FORVALTNINGSREVISJONSRAPPORT

SARPSBORG KOMMUNE
8. SEPTEMBER 2020

IT-sikkerhet

Sikkerhetskultur i Sarpsborg kommune

Delrapport 2 av 2

Deler av rapporten er unntatt offentlighet jamfør offentleglova § 24 (3).
Denne versjonen er sladdet.

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 - juli 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. Denne revisjonen er gjennomført før og under perioden med Korona-tiltak i Norge. Spørreundersøkelsen, som store deler av delrapport 2 er basert på, ble utsatt. For å sikre fremdrift i prosjektet besluttet revisjonen i samråd med sekretariatet og kommunens kontaktperson, å utarbeide en rapport som består av to deler. Denne rapporten er delrapport 2 og omhandler sikkerhetskulturen i kommunen. Delrapport 1 er ferdigstilt og omhandler planer og rutiner for IT-sikkerhet og iverksatte sikkerhetstiltak.[3]

Vi har kvalitetssikret faktagrunnlaget underveis gjennom verifisering av intervjuer og referater fra systemgjennomgang. Revisjonen har gjennomført høringsmøte med administrasjonen 27. august 2020. I etterkant av møtet er rapporten sendt på offisiell høring i kommunen. Kommunedirektørens uttalelse fremgår av kapittel 4.

Prosjektets del 2 er gjennomført av Unn Elisabeth West med bistand fra Odd Henning Aure. Revisorenes habilitet og uavhengighet er vurdert opp mot kommunen og undersøkte virksomheter, og revisjonen finner de habile til å utføre prosjektet.

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

Østre Viken Kommunerevisjon IKS
Rolvsøy, 8. september 2020

Lene Brudal
Oppdragsansvarlig revisor

Unn Elisabeth West
Forvaltningsrevisor

Odd Henning Aure
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.

[3] Rapporten ble behandlet i kontrollutvalgets møte 9. juni 2020, sak 20/20.

Sammendrag

Sikkerhetskulturen er en del av organisasjonskulturen, og handler om hvilke verdier som ligger til grunn for den enkeltes valg for håndtering av informasjon og systemer. Sikkerhetskultur er dermed den felles oppfattelsen i virksomheten som har positive eller negative konsekvenser for informasjonssikkerheten.

Sarpsborg kommune har et uttalt mål om å etablere en sikkerhetskultur som omfatter alle ansatte, også deltidsansatte i kommunen.

Revisjonen har i denne rapporten – del 2, sett på flere ulike aspekter ved sikkerhetskulturen i kommunen ved å gjennomføre en spørreundersøkelse. Flere av revisjonens vurderinger bygger i til dels betydelig grad på resultater fra spørreundersøkelsen, i tillegg til opplysninger fra intervjuer og gjennomgang av dokumenter.

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 for å identifisere kriterier å måle kommunen opp mot. 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. Data er hentet inn gjennom en spørreundersøkelse til ansatte i kommunen, analyse av dokumenter oversendt fra kommunen, intervjuer med ansatte og ledere i organisasjonen, gjennomgang av systemer for overvåking og IT-sikkerhet, og gjennomgang av kommunens kvalitetssystem RiskManager. Det er også gjennomført en test av kommunens IT-sikkerhet. Testen er utført av et eksternt firma, Netsecurity.

Revisjonens funn og konklusjoner
Vi har i denne rapporten sett at kommunen har etablert flere tiltak for å skape en god sikkerhetskultur. Å skape en god sikkerthetskultur krever et kontinuerlig arbeid i organisasjonen. Vi har påpekt noen forbedringsområder som vi mener er hensiktsmessig at kommunen arbeider videre med for å etablere en tilfredsstillende sikkerhetskultur, og et enda bedre nivå på sikkerheten. For enkelte av områdene er det allerede knyttet anbefalinger til i delrapport 1.

Revisjonens anbefaler at Sarpsborg kommune bør

- gjøre ansatte kjent med rutiner for risikovurdering, herunder vurdere å involvere ansatte i arbeidet med å identifisere, vurdere og dokumentere risiko på området
- gjøre ansatte kjent med rutiner for registrering av avvik på området, herunder sørge for at de ansatte vet når og hvor de skal melde avvik
- sørge for at de ansatte har relevante styringsdokumenter på området lett tilgjengelig

1 Gjennomføring av prosjektet

Bakgrunnen for prosjektet fremgår av prosjektplanen datert 5. desember 2019 *«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). Den nye personvernforordningen som tredde i kraft 25. mai 2018 innebar strengere regler knyttet til 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 Problemstilling og avgrensning

I del 2 av denne forvaltningsrevisjonsrapporten har vi følgende problemstilling:

Har kommunen etablert en god sikkerhetskultur i organisasjonen?

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. Vi har i denne delen av prosjektet undersøkt om det er etablert en god sikkerhetskultur i organisasjonen. Dette innebærer blant annet at ansatte kjenner kommunens sikkerhetsmål- og strategi og om prosedyrer og rutiner på sikkerhetsområdet er kjent.

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:

- *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 omsorgstjenesten*
- *Nasjonal strategi for digital sikkerhet 05/2019*
- *ISO/IEC 27001 (Information technology)*

Revisjonskriteriene fremkommer i kapittel 2.1, utledningen av revisjonskriteriene fremkommer i vedlegget.

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 denne delen av prosjektet er informasjonen hentet inn gjennom bruk av følgende metoder

- spørreundersøkelse
- dokumentanalyse (beskrevet i delrapport 1)
- intervjuer (beskrevet i delrapport 1)

Vi viser også til delrapport 1 der det er relevant. I delrapport 1 er det også benyttet andre metoder.[4]

Spørreundersøkelsen

Det er gjennomført en spørreundersøkelse der kommunens ansatte har svar på spørsmål om hvordan de forholder seg til IT-sikkerheten i kommunen – sikkerhetskulturen. Undersøkelsen er gjennomført ved hjelp av det nettbaserte spørreundersøkelsesverktøyet Questback.

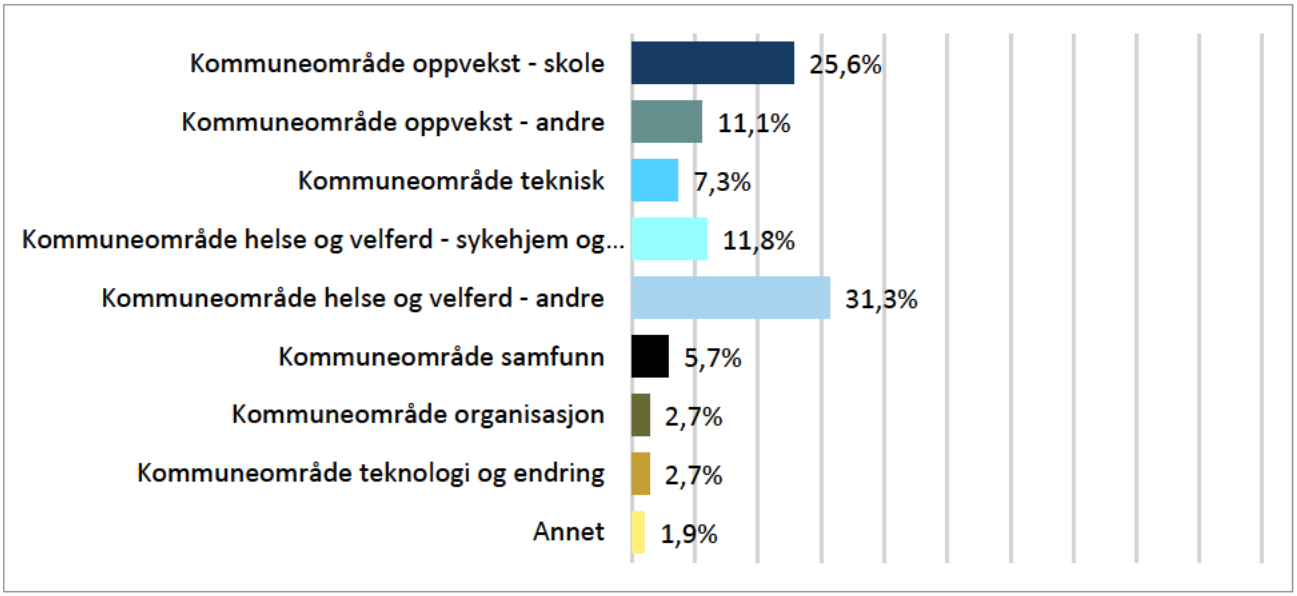
Undersøkelsen ble sendt ut 16. april 2020 med svarfrist 22. april 2020. Den er sendt til totalt 731 ansatte i kommunen og alle de ulike fagområdene i kommunen er inkludert i undersøkelsen. Revisjonen har fått opplyst om at en stor del av de ansatte har/har hatt hjemmekontor på grunn av Korona-tiltakene. Revisjonen ba kommunens kontaktperson om å sende ut et forhåndsvarsel til de ansatte, for å varsle at det ville komme en spørreundersøkelse. Dette for at de ansatte skulle vite at det var trygt å gå inn på lenken til undersøkelsen.

Totalt 262 ansatte svarte på undersøkelsen. Dette gir en svarprosent på 35,8 prosent, noe vi mener gir et godt grunnlag for å trekke konklusjoner fra besvarelsene.

Fordelingen av hvilke kommuneområder de ansatte som besvarte spørreundersøkelsen tilhører, er vist i figur 1. Vi ser at 80 prosent av respondentene jobber innenfor de to store kommuneområdene Helse og velferd og Oppvekst og utdanning.

[4] I delrapport 1 er følgende metoder benyttet:
- Dokumentanalyse
- Intervjuer
- Testing av IT-sikkerheten
- Systemgjennomgang

Figur 1: Respondentenes plassering per kommuneområde.

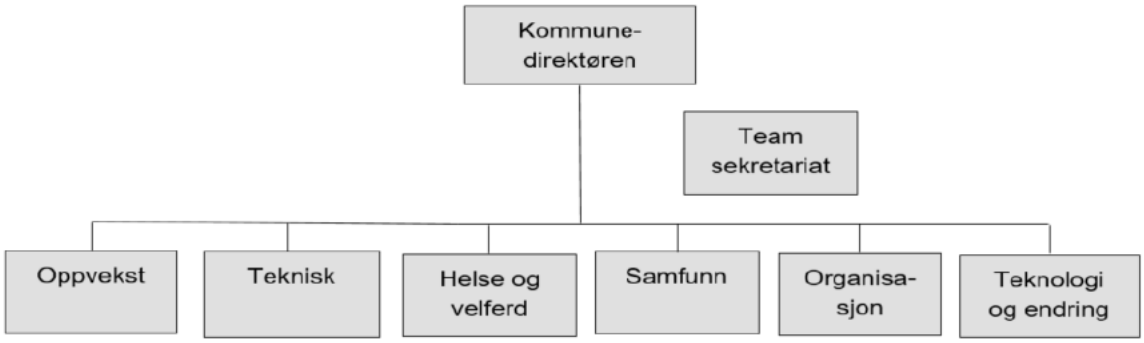


n=262

Om kommunen

Sarpsborg kommune har 4 410 ansatte per 1. januar 2020. Under kommunedirektøren er kommunen organisert i seks kommuneområder jf. figur 2. I tillegg er det en stab direkte underlagt kommunedirektør – team sekretariat.

Figur 2: Organisasjonskart Sarpsborg kommune.



2 Sikkerhetskultur

Problemstilling: Har kommunen etablert en god sikkerhetskultur i organisasjonen?

2.1 Revisjonskriterier

Sikkerhetskulturen er en del av organisasjonskulturen, og handler om hvilke verdier som ligger til grunn for den enkeltes valg for håndtering av informasjon og systemer. Sikkerhetskultur er dermed den felles oppfattelsen i virksomheten som har positive eller negative konsekvenser for informasjonssikkerheten.[5] Det forventes at ansatte skal følge prosedyrer og retningslinjer, slik at de ikke utsetter seg selv eller virksomheten for unødvendig risiko. For å få til dette kreves det at de ansatte har kunnskap. Virksomheten må sørge for at ansatte har tilstrekkelig kunnskap for å kunne ta de riktige valgene på jobb. Metodene som benyttes må motivere og skape læring hos de ansatte.

Revisjonskriterier:

- Kommunen har fastsatt ønsket kultur for informasjonssikkerhet og gjennomfører tilpasset (årlig) opplæring for å fremme god sikkerhetskultur.
- Kommunens ansatte har fått opplæring og tilstrekkelig kompetanse i de relevante delene av kommunens sikkerhetssystemer.
- Ansatte kjenner kommunens sikkerhetsstrategi.
- Kommunens prosess for risikostyring er kjent for ansatte i virksomheten.
- Kommunens styringsdokumenter for sikkerhetsarbeidet er tilgjengelig for virksomhetens ansatte.
- Kommunens ansatte sørger for forsvarlig oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder o.l.
- Ansatte varsler straks den som er utpekt til å motta varsel, dersom det oppstår mistanke om at passord/PIN-koder o.l. er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt.
- Ansatte vet når og hvor de skal melde avvik på informasjonssikkerheten.
- Kommunens ansatte følger instruksene arbeidsgiver har fastsatt om bruk og sikring av virksomhetens informasjonssystemer.

[5] Kilde: Difi's veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet

2.2 Revisjonens undersøkelse

Sarpsborg kommune har et uttalt mål om å etablere en sikkerhetskultur som omfatter alle ansatte, også deltidsansatte i kommunen. Kommunens sikkerhetsmål og sikkerhetsstrategi beskriver hva som er målene på ulike områder i sikkerhetsarbeidet og hva som er kravene/forventningene for at disse målene skal kunne nås.

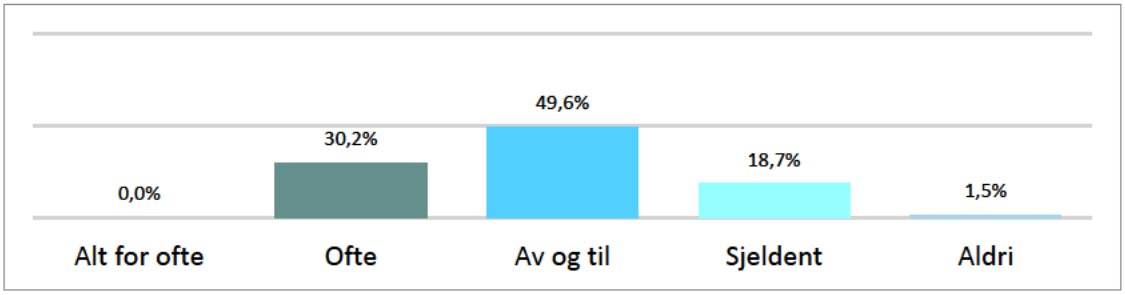
Ifølge direktør på kommuneområde Teknologi og endring (KTE) forsøker kommunen å få til en tredeling i arbeidet med informasjonssikkerhet. Avdelingsleder IKT drift skal være ansvarlig for å levere de tekniske løsningene for sikkerheten. Fagansvarlig informasjonssikkerhet skal jobbe kontinuerlig med sikkerhetskultur, risiko og sårbarhet, samt ha totaloversikten og stille de riktige og relevante spørsmålene på sikkerhetsområdet. Personvernombudet skal være den som håndhever GDPR. Fagansvarlig informasjonssikkerhet skal påse at det er kontinuitet, kvalitet og fremdrift i arbeidet med sikkerhetskulturen i kommunen.

Kommunens ansatte og IT-sikkerhet

I delrapport 1 fremkom at det gjenstår arbeid med å få etablert en sikkerhetskultur som har innsikt og forståelse for sikkerhetsarbeidet og de prosesser som må gjennomføres. I revisjonens spørreundersøkelse ble det stilt noen spørsmål til kommunens medarbeidere om deres oppfatninger og tanker rundt IT-sikkerhet i kommunen.

Fra figur 3 ser vi at om lag halvparten av respondentene har svart at IT-sikkerhet blir diskutert «av og til» i vedkommende sin virksomhet, mens hhv. 19 og 30 prosent svarer at IT-sikkerhet blir diskutert sjelden, eller ofte.

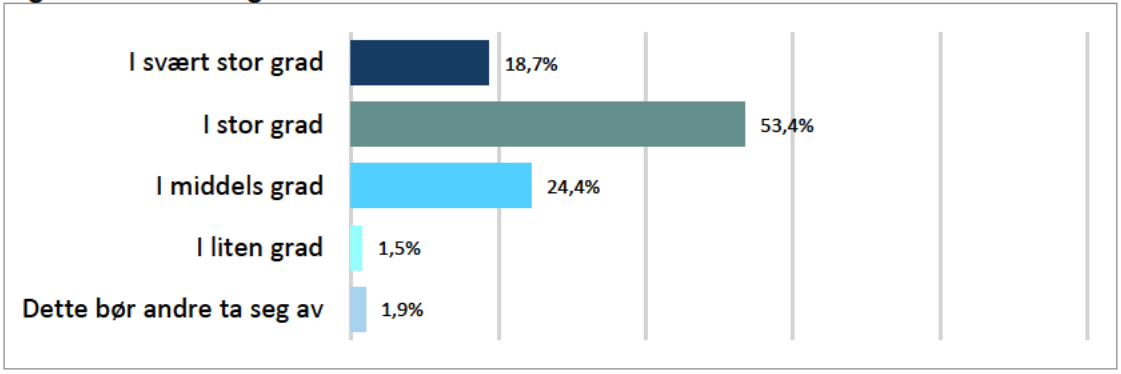
Figur 3: Diskuterer dere ofte IT-sikkerhet i din virksomhet?



n=262

På spørsmål i hvor stor grad de ansatte skal involveres i arbeidet med IT-sikkerhet, svarer i overkant av 72 prosent av respondentene at de ansatte bør involveres i stor, eller svært stor grad, jf. figur 4. Henholdsvis 1,5 prosent og 1,9 prosent av respondentene mener dette er noe som i liten grad, eller ikke i det hele tatt, skal involvere de ansatte.

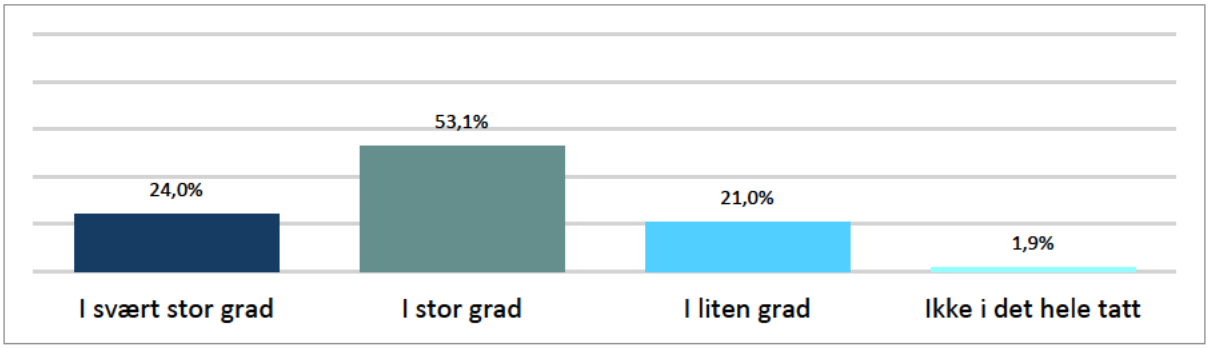
Figur 4: I hvor stor grad tenker du at ansatte skal involveres i arbeidet med IT-sikkerhet?



n=262

Videre mener mer enn halvparten av respondentene at deres atferd påvirker IT-sikkerheten i stor grad, samtidig som at nær en fjerdedel vurderer dette å gjelde i svært stor grad, jf. figur 5. 1,9 prosent av respondentene, mener at deres atferd ikke påvirker IT-sikkerheten.

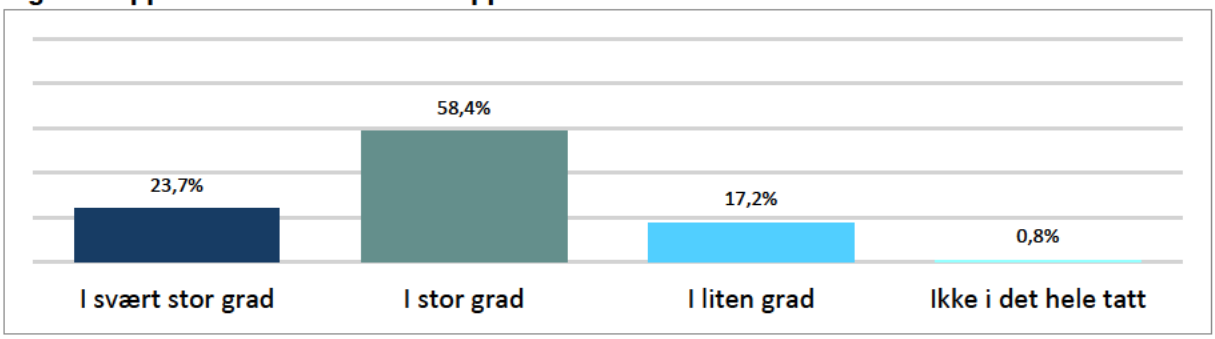
Figur 5: I hvilken grad tenker du at din atferd påvirker IT-sikkerheten?



n=262

Samtidig ser vi fra figur 6 at 82 prosent av respondentene opplever at deres leder i stor grad er opptatt av IT-sikkerhet, mens resten svarer at dette gjelder i liten, og i et par tilfeller, «ikke i det hele tatt».

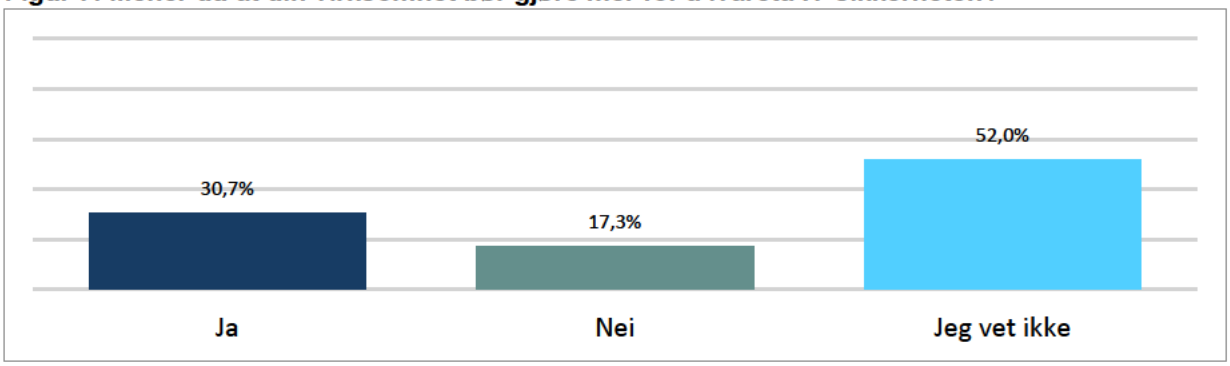
Figur 6: Opplever du at din leder er opptatt av IT-sikkerheten?



n=262

På spørsmålet om virksomhetene som den enkelte ansatte tilhører bør gjøre mer for å ivareta IT-sikkerheten, svarer halvparten av respondentene at de ikke vet dette, jf. figur 7. Nærmere 31 prosent av respondentene har svart at vedkommende sin virksomhet bør gjøre mer for å ivareta IT-sikkerheten.

Figur 7: Mener du at din virksomhet bør gjøre mer for å ivareta IT-sikkerheten?



n=262

[redacted]

[redacted]

Opplæring

I dokumentene *Arbeidsreglement*, udatert, og *Ansettelsesprosedyre nr. 01 til 04 sjekklister* fremkommer momenter som leder skal følge opp overfor nyansatte til ulike tidspunkt gjennom det første året. Fra dokumentene fremgår det at leder skal sørge for utstyr, gå gjennom låse- og alarmsystemet, vise pålogging og e-post, og informere om viktige kommuneovergripende dokumenter. Det blir vist til at det finnes mange nyttige dokumenter i RiskManager under arkfanen "Nyansatt". Av oversendt

dokumentasjon fra kommunen finnes det her blant annet *Brosjyre for informasjonssikkerhet Sarpsborg kommune* og *Retningslinjer for bruk av sosiale medier*. I dokumentet *Retningslinjer for bruk av kontorstøtteverktøy*, datert 13. mai 2014 fremkommer det informasjon om bruk av e-post, kalender, Chat-verktøy, Sarpedia og lagring av informasjon og dokumenter.

Fagansvarlig informasjonssikkerhet forteller at det er stor etterspørsel i kommunen etter mer informasjon og kompetanse på de ulike områdene innen informasjonssikkerhet, noe som betyr at de er oppmerksomme på sikkerheten.

Fagansvarlig informasjonssikkerhet opplyser om at kommunen har gjennomført nanolæring i oktober i flere år på rad. De har nå utarbeidet en større pakke for å sikre opplæringen av de ansatte. Dette er etablert gjennom KS læring. Det er opprettet en opplæring for ledere, en for ansatte som behandler sensitive data, og en for ansatte generelt. Pakken er ferdig og har åtte moduler. Opplæringspakken lærer bort det som er policyen til kommunen på informasjonssikkerhetsområdet. Planen er at pakken skal bli introdusert gjennom IT-avdeling og ledelsen i de ulike kommuneområdene. De første som skal få opplæring er kommuneledelsen. Det blir vurdert en enklere opplæring til ansatte som ikke har lederstillinger, som ikke er databrukere eller ikke bruker systemer direkte i jobben.

I en redegjørelse fra kommunen, udatert, fremkommer det at kommunen har flere opplæringsprogram som er rettet mot IT-sikkerhet.

- Obligatorisk E-Læringskurs i IKT-reglementet skal gjennomføres av alle ansatte.
- E-læringskurset «Nyansatt i Sarpsborg kommune» skal gjennomføres av alle nyansatte
- E-læringskurset «IKT-opplæring for medarbeidere i Sarpsborg», som inneholder følgende elementer
    - Informasjonssikkerhet
    - IKT-utstyr og fellessystemer
    - E-post og kalender
    - Sarpedia (intranettet)
    - Kontakt med jobben hjemmefra
- Nytt kurs i informasjonssikkerhet og personvern. Planlagt for alle ansatte i 2020, som inneholder følgende elementer:
    - Informasjonssikkerhet for ledere
    - Informasjonssikkerhet for medarbeidere - sensitive opplysninger
    - Informasjonssikkerhet for medarbeidere
- Introduksjonsdag for nyansatte med 20 minutter om informasjonssikkerhet
- Lederopplæring, nye ledere med en halv dag med personvern og informasjonssikkerhet

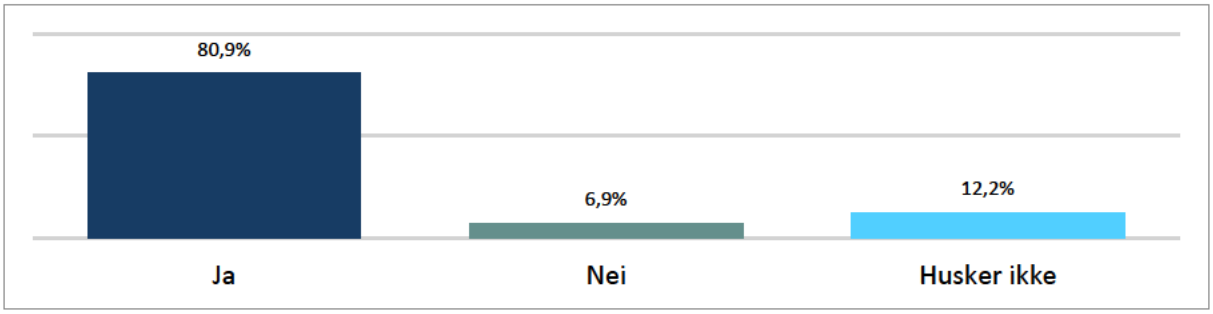
Kommunen har en egen sikkerhetsinstruks for ansatte som benytter Gerica i sitt arbeid *Sikkerhetsinstruks for brukere av Gerica*, datert 5. desember 2008. Her fremkommer det blant annet at ansatte skal ha lest folderen *Min elektroniske arbeidsplass*, og ha lest og undertegnet skjemaet *Sikkerhetsinstruks bruker*. I vedlegget til dette skjemaet, siste oppdatert 19. august 2015, fremkommer det informasjon om at den ansatte skal ha lest *Internkontroll Gerica*, *Informasjonssikkerhet* og etterfølge sikkerhetsinstrukser som gjelder for IKT og Gerica. Det fremkommer også informasjon om rapportering og avvik, bruk av internett og e-post, samt håndtering og lagring av informasjon og dokumenter.

I intervjuene med ansatte som jobber på helseområdet fremkommer det at kommunen har ca. 2 500 aktive brukere i Gerica og ca. 5 000 pasienter. Norm for e-helse ble implementert i kommunen for 6-7 år siden. Alle ansatte som jobber på helse- og velferdsområdet mottar og signerer skjemaet *Sikkerhetsinstruks bruker.* I intervjuene har det blitt påpekt at helseområdet har for mange prosedyrer og rutiner i RiskManager, noe som gjør det vanskelig for ansatte å finne frem i systemet.

I intervjuene blir det opplyst om at de på helseområdet har superbrukere som skal gi opplæring til nyansatte. Dette følges opp på superbrukermøter.

Fra svarene i spørreundersøkelsen ser vi at de fleste respondentene, 81 prosent, svarer at de har fått opplæring i IT-sikkerhet, mens 7 prosent svarer at de ikke har fått noen opplæring jf. figur 10.

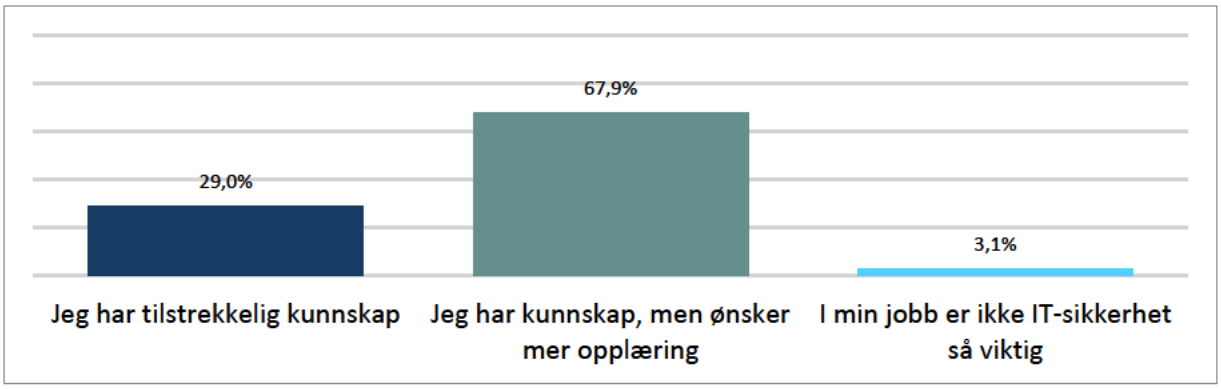
Figur 10: Har du fått opplæring i IT-sikkerhet?



n=262

Samtidig ser vi fra figur 11 at rundt to tredjedeler av respondentene ønsker mer opplæring, mens 29 prosent mener de har tilstrekkelig kunnskap på området. Flere av de ansatte som svarte at IT-sikkerhet ikke er så viktig i deres jobb, begrunnet dette med at de brukte lite pc i jobben.

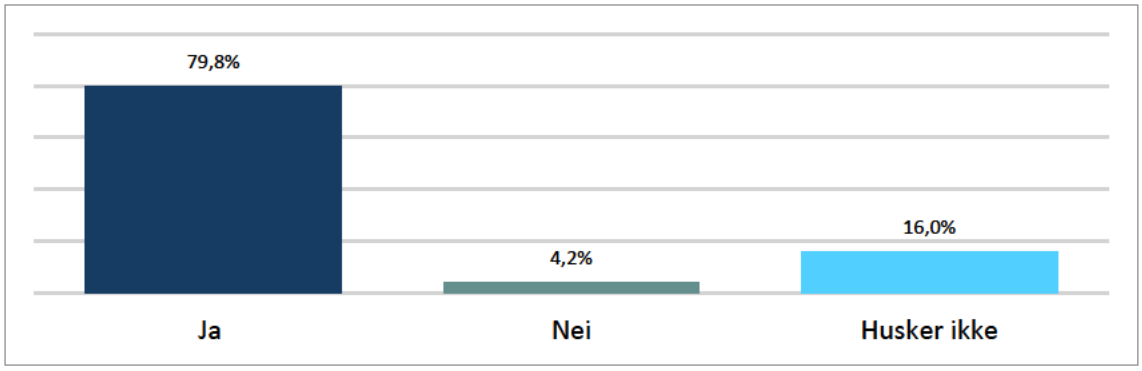
Figur 11: Mener du at du har tilstrekkelig kunnskap om IT-sikkerhet?



n=262

Fra figur 12 ser vi at 80 prosent av respondentene i spørreundersøkelsen har gjennomført, og dermed signert IKT-reglementet i Sarpsborg kommune. Litt over 4 prosent har ikke gjennomført e-læringskurset, mens 16 prosent ikke husker om de har tatt kurset eller ikke.

Figur 12: Har du gjennomført det obligatoriske e-læringskurset *IKT-reglement for Sarpsborg kommune*?



n=262

IKT-reglementet gjelder for bruk av Sarpsborg kommunes IKT-ressurser. Reglementet gjelder også for bruk av eksterne IKT-ressurser som for eksempel løsninger levert over Internett av eksterne

leverandører. Som en del av *Sjekkliste for egenkontroll av informasjonssikkerhet*[6] skal leder rapportere inn en gang per år at medarbeidere har signert IKT-reglementet. Signering av IKT-reglementet gjøres ved å gjennomføre E-læringskurset «IKT-reglementet». Alle medarbeidere er automatisk påmeldt kurset.

Når den enkelte medarbeider har gjennomgått hele IKT-reglementet, signerer vedkommende på slutten av kurset. Hvis noen har vært aktive, men ikke bestått, betyr dette at de ikke har signert. Et par steder i leksjonen må det svares riktig for å komme videre. Det godtas feil svar før man til slutt ender opp med riktig svar.

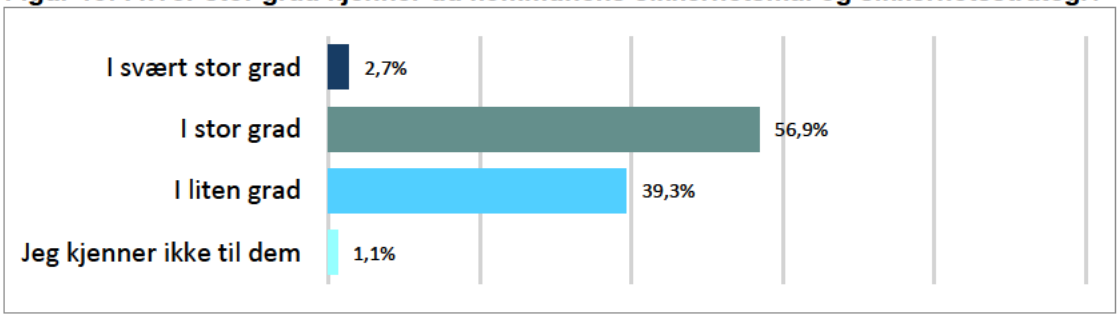
Ansattes kjennskap til kommunens sikkerhetsmål- og strategi og styringsdokumenter i sikkerhetsarbeidet

Kommunens sikkerhetsmål- og strategi er beskrevet i dokumentet med samme navn, datert 26. mars 2019. Strategien skal sikre at kommunen forvalter all informasjon i henhold til krav om konfidensialitet, integritet og tilgjengelighet, i lovverket. Dokumentet gjelder for alle ansatte og folkevalgte.

Det fremgår av intervjuene at samtlige vi har snakket med i denne revisjonen kjenner kommunens sikkerhetsmål- og strategi. Det blir også sagt at sikkerhetsmålene- og strategien er formidlet ut i virksomhetene, og at det er virksomhetslederne som har ansvaret for det.

Vi ser fra figur 13 at flertallet av respondentene i spørreundersøkelsen, nærmere 60 prosent, kjenner til kommunens sikkerhetsmål- og strategi i stor grad, og i noen tilfeller, i svært stor grad. Samtidig er det mer enn 39 prosent av respondentene som kjenner til disse i liten grad. Om lag en prosent kjenner ikke til dem.

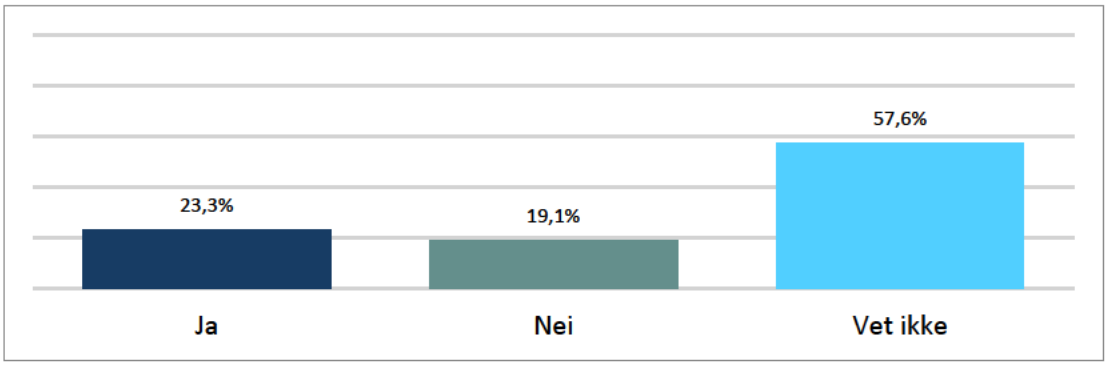
Figur 13: I hvor stor grad kjenner du kommunens sikkerhetsmål og sikkerhetsstrategi?



n=262

På spørsmål om de ansatte har tilgang til kommunens styringsdokumenter for sikkerhetsarbeidet, ser vi fra figur 14 at mer enn 57 prosent av respondentene ikke vet om de har en slik tilgang. Om lag 19 og 23 prosent av respondentene, svarer henholdsvis nei og ja på dette spørsmålet.

Figur 14: Har du tilgang til kommunens styringsdokumenter for sikkerhetsarbeidet?



n=262

[6] Denne sjekklisten skal blant annet også sikre at virksomheten har rutiner på IKT-området og at avvik innenfor informasjonssikkerhetsområdet blir meldt og behandlet.

I delrapport 1 fremkommer at ikke alt er helt på plass i kvalitetssystemet når det gjelder arbeidet på sikkerhetsområdet. Videre fremkommer at 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 blant kommunens ledere.

I delrapport 1 fremkommer 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.

Risikostyring

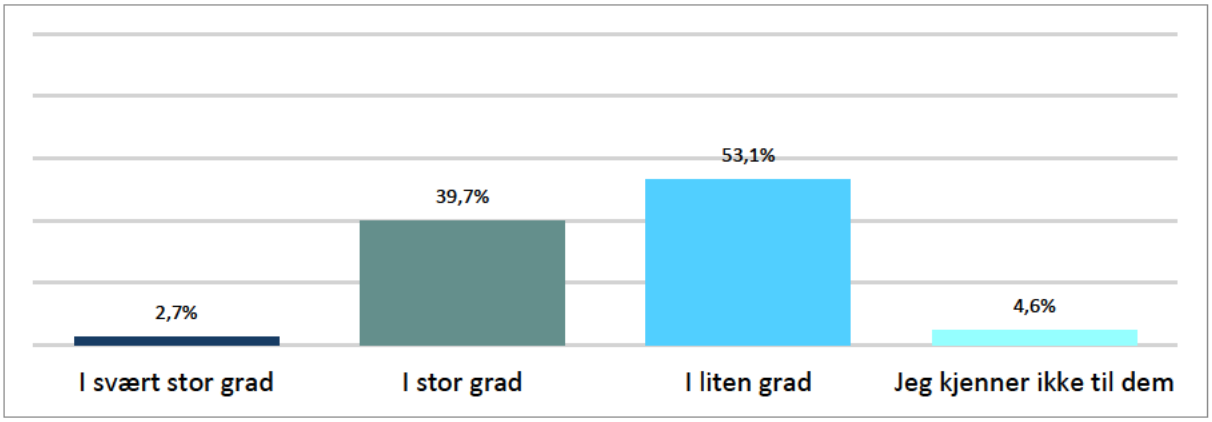
Fagansvarlig informasjonssikkerhet opplyser om at de enkelte avdelingene og virksomhetene i kommunen er ansvarlig for å vurdere sine risikoområder, vurdere bruken av sine systemer og prosesser, hvor de lagrer data og om de vurderer om ansatte har tilstrekkelig forståelse for IT-reglementet. Det fremkommer fra intervjuene at kommunikasjonen rundt IT-sikkerheten varierer fra kommuneområde til kommuneområde.

Ifølge direktør KTE har kommunen fokus på alle sider av arbeidet med IKT-sikkerhet. Kommunen har utarbeidet mange prosedyrer og rutiner på sikkerhetsområdet, han tror derfor at det kan være utfordrende for medarbeiderne å være oppdatert på alle disse prosedyrene og rutinene.

Kommunen har skriftlige rutiner på når og hvem som skal gjøre risikovurderinger på de ulike områdene, jf. *Rutiner for gjennomføring av risikovurderinger informasjonssikkerhet,* datert 1. mars 2015. Rutinene og risikovurderingene ligger i kvalitetssystemet – RiskManager. I rutinen fremkommer det at risikovurderinger skal gjennomføres og dokumenteres minimum en gang i året. Rutinen gjelder for alle medarbeiderne i kommunen.

Vi ser fra figur 15 at mer enn 42 prosent av kommunens ansatte kjenner godt til kommunens *Rutiner for gjennomføring av risikovurderinger informasjonssikkerhet*. Samtidig kjenner 53 prosent av respondentene i liten grad til disse rutinene. Nær 5 prosent kjenner ikke til dem.

Figur 15: I hvor stor grad er du kjent med kommunens *Rutiner for gjennomføring av risikovurderinger informasjonssikkerhet*?



n=262

Det fremkommer i gjennomgangen av RiskManager at kommunen har gjennomført risikovurderinger i flere år. Fra intervjuene fremgår det at det gjøres flere typer risikovurderinger i forbindelse med IT-sikkerhet. For eksempel har IT-avdelingen fokus på at alle nye systemer blir risikovurdert.

De som jobber med informasjonssikkerheten i kommunen sier at det imidlertid ikke er tilstrekkelig forståelse i organisasjonen for når i prosessen en gjør hvilke vurderinger. Her blir det påpekt at det blir gjort mange risikovurderinger, samtidig er det manglende forståelse for når i prosessen man gjør hvilke vurderinger.

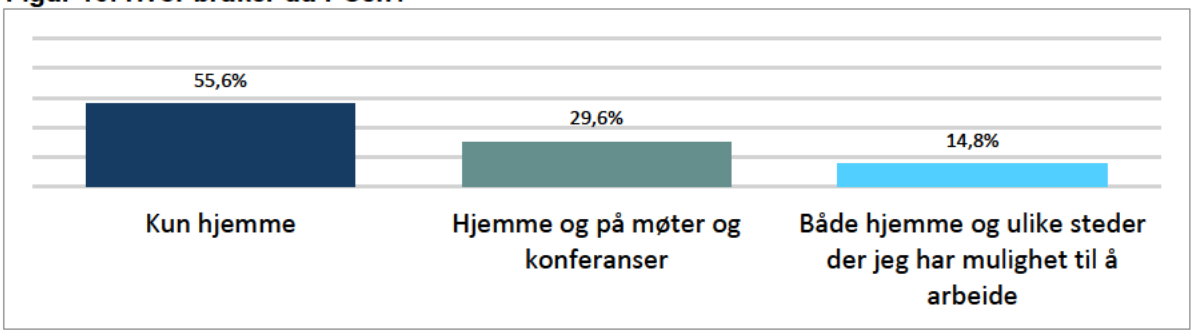
Videre er mange av risikovurderingene dokumentert i Excel/Word-dokumenter som er lagret i RiskManager, og dermed ikke i risikomodulen til systemet. Ifølge kommunens personvernombud vil en da miste noe av oversikten og et hjelpemiddel til gjennomføring av tiltak.

Leder IT-drift opplyser om at IT-avdelingen gjennomfører ROS-analyser sammen med de som skal bruke tjenesten, for deretter å foreta tiltak for å redusere risikoen på området. Det er opp til systemeier, som eier dataene, å vurdere om den gjenværende risikoen er akseptabel. I intervjuene med de ansatte i IT-avdelingen kommer det også frem at de opplever at IT-avdelingen er gode på ROS-analyser. De har egne rutiner og system for å håndtere endringer. De har også et eget verktøy for dette - *Pureservice*[7].

Passord og bruk av pc

I spørreundersøkelsen ble de ansatte stilt noen spørsmål angående bruk av pc. Av figur 16 fremgår det at flertallet av respondentene som bruker jobb-pcen utenfor kontorstedet, bruker den kun hjemme. I underkant av 30 prosent av respondentene tar også pcen med seg på møter og konferanser, i tillegg til hjemme. Resterende respondenter gjør bruk av jobb-pcen ytterligere flere steder.

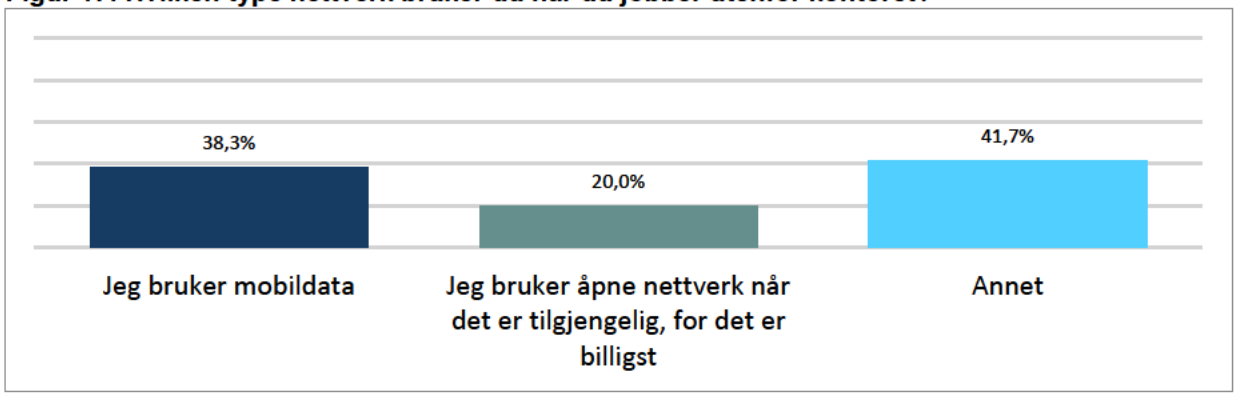
Figur 16: Hvor bruker du PCen?



n=262

Av respondentene svarer 38 prosent at de kobler seg på nettet gjennom mobildata, og 20 prosent kobler seg på gjennom åpne nettverk, jf. figur 17. I underkant av 42 prosent kobler seg på nettet gjennom andre løsninger.

Figur 17: Hvilken type nettverk bruker du når du jobber utenfor kontoret?



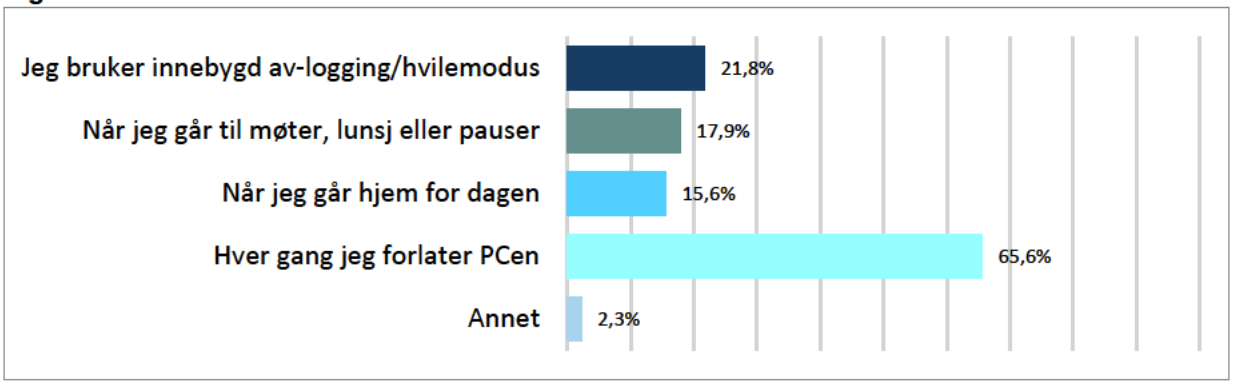
n=262

Systemansvarlig-stab oppvekst nevner at det finnes en rutine for bruk av bærbar PC, for eksempel at PC-en låses når man forlater den. Denne rutinen gjelder både hjemme og på jobb.

[7] *Pureservice change management* har som mål å sørge for planlegging, oppfølging og oversikt over endringer, til håndtering og beslutning av endringer.

I brosjyren *Min elektroniske arbeidsplass* fremkommer at det er et krav at de ansatte logger seg ut etter endt bruk og når de forlater arbeidsplassen. Fra spørreundersøkelsen ser vi at nærmere to tredjedeler av respondentene oppgir at de låser pcen hver gang de forlater den, jf. figur 18.[8] I underkant av 22 prosent benytter innebygd avlogging/hvilemodus.

Figur 18: Når låser du PCen din?



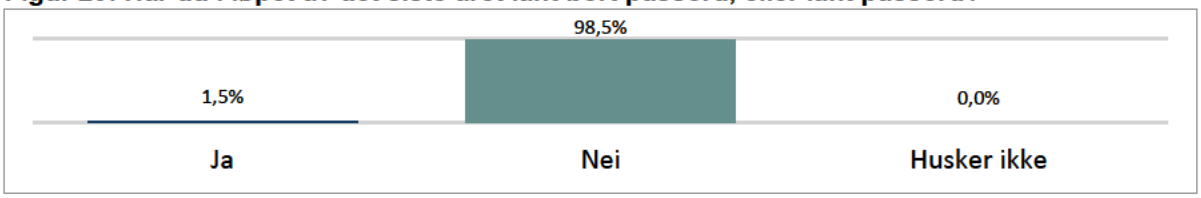
n=262

[redacted]

[8] I dette spørsmålet var det mulig å oppgi mer enn ett svaralternativ, slik at besvarelsene summerer seg til mer enn 100 prosent.

I brosjyren om informasjonssikkerhet *Min elektroniske arbeidsplass* står det at det er ikke tillatt å låne ut egen brukeridentitet til andre eller å avsløre eget eller andres passord.[9] Fra figur 20 ser vi at nesten alle respondentene, 98,5 prosent, har svart at de ikke har lånt bort, eller lånt andres passord, det siste året.

Figur 20: Har du i løpet av det siste året lånt bort passord, eller lånt passord?

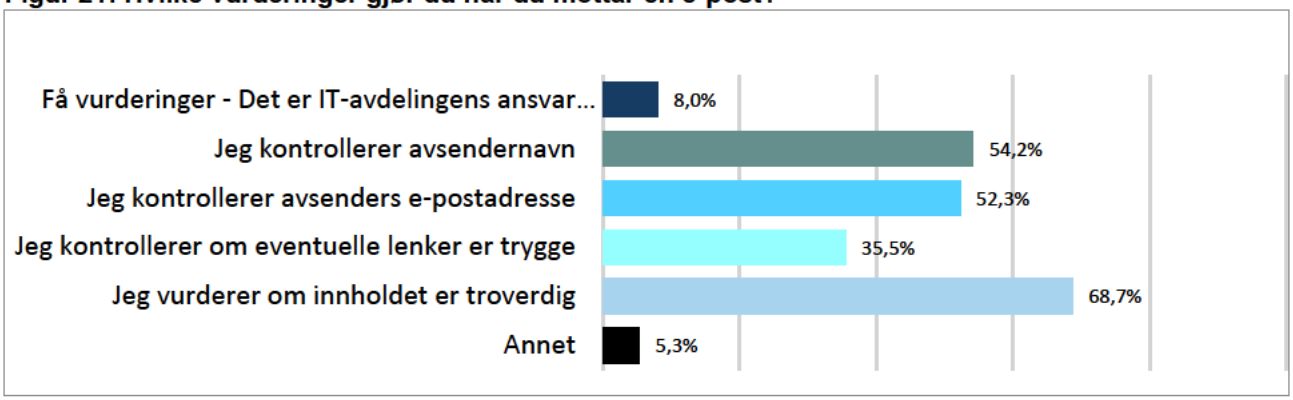


n=262

Varsling ved mistanke om brudd på IT-sikkerheten

I *Retningslinjer for bruk av kontorstøtteverktøy og lagring av dokumenter*[10] står det at ansatte aldri skal åpne «mistenkelig» epost, og at «useriøs epost» skal slettes umiddelbart. Fra figur 21 ser vi at mer en to tredjedeler av respondentene vurderer om innholdet er troverdig når de mottar en epost. Få overlater disse vurderingene i sin helhet til IT-avdelingen – 8 prosent.[11] Litt over halvparten kontrollerer avsendernavn og avsenders epostadresse. Drøyt en tredjedel kontrollerer om lenker er sikre.

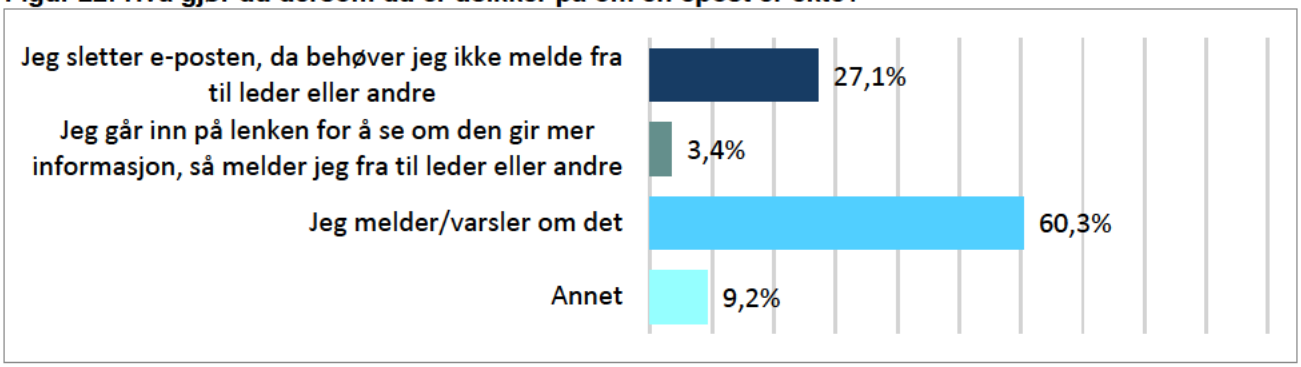
Figur 21: Hvilke vurderinger gjør du når du mottar en e-post?



n=262

De fleste av respondentene varsler hvis de er usikre på om en epost er «ekte», jf. figur 22. Noe over en fjerdedel av respondentene sletter eposten, uten å melde videre til leder eller andre.

Figur 22: Hva gjør du dersom du er usikker på om en epost er ekte?



n=262

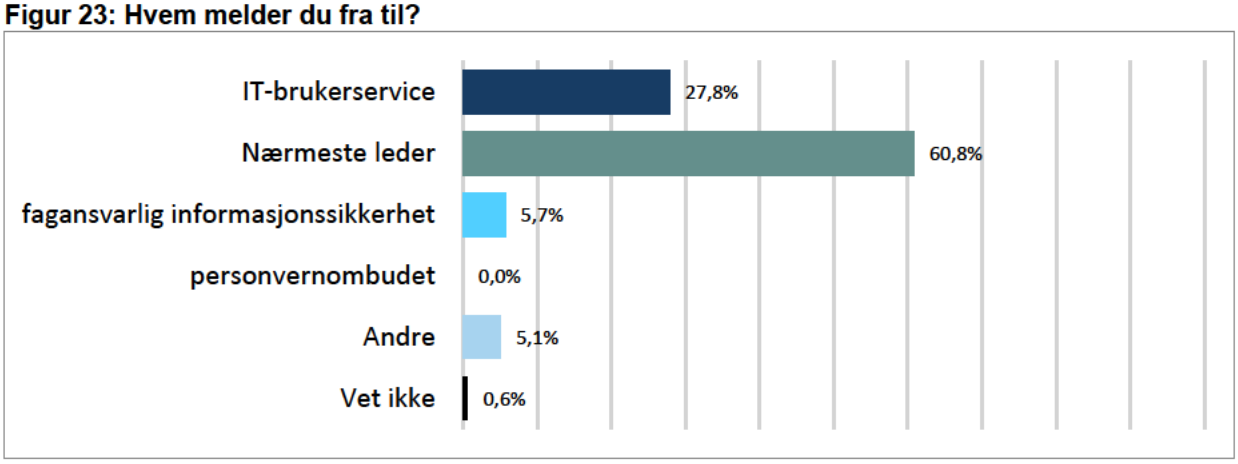
[9] I rapporteringen fra virksomhetene i *Ledelsens gjennomgang for 2018* har 82 prosent av de ansatte i kommunen fått denne brosjyren.

[10] Rutinen gjelder for alle ansatte i kommunen.

[11] Det var mulig å velge flere svaralternativer på dette spørsmålet.

Av de som varsler videre, vil over 60 prosent varsle nærmeste leder, nærmere 28 prosent ville kontaktet IT-brukerservice, mens knappe 6 prosent ville varslet fagansvarlig jf. figur 23.

Figur 23: Hvem melder du fra til?



n=262

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. Som vist til i delrapport 1 gikk 54 av de 750 (7%) ansatte på revisjonens phishingtest[12] og ga fra seg passordet sitt, og 13 besøkte phishing-siden, men ga ikke fra seg passordet. Resultatene av testen viste også noe usikkerhet blant ansatte på hvor og hva de skal rapportere ved slike hendelser. 20 ansatte tok kontakt med brukerservice og to av disse informerte om å ha gitt fra seg passordet. To ansatte rapporterte til egen leder, hvor en informerte om å ha gitt fra seg passordet.

Avviksmeldinger på informasjonssikkerhet[13]

Kommunen har en *Prosedyre for avviksbehandling*, datert 20. oktober 2017, hvor det fremkommer at alle ansatte er ansvarlige for å rapportere avvik innenfor sitt ansvars-/arbeidsområde, og at avvik skal registreres i kvalitetssystemet RiskManager. Det er den enkelte virksomhetsleder som har ansvar for oppfølging av rapportert avvik, når det gjelder iverksetting av tiltak og lukking av avvik, jf. *Retningslinje for kvalitetssystem.* Fra intervjuene fremkommer det at dette er kjent for de ansatte på IT-avdelingen.

KTE-direktør mener at avvikssystemet er godt innarbeidet i kommunen, men antar at det er underrapportering av avviksmeldinger.

Fra flere som har blitt intervjuet blir det hevdet at på området informasjonssikkerhet er det en underrapportering av avvik. Det har vært rapportert langt færre avvik på ikt-sikkerhet nå enn tidligere. Siden 2015 har det kun vært rapportert 3 avvik på området.

Personvernombudet opplyser om at de har jobbet mye med å få folk til å registrere avvik generelt. Mens de ansatte innenfor helse har en kultur for å melde avvik, er det andre tjenesteområder som mangler kultur for dette.

En av årsakene som blir trukket frem under intervjuer er at det kan være faglige utfordringer med å forstå hva som er et avvik og hva som ikke er det, når det gjelder informasjonssikkerhet.

[12] Se delrapport 1 for nærmere informasjon om phishingtesten.

[13] Mer utfyllende beskrivelse av avviksrapporteringen i kommunen finnes i rapportens del 1.

2.3 Revisjonens vurderinger

I delrapport 1 fremkom at det gjenstår arbeid med å få etablert en sikkerhetskultur som har innsikt og forståelse for sikkerhetsarbeidet og de prosesser som må gjennomføres. Revisjonen har i denne delen av undersøkelsen sett på flere ulike aspekter ved sikkerhetskulturen i kommunen ved å gjennomføre en spørreundersøkelse. Flere av vurderingene bygger i til dels stor grad på resultater fra spørreundersøkelsen, supplert med opplysninger fra intervjuer og gjennomgang av dokumenter. Flere av spørsmålene er generelle og vil speile de ansattes oppfatning rundt kommunens arbeid med IT-sikkerhet og egne holdninger.

80 prosent av respondentene mener at IT-sikkerhet ofte eller av og til blir diskutert i virksomheten. Over 80 prosent opplever også at lederne er opptatt av IT-sikkerhet. Dette indikerer at det er oppmerksomhet rundt IT-sikkerhet blant medarbeiderne i kommunen, noe som revisjonen mener er positivt. [redacted]

Gjennom sikkerhetsmål og sikkerhetsstrategi har kommunen fastsatt ønsket kultur for informasjonssikkerheten. Tilfredsstillende opplæring er avgjørende i arbeidet med å etablere en sikkerhetskultur. Fra revisjonens undersøkelser fremkommer det at kommunen har etablert flere tiltak som er egnet til å sikre de ansatte opplæring i IT-sikkerhet, blant annet flere e-læringskurs. Kommunen har også nylig utviklet en større opplæringspakke, som skal omhandle kommunens policy på området. Det finnes også brosjyrer som er rettet inn mot opplæring av ansatte innen informasjonssikkerhet. Det er etter vår oppfatning positivt at flere av tiltakene er obligatoriske.

De aller fleste respondentene i spørreundersøkelsen opplyser at de har fått opplæring i IT-sikkerhet, men to tredjedeler ønsker også mer opplæring på området. Revisjonen finner dette positivt, både fordi det viser at de fleste ansatte har fått en opplæring, men også fordi det kan tyde på at de ansatte også ønsker ytterligere opplæringstiltak, noe vi mener er viktig for å sikre effekt og nytteverdi av den opplæringen som gis. Revisjonen registrerer at flere respondenter etterlyser opplæring på andre måter enn via e-post.

Kjennskap til kommunens sikkerhetsmål- og strategi er også sentralt i kommunens arbeid med å etablere en sikkerhetskultur. Disse dokumentene beskriver hva som er målene på ulike områder i sikkerhetsarbeidet og hva som er kravene/forventningene for at disse målene skal kunne nås. Flertallet av respondentene fra spørreundersøkelsen kjenner i stor grad til kommunens sikkerhetsstrategi. Etter revisjonens oppfatning er det positivt at flertallet av respondentene kjenner til kommunens sikkerhetsstrategi, samtidig er det mange som i liten grad kjenner til den.

På den annen side er flertallet av respondentene fra spørreundersøkelsen i liten grad kjent med kommunens rutiner for risikovurdering. I delrapport 1 fremkommer også at ansatte har manglende forståelse for de prosesser som må til i forkant av innføringen av nye systemer og app'er, herunder risikovurderinger og sikringstiltak. Sikkerhetstiltak bør være basert på risiko, og at ansatte involveres i dette arbeidet kan være avgjørende for at de har forståelse for og motivasjon til å følge de sikkerhetstiltakene som iverksettes, og kan dermed ha en viktig betydning i arbeidet med å styrke sikkerhetskulturen. Mange av respondentene, mer enn halvparten, kjenner i liten grad, eller ikke i det hele tatt, til kommunens *Rutiner for gjennomføring av risikovurderinger informasjonssikkerhet.* Etter revisjonens vurdering er andelen av respondentene som ikke kjenner til rutinene for høyt, og medfører at et sentralt element i kommunens arbeid med sikkerhetskultur blir svekket.

Tilgang til relevante styringsdokumenter og rutiner/retningslinjer er også viktig for at de ansatte skal kunne sette seg inn i ønsket praksis og kultur i Sarpsborg kommune. Over halvparten av respondentene vet ikke om de har tilgang til kommunens styringsdokumenter for sikkerhetsarbeidet. Dette er et høyt antall. Noe av usikkerheten kan skyldes at det er uklart hva som ligger i begrepet «styringsdokumenter», slik at mye av usikkerheten kan ligge her. Men som beskrevet i delrapport 1 opplever flere at kvalitetssystemet er uoversiktlig, med svært mange dokumenter og dårlig sortering, og det kan være vanskelig for ansatte å orientere seg i systemet. I delrapport 1 pekte vi også på ulik begrepsbruk i de ulike rutinene og prosedyrene, samt at de til dels er overlappende, noe som også kan påvirke tilgangen til informasjonen.

Kommunen har rutiner som blant annet skal sørge for elektronisk sikkerhet gjennom utlogging etter endt bruk og når arbeidsplassen forlates, at brukeridentitet og passord ikke skal lånes bort og at regler for passord skal følges. Resultater fra spørreundersøkelsen viser at nærmere to tredjedeler av respondentene låser pcen hver gang de forlater den. Det er positivt at de fleste følger rutinene på området, men i utgangspunktet bør de ansatte låse pcen hver gang de forlater den, så her er det noe rom for forbedring. Samtidig bruker flere ansatte åpne nett og har med jobbpc på ulike steder. Spørreundersøkelsen viser videre at det er svært få som har lånt bort, eller lånt andres passord.

[redacted]

Kommunens systemer kan bli angrepet utenfra via e-post. Vi har undersøkt hvordan de ansatte håndterer e-post. Resultatet viser at de aller fleste av respondentene gjør flere vurderinger av e-posten, og melder fra ved usikkerhet. Det er etter revisjonens oppfatning positivt at et stort flertall av respondentene har denne tilnærmingen til ukjente e-poster. I overkant av 60 prosent av respondentene i spørreundersøkelsen varsler videre når de er usikre på om eposten er ekte, mens flesteparten av de resterende sletter eposten. De fleste varsler nærmeste leder.

[redacted]

Melding av avvik er i utgangspunktet et viktig element i virksomheters forbedringsarbeid, og å avdekke svakheter kan bidra positivt i arbeidet med å skape forståelse og god kultur knyttet til sikkerhetsarbeidet. Det er derfor positivt at kommunen har skriftliggjort rutiner for å melde avvik, og at det skal meldes avvik på informasjonssikkerhetsområdet særskilt. Det har imidlertid kun vært rapportert tre avvik på informasjonssikkerhet over en periode på fire år (siden 2015). Dette tyder på at de ansatte ikke vet når og hvor de skal melde avvik, og at det ikke er etablert noen kultur i kommunen for å melde avvik på dette området.

På de ovenfor nevnte områdene er det revisjonens vurdering at kommunens ansatte delvis følger arbeidsgivers instrukser. På enkelte områder fremstår praksis og kulturen i stor grad som god, eksempelvis knyttet til låsing av pc og kjennskap til sikkerhetsstrategi, mens på andre områder, som eksempelvis avvik, følges kommunens rutiner i liten grad. På enkelte områder er det også svakheter i kommunens rutiner som gjør at det er vanskelig å etablere en god sikkerhetskultur på området. Dette gjelder i særlig grad passord.

[14] Se delrapport 1 for nærmere informasjon om phishingtesten.

3 Konklusjon og anbefaling

I delrapport 1 var det vår foreløpige vurdering at kommunen var på god vei til å få et egnet sikkerhetsnivå sett opp mot regelverk og normer på området. Revisjonen står ved denne vurderingen også etter å ha sett nærmere på sikkerhetskulturen. Kommunen har etablert flere tiltak for å skape en god sikkerhetskultur. Vi har påpekt noen forbedringsområder som vi mener er avgjørende at kommunen arbeider videre med for å etablere en tilfredsstillende sikkerhetskultur og et enda bedre nivå på sikkerheten. Enkelte av områdene er det allerede knyttet anbefalinger til i delrapport 1. Vi anbefaler i tillegg at kommunen bør

- gjøre ansatte kjent med rutiner for risikovurdering, herunder vurdere å involvere ansatte i arbeidet med å identifisere, vurdere og dokumentere risiko på området
- gjøre ansatte kjent med rutiner for registrering av avvik på området, herunder sørge for at de ansatte vet når og hvor de skal melde avvik
- sørge for at de ansatte har relevante styringsdokumenter på området lett tilgjengelig

4 Kommunedirektørens uttalelse

Sarpsborg kommune

Unntatt offentlighet
OFL §5

ØSTRE VIKEN KOMMUNEREVISJON IKS
Råkollveien 103
1664 ROLVSØY

Deres ref.:	Vår ref.:	Dato:
	19/12318-21	04.09.2020

Kommunedirektørens uttalelse revisjonsrapport IT-sikkerhet del-2

Kommunedirektøren viser til uttalelse gitt i forbindelse med delrapport 1 og vil igjen takke Østre Viken Kommunerevisjon IKS for en godt gjennomført og grundig revisjon.

Kommunedirektøren merker seg at i delrapport 2 som handler om sikkerhetskultur, har revisjonen funnet at kommunen har etablert flere tiltak for å skape god sikkerhetskultur. God sikkerhetskultur er en forutsetning for å kunne opprettholde tilfredsstillende informasjonssikkerhet. Opplæring og bevisstgjøring av ansatte er en viktig del av arbeidet med å ha en god sikkerhetskultur, og vårt nye obligatoriske e-læringskurs rulles nå ut for alle ansatte. 1. september var over 1000 ansatte i gang og det gis meget gode tilbakemeldinger fra de som til nå har gjennomført.

I delrapport 1 var den foreløpige vurderingen at kommunen var på god vei til å få et egnet sikkerhetsnivå sett opp mot regelverk og normer på området. Kommunedirektøren merker seg at revisjonen står ved denne vurderingen også etter at sikkerhetskulturen er undersøkt.

Sikkerhetskultur er en del av organisasjonskulturen og bygges over tid i en pågående prosess. I rapporten fremkommer at kommunen har etablert metodikk og tiltak som gir effekt. Denne bekreftelsen på at innsatsen gjøres der det har effekt er av stor verdi for kommunen.

Kommunedirektøren ser videre at det finnes forbedringsområder slik revisjonen påpeker. Dette er områder som er hensiktsmessige i det videre arbeidet med å forbedre sikkerhetskulturen og styrke informasjonssikkerheten ytterligere.
Kommunedirektøren har følgende kommenterer til de tre anbefalte tiltakene i delrapport 2:

Revisjonen anbefaler at Sarpsborg kommune bør:

- gjøre ansatte kjent med rutiner for risikovurdering, herunder vurdere å involvere ansatte i arbeidet med å identifisere, vurdere og dokumentere risiko på området

Svar:

Kommunedirektøren ser betydningen av bred involvering og god forankring i ledelsen for å lykkes med dette arbeidet. Det vil bli gjort en ny runde med å informere om rutinene for risikovurdering i de enkelte kommuneområdenes ledergrupper. For å

www.sarpsborg.com

bedre sikre at ledere og medarbeidere utover i organisasjonen har tilgang på nødvendige verktøy og bistand til å gjennomføre risikovurderinger utarbeides det ny veileder som sammen med eksisterende rutiner på området sendes ut til alle med lederrolle i kommunen. Både fagansvarlig informasjonssikkerhet og personvernombud bidrar med råd og veiledning, i tillegg til at det bygges kompetanse ute i virksomhetene. Det vil gjennomføres ny opplæring for alle når kommunen tar i bruk nytt kvalitetssystem og verktøy for risikovurderinger. Dette arbeidet har mål om å sluttføres første halvår 2021

- gjøre ansatte kjent med rutiner for registrering av avvik på området, herunder sørge for at de ansatte vet når og hvor de skal melde avvik

Svar:

Avviksregistrering og risikovurderinger er sentrale komponenter i kommunens internkontroll, og begge er nødvendig for å ha god informasjonssikkerhet. Dette tiltaket vil følge samme metodikk som punktet ovenfor. I tillegg vil punktet få økt oppmerksomhet i den årlige egenkontrollen. Avdelinger med få eller ingen avvik vil bli fulgt opp med ekstra fokus på opplæring og bevisstgjøring knyttet til rutiner for avviksregistrering.

- sørge for at de ansatte har relevante styringsdokumenter på området lett tilgjengelig

Svar:

Styringsdokumentene har blitt revidert i forbindelse med ledelsens gjennomgang i juni 2020. I etterkant har også kommunens nåværende kvalitetssystem, RiskManager blitt oppdatert med nytt innhold, og uaktuelt innhold har blitt tatt bort. Ved overgang til nytt kvalitetssystem vil styringsdokumentene bli lettere tilgjengelig for kommunens ansatte. Det vil bli gitt informasjon til alle ansatte om hvor man finner dokumentene og hva de inneholder.

Med hilsen

Turid Stubø Johnsen
Kommunedirektør

Dette brevet er signert elektronisk

2

5 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 2019
- 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*

Vedlegg

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[15]. 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.

[15] 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).

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
- 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.

Kommunikasjonssikkerhet

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.

Revisjonskriterier

PROBLEMSTILLING
Har kommunen etablert en god sikkerhetskultur i organisasjonen?

1. Kommunen har fastsatt ønsket kultur for informasjonssikkerhet og gjennomfører tilpasset (årlig) opplæring for å fremme god sikkerhetskultur.

2. Kommunens ansatte har fått opplæring og tilstrekkelig kompetanse i de relevante delene av kommunens sikkerhetssystemer.

3. Ansatte kjenner kommunens sikkerhetsstrategi.

4. Kommunens prosess for risikostyring er kjent for ansatte i virksomheten.

5. Kommunens styringsdokumenter for sikkerhetsarbeidet er tilgjengelig for virksomhetens ansatte.

6. Kommunens ansatte sørger for forsvarlig oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder o.l.

7. Ansatte varsler straks den som er utpekt til å motta varsel, dersom det oppstår mistanke om at passord/PIN-koder o.l. er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt.

8. Ansatte vet når og hvor de skal melde avvik på informasjonssikkerheten.

9. Kommunens ansatte følger instruksene arbeidsgiver har fastsatt om bruk og sikring av virksomhetens informasjonssystemer.