører øvelser som tester planverket. Jf. NSMs grunnprinsipper for IKT-sikkerhet

17. Kommunen har en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. eforv.forskr. § 15

18. Kommunens internkontrollen er en integrert del av virksomhetens helhetlige styringssystem. eforv.forskr. § 15

19. Kommunen har planer for gjennomføring av sikkerhetsrevisjoner, jf norm for e-helse

PROBLEMSTILLING 2
Har kommunen implementert anbefalte sikkerhetstiltak mot dataangrep og uautorisert tilgang til informasjon?

1. Kommunen gjennomfører risikovurderinger på informasjonssikkerhetsområdet. eforv.forskr § 15, norm for e-helse

2. Kommunens prosess for risikostyring er en del av en helhetlig styringsstruktur og er kjent i virksomheten. Jf. NSMs grunnprinsipper for IKT-sikkerhet.

3. Kommunen har, med bakgrunn i risikoene forbundet med de ulike behandlingene etablert et egnet sikkerhetsnivå knyttet til IT-sikkerheten, personvernforordn. art 32

4. Kommunen har iverksatt tiltak som sikrer at alle som har tilgang til personopplysninger, behandler nevnte opplysninger kun etter instruks fra kommunen. personvernforord. Art 32,

5. Kommunen har informert sine ansatte om hvilke sikkerhetstjenester og -produkter de skal benytte under tjeneste for organet, og hvorledes de skal gå frem for å anskaffe nødvendig utstyr og data, inkludert passord, PIN-koder mv. eforv.forskr § 17

6. Kommunen har prosedyrer for og sørger for sikker konfigurasjon Jf. NSMs grunnprinsipper for IKT-sikkerhet og norm for e-helse

7. Kommunen har kontroll på nettverk og komponenter, Jf. NSMs grunnprinsipper for IKT-sikkerhet, norm for e-helse

8. Kommunen sørger for god e-post og Websikkerhet, Jf. NSMs grunnprinsipper for IKT-sikkerhet

9. Kommunens internkontroll (styring og kontroll) på informasjonssikkerhetsområdet er basert på kommunens sikkerhetsmål og sikkerhetsstrategi. eforv.forskr § 15, norm for e-helse

10. Kommunens internkontroll har et omfang og en innretning som er tilpasset risikoen på informasjonssikkerhetsområdet. eforv.forskr § 15

11. Kommunen gjennomfører sikkerhetsrevisjoner jevnlig, norm for e-helse

12. Kommunen følger opp resultater fra disse sikkerhetsrevisjoner, norm for e-helse

13. Kommunen har etablert effektive rapporteringslinjer til toppledelse Jf. NSMs grunnprinsipper for IKT-sikkerhet.

14. Ledelsens gjennomgang skal være minimum årlig og dekke bl.a. avvikshendelser og eventuelle korreksjoner i styringssystemet, jf norm for e-helse