Rogaland Revisjon IKS

FORVALTNINGSREVISJON AV

INFORMASJONSSIKKERHET, DRIFT OG SÅRBARHET

SANDNES KOMMUNE

FEBRUAR 2019

Forsidefoto: pixabay.com

INNHOLD

SAMMENDRAG

BAKGRUNN OG FORMÅL

Prosjektets formål er å vurdere kommunens organisatoriske tiltak for informasjonssikkerhet, og avgrenset til å kun gjelde elektronisk behandling av opplysninger. I prosjektet har vi sett på hvilke systemer og rutiner kommunen har for å ivareta kravene til informasjonssikkerhet, og hvordan disse blir etterlevd. Det har også blitt sett på arkivering av elektronisk informasjon, samt innsyn og offentliggjøring.

I tillegg har kontrollutvalget bedt revisjonen å vurdere risikoen for hacking, og hvordan kommunen beskytter seg mot det.

Sandnes kommune har et styringssystem for informasjonssikkerhet som omfatter en digital strategi, håndbok for HMS, samt et internkontrollsystem for informasjonssikkerhet. Vi har i prosjektet vurdert Sandnes kommunes systemer og rutiner opp mot blant annet kravene i personopplysningsloven og personvernforordningen og veileder for internkontroll og informasjonssikkerhet fra Datatilsynet.

HOVEDINNTRYKK

Hovedinntrykket er at Sandnes kommune jobber aktivt for å bevisstgjøre medarbeiderne i forhold til informasjonssikkerhet og personvern, blant annet gjennom lederskolen, kurs for nyansatte, samt at det er et tema på ledermøter.

Kommunen bruker relativt lite ressurser, og sier selv at dette gir utfordringer i forhold til å bistå, veilede og følge opp enhetene i forhold til internkontroll og informasjonssikkerhet. Samtidig er kommunen bevisst på få informasjonssikkerhet inn som en del av «ryggmargen» i organisasjonen. Svarene fra spørreundersøkelsen blant de systemansvarlige tyder på at kommunen i stor grad har lykkes med å gjøre de systemansvarlige bevisste på informasjonssikkerhet.

SYSTEMER OG RUTINER FOR Å IVARETA INFORMASJONSSIKKERHET

Sandnes kommune er i gang med implementering av et nytt styringssystem for informasjonssikkerhet (SAKIS). Som en følge av dette finnes det per i dag ingen informasjon på intranett i forhold til kommunens retningslinjer for informasjonssikkerhet. Det er anslått fra sikkerhetsansvarlig i Sandnes kommune at arbeidet med å implementere skal være ferdig innen 1. mars 2019. Revisjonen har i stor grad tatt utgangspunkt i den tidligere informasjonssikkerhetshåndboken.

Selv om retningslinjene ikke er tilgjengelig for de ansatte på intranett per i dag, så viser spørreundersøkelsen blant de systemansvarlige at de fleste kjenner kommunens retningslinjer og at de følges.

Rådmannens ledergruppe har årlig en gjennomgang av informasjonssikkerheten i kommunen. Gjennomgangen inkluderer registrerte avvik på brudd på informasjonssikkerhet, samt endringer i trusselbilde. Informasjonssikkerhet vurderes også i forhold til organisasjonsendringer og bygningsmessige endringer. I tillegg er ressursinnsats et tema, og det vurderes om det er tilstrekkelige ressurser for å ivareta internkontroll og informasjonssikkerhet.

Både i intervju med sikkerhetsansvarlig, IT-sjef og via spørreundersøkelsen til de systemansvarlige kommer det fram at kommunen bruker lite ressurser på informasjonssikkerhet. Halvparten av de systemansvarlige svarer også at de i liten grad får nødvendig støtte og bistand fra IT. I henhold til digital strategi skal IT-enheten ikke ha brukerkompetanse i det enkelte fagsystem. Det er viktig at kommunen sikrer at de systemansvarlige har nok mulighet til å utøve sitt ansvar som systemansvarlig.

Fra 2019 blir det en endring i forhold til sikkerhetsansvarlig i kommunen. Ansvaret for den organisatoriske delen av informasjonssikkerheten flyttes fra personvernombudet hos organisasjon til området digitalisering og innovasjon. Den tekniske delen utføres av IT i området organisasjon. Dette fører til at det blir en sikkerhetsansvarlig i kommunen. Sikkerhetsansvarlig og personvernombudet vil arbeide tett for å bygge et godt styringsverktøy for informasjonssikkerheten som også ivaretar personvernet.

I 2017/2018 ble det gjennomført en risikoanalyse på bakgrunn av beredskapsplanen til IT. Analysen viste behov for flere tiltak, men IT-enheten har ikke hatt kapasitet til å utarbeide en plan for alle punktene som trenger oppfølging.

ARKIVERING OG OFFENTLIGGJØRING

Arkivverket gjennomførte i 2018 et tilsyn av arkivet i Sandnes kommune. Tilsynet avdekket 6 pålegg. Sandnes kommune har fulgt opp påleggene fra tilsynsrapporten.

Spørreundersøkelsen viser at de systemansvarlige i Sandnes kommune i stor grad vet hva som regnes som arkivverdig materiale og at dokumentbehandlingen og arkiveringen i sin enhet er tilfredsstillende. Det er noe lavere score på spørsmål om kjennskap til kommunens rutiner for arkivering av e-post. E-post er et viktig kommunikasjonsmiddel i kommunen, og det er viktig at Sandnes kommune har fokus på å informere de ansatte om rutiner for arkivering av e-post. I forhold til dokumenter som skal unntas offentlighet viser undersøkelsen at de ansatte i stor grad kjenner til lovbestemmelsene og hvordan man i praksis unntar dokumenter fra offentlighet i Public 360. Kontroll av offentlig journal avdekket heller ingen feil.

Personvernombudets uavhengighet vil styrkes fra 2019 når sikkerhetsansvaret samles under området digitalisering og innovasjon. Personvernombudet har i intervju selv pekt på utfordringer ved tidligere å inneha ulike roller.

Sandnes kommune har i 2018 hatt et stort fokus på innføringen av ny personvernforordning (GDPR[1]). Det har blitt gjennomført kurs og opplæring både for ledere, systemansvarlige og andre ansatte ved behov. Registrering av behandlinger av personopplysninger i Draftit er kommet godt i gang, men det gjenstår å kontrollere registreringene. Sandnes kommune bør både kontrollere at alle systemene som behandler personopplysninger er registrert i Draftit, og at utfyllingen er fullstendig og at det er skriftlige databehandleravtaler der det er påkrevd.

HACKING

Sandnes kommune har i liten grad implementert tekniske sikkerhetsløsninger som overvåker systemet, men benytter de innebygde løsningene som allerede finnes. IT-enheten gjennomfører heller ingen systematisk gjennomgang av logger i systemet, og kommunen bør vurdere å anskaffe et sikkerhetsovervåkingssystem. Et tiltak som har bedret sikkerheten for kommunens data er flytting av server til Green Mountain[2].

Sandnes kommune er kjent med at de har blitt utsatt for to hacking-angrep de siste to årene. Ingen av angrepene har vært vellykket. Det har i tillegg vært flere tilfeller der ansatte har oppgitt brukernavn og passord til uvedkommende, noe som kan svekke både sikkerheten og omdømmet til kommunen.

IT-sjefen peker på at det er sluttbrukeren som er den største risikoen for at forsøk på hacking blir vellykket. Sandnes kommune har derfor fokus på opplæring og bevisstgjøring av ansatte.

ANBEFALINGER

Revisjonen anbefaler at Sandnes kommune:

- påser at retningslinjer og prosedyrer blir tilgjengelig for ansatte på intranett så fort som mulig.
- sikrer at de systemansvarlige får tilstrekkelig tid og mulighet til å utøve sitt ansvar som systemansvarlig.
- prioriterer å utarbeide en plan for oppfølging av risikoanalysen fra 2017/2018.
- foretar en kontroll av registreringene i Draftit, både i forhold til hvilke systemer det er registrert behandlinger i forhold til og fullstendigheten i utfyllingen av skjemaene. Det må også kontrolleres at det foreligger nødvendige databehandleravtaler der det er påkrevd.
- vurdere behovet for et sikkerhetsovervåkingssystem som et proaktivt vern mot stadig mer avanserte og komplekse trusler og angrep.

[1] General Data Protection Regulation
[2] Datasenter på Rennesøy.

RÅDMANNENS KOMMENTAR

Rådmannen sin oppfatning er at rapporten gir en riktig framstilling av de utfordringer Sandnes kommune har i arbeidet med informasjonssikkerhet.

Kommunens formål med informasjonssikkerhetsarbeidet, med hensyn til konfidensialitet, integritet og tilgjengelighet er riktig behandling av personopplysninger. Alle tiltak skal dokumenteres, og dokumentasjonen skal være tilgjengelig for den som har et behov og krav ihht relevant lov.

Rapporten viser at Sandnes kommune har jobbet godt med informasjonssikkerhet, både det som gjelder opplæring og tekniske barrierer, men det gjenstår fremdeles forbedringer.

Organisasjonen gir tilbakemelding på at de har den nødvendige kunnskapen om

- hva personopplysninger og sensitive personopplysninger er
- taushetsplikten
- kommunens arkivrutiner

Kommunen har et pågående arbeid med å få ferdigstilt et styringsverktøy for informasjonssikkerhet (Sandnes Kommune informasjonssikkerhet = SAKIS), som erstatter den gamle håndboka.

Sandnes kommune har iverksatt tiltak fra årsskiftet 2019:
Rollen som Personvernombud og ansvarlig for informasjonssikkerhet er delt.

- Personvernombud: Sigrun Homleid
- Ansvarlig for informasjonssikkerhet: Kari Ødegård Aas

Dette innebærer et tydeligere skille i forhold til roller og ansvar både strategisk og operativt for det videre informasjonssikkerhetsarbeidet. IT-drift vil, som tidligere, ivareta den tekniske informasjonssikkerheten.

RAPPORTEN

1 INNLEDNING

1.1 FORMÅL OG PROBLEMSTILLINGER

Kontrollutvalget i Sandnes bestilte 08.09.2017 en forvaltningsrevisjon av IKT.

Formålet med dette prosjektet er å vurdere kommunens systemer og rutiner for informasjonssikkerhet, med spesielt henblikk på kommunens organisatoriske tiltak.
Prosjektet vil kartlegge og vurdere følgende konkrete problemstillinger:

- Hvilke systemer og rutiner har kommunen for å ivareta krav til informasjonssikkerhet?
- I hvilken grad etterlever kommunen kravene til informasjonssikkerhet?
- Blir krav til arkivering og offentliggjøring ivaretatt og har de ansatte kjennskap til regelverket?
- Hvilke korrigerende tiltak bør eventuelt iverksettes for å sikre tilfredsstillende informasjonssikkerhet?

I kontrollutvalgsmøte den 24.11.2017 ble følgende tillegg vedtatt:

- Hva er risikoen for hacking, og hvordan beskytter kommunen seg mot det?

1.2 REVISJONSKRITERIER OG METODE

Revisjonskriteriene er krav eller forventninger som brukes for å vurdere funnene i undersøkelsene. Revisjonskriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området, for eksempel lovverk og politiske vedtak. I dette prosjektet er kriteriene utledet fra følgende kilder:

- Krav til informasjonssikkerhet i personopplysningsloven og personvernforordningen (GDPR)
- Datatilsynets føringer og veiledere for informasjonssikkerhet[3]
- Difi's veileder for internkontroll i praksis - informasjonssikkerhet[4]
- Politiske vedtak, mål og føringer
- Administrative retningslinjer, mål, og føringer
- Andre myndigheters praksis

Ut fra disse kildene har vi utledet konkrete kriterier som vi måler praksis i kommunen mot. Disse beskrives innledningsvis i kapitlene.

[3] https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/
[4] https://internkontroll-infosikkerhet.difi.no/

Metodisk er det benyttet intervju med sikkerhetsansvarlig i Sandnes kommune, IT-sjef og rådgiver på IT. Vi har også gjennomgått en rekke dokumenter fra Sandnes kommune som strategier, politiske saker, arkivplan og prosedyrer og retningslinjer for informasjonssikkerhet. I tillegg har veiledere fra Datatilsynet og Difi vært sentrale i prosjektet.

I prosjektet ble det gjennomført en spørreundersøkelse som ble sendt til alle de systemansvarlige i Sandnes kommune (43 respondenter). Undersøkelsen fikk en svarprosent på 65 prosent. Spørsmålene ligger i vedlegg 1.

Vår samlete vurdering er at metodebruk og kildetilfang har gitt et tilstrekkelig grunnlag til å besvare prosjektets formål og de problemstillinger kontrollutvalget vedtok.

1.3 AVGRENSNING AV UNDERSØKELSEN

Det er kun elektronisk behandling av personopplysninger som er undersøkt. Hvordan informasjonssikkerheten er ivaretatt for opplysninger lagret i papirform er ikke undersøkt.

Problemstilling 4 *«Hvilke korrigerende tiltak bør eventuelt iverksettes for å sikre tilfredsstillende informasjonssikkerhet?»,* er ikke omtalt spesifikt i kapittel 2, men kommer i form av anbefalinger gjennom hele rapporten.

2 REGELVERK OG REVISJONSKRITERIER

2.1.1 REGELVERK

Sentrale bestemmelser som skal sikre informasjonssikkerheten i kommunen er personopplysningsloven med forskrift og personvernforordningen (GDPR). For arkivering og offentliggjøring er arkivloven med forskrift det sentrale regelverket.

PERSONOPPLYSNINGSLOVEN MED EUS PERSONVERNFORORDNING

Ny personopplysningslov av 15. juni 2018 avløser den tidligere personopplysningsloven fra 2000 om behandling av personopplysninger. Loven handler om behandling, innsamling og bruk av personopplysninger. Reglene gir virksomhetene en rekke plikter, samtidig som den gir enkeltpersoner en rekke rettigheter.

Personopplysningsloven inneholder:

- Nasjonale regler med norske tilpasninger
- EUs personvernforordning (GDPR), som består av
    - Artikler – personvernreglene i personopplysningsloven
    - Fortale – tolkningshjelp som kan utfylle eller forklare artiklene

Det er bare artiklene som er juridisk bindende.

Forordningen oppstiller et omfattende generelt personopplysningsregelverk, herunder de grunnleggende prinsippene og vilkårene for å behandle personopplysninger, rettigheter for enkeltpersoner, plikter for behandlingsansvarlige og databehandlere, overføring av personopplysninger over landegrensene og regler om tilsyn og sanksjoner.

Personvernforordningen stiller krav til internkontroll i form av egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med personvernforordningen. Internkontrollsystemet skal bidra til at ledelsen har et verktøy for å ivareta sitt ansvar og demonstrere etterlevelse etter personvernregelverket, og at ansatte har et verktøy for å utføre oppgaver på en forsvarlig og sikker måte.

Det skal utarbeides rutiner som er nødvendige for å oppfylle virksomhetens plikter og de registrertes rettigheter. Rutiner som kan være aktuelle, jfr. Datatilsynets veileder om internkontroll og informasjonssikkerhet:

- Iverksettelse og opphør av behandlingen
- Informasjon (rettferdig og gjennomsiktig behandling, artikkel 12, 13 og 14)
- Innhenting av kontroll av samtykke (artikkel 7 og 8)
- Innsyn (artikkel 15)
- Dataportabilitet (artikkel 20)

- Retting og sletting (artikkel 16, 17 og 19)
- Begrensning (artikkel 18 og 19)
- Protestere (artikkel 21)
- Særskilte regler for automatiserte avgjørelser (artikkel 22)
- Utlevering av personopplysninger til andre

Behandling av personopplysninger og særlige kategorier av personopplysninger (sensitive opplysninger) er regulert i personopplysningslovens §§ 8 og 9.

Personopplysninger kan behandles uten samtykke[5] dersom behandlingen er nødvendig for «… *arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål»* (jfr. personopplysningsloven §§ 8 og 9), så lenge det foreligger visse tiltak og behandlingen har hjemmel i lov. Sensitive personopplysninger kan også behandles uten samtykke dersom samfunnets interesse i at behandlingen finner sted klart overstiger ulempene til den enkelte. Det må også foreligge visse tiltak og man må ha rådført seg med personvernombudet.

Personopplysningsloven skiller mellom personopplysninger og særlige kategorier av personopplysninger, ofte omtalt som sensitive personopplysninger. Dette er opplysninger om:

- rasemessige eller etnisk opprinnelse
- politisk oppfatning
- religion
- filosofisk overbevisning
- fagforeningsmedlemskap
- genetiske opplysninger
- biometriske opplysninger med det formål å entydig identifisere noen
- helseopplysninger
- seksuelle forhold
- seksuell legning
- straffedommer
- lovovertredelser

Kommunen skal utpeke et personvernombud, jfr. artikkel 37. Personvernombudets hovedoppgave er å informere og gi råd om de forpliktelsene virksomheten har etter personvernlovgivningen til den behandlingsansvarlige[6] eller databehandleren, samt til de ansatte som utfører behandlingen av personopplysninger[7]. Kontaktopplysninger til personvernombudet skal registreres hos Datatilsynet via Altinn.

[5] Jfr. Datatilsynets veileder om behandlingsgrunnlag.
[6] Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
[7] All bruk av personopplysninger, slik som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.

I personvernforordningens artikkel 39 gis det en oversikt over oppgaver som et personvernombud har:

- Kontrollere overholdelsen av personvernregelverket.
- Gi råd om vurdering av personvernkonsekvenser.
- Samarbeid med Datatilsynet og funksjon som kontaktpunkt.
- Prioritert innsats der personvernrisikoen er høyest.
- Bidra til å få en oversikt over behandlingene i virksomheten.

Forskrift om behandling av personopplysninger regulerer personvernnemda. Personvernnemda (PVN) er klageorgan for vedtak fattet av Datatilsynet.

ARKIVLOVEN MED FORSKRIFTER

Arkivloven pålegger kommunen å ha et arkiv som sikrer at dokumenter er sikret som informasjonskilder for samtid og ettertid, jfr. § 6. Forskrift om offentlige arkiv gir mer detaljerte rutiner for håndtering av arkivfunksjonen. Det er administrasjonssjefen som har overordnet ansvar for arkiv, jfr. forskriftens § 1.

I følge arkivforskriften § 4 skal offentlige organer ha en oppdatert arkivplan. Arkivplanen skal gi oversikt over arkivmaterialet og hvilke instrukser, regler og planer som gjelder for arkivarbeidet. Arkivplanen skal også kunne fungere som et verktøy i internkontrollen for arkivarbeidet. Arkivplanen er nødvendig for å kunne forvalte arkivet i henhold til arkivlovens forskrift.

Arkivplanen skal omfatte alt av elektronisk arkivmateriale og henvisning til systemdokumentasjon for alle bevaringsverdige systemer. Elektroniske arkiv omfatter tradisjonelle journal- og arkiv system (Noark), fagsystem og registre. Elektronisk saksbehandling generelt utgjør en av de store utfordringer for arkivene i offentlig forvaltning med tanke på personvern, informasjonssikkerhet, arkivplikt og bevaring, jfr. Riksrevisjonens undersøkelse av arbeidet med å sikre og tilgjengeliggjøre arkivene i kommunal sektor (2009-2010).

Det skal utarbeides rutiner for oppretting, mottak, utveksling, arkivering, vedlikehold og bruk av dokumenter som skal inngå i arkivet, jfr. forskriftens § 12. Rutinene skal sikre at:

- Det går fram hvem som har opprettet og registrert dokumentene, og at bare personer med rett autorisasjon kan gjøre det.
- Dokumentene er sikret mot ikke-autoriserte tilføringer, slettinger og endringer
- Dokumentet er tilgjengelig for bruk.
- Alle dokumenter for organet som blir sendt fra eller til eller lagt fram for tilsatte i organet blir behandlet som dokumenter til eller fra organet. Det samme gjelder for dokumenter til eller fra den politiske ledelsen i et organ.

Alt arkivverdig materiale som ikke behandles i annet system skal inn i Public 360. På intranett er det listet opp eksempler på hva som skal arkiveres:

- Innkommende post.
- Utgående, egenprodusert post.
- Internpost som sendes mellom kommunale avdelinger og virksomheter.
- E-post som saksbehandles eller har verdi som dokumentasjon.

Det presiseres også at dokumenter som skal arkiveres er medieuavhengige og skal registreres uavhengig av om de er papirdokumenter, elektroniske filer, foto, film, lydopptak, SMS, sosiale medier, Skypesamtaler eller andre formater.

OFFENTLIGHETSLOVEN MED FORSKRIFT

Lov om rett til innsyn i dokument i offentleg verksemd regulerer journalføring og offentliggjøring av dokumenter i offentlig virksomhet. Hovedprinsippet i offentlighetsloven er at alle saksdokumenter i offentlig virksomhet er åpne for innsyn, jfr. § 3, så lenge opplysninger ikke er underlagt lovhjemlet taushetsplikt eller av andre grunner er unntatt fra offentlig innsyn.

Kommunen har plikt til å føre journal, jfr. offentlighetsloven § 10. Journalføring skal gi systematisk og fortløpende registrering av opplysninger om alle inngående og utgående saksdokumenter som er gjenstand for saksbehandling og har verdi som dokumentasjon. Ved registrering i journalen skal journalføringsdato, saks- og dokumentnummer, navn på sender eller mottaker, datering, klasse, ekspedisjons- eller avskrivingsdato og avskrivingsmåte være med. Journalføringsplikten omfatter «*… alle inngåande og utgåande dokument som etter offentleglova § 4 må reknast som saksdokument for organet, dersom dei er eller blir saksbehandla og har verdi som dokumentasjon*», jfr. forskriften § 9.

Interne dokumenter kan unntas fra innsyn, jfr. offentlighetsloven § 14 første ledd. Men dette gjelder ikke dersom dokumentet blant annet inneholder endelige avgjørelser, generelle retningslinjer (jfr. offentlighetsloven § 14 andre ledd), og saksframlegg, sakslister og dokumenter til folkevalgt organ, kontrollutvalg og revisor (jfr. offentlighetsloven § 16).

Kommunen har plikt til å vurdere «meroffentlighet», jfr. § 11, det vil si å innvilge mer enn minimumskravet. Det kan for eksempel innvilges delvis innsyn i stedet for å avvise kravet.

Elektronisk journalføring skal gjøres i et system som følger krav fastsatt av Riksarkivaren i Norsk arkivstandard (Noark), jfr. forskriftens § 11. Krav til arkivsystem og elektronisk behandling av arkivdokument finnes i Riksarkivarens forskrift kapittel 3.

Dokumenter som er tilgjengelig på internett skal, etter offentlighetsforskriften § 7, blant annet ikke inneholde opplysninger som er underlagt taushetsplikt i lover eller i medhold av lov, sensitive personopplysninger (jfr. personvernforordningen artikkel 9) og fødsels- og personnummer.

2.1.2 KS' DIGITALISERINGSSTRATEGI FOR 2017-2020

Visjonen til KS' digitaliseringsstrategi er: *Gode og tilgjengelige digitale tjenester styrker dialogen med innbyggere og næringsliv og gir gode lokalsamfunn.*

Digitalisering dreier seg i stor grad om endring og fornyelse av tjenester, prosesser og arbeidsmåter. Alle kommuner bør derfor utarbeide en overordnet digitaliseringsstrategi og en årlig handlingsplan som en del av budsjettprosessen. Disse må ses i sammenheng med organisasjonens overordnede planer og tjenesteområdenes behov.

Strategien viser til Meld. St. 27 (2015-2016) Digital agenda for Norge. Her er det formulert frem hovedprioriteringer for den nasjonale IKT-politikken. Ett av disse punktene er informasjonssikkerhet, personvern og dokumentasjonsforvaltning.

Informasjonssikkerhet og personvern på alle områder er en forutsetning for tillit til digitale løsninger. Digitalisering gir offentlig sektor et større ansvar for å ivareta rettighetene hver enkelt innbygger har til innsyn i egne saker. Opplysningene skal være tilgjengelige ved behov samtidig som opplysningene ikke skal komme på avveie. Innbyggerne skal i størst mulig grad ha råderett over egne personopplysninger.

Datakriminalitet, sabotasje og digitale innbrudd på kommunale IKT-systemer kan få store samfunnsmessige konsekvenser. Håndtering av slike hendelser krever systemer for avvik- og krisehåndtering.

Skytjenester og innsamling og bruk av stordata utfordrer informasjonssikkerhet og personvern. En helhetlig dokumentasjons- og arkivforvaltning skal sikre riktig tilgang, hensiktsmessig bruk, rettidig sletting og bevaring av bevaringsverdige opplysninger.

Informasjonssikkerhet skal ivaretas med utgangspunkt i risikovurderinger basert på trussel og sårbarhetsinformasjon, og følges opp gjennom god internkontroll.

Mål for informasjonssikkerhet, personvern og dokumentasjonsforvaltning:

- Kommunal sektor skal ivareta informasjonssikkerhet og personvern på alle områder.
- Kommunal sektor skal sikre at riktig informasjon er tilgjengelig for rett person.
- Kommunal sektor skal sørge for innebygd personvern i nye løsninger.
- Kommunal sektor skal ha styringssystem for informasjonssikkerhet.
- Kommunal sektor skal dele informasjon om sikkerhetshendelser de har vært utsatt for.
- Kommunal sektor skal ha helhetlig dokumentasjons- og arkivforvaltning.

2.1.3 DATATILSYNETS VEILEDER OM INTERNKONTROLL OG INFORMASJONSSIKKERHET

Gjennom å ha god internkontroll og god informasjonssikkerhet sikrer virksomheten at den behandler personopplysninger lovlig, sikkert og forsvarlig. Veilederen til Datatilsynet gir en innføring i hva internkontroll handler om, og hvordan man kan etablere og følge den opp.

Følgende elementer bør i følge veilederen være med i et system for informasjonssikkerhet:

- Sikkerhetsmål som omfatter ledelsens beslutning om hva informasjonsteknologien skal brukes til i virksomheten og hvordan den skal benyttes for å nå virksomhetens øvrige mål.
- Sikkerhetsstrategi som omfatter grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet.
- Sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene skal årlig gjennomgås av virksomhetens ledelse.
- Roller og ansvar knyttet til personvern og sikkerhet må klargjøres internt, og skal være dokumentert. I tillegg plikter alle kommuner å ha personvernombud, jfr. personvernforordningen artikkel 37-39.
- Akseptabelt risikonivå avgjøres av virksomhetens leder, og skal uttrykkes i virksomhetens sikkerhetsmål.
- Risikovurderingen må ta høyde for hvilke risikoer som er forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller uautorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.
- Virksomheten bør har prosedyrer som skal sikre at tilfredsstillende informasjonssikkerhet kan oppnås etter risikovurdering og beslutning om sikkerhetstiltak.

Internkontroll er en kontinuerlig prosess som krever oppfølging. Virksomheten må sørge for at internkontrollen gjøres kjent og at den etterleves blant de ansatte. Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på informasjonssikkerheten, skal virksomheten iverksette avviksbehandling. Ved brudd på informasjonssikkerheten der det er risiko for fysiske personers rettigheter og friheter skal Datatilsynet varsles. Dersom det vurderes at det er høy risiko for fysiske personers rettigheter og friheter skal også de registrerte varsles.

Virksomheten skal kontrollere at rutinene for håndtering av personopplysninger brukes og fungerer etter hensikten. Sikkerhetsrevisjon består vanligvis av egenkontroller, internrevisjon og revisjon av eksterne parter.

2.1.4 HACKING

Hacking defineres ofte som datakriminalitet som er straffbare handlinger der datateknologi utnyttes. Slike handlinger kan grovt sett deles i tre undergrupper; endring og sletting av data, urettmessig innsyn i og bruk av data og ulovlig bruk av datautstyr. I denne sammenhengen regnes ikke straffbare handlinger som bare gjelder selve datautstyret, som for eksempel tyveri av en datamaskin som datakriminalitet.

Datakriminalitet kan blant annet være[8]:

- **Datainnbrudd:** En uberettiget inntrengning i et datasystem for å skaffe seg tilgang til beskyttet informasjon. Angriperen kan skaffe seg tilgang ved for eksempel å misbruke passord eller utnytte sikkerhetshull.

- **Løsepengevirus:** En type skadevare som låser eller krypterer hele eller deler av innholdet på datamaskinen. Målet er å få brukeren til å betale løsepenger til angriperen.

- **Tjenestenektangrep (DDoS):** Et elektronisk angrep gjennomført over internett hvor hensikten er å hindre at brukeren av en tjeneste får tilgang. Det kan gjøres ved å binde opp ressurser enten hos tjenesten eller på en eller flere av systemene på vei til tjenesten. Det kan gjøres ved at store mengder forespørsler eller data sendes mot en nettside som gjør at tjenesten stopper opp.

- **CEO-bedrageri (direktørsvindel):** En bedrageriform som kjennetegnes ved at personer, som utgir seg for å være direktør i et selskap, tar kontakt med en underordnet i selskapet og manipulerer vedkommende til å bryte bedriftens rutiner og foreta urettmessige transaksjoner.

[8] Jfr. Politiet

2.1.5 REVISJONSKRITERIER

Ut fra gjennomgangen over er følgende revisjonskriterier lagt til grunn for å vurderingen av problemstillingene i prosjektet:

- Kommunen skal ha styringssystem for informasjonssikkerhet.
- Det skal beskrives sikkerhetsmål og -strategi for informasjonssikkerhet i kommunen.
- Ledelsen skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssikkerheten.
- Det skal klargjøres roller og ansvar knyttet til personvern og sikkerhet.
- Akseptabelt risikonivå for sikkerhet skal dokumenteres.
- Kommunen skal foreta risikovurderinger og iverksette nødvendige sikkerhetstiltak.
- Det skal utarbeides prosedyrer for informasjonssikkerhet.
- Det skal være etablert rutiner for håndtering og dokumentering av avvik.
- Sikkerhetsrevisjon av bruk av systemet skal gjennomføres jevnlig og dokumenteres.
- Kommunen skal ha en ajourført arkivplan, som viser hva arkivet omfatter, hvordan det er organisert og hvilke rutiner som gjelder.
- Kommunen skal dokumentere alle sine elektroniske systemer som inneholder arkivverdig informasjon i arkivplanen.
- Kommunen skal ha personvernombud.
- Det skal finnes en oversikt over hvilke personopplysninger som lagres og behandles i kommunen.
- Kommunen har systemer og rutiner for innsyn og retting av personopplysninger.
- Saksbehandlere er bevisst på hvilke saker som skal unntas fra offentlighet.
- Offentlig journal skal ikke inneholde sensitiv informasjon.
- Det skal være etablert betryggende systemer og prosedyrer for å sikre kommunen mot uønskede handlinger.

3 FAKTA OG VURDERINGER

I dette kapitlet følger data og vurderinger for alle problemstillingene. Revisjonskriterier er utledet i kapittel 2.

3.1 ORGANISERING, ROLLER OG REGELVERK

Dette kapittelet beskriver Sandnes kommune sin organisering, roller og regelverk i forhold til prosjektets formål. Det er ikke utledet revisjonskriterier til dette kapitlet.

3.1.1 ORGANISERING AV IT I SANDNES KOMMUNE

IT-enheten yter følgende tjenester til alle kommunens enheter[9]:

Utvikling (strategisk):

- er delegert kommunens IKT strategiansvar fra rådmannen via organisasjonsdirektøren.
- bidrar i alle større anskaffelsesprosjekter av IKT-løsninger godkjent av IKT-rådet og skal påse at den anskaffede løsningen er i tråd med kommunens virksomhetsarkitektur og teknisk plattform.
- aktivt bidra i arbeidet med å etablere effektive arbeidsprosesser med sin kompetanse på IKT-løsninger og kjennskap til de muligheter ny teknologi gir.

Drift:

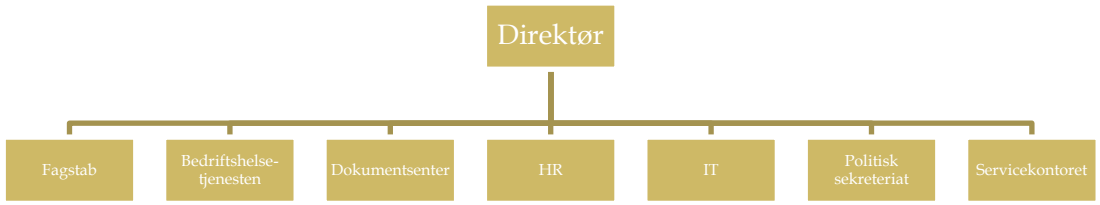
- tilpasse og drifte løsninger som sikrer effektiv utveksling av data mellom IKT-løsninger internt i kommunen og mot eksterne samarbeidspartnere.
- fremforhandle og inngå rammeavtaler for innkjøp av teknisk IKT-utstyr som PC'er, nettverksutstyr, servere, samband, telefoni, multifunksjonsskrivere med mer.
- avtaleforvalter og ansvarlig for drift av kommunens kontorstøttesystemer (e-post, tekstbehandling, regneark og presentasjonsverktøy).
- utarbeide krav til nettverksutstyr i alle kommunale bygg samt drift og videreutvikling av teknisk IKT infrastruktur som serverrom, nettverk, databaser, fillagringsområder og telefonsentraler.
- IKT-sikkerhet på systemnivå inkludert drift av tilhørende sikkerhetsløsninger (brannmur, antivirus, webfilter mm)
- styre overordnet brukertilgang til kommunens nettverk, tilganger i den enkelte IKT-løsning gis av systemeier.
- gi brukerstøtte til kommunens ansatte. IT-enheten skal ikke ha brukerkompetanse i de enkelte fagsystemer, men skal gi brukerstøtte på generelt nivå.
- drift og vedlikehold av kommunens PC'er, herunder installasjon og distribusjon av programvare.

[9] Jfr. digital strategi for Sandnes kommune

IT-enheten bruker et eget verktøy for mottak og behandling av brukerstøttehenvendelser og dokumentering av IKT-løsningene. Fra 2019 vil IT ta i bruk endringslogg.

IT er i Sandnes kommune organisert under direktør for organisasjon.

Figur 1 - Organisasjonskart for organisasjon. Kilde: Sandnes kommune.



IT-enheten består for tiden av 16 faste ansatte, og fire lærlinger. Sandnes har en lav bemanning på IT. Sammenlignet med andre kommuner av tilsvarende størrelse er IT-bemanningen om lag 50 prosent lavere, jfr. digital strategi for Sandnes kommune. Sammenligning av bemanningstettheten i Sandnes med bemanningstettheten i Stavanger kan det tyde på at bemanningen i Sandnes er noe lavere, men ikke så mye som 50 prosent lavere[10]. IT avdelingen i Stavanger kommune drifter også Finnøy kommune, Forsand kommune og Rennesøy kommune. Dersom Sandnes skal ha lik dekning av faste ansatte i IT-enheten som Stavanger har, mangler de 5 årsverk. Sammenlignet med Stavanger kommune har Sandnes om lag 30 prosent lavere IT-bemanning.

3.1.2 IKT STYRINGSMODELL OG ROLLEBESKRIVELSER

IKT styringsmodellen til Sandnes kommune ligger i vedlegg 1 til kommunens digitale strategi.

Digital strategi og strategisk plan utarbeides av IT på oppdrag fra rådmannens ledergruppe. Tjenesteområdene og informasjonssikkerhetskoordinator gir innspill. I digital strategi refereres det til kommunens IKT- råd som fungerer som en referansegruppe. IKT-rådet er erstattet med digitaliseringskontoret. Endelig plan og strategi godkjennes av rådmannens ledergruppe.

Rådmannens ledergruppe:

- er oppdragsgiver, og skal gi føringer og godkjenner endelig strategisk plan og digital strategi.
- prioriterer og godkjenner anskaffelser av IKT-løsninger.

[10] Antall faste ansatte på IT i forhold til antall ansatte i kommunen. For å være på samme nivå som Stavanger kommune skulle Sandnes hatt 21 årsverk i sin IT-enhet.

- setter budsjettrammen for IT-enheten, prioriterer tiltak i rådmannens forslag til økonomiplan og bestemmer størrelsen på IKT-midlene i økonomiplanen.
- godkjenner overordnet virksomhetsarkitektur.
- godkjenner infrastruktur og delegerer til IT.
- øverste sikkerhetsansvarlig.

IKT-råd:

- er erstattet av digitaliseringskontoret.

Systemeier/eier:

- initierer behov for anskaffelser av IKT-løsninger og melder inn til IKT-rådet.
- leder anskaffelsesprosjekter.
- finansierer og deltar i prosjekter for integrasjon og ID-håndtering.
- finansierer driftskostnadene for sine IKT-løsninger.
- ansvarlig for tilgangsstyring, applikasjonssikkerhet og behandling av personopplysninger.
- ansvarlig opplæring/brukerstøtte for fagsystem man er systemeier for.

Tjenesteområde, resultatenhet, stab/støtte:

- gir innspill til digital strategi og strategisk plan.
- initierer og avklarer systemeierskap.
- melder inn ønske om planlagte anskaffelser.
- prosjektdeltaker ved anskaffelse av IKT-løsninger.
- melder inn behov som ikke lar seg finansiere innen eksisterende ramme.
- melder inn prosjekt.
- prosessmodellering av virksomhetsarkitektur.
- initierer behov for infrastruktur.
- ansvarlig for IKT-opplæring i enheten.

IT-enhet:

- utarbeider digital strategi og strategisk plan.
- mottar melding om planlagte anskaffelser.
- er rådgiver og bidragsyter i anskaffelser.
- ansvarlig for drift og oppsett av integrasjonsløsninger.
- utarbeider overordnede integrasjonsprinsipper.
- prosjektleder ved integrasjonsprosjekter.
- finansierer driftskostnader for infrastruktur.
- kvalitetssikring og konsekvensvurdering av innmeldte behov for IKT-løsninger.
- utarbeider og vedlikeholder IT-arkitekturen i henhold til de overordnede arkitekturprinsippene.
- ansvarlig for drift, oppsett og vedlikehold av infrastruktur.
- sikkerhetsansvarlig for infrastruktur og IKT-beredskapsplan.
- generell brukerstøtte.

Anskaffelser:

- rådgiver og deltaker ved anskaffelse av IKT-løsninger.
- vedlikeholder anskaffelsesrutiner, kvalitetssikre anbudsprosess og kontrakt.
- påser at integrasjonsprinsipper legges til grunn i anskaffelsesprosesser.

Informasjonssikkerhetskoordinator:

- gir innspill til digital strategi og strategisk plan.
- ansvarlig for vedlikehold av informasjonssikkerhetshåndbok, sikkerhetsrevisjon og registeroversikt.

DIGITALISERINGSKONTOR

Sandnes kommune vedtok i økonomiplanen 2018-2021 å avsette kr 40 millioner til et digitaliserings- og innovasjonsfond. Det er opprettet et digitaliseringskontor som har erstattet IKT-rådet. Digitaliseringskontoret ledes av IT-sjefen, og består av digitaliseringssjefen, personvernombudet/sikkerhetsansvarlig, samt to representanter fra IT. Digitaliseringskontoret behandler de ulike behovene som kommer inn og gir også prosjektstøtte. Det avholdes ukentlige møter, og hvert møte har informasjonssikkerhet og personvern som første sak på agendaen.

Digitalisering skal være en sentral del av utviklingen av tjenestetilbudet i Sandnes kommune. Formålet med digitalisering er å utvikle og levere gode og effektive tjenester til innbyggere, næringsliv og ansatte.

Det er utarbeidet arkitekturprinsipper for digitalisering som skal legges til grunn ved implementering av digitale tjenester. Prinsippene fungerer som retningslinjer ved innføring av nye IT-løsninger. Formålet er å bidra til at IT-løsninger og datasett henger sammen med kommunens tjenester og oppgaveløsning og som igjen bidrar til bedre og mer helhetlige digitale tjenester i henhold til digital strategi for Sandnes kommune[11].

Sandnes har utarbeidet 11 spesifikke arkitekturprinsipper:

- Digitalt førstevalg med brukeren i sentrum
- Bruk av informasjon som ressurs
- Gevinstrealisering Sandnes kommune som helhet
- Helhetlig livssyklus
- Tjenesteorientert arkitektur
- Interoperabilitet (sikre samhandlingsevne)
- Tilgjengelighet
- Sikkerhet
- Åpenhet
- Fleksibilitet
- Skalerbarhet

[11] Arkitekturprinsipper for digitalisering, Sandnes kommune

Arkitekturprinsippene sikrer at sikkerheten ivaretas ved anskaffelse av nye systemer. Sikkerhetsprinsippet skal sikre at offentlige IT-løsninger blir etablert og driftet på en sikkerhetsmessig god måte. Det skal samtidig sikre at informasjon og tjenester er elektronisk tilgjengelig for de som har behov for og/eller rettigheter til disse. I forhold til arkitekturprinsippet skal enhver elektronisk tjeneste som etableres defineres til et gitt sikkerhetsnivå (klassifisering) basert på en risikoanalyse. Tjenestene skal også konstrueres slik at sikkerhetsnivået kan endres ved behov. Sikkerhetsnivået skal dokumenteres, slik at den som tar i bruk løsningen ser hvilke krav som er oppfylt.

Krav om konfidensialitet, integritet og tilgjengelighet skal oppfylles. Sikkerhetsprinsippet kan begrense andre prinsipper, dersom dette er avgjørende for tilliten til offentlig sektor.

For å oppfylle sitt krav til sikkerhet må Sandnes kommune kartlegge relevante krav til informasjonssikkerhet som følger av regelverk, instrukser og avtaler med tredjepart og dokumentere at IT-løsningen oppfyller disse.

Ved implementering av IT-løsninger må virksomheten kartlegge hvilke informasjonsinnhold løsningen skal omfatte. Virksomheten må også gjennomføre en risikoanalyse av løsningen og ha definert et nivå for hvilken risiko som aksepteres. Det må implementeres sikkerhetstiltak for IT-løsningen som tilfredsstiller det sikkerhetsnivået som virksomheten har besluttet. Sikkerhetstiltakene må også testes.

SYSTEMEIER

Systemeier er en organisatorisk enhet ved leder, jfr. digital strategi vedlegg 3. Systemeier oppnevner en person som systemansvarlig for daglig ivaretakelse av systemeierrollen.

Alle IKT-løsninger skal ha en systemeier:

- Systemeieransvaret legges til den enheten som naturlig har et hovedansvar for det fag- eller tjenesteområde som IKT-løsningen omfatter.
- Kommunaldirektørene er systemeiere for kommuneovergripende fellesprogrammer innen sine respektive hovedområder.

Systemeier har det funksjonelle ansvaret for IKT-løsningene:

- Avklare om IKT-løsningen bør oppgraderes eller erstattes.
- Gi brukere opplæring og veiledning i bruk av IKT-løsningen.
- Koordinere endringer og kommunikasjon mot brukerne.
- Utvikling og kontroll av rutiner knyttet til bruk av IKT-løsningen.
- Ansvar for utviklingsprosjekt for IKT-løsningen både økonomisk og funksjonelt.

Systemeier er økonomisk ansvarlig og skal:

- Sikre at IKT-løsningen utnyttes best mulig og henter ut maksimale gevinster.
- Sikre at IKT-løsningen totalt sett er fornuftig i forhold til kost/nytte.
- Sikre at IKT-løsningen passer inn i kommunens øvrige tekniske infrastruktur.

Systemeier er ansvarlig for leverandørkontakt:

- Tegner drifts- og vedlikeholdsavtale med leverandør.
- Kontrollere at drift og funksjonalitet er i henhold til kontrakt og avtale.
- Følger opp leverandør i forhold til rapportering og avvik.
- Melde utviklingsbehov og ønsker om videreutvikling til leverandør.

Systemeier er sikkerhetsmessig ansvarlig for IKT-løsningen og de opplysninger som forvaltes i denne:

- Behandlingsansvarlig for personopplysninger i IKT-løsningen.
- Ansvar for oppfølging av lover og regler relatert til IKT-løsningen (personregister, arkivering med videre).
- Sørge for at bevaringspliktige data blir tilgjengelig for fremtiden.
- Etablere, endre og fjerne tilganger.
- Påse at aktuelle tjenester kan drives videre ved eventuelle strømbrudd eller uønsket nedetid gjennom å ha manuelle rutiner.

3.2 SYSTEMER OG RUTINER

Dette kapitlet fokuserer på følgende problemstilling:

Hvilke systemer og rutiner har kommunen for å ivareta krav til informasjonssikkerhet?

Til denne problemstillingen har vi utledet følgende revisjonskriterier:

- Kommunen skal ha styringssystem for informasjonssikkerhet

Dette kapitlet ser overordnet på hvilke strategier og systemer Sandnes kommune har for informasjonssikkerhet. I kapittel 3.3 Informasjonssikkerhet i Sandnes kommune vil vi komme mer inn på de konkrete prosedyrer og retningslinjer Sandnes kommune har for informasjonssikkerhet.

DIGITAL STRATEGI FOR SANDNES KOMMUNE

Digital strategi ble vedtatt 16. april 2013. Styringsmodellen i Sandnes kommune er i stor grad lagt opp til delegert myndighet fra rådmannsnivå ned til resultatenhetene. I digital strategi pekes det på at denne styringsmodellen har medført utfordringer med hensyn til mangelfull overordnet koordinering av anskaffelser og presset drift av IKT-løsninger og infrastruktur.

Digital strategi er bygd opp etter en tredelt mal;

- strategiske veivalg
- effektiv ressursbruk
- leveranse

De overordnede IKT-prinsippene skal ligge til grunn for anskaffelse, drift og vedlikehold av kommunens IKT-løsninger:

- Intern rutine for overordnet koordinering av all anskaffelse av IKT-løsninger.
- Ubrukte funksjonaliteter ved eksisterende løsninger skal inkluderes i vurderingen av nye behov.
- Konsekvenser og muligheter for økt tilgjengelighet, mer effektive arbeidsprosesser, økt gjenbruk av data, økt kompetanse og mer effektiv ressursbruk skal inngå i vurderingen av en hver ny investering.
- Nasjonale fellesløsninger skal benyttes og standarder der de finnes fremfor leverandørspesifikke løsninger.
- Publikumsrettede IKT-løsninger skal følge nasjonale prinsipper for universell utforming[12] og skal følge anbefalte og pålagte standarder i Referansekatalog for IKT-standarder i offentlig sektor[13].

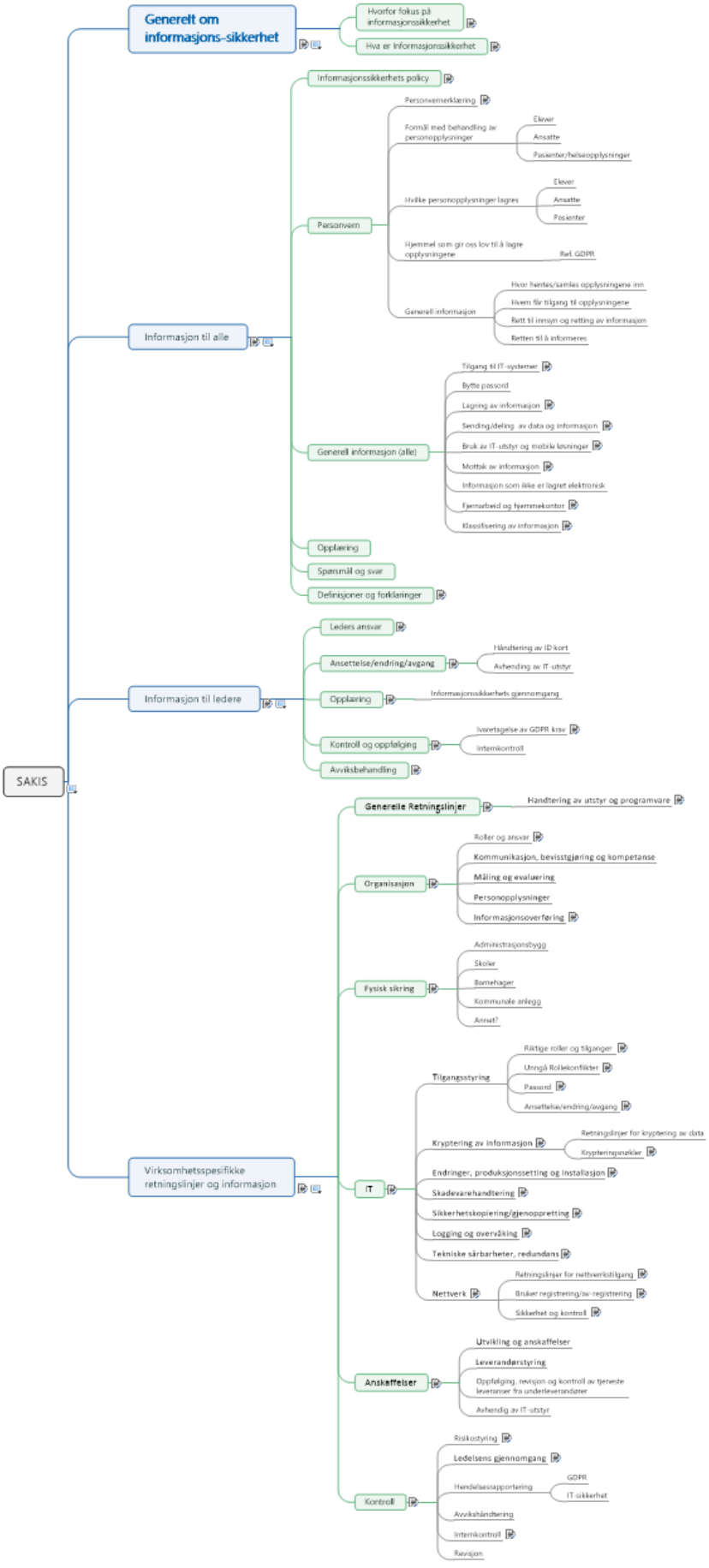
[12] http://universellutforming.difi.no
[13] Referansekatalog for IKT-standarder i offentlig sektor: http://standard.difi.no/forvaltningsstandarder/referansekatalog-html-versjon

INTERNKONTROLLSYSTEM FOR INFORMASJONSSIKKERHET

Rådmannen har det overordnete ansvar for at informasjonssikkerheten er i samsvar med personopplysningsloven og -forskrift. Kommunen har en informasjonssikkerhetsorganisasjon, jfr. kapittel 3.1.2, som består av rådmannen, informasjonssikkerhetsansvarlig, informasjonssikkerhetskoordinator og IT-ansvarlig.

Sandnes kommune er i gang med implementering av et nytt styringssystem for informasjonssikkerhet. Systemet har fått navnet SAKIS, og bygger på standarden ISO 27001. Kommunen har fått konsulentbistand fra eksterne for å omarbeide standarden slik at den passer for Sandnes kommune.

Figur 2 – Oppbyggingen av SAKIS. Kilde: Sandnes kommune.



Figuren over viser oppbyggingen av SAKIS. Alle dokumenter angående informasjonssikkerhet samles i SAKIS, og det er også her dokumentasjonen oppdateres. I SAKIS vil det fremgå hvem som har ansvaret for å oppdatere de ulike dokumentene. SAKIS vil bli koblet mot kommunens intranett (Pulsen), og det er her de ansatte vil se informasjonen.

Arbeidet med å flytte informasjonen over fra den tidligere håndboken for informasjonssikkerhet og over til SAKIS er i gang, men det gjenstår fortsatt en del. Kommunens personvernombud anslår at informasjonen fra den tidligere informasjonssikkerhetshåndboken vil være overført til SAKIS innen 1. mars 2019.

Informasjonssikkerhetshåndboken har ikke vært tilgjengelig på intranett siden det nye intranettet ble tatt i bruk i 2018, allikevel svarer 82 prosent[14] av de systemansvarlige at de er kjent med kommunens retningslinjer og prosedyrer for informasjonssikkerhet. Hele 86 prosent[15] svarer også at de vet hvor de finner retningslinjene. De fleste systemansvarlige svarer også at rutiner for informasjonssikkerhet blir fulgt i det daglige[16]. Noe av grunnen til de høye svarene på spørsmål om kommunens retningslinjer og prosedyrer kan skyldes at 86 prosent[17] svarer at de sjelden søker informasjon i retningslinjene.

Sandnes kommune har et informasjonssikkerhetsforum som er et rådgivende organ i arbeidet med informasjonssikkerhet, og ledes av sikkerhetsansvarlig. I forumet sitter representanter fra de største systemene i Sandnes kommune i tillegg til to tillitsvalgte. Forumet møtes 4 ganger i året, og behandler saker knyttet til forvaltning av informasjon, gode rutiner, aktuelle saker, personvern samt avvik meldt i Compilo. De arrangerer også Nasjonal sikkerhetsmåned ut til alle ansatte, og faglige samlinger mot systemansvarlige.

BEREDSKAPSPLAN IT

Beredskapsplanen til IT er sist revidert i mai 2017.

Formålet med beredskapsplanen er å utarbeide en IT risikoanalyse som skal:

- Definere risiko og konsekvens ved alvorlige IT-hendelser.
- Definere beredskapsorganisasjonen for IT-hendelser.
- Definere ansvar og roller tilknyttet krisesituasjoner.

IT gjennomførte en risikoanalyse i 2017/2018. Analysen viser behov for flere tiltak som IT-sjef og direktør for organisasjon er varslet om. IT-enheten har ikke hatt kapasitet til å utarbeide en plan for alle punktene som trenger oppfølging.

[14] Respondenter som har svart alternativ 4-6. N=28.
[15] N=28.
[16] 85 prosent av respondentene har svart alternativ 4-6. N=27.
[17] N=28.

FORVALTNINGSREVISJON AV ELEKTRONISK BEHANDLING AV SENSITIVE PERSONOPPLYSNINGER 2010

I 2010 ble det gjennomført en forvaltningsrevisjon av sensitive personopplysninger i Sandnes kommune. Rådmannen har i sin kommentar til rapporten listet opp fem forbedringsområder på bakgrunn av revisjonens anbefalinger:

1. Avsette tilstrekkelige ressurser, slik at tilfredsstillende informasjonssikkerhet opprettholdes.
2. Gjennomføre risikovurderinger når datasystemene endres, eller når det oppstår endringer i trusselbildet.
3. Sørge for tilfredsstillende rutiner for og gjennomføre egenkontroller.
4. Gjennomføre ledelsens årlige gjennomgang med utgangspunkt i vedtatte rutiner.
5. Forbedre rutinene for avviksbehandling.

OPPVEKST ADMINISTRATIVT SYSTEM

Oppvekst administrativt system er en felles kommunikasjonsløsning for barnehager, skoler og SFO i Sandnes kommune. Det ligger også innen en opsjon for å knytte på PPT.

Det er laget en konseptbeskrivelse for prosjektet som ivaretar arkitekturprinsippene for digitalisering i Sandnes kommune.

Løsningen vil behandle sensitive personopplysninger, og det har derfor vært nødvendig å vurdere tiltak og mekanismer for å beskytte integritet, konfidensialitet og tilgjengelighet. Løsningen skal integreres mot Public 360.

Nøkkelprinsipper for sikkerhet i løsningen er[18]:

- **Sikkerhet i dybden**: Det benyttes flere lag med sikkerhetsmekanismer/barrierer slik at system og informasjon benyttes selv om en mekanisme svikter eller blir kompromittert.
- **Enkelhet i design, operasjon og administrasjon:** Komplekse sikkerhetssystemer gir større mulighet for feil i design, implementasjon og bruk.
- **Innebygd personvern:** Datatilsynets «syv steg til innebygd personvern» er en sentral del av alle utviklingsfaser.
- **Sikkerhet i hele livsløpet:** Både systemet/løsningen og vedlikeholds prosedyrer skal være tilpasset slik at oppgraderinger basert på nye funn eller endringer i trusselbildet kan utføres og kontrolleres på en effektiv måte.
- **Sporbarhet**: Arkitekturen skal sikre at en kan undersøke hva som er skjedd ved sikkerhetsbrudd og hvem/hva som har utløst hendelsen.
- **Arkitektur med preventive, detekterende og korrigerende mekanismer:** Arkitekturen har mekanismer for deteksjon av innbrudd/angrep samt operasjonelle planer for å reagere på sikkerhetsbrudd.
- **Minimere tillit:** Systemer og komponenter som håndterer sensitive data bør i størst mulig grad beskytte seg selv og ha minst mulig tillit til omkringliggende systemer og nettverk.

[18] Jfr. Konseptbeskrivelse oppvekst administrativt system

- **Separasjon av sikkerhetskomponenter (compartmentalization):** Komponenter som inneholder sikkerhetsfunksjoner eller behandler sensitiv informasjon bør i minst mulig grad blandes sammen med komponenter som utfører andre funksjoner.
- **Fokus på brukervennlighet og tilgjengelighet:** Sikkerhetsarkitekturen skal støtte opp rundt visjonen bak «digitalt førstevalg» hvor kommunens tjenester skal åpnes opp og gjøres tilgjengelig for publikum. Dersom disse tjenestene skal bli brukt må sikkerhetsmekanismene være så enkle og brukervennlig som mulig.
- **Minimal angrepsflate:** Angrepsflaten minimeres gjennom blant annet konfigurasjonsstyring og komponentkontroll på system og infrastruktur.

Sandnes kommune har ikke valgt leverandør, og har derfor ikke sett på konsekvensene av overgang og risikoer knyttet til løsningen.

3.3 INFORMASJONSSIKKERHET I SANDNES KOMMUNE

Dette kapitlet fokuserer på følgende problemstilling:

I hvilken grad etterlever kommunen kravene til informasjonssikkerhet?

Til denne problemstillingen har vi utledet følgende revisjonskriterier:

- Det skal beskrives sikkerhetsmål og -strategi for informasjonssikkerhet i kommunen.
- Ledelsen skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssikkerheten.
- Det skal klargjøres roller og ansvar knyttet til personvern og sikkerhet.
- Akseptabelt risikonivå for sikkerhet skal dokumenteres.
- Kommunen skal foreta risikovurderinger og iverksette nødvendige sikkerhetstiltak.
- Det skal utarbeides prosedyrer for informasjonssikkerhet.
- Det skal være etablert rutiner for håndtering og dokumentering av avvik.
- Sikkerhetsrevisjon av bruk av systemet skal gjennomføres jevnlig og dokumenteres.

Informasjonssikkerhet er sikring av opplysninger ved å bruke prinsippene om konfidensialitet, integritet, tilgjengelighet og robusthet. Man skal sikre at informasjonen ikke blir kjent for uvedkommende (konfidensialitet) og at informasjonen ikke blir endret utilsiktet eller av uvedkommende (integritet). Informasjonen skal også være tilgjengelig ved behov og organisasjonen og systemene må være motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser (robusthet). Dersom kommunen har god internkontroll og god informasjonssikkerhet sikrer man at personopplysninger behandles lovlig, sikkert og forsvarlig.

Personopplysninger er opplysninger eller vurderinger som kan knyttes til en enkeltperson. Dette kan være navn, adresse, telefonnummer, e-postadresse, bilnummer, bilder eller fødselsdato.

I dette kapitlet vil vi se på hvordan Sandnes kommune etterlever kravene til informasjonssikkerhet basert på Datatilsynets veileder om internkontroll og informasjonssikkerhet og Difi's veileder om internkontroll i praksis. Det er også foretatt vurderinger sett opp mot aktuelle lover og forskrifter og kommunens egne strategier, planer og rutiner (jfr. kapittel 2). Når det refereres til den tidligere håndboken brukes begrepet informasjonssikkerhetshåndbok, og den nye omtales som SAKIS.

3.3.1 MÅL OG STRATEGIER FOR INFORMASJONSSIKKERHET

I Sandnes kommune sin tidligere informasjonssikkerhetshåndbok er mål og strategier for informasjonssikkerhet definert. Sandnes har følgende sikkerhetsmål:
Sandnes kommune skal ved behandling av personopplysninger sikre at:

- *Personopplysninger kun samles inn eller bearbeides når den opplysningene omhandler har gitt samtykke, eller det er fastsatt i lov at det er adgang til slik behandling.*
- *Konfidensialitet blir ivaretatt ved å hindre uvedkommende i å få tilgang til opplysningene.*
- *Integritet beskyttes gjennom at informasjonen ikke er utsatt for uautorisert eller utilsiktet endring.*
- *Tilgjengelighet ivaretas ved at autoriserte brukere har tilgang til nødvendige opplysninger når de utfører pålagte oppgaver.*

I forhold til sikkerhetsnivå sier informasjonssikkerhetshåndboken *«Ved etablering av nye behandlinger av personopplysninger skal det gjennomføres risikovurderinger. I rutinen for risikovurdering skal det være regler for fastsettelse av akseptabel risiko. Etablering av nye sikringstiltak skal være basert på gjennomførte risikovurderinger».*

Sikkerhetsstrategien definerer hvilke valg og prioriteringer som skal tas for å sikre personopplysninger og behandlingen av disse.

- *Det skal opprettes en sikkerhetsorganisasjon med klare ansvars- og myndighetsforhold.*
- *Arbeidet med informasjonssikkerhet skal forankres i øverste ledelse og inngå i ansvarsområdet en leder til enhver tid har.*
- *Alle behandlinger av personopplysninger skal registreres i en samlet oversikt.*
- *Det skal gjennomføres risikovurderinger ved etablering av nye behandlinger av personopplysninger, samt endringer av trusselbildet.*
- *Den datatekniske løsningen skal støtte opp om sikkerhetsmål og -strategier gjennom tilfredsstillende forvaltning av utstyr, system og data.*
- *Tilgang til systemer og informasjon gis til ansatte etter behov relatert til arbeidsoppgaver.*
- *Det skal gis opplæring og informasjon til brukere av kommunens datasystem for å sikre at gjeldende sikkerhetskrav blir ivaretatt.*
- *Uvedkommende skal hindres tilgang til systemer og informasjon.*
- *Det skal sikres at personopplysninger ikke forandres utilsiktet eller uautorisert.*
- *Det skal være mulig å spore uønskede hendelser knyttet til bruk av kommunens datasystem.*
- *Fysisk sikring skal hindre at uautoriserte får adgang til lokaler der personopplysninger lagres og behandles.*
- *Det skal være tatt i bruk rutiner og prosesser for å håndtere uønskede hendelser, avvik.*
- *Det skal gjennomføres tilfredsstillende intern kontroll, herunder sikkerhetsrevisjoner og ledelsens årlige gjennomgang.*

Ledelsens årlige gjennomgang var ett av forbedringsområdene rådmannen hadde etter forvaltningsrapporten om sensitive personopplysninger i 2010. Kommunen gjennomfører årlige gjennomganger, og revisjonen har fått tilgang til referat fra de to siste gjennomgangene. Ledelsens gjennomgang gjøres i rådmannens ledergruppe, og gjennomgangen hadde følgende tema i 2018:

- Resultater og hovedkonklusjoner fra revisjoner informasjonssikkerhet
- Registrerte avvik
- Rapporter fra offentlige og interne tilsyn
- Endringer i lover, forskrifter og offentlige sikkerhetskrav
- Endringer i elektroniske system som behandler personopplysninger
- Endringer i trusselbilde
- Organisatoriske endringer
- Bygningsmessige endringer
- Ressurser for å ivareta internkontroll og informasjonssikkerhet

Av referatet ser vi at gjennomgangen av avvik viste totalt 58 avvik, der 1 avvik var alvorlig. På tidspunktet for ledelsens gjennomgang var det for 2018 ikke blitt sendt ut egenkontroller. Grunnen er at arbeidet med innføring av ny personvernforordning (GDPR) har hatt fokus. Kommunen opplyser imidlertid at egenkontroller ble sendt ut til enhetene rett før jul. Revisjonen har ikke sette på resultatet av egenkontrollen for 2018.

Av bygningsmessige endringer er serverrom flyttet til Green Mountain. Dette bidrar til et høyteknologisk serverrom med fokus på sikkerhet som adgangskontroll, strømaggregat, UPS[19], brannsikring, kjøling og bombesikring. Dette bidrar til fysisk og virtuell sikring av kommunens samlede data.

I forhold til trusselbilde pekes det på at ansatte er den største risikoen. Opplæring og kunnskap øker tryggheten og minsker faren. Kommunen har hatt om lag 10 hendelser siste året der ansatte har oppgitt brukernavn og passord til uvedkommende. Det er satt i verk tiltak som opplæring av ansatte, og tekniske tiltak ved blant annet å begrense tilgang til diverse web-sider, Geo-blokk (utelukke enkelte land) og 2 faktor autentisering. Det ble også vurdert å abonnere på programvare som kan stoppe en del angrep mot kommunen.

Når det gjelder ressurser for å ivareta internkontroll og informasjonssikkerhet står det i referatet fra rådmannens ledergruppe at kommunen har utfordringer med å bistå, veilede og følge opp. Sikkerhetsansvarlig sier at dette er et ressursspørsmål. Men kommunen jobber systematisk med å få informasjonssikkerhet som en del av «ryggmargen» i organisasjonen, og spørsmål om informasjonssikkerhet tas jevnlig opp, blant annet som fast punkt på digitaliseringskontoret sine møter.

[19] Uninterruptible power supply, UPS (avbruddsfri strømforsyning)

Figur 3 – I hvilken grad er du kjent med kommunens retningslinjer/prosedyrer for informasjonssikkerhet og kommunens sikkerhetsmål og -strategi?[20] Kilde: Spørreundersøkelse fra Rogaland Revisjon.

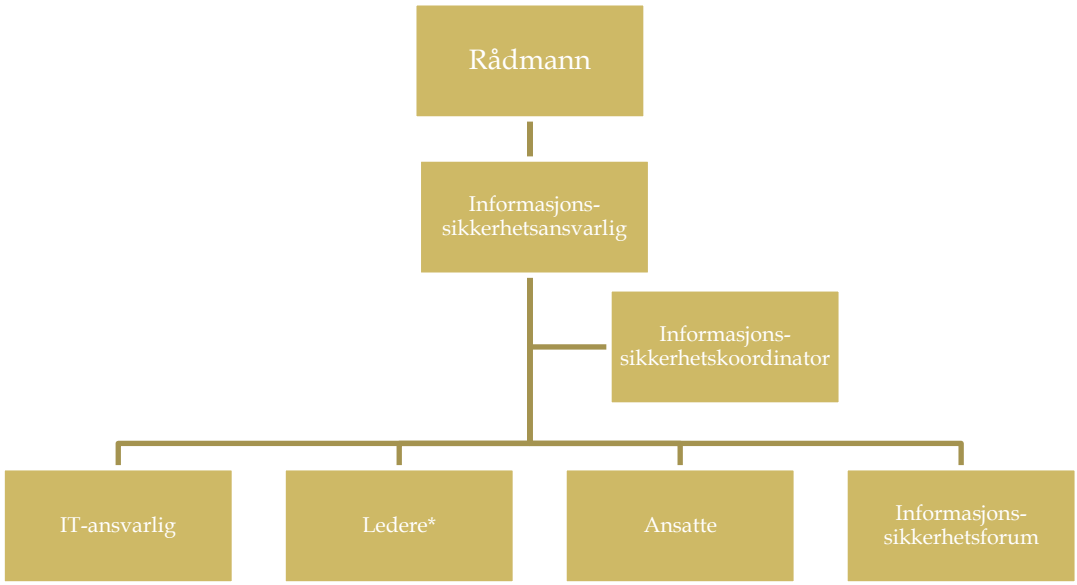
Kommunens sikkerhetsmål og -strategi er godt kjent blant de systemansvarlige både i Sandnes og Stavanger, men ikke i like stor grad som retningslinjene. 86 prosent svarer at de sjelden søker informasjon i retningslinjene for informasjonssikkerhet.

3.3.2 ORGANISERING OG ANSVAR FOR INFORMASJONS-SIKKERHETEN

Det er rådmannen i Sandnes som har det overordnete ansvaret for at informasjonssikkerheten er i samsvar med kravene i lov og forskrift.

[20] Respondenter som har svart alternativ 4-6, Sandnes N=28, Stavanger N=48.

Figur 4 – Informasjonssikkerhetsorganisasjon i Sandnes kommune. Kilde: Informasjonssikkerhetshåndbok Sandnes kommune.



* Alle ledere med personalansvar, for eksempel rådmann, direktører, resultatenhets- og stabsledere.

For å ivareta rådmannens ansvar knyttet til informasjonssikkerhet er det etablert en sikkerhetsorganisasjon med følgende roller[21]:

1. Rådmann
2. Informasjonssikkerhetsansvarlig
3. Informasjonssikkerhetskoordinator
4. IT-ansvarlig
5. Direktører, resultatenhets- og stabsledere
6. Ansatte
7. Informasjonssikkerhetsforum

Rådmannen skal sørge for:

- Tilstrekkelige ressurser, både personell og økonomiske, slik at tilfredsstillende informasjonssikkerhet kan opprettholdes.
- Kommunen har en sikkerhetsorganisasjon med ansvar for å etablere, gjennomføre og vedlikeholde dokumentasjon.
- Tiltak knyttet til informasjonssikkerheten.
- Jevnlig gjennomføring av intern kontroll.
- Rådmannen kan delegere ansvar for daglige arbeidsoppgaver, men ikke ansvaret i forhold til loven.

[21] Jfr. Informasjonssikkerhåndbok Sandnes kommune

Det er organisasjonsdirektøren som er **informasjonssikkerhetsansvarlig** i Sandnes kommune. Informasjonssikkerhetsansvarlig skal sørge for en hensiktsmessig og velfungerende sikkerhetsorganisasjon, samt lede og gjennomføre ledelsens årlige gjennomgang.

Informasjonssikkerhetskoordinatoren har ansvar av koordinerende og samordnede art:

- Etablere og vedlikeholde Sandnes kommunes internkontrollsystem for informasjonssikkerhet.
- Sørge for etablering og opprettholdelse av vedtatt sikkerhetsnivå.
- Gjennomføre sikkerhetsrevisjon.
- Sørge for at det gjennomføres risikovurderinger.
- Forbedre og delta i gjennomføringen av ledelsens gjennomgang.
- Sørge for at informasjonssikkerhetsorganisasjonen fungerer i henhold til definert ansvar.
- Sørge for gjennomføring av opplærings- og motivasjonstiltak for å ivareta informasjonssikkerhet.
- Vedlikeholde registeroversikt over alle behandlinger.
- Sørge for at det oversendes melding om nye/fornying av behandlinger til Datatilsynet.
- Lede informasjonssikkerhetsforum.
- Delta i faglige forum og samarbeide med andre virksomheter for å opprettholde og øke kunnskapen knyttet til informasjonssikkerhetsarbeid, og dele denne med organisasjonen.

IT-ansvarlig har ansvar for:

- Bygge sikkerhet i samsvar med sikkerhetspolitikken inn i nettverk og IKT-system.
- Sørge for at alle elementer i datanettverket er dokumentert med iverksatte sikkerhetstiltak og at dokumentasjonen er tilgjengelig.
- Sikre at den daglige driften av kommunens datanettverk og IKT-system drives i samsvar med sikkerhetspolitikken.
- Delta i forberedelse og gjennomføring av ledelsens gjennomgang.
- Vedlikeholde IT-beredskapsplanen.
- Delta i faglige forum og samarbeide med andre virksomheter for å opprettholde og øke kunnskapen knyttet til informasjonssikkerhetsarbeid, og dele denne med organisasjonen.

Direktører, resultatenhets- og stabsledere skal blant annet:

- Melde avvik i henhold til avvikshåndteringsrutine og -skjema.
- Følge rutinen for innsyn i personalmappe, personalopplysninger og krav om retting/sletting av personopplysninger.
- Bidra til gjennomføring av informasjonssikkerhetsrevisjon i egen enhet.

- Registrere alle behandlinger av personopplysninger i fagsystem som leder er systemeier for.
- Vurdere behov for risikoanalyse ved endringer, organisatoriske eller tekniske, som berører måten det jobbes på i fagsystemet.
- Gjennomføre risikoanalyse ved innføring av et nytt fagsystem.

Ansatte skal blant annet:

- Melde avvik i henhold til avvikshåndteringsrutine og -skjema.
- Holde bruker ID og passord skjult.
- Bytte passord ved mistanke om at det er blitt kjent av uvedkommende/andre.
- Logge av/låse PC når den forlates eller overlates til andre.
- Sikre bærbart datautstyr (PC, minnepinne, DVD, mobiltelefon) ved lagring av personopplysninger.
- Ikke sende sensitive/taushetsbelagte personopplysninger i e-post, såfremt disse ikke er avpersonifisert eller sendes kryptert.
- Melde fra til leder dersom adgangskort eller nøkler mistes.

Informasjonssikkerhetsforumet ledes av informasjonssikkerhetskoordinatoren, se også kapittel 3.2. Forumets ansvar og oppgaver er:

- Rådgivende organ innen informasjonssikkerhet knyttet til behandling av informasjonssikkerhet.
- Forholde seg til gjeldende retningslinjer og rutiner for informasjonssikkerhet i Sandnes kommune.
- Skal i hovedsak behandle saker og foreslå tiltak som har med mer enn en enhet å gjøre.
- Delta i planlegging og gjennomføring av besluttede tiltak knyttet til informasjonssikkerhet.
- Være pådriver for tiltak som fører til økt læring og motivering innen informasjonssikkerhetsområdet.

Informasjonen om ansvar knyttet til de ulike rollene er i noen grad utdatert blant annet som følge av ny personopplysningslov.

3.3.3 RISIKOVURDERING OG SIKKERHETSTILTAK

Prosedyre for risikovurdering finnes i informasjonssikkerhetshåndboken til Sandnes kommune. Målet med risikovurdering er å *«få oversikt over hvilken risiko virksomheten er utsatt for med eksisterende dataløsninger, og bruke oversikten som beslutningsgrunnlag for iverksetting av sikkerhetstiltak i tråd med sikkerhetsmål og fastsatt akseptabel risiko.»*

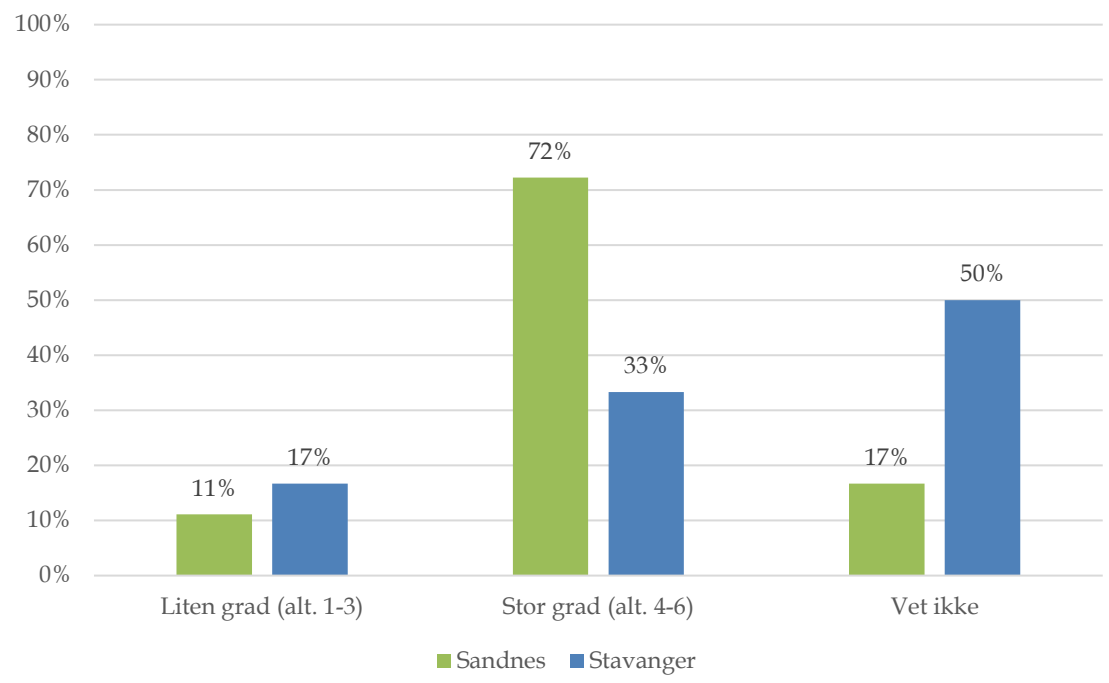
I henhold til sikkerhetsnivået i informasjonssikkerhetshåndboken til Sandnes kommune skal det gjennomføres risikovurderinger ved nye behandlinger av personopplysninger. Rutinen for risikovurdering har regler for fastsettelse av akseptabel risiko. Sikringstiltak skal være basert på gjennomførte risikovurderinger.

Det er systemeier som er ansvarlig for gjennomføring av risikovurdering i Sandnes kommune, jfr. prosedyre for risikovurdering i informasjonssikkerhetshåndboken. Det skal gjennomføres risikoanalyse før:

- Innføring av nytt og vesentlig endring i fagsystemet.
- Overføring av nye typer personopplysninger eller til nye partnere.
- Organisatoriske endringer som medfører endring i rutinene knyttet til behandling av personopplysninger.

Ved endringer i fagsystem, tekniske og bygningsmessige endringer eller endring i trusselbilde kan det vurderes behov for en ny risikoanalyse. Alle risikovurderinger skal dokumenteres og arkiveres.

Figur 5 – I hvilken grad vil du si at risikovurderingen var tilstrekkelig?[22] Kilde: Spørreundersøkelse fra Rogaland Revisjon.



67 prosent[23] svarer i spørreundersøkelsen at det er gjennomført risikovurdering i forhold til fagsystemene. Tilsvarende svarte kun 34 prosent[24] at det var gjennomført risikovurdering i Stavanger kommune, men det var også 34 prosent som svarte vet ikke (mot 15 prosent i Sandnes). De fleste systemansvarlige i Sandnes mener i tillegg at risikovurderingen som er gjennomført var tilstrekkelig. Svarene kan tyde på at det er et større fokus på risikovurderinger i Sandnes sammenlignet med Stavanger.

Spørreundersøkelsen ble sendt ut til alle som kommunen har registrert som systemansvarlige. Sandnes kommune har en manuell e-post liste over de systemansvarlige, som

[22] Sandnes N=18, Stavanger N=42.
[23] N=27.
[24] N=44.

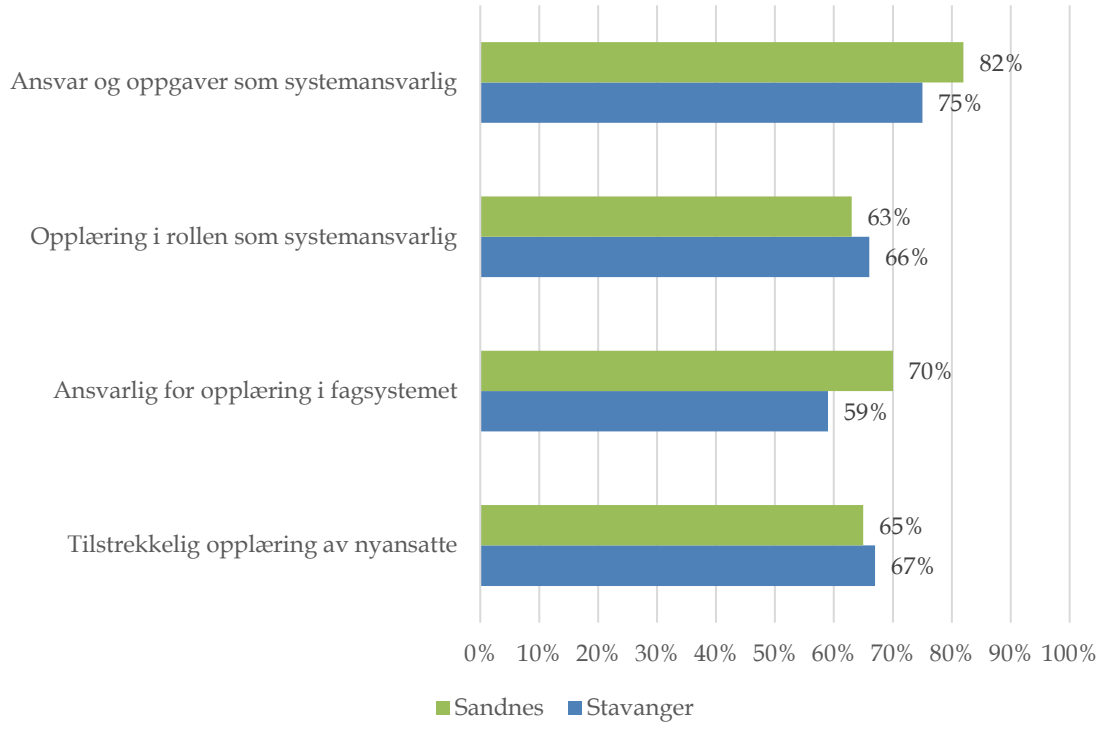
krever kontinuerlig oppdatering ved endringer. I undersøkelsen var det en av respondentene som svarte at vedkommende ikke var systemansvarlig. Sikkerhetsansvarlig i kommunen er opptatt av at listen skal vært mest mulig oppdatert til enhver tid, men presiserer at denne listen ikke er styrende for hvilke tilganger den enkelte har.

Systemansvarlig er oppnevnt av systemeier og har det daglige ansvaret for ivaretakelsen av systemeierrollen. I det videre er det systemansvarlig som vil bli omtalt, og det forutsettes at systemansvarlig har fått delegert alle systemeiers ansvar og oppgaver, jfr. vedlegg 3 i digital strategi: Definisjon av systemeier av IKT-løsninger i Sandnes kommune.

I henhold til Sandnes kommune sin sikkerhetsstrategi skal det gis opplæring og informasjon til brukere av kommunens datasystem for å sikre at gjeldende sikkerhetskrav blir ivaretatt. Tjenesteområdene, ved systemansvarlig, har ansvaret for å gi opplæring og veiledning til brukerne av fagsystemet. Informasjonssikkerhetsforumet gjennomfører også årlig en informasjonskampanje ut til alle ansatte via nasjonal sikkerhetsmåned. De arrangerer også faglige samlinger mot de systemansvarlige.

Opplæringen av ansatte bør omfatte krav til internkontroll og informasjonssikkerhet, juridisk ansvar og interne sikringstiltak, så vel som opplæring i riktig bruk av informasjonssystemer, jfr. Datatilsynets veileder om internkontroll og informasjonssikkerhet.

Figur 6 – Opplæring og ansvar for fagsystemet[25]. Kilde: Spørreundersøkelse fra Rogaland Revisjon.

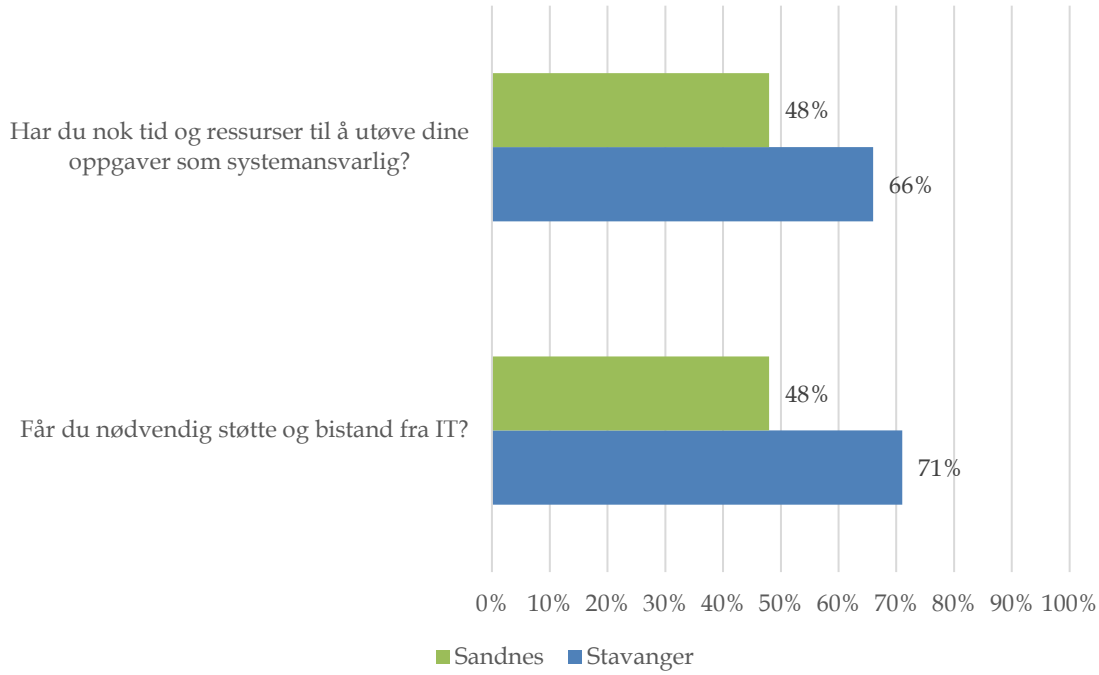


[25] Respondenter som har svart alternativ 4-6, Sandnes N=27, Stavanger N=44.

De systemansvarlige i Sandnes kommune er i stor grad kjent med sitt ansvar og sine oppgaver som systemansvarlig. På spørsmål om de har fått tilstrekkelig opplæring i rollen som systemansvarlig svarer 63 prosent i stor grad.

De fleste, 70 prosent av respondentene, svarer at de er ansvarlig for opplæringen, men det er noe lavere score på spørsmålet om opplæringen er tilstrekkelig for nyansatte (65 prosent).

Figur 7 – Ressurser og støtte og bistand fra IT[26]. Kilde: Spørreundersøkelse fra Rogaland Revisjon.



På spørsmål om de systemansvarlige har nok tid og ressurser til å utøve oppgavene som systemansvarlige svarer under halvparten at de har det. Det er også en lav score på spørsmålet om de får nødvendig støtte og bistand fra IT. Sammenlignet med svarene fra Stavanger kommune er dette svært lav score.

Sandnes har en desentralisert styringsmodell, jfr. digital strategi, der mye ansvar er delegert ut til virksomhetene. Det er også definert at IT-enheten i Sandnes ikke skal ha brukerkompetanse i det enkelte fagsystem, men gi brukerstøtte på et generelt nivå. Siden mye av ansvaret er delegert ned i organisasjonen er det viktig at de systemansvarlige har nok tid og ressurser til å utøve sine oppgaver for å sikre en forsvarlig informasjonssikkerhet.

[26] Respondenter som har svart alternativ 4-6, Sandnes N=26-27, Stavanger N=43-44.

3.3.4 PROSEDYRER FOR INFORMASJONSSIKKERHET

Sandnes kommune sikrer informasjonens konfidensialitet, integritet og tilgjengelighet gjennom[27]:

- Tilgangsstyring, for eksempel registrering og følging av besøkende, personlige brukere på IT-systemene.
- Klassifisering av informasjon, for å vite hvem som skal ha tilgang til hvilken informasjon.
- Regler for spredning av informasjon i sosiale medier.
- Rutiner for håndtering av medier som brukes for datalagring.
- Regler for passordhåndtering.
- Sikring av arbeidsplassen og arbeidsverktøy som PC, telefon, nettbrett slik at uvedkomne ikke får tilgang. Låse PC'en når en forlater arbeidsplassen og ha kode på mobiltelefonen.
- Rutiner for beskyttelse av enheter tilkoblet bedriftens nettverk, antivirus, brannmur og lignende.
- Sikker lagring og back-up av data som tilhører kommunen og tjenestemottakere.
- Rutiner for hva som defineres som sikkerhetshendelser og hvordan man rapporterer og håndterer brudd på sikkerheten.

I arkitekturprinsippene for digitalisering ligger det sikkerhetsprinsipper som skal sikre at IT-løsninger blir etablert og driftet på en sikkerhetsmessig god måte. Ved utarbeidelsen av konseptbeskrivelse for system for felles oppvekstadministrativt system ble prinsipper for sikkerhet i løsningen beskrevet. Endelig risikovurdering vil bli gjennomført når valg av leverandør er tatt.

I kapittel 3.5 Hacking er kommunens praktisering av rutinene omtalt.

Sandnes kommune sin beredskapsplan for IT ble sist revidert mai 2017. Beredskapsplanen gjelder ved alle IT-hendelser der krisesituasjon erklæres, uavhengig av lokasjon. Planen definerer beredskapsorganisasjonen og ansvar og roller tilknyttet krisesituasjoner.

Planen skal revideres ved behov. Det står ingenting i planen om beredskapsøvelser, og kommunen opplyser at det ikke har vært gjennomført beredskapsøvelser som går på IT.

3.3.5 AVVIKSHÅNDTERING

Rutiner for avviksbehandling i Sandnes kommune er beskrevet i HMS-håndboka, jfr. kommunes intranett.

[27] Jfr. SAKIS.

Kommunen bruker Compilo som kvalitets- og avvikssystem. Alle ansatte har tilgang til Compilo via Pulsen[28].

Sandnes kommune definerer et avvik som brudd på kvalitetskrav, sett i forhold til gjeldende lover, forskrifter, prosedyrer eller rutiner. Avvik kan også forklares som uønskede hendelser og/eller forhold som har ført til eller kan føre til skade på mennesker, miljø eller materiell.

Alle avvik skal meldes elektronisk i Compilo. Hensikten med å melde og følge opp avvik skal være å redusere risiko for uønskede hendelser og tilstander og at avvikssystemet på den måten brukes som et verktøy for å forbedre arbeidsmiljø og tjenesteyting.

Ved registrering av avvik velges en av tre avvikskategorier:

- HMS
- Organisasjon/internt
- Tjeneste/bruker

I tillegg kan det velges underkategorier. Kategoriseringen sørger for at avvikene får rett behandling og oppfølging, og vil kunne danne et godt grunnlag for gode oversikter og statistikker og være et nyttig verktøy når tiltak og oppfølging av hendelser skal vurderes. Avvikene skal også gis en alvorlighetsgrad. Leder/avviksbehandler har mulighet til å endre alvorlighetsgraden hvis det vurderes på en annen måte.

Sandnes kommune har i informasjonssikkerhetshåndboken en prosedyre for avvikshåndtering for avvik som gjelder brudd på informasjonssikkerhet. Målet er at rapporteringen skal sikre at avvik blir registrert og meldt videre til rette vedkommende, slik at nødvendige tiltak kan bli iverksatt for å forebygge, avdekke og rett opp feil og mangler.

Alle ansatte som oppdager avvik er ansvarlig for å melde dette straks avviket oppdages. Medarbeideren som oppdager avvik innen eget eller andres arbeidsområde skal iverksette nødvendige tiltak for å lukke avviket så raskt som mulig og på lavest mulig nivå. Informasjonssikkerhetshåndboken refererer til et avviksskjema som skal fylles ut for å dokumentere avviket. Sandnes kommune bruker i dag avvikssystemet Compilo og alle avvik skal meldes her.

I forhold til den nye personvernforordningen (GDPR) vil det ved registrering av avvik i Compilo komme opp informasjon om at dersom det er personopplysninger på avveie skal dette meldes til personvernombudet eller dokumentsenteret. Disse vil da vurdere om avviket skal meldes inn til Datatilsynet. Alle avvik som meldes til Datatilsynet er også registrert i Compilo.

[28] Sandnes kommune sin intranettside.

Sikkerhetsansvarlig i Sandnes kommune sier hun jevnlig sjekker og vurderer avvik som er registrert i Compilo med høy risiko. Informasjonssikkerhetsforumet vurderer også antall avvik, avvik som det bør komme frem mer opplysninger om og de avvikene med høy risiko. I tillegg er gjennomgang av avvik en del av ledelsens årlige gjennomgang.

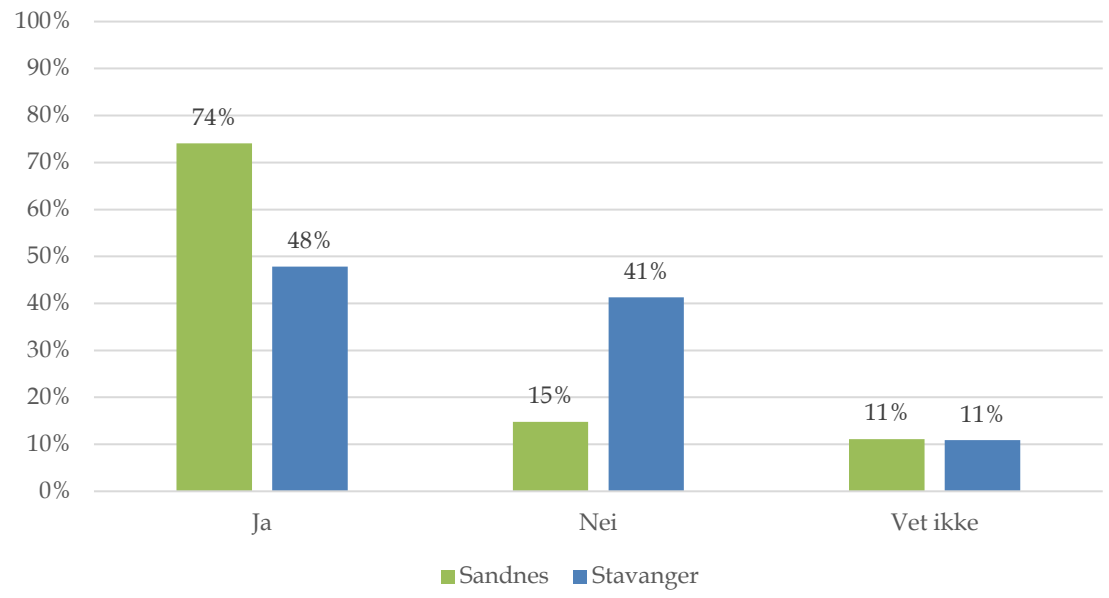
IT-sjefen sier også at det er et større fokus i IT-enheten for å melde feil i Compilo. I forbindelse med flytting av server til Green Mountain fikk kommunen en kritisk feil vedrørende en switch. Denne feilen ble ikke registrert i Compilo, men IT-sjefen laget en rapport som gikk til rådmannens ledergruppe. IT har i tillegg et brukerstøttesystem der feil logges.

Compilo ble tatt i bruk 1. januar 2016. I 2016 ble det totalt registrert 49 avvik som gjaldt brudd på informasjonssikkerhet. Av disse var 3 avvik med høy alvorlighetsgrad. I 2017 ble det registrert 60 avvik, der 13 var med høy alvorlighetsgrad. Og frem til og med oktober 2018 var det registrert 76 avvik, der 3 var med høy alvorlighetsgrad og 1 avvik var meldt til Datatilsynet.

Et av de alvorlige avvikene som ble meldt i 2018 var maskiner som var infisert av virus. Det meldes at maskinene har blitt infisert ved at ansatte har åpnet infiserte word-vedlegg på e-post.

De fleste avvikene skyldes ansatte som ikke følger rutiner, som blant annet; glemmer å låse dører, glemmer dokumenter med sensitive opplysninger i biler og hos bruker, glemmer å låse PC skjerm, feil i medisinhåndtering, feil ved scanning og oppkobling av privat utstyr mot kommunens nettverk. Tre avvik gjelder også passord på avveie og masseutsendelse av uønsket e-post. Dette skyldes ansatte som har latt seg lure til å oppgi brukernavn og passord. Konsekvensene av masseutsendelse (phising angrep) av uønsket e-post kan være svekket omdømme for kommune og i verste fall at kommunen blir svartelistet hos mottakerene. Ett av angrepene ble stoppet ved at IT-sjefen i den andre kommunen tok kontakt med den ansatte som mailene kom fra. Den ansatte i Sandnes kommune var ikke klar over at mail ble sendt ut fra sin e-post.

Figur 8 – Er det etablert rutiner for melding om uønskede hendelser, avvik eller sikkerhetsbrudd i fagsystemet?[29]. Kilde: Spørreundersøkelse fra Rogaland Revisjon.



Det er etablert rutiner for melding om uønskede hendelser, avvik eller sikkerhetsbrudd i langt flere fagsystemer i Sandnes kommune sammenlignet med Stavanger kommune.

Det er kun 2 av respondentene som har meldt avvik på brudd på informasjonssikkerhet i løpet av det siste året. Begge har meldt avviket i Compilo, og håndteringen av avviket ble beskrevet og dokumentert[30].

3.3.6 SIKKERHETSREVISJON OG EGENKONTROLL

Sandnes kommune har tidligere gjennomført egenkontroller og stedlig tilsyn av informasjonssikkerheten i enhetene. I 2017 ble det kun gjennomført egenkontroll. Tidligere var det en kombinasjon av egenkontroller og fysiske tilsyn, slik at alle virksomheter skulle hatt besøk i løpet av en treårsplan. Dette har det ikke vært ressurser til de siste årene etter at den som hadde ansvaret sluttet og ikke ble erstattet.

I 2018 ble det gjennomført egenkontroller helt på slutten av året. Revisjonen har ikke hatt anledning til å vurdere egenkontrollene for 2018. Det har ikke blitt gjennomført stedlig tilsyn for 2018.

Kommunen ser for seg å bruke Draftit som et system for egenkontroll i 2019, og tilpasse kontrollene slik at de passer med de nye kravene etter personvernforordningen (GDPR). Dette fordi alle enheter er/skal være representert i Draftit, og at kravene til personvernforordningen da blir inkludert i internkontrollen.

[29] Sandnes N=27, Stavanger N=46.
[30] En av respondentene har svart alternativ annet, men har svart nei på spørsmålet *«Har du meldt avvik på brudd på informasjonssikkerhet i løpet av det siste året?»*.

3.4 ARKIVERING OG OFFENTLIGGJØRING

Dette kapitlet fokuserer på følgende problemstilling:

> *Blir krav til arkivering og offentliggjøring ivaretatt og har de ansatte kjennskap til regelverket?*

Til denne problemstillingen har vi utledet følgende revisjonskriterier:

- Kommunen skal ha en ajourført arkivplan, som viser hva arkivet omfatter, hvordan det er organisert og hvilke rutiner som gjelder.
- Kommunen skal dokumentere alle sine elektroniske systemer som inneholder arkivverdig informasjon i arkivplanen.
- Kommunen skal ha personvernombud.
- Det skal finnes en oversikt over hvilke personopplysninger som lagres og behandles i kommunen.
- Kommunen har systemer og rutiner for innsyn og retting av personopplysninger.
- Saksbehandlere er bevisst på hvilke saker som skal unntas fra offentlighet.
- Offentlig journal skal ikke inneholde sensitiv informasjon.

Arkivverket gjennomførte i 2018 en tilsynsrapport for arkivet i Sandnes kommune. Tilsynet hadde hovedfokus på arkivorganisering og elektronisk arkivdanning, herunder arkivplan, journalføring og fagsystemer.

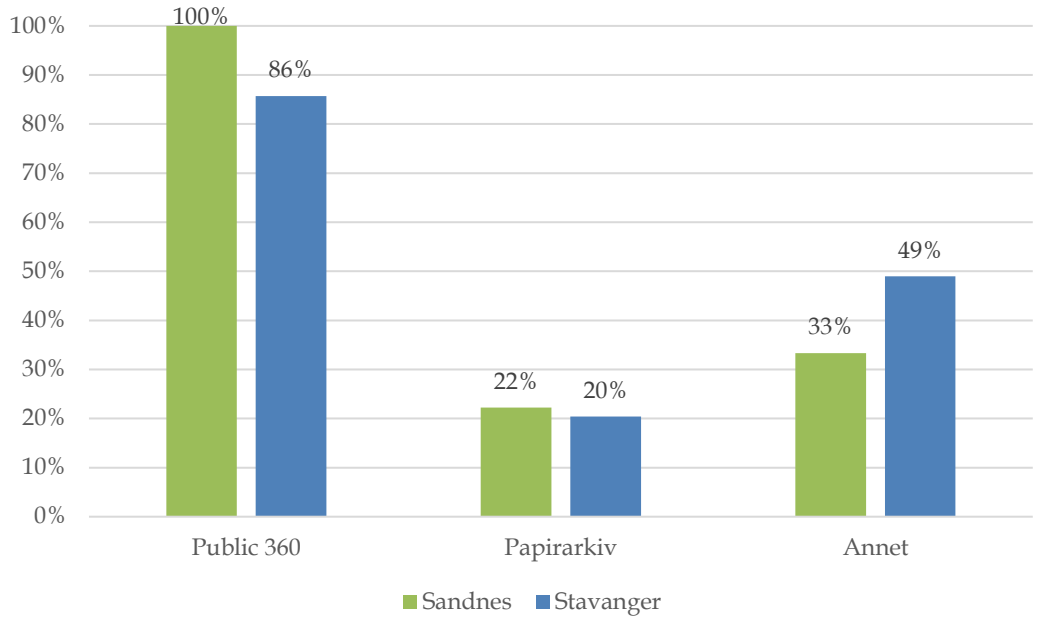
Rapporten har 6 pålegg om utbedringer:

1. Arkivplanen må oppdateres
2. Kvalitetssikring av sak-/arkivsystemet
3. Dokumentere elektroniske arkivsystemer
4. Sikre behandling av arkivdokumenter som lagres elektronisk
5. Deponere uttrekk fra journalsystem
6. Sikre eldre og avsluttede papirarkiver

Alle påleggene skal være utbedret i løpet av 2018. I dialog med kommunen har tiltak og oppfølging av påleggene i Arkivverkets rapport vært sentralt.

Sandnes kommune har i tillegg svart på Riksarkivarens undersøkelse for 2018.

Figur 9 – System for arkivering[31]. Kilde: Spørreundersøkelse fra Rogaland Revisjon.



I Sandnes kommune svarer alle respondentene at de arkiverer sine dokumenter og saker i Public 360. I tillegg er det noen som også arkiverer i papirarkiver og i andre fagsystemer.

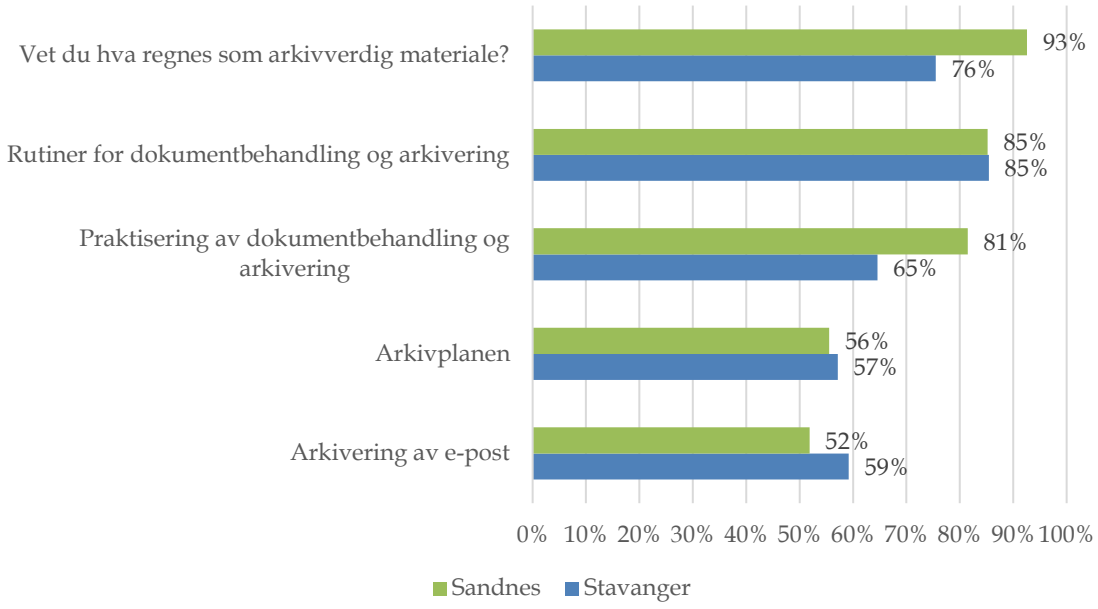
3.4.1 ARKIVPLAN

Arkivplanen til Sandnes kommune er tilgjengelig via intranett[32], og består av flere dokumenter.

Arkivverket påpeker i sin tilsynsrapport at en del kapitler i arkivplanen ikke er oppdatert eller under utarbeidelse. Konstituert arkivsjef melder at alle avvik som gjelder arkivplanen er lukket innen fristen.

[31] Sandnes N=27, Stavanger N=49.
[32] Linker til siden arkivplan.no.

Figur 10 – Arkivplan og rutiner for dokumentbehandling og arkivering[33]. Kilde: Spørreundersøkelse fra Rogaland Revisjon.



Sammenlignet med svarene fra Stavanger kommune er det betydelig flere av respondentene i Sandnes som vet hva som regnes som arkivverdig materiale. Det fleste (85 prosent) svarer også at rutiner for dokumentbehandling og arkivering er kjent for de ansatte ved deres enhet. For å kartlegge om de ansattes praktisering av rutiner har revisjonen inkludert et spørsmål som omhandler rutiner satt ut i praksis. Hele 81 prosent svarer at praktiseringen av dokumentbehandling og arkivering er tilfredsstillende ved deres enhet. Sammenlignet med svar fra systemansvarlige i Stavanger kommune tyder dette på at systemansvarlige i Sandnes kommune i større grad vet hva som regnes som arkivverdig materiale og at rutiner for dokumentbehandling og arkivering praktiseres i det daglige.

Både i Sandnes og Stavanger er det noe begrenset kjennskap til innholdet i kommunens arkivplan, men i Sandnes svarer 78 prosent[34] av de systemansvarlige at de vet hvor de finner arkivplanen mot 53 prosent[35] i Stavanger kommune. Men bare om lag halvparten av de systemansvarlige i Sandnes kommune sier de kjenner rutinen for arkivering av e-post.

I Arkivverkets tilsynsrapport kom det frem at dokumentsenteret ikke alltid ble informert og/eller involvert i forbindelse med anskaffelser av nye systemer som får konsekvenser for arkivarbeidet i Sandnes kommune. Det kom også fram at IT-sjefen heller ikke alltid involveres i nyanskaffelser av systemer. Konstituert arkivsjef sier at dette er noe som både dokumentsenteret og digitaliseringskontoret har fokus på. Risikoen for

[33] Spørsmål om i hvilken grad systemansvarlige kjenner til arkivplan og rutiner for dokumentbehandling og arkivering. Figuren viser respondenter som har svart alternativ 4-6, Sandnes N=27, Stavanger N=48-49.
[34] N=27.
[35] N=49.

at det anskaffes systemer uten dokumentsenterets involvering er i de tilfellene enheten selv gjennomfører hele anskaffelsesprosessen. I prosessen for anskaffelse av et nytt oppvekst administrativt system har dokumentsenteret vært involvert fra start.

ELEKTRONISKE SYSTEMER

Utfordringen med elektronisk lagret informasjon er at den blir automatisk uleselig for oss etter relativt kort tid hvis den bevares i samme form som den til daglig brukes. Elektronisk informasjon kan vanligvis bare leses med hjelp av spesifikke verktøy, og oppdateringer og teknologiskifter vil gjøre at informasjonen ikke lenger er tilgjengelig.

For å bevare elektronisk informasjon må det lages en migrasjonsstrategi. De originale systemene eller databasene bevares ikke, men det trekkes ut informasjonen fra systemene i en form som er flyttbar mellom teknologiplattformer, og bevarer den sammen med en definisjon av det opprinnelige databasesystemet. Elektroniske arkiver er arbeidskrevende fordi de krever et kontinuerlig vedlikehold for ikke å gå tapt.

Sandnes kommune oppgir i Riksarkivarens undersøkelse for 2018 at kommunen i stor grad[36] har dokumentert alle sine elektroniske systemer som inneholder arkivverdig informasjon i arkivplanen.

Arkivverket sin tilsynsrapport gav kommunen flere pålegg som gjaldt både å sikre behandling av arkivdokumenter som lagres elektronisk og dokumentere elektroniske systemer. Kommunen opplyser i sin oppfølging til Arkivverket at de har gjennomgått dokumentasjonen som ligger i arkivplanen. Men noe arbeid gjenstår, og vil bli oppdatert etter hvert som arbeidet med kommunesammenslåing skrider frem.

3.4.2 PERSONOPPLYSNINGER

Protokoll over personopplysninger er ikke en ny oppgave for kommunene, og Sandnes kommune har en oversikt som viser hvilke behandlinger av personopplysninger som tidligere krevde konsesjon og meldeplikt. Etter den nye personopplysningsloven skal ytterligere opplysninger supplere protokollene. For å sikre at protokollen dekker de lovpålagte kravene har kommunen tatt i bruk en elektronisk løsning, Draftit, for innsamling og årlig revisjon av data. Den nye løsningen vil også avdekke eventuelle mangler knyttet til risikovurderinger og databehandleravtaler. Prosjektleder for implementering av ny personvernforordning i Sandnes kommune ble lagt til personvernombudet/sikkerhetsansvarlig. I tillegg ble det nedsatt en arbeidsgruppe som tok for seg ulike tema, blant annet ROS-analyser, avviksbehandling, informasjonssikkerhet generelt, databehandleravtaler, opplæring og samtykke.

I Sandnes kommune har det blitt gjennomført gruppeopplæring av ledere og systemansvarlige via kompetansesenteret i forhold til kommunens plikter og de registrertes rettigheter etter den nye personvernforordningen. Andre ansatte som har behov har også fått tilbud om kurs via kompetansesenteret. Alle ledere har også deltatt på/fått

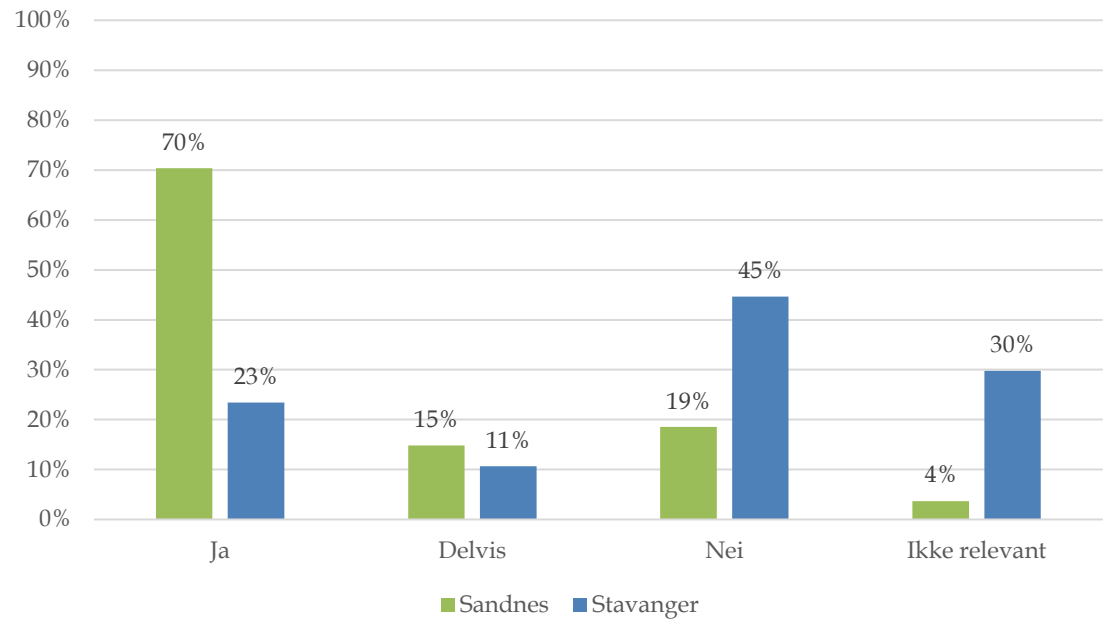
[36] Svar 4 på spørsmål med svar alternativer 1-4 der 1= passer ikke i det hele tatt og 5= passer svært godt

tilbud om kurs i ny personvernforordning via Kommunal Informasjonssikkerhet (Kins). I tillegg har det blitt gjennomført e-læringskurs. I spørreundersøkelsen til de systemansvarlige svarer 70 prosent[37] at de har fått tilstrekkelig opplæring. De fleste vet også hvem som er personvernombud i Sandnes og får hjelp og veiledning dersom de har spørsmål som gjelder personopplysninger. I Sandnes kommune var rollen som sikkerhetsansvarlig og personvernombudet tidligere tillagt samme person. Fra 2019 vil rollen som sikkerhetsansvarlig for den organisatoriske samles hos en person under området digitalisering og innovasjon. Den tekniske delen av informasjonssikkerheten vil fortsatt utføres av IT. Personvernombudet har selv pekt på utfordringer med å inneha flere roller i intervju med revisjonen. En splitting av personvernombud og sikkerhetsansvarlig vil legge til rette for ombudets uavhengighet for å unngå en interessekonflikt.

I Draftit er det 154 registreringer til nå. Personvernombudet i Sandnes kommune opplyser at kommunen ikke er ferdig med å registrere behandlinger i Draftit. Det er de systemansvarlige som har ansvaret for å registrere behandlinger av personopplysninger. Leder skal påse at sin enhet har registrert sine behandlinger i Draftit.

De fleste registreringene i Draftit har ikke fått angitt risiko og status. Det er leder som skal angi risiko og status for behandlinger. I følge personvernombudet har fokuset i Sandnes vært å starte med registreringsarbeidet. Neste skritt blir å kvalitetssikre det som er registrert, blant annet ved å angi risiko.

Figur 11 – Har du registrert behandling av personopplysninger i Draftit?[38]. Kilde: Spørreundersøkelse fra Rogaland Revisjon.



[37] Respondenter som har svart alternativ 4-6, N=27.
[38] Sandnes N=27, Stavanger N=47.

Sammenlignet med undersøkelsen som ble gjennomført i Stavanger kommune er det langt flere som har registrert behandlinger i Draftit blant de systemansvarlige i Sandnes. Det er også langt færre som svarer at registrering av behandling av personopplysninger ikke er relevant for dem.

Revisjonen har sammenlignet registreringer i Draftit i forhold til det tidligere behandlingsregisteret[39]. Revisjonen finner manglende registreringer av behandlinger innenfor levekårsområdet, PPT og HMS. Avvikene kan skyldes at virksomhetene har fått nye systemer eller at registreringene i Draftit ikke er fullstendige.

For å sikre personvernet har personvernforordningen et krav om at alle nye løsninger skal ha innebygd personvern. Sandnes har ingen egne løsninger, og det er derfor leverandørene som har ansvaret for at løsningen de tilbyr kommunen har innbygd personvern.

Alle fagsystemer som brukes til å behandle personopplysninger skal ha en databehandleravtale med leverandøren. I Draftit er det svart ja på spørsmål om det benyttes dataavtale på 70 skjemaer. Av disse er det 38 som svarer at det er inngått en skriftlig databehandleravtale, mens 11 svarer nei og 21 svarer vet ikke.

Gjennomgangen viser blant annet at det er 18 registreringer der Public 360 oppgis å være hovedsystem. 9 har svart at det benyttes databehandler, 6 svarer nei og 3 vet ikke. Ingen svarer ja på om det foreligger en skriftlig avtale med leverandøren.

3.4.3 OFFENTLIGHET OG INNSYN

Dokumentsenteret har utarbeidet retningslinjer for offentlighetsvurdering og skjerming av dokumenter i Public 360. Disse retningslinjene ligger tilgjengelig for de ansatte i arkivplanen til Sandnes kommune. Hovedregelen er at kommunens dokumenter, journaler og lignende registre er åpne for allment innsyn. Det må foreligge en hjemmel/unntaksbestemmelse som gir adgang til å unnta hvis et dokument skal unntas fra offentligheten, jfr. offentlighetsloven § 3.

Hjemlene for å unnta et dokument fra offentlighet skiller mellom

- om det skal eller kan gjøres unntak fra hovedregelen om allment innsyn, og
- om unntaket gjelder for
    - kun opplysninger i et dokument
    - deler av et dokument, eller
    - hele dokumentet

Hva som skal unntas må vurderes konkret i hvert enkelt tilfelle. Kommunen har i sine retningslinjer en liste over hva en bør tenke på når man vurdere å unnta et dokument

[39] Tidligere oversikt som viser behandlinger av personopplysninger i Sandnes kommune som krevde konsesjon og meldeplikt.

fra offentlighet, og også konkrete eksempler på offentlighetsvurderinger. Det presiseres også at det aldri er anledning til å unnta et dokument av bekvemmelighetshensyn.

Aktuelle lovhjemler som benyttes når dokumenter eller saker vurderes å være unntatt offentligheten:

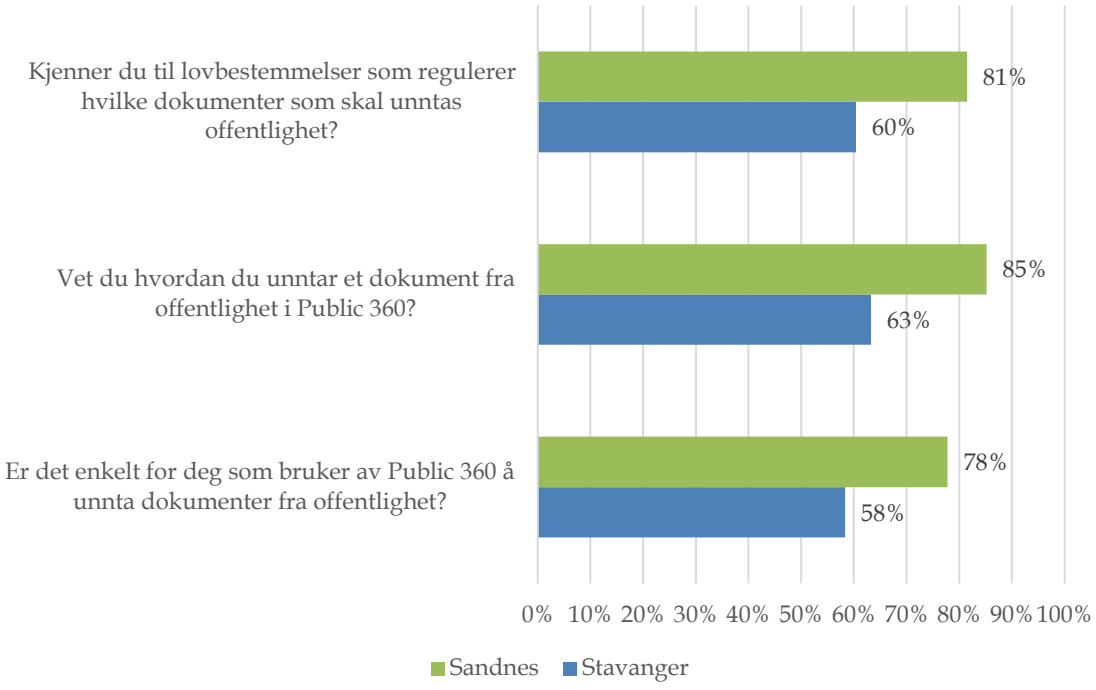
Figur 12 – Oversikt over aktuelle hjemler som benyttes når et dokument eller en sak skal unntas offentlighet. Kilde: Arkivplan Sandnes kommune.

Type sak	Paragrafer	Lovtekst
Personlige forhold	Offl. § 13, fvl. § 13.1	Unntak for noens personlige forhold
Drifts-, eller forretningsforhold	Offl. § 13, fvl. § 13.2	Unntak for drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.
Interne dokumenter utenfra	Offl. § 15	Interne dokumenter utenfra
Organinterne dokumenter	Offl. § 14	Organinterne dokumenter
Rettspleielovene	Offl. § 18	Saker som behandles etter rettspleielovene
Økonomi-, lønns- eller personalforvaltning	Offl. § 23.1	Av hensyn til en forsvarlig gjennomføring av statens, kommunens eller vedkommende organs økonomi-, lønns- eller personalforvaltning
Økonomiske rammeavtaler	Offl. § 23.2	Av hensyn til en forsvarlig gjennomføring av økonomiske rammeavtaler med næringslivet
Rikets sikkerhet	Offl. § 24	Dokument som inneholder opplysninger som om de ble kjent, ville kunne skade rikets sikkerhet, landets forsvar eller forholdet til fremmede makter eller internasjonale organisasjoner
Offentlige kontroll- eller reguleringstiltak	Offl. § 24.1	Fordi offentlighet ville motvirke offentlige kontroll- eller reguleringstiltak eller andre nødvendige pålegg eller forbud, eller medføre fare for at de ikke kan gjennomføres
Lovovertredelse	Offl. § 24.2	Anmeldelse, rapport og annet dokument om lovovertredelse
Opplysningene som kan lette utføring av straffbare handling	Offl. § 24.3	Unntak der opplysningene vil lette utføring av straffbare handling
Ansettelsessak	Offl. § 25	Dokument i sak om ansettelse eller forfremmelse i offentlig tjeneste. **NB:** Unntaket gjelder ***ikke*** søkerliste. Opplysninger om en søker kan likevel unntas fra offentlighet dersom søkeren selv anmoder om dette
Besvarelser	Offl. § 26.1	Besvarelse til eksamen eller lignende prøve samt innlevert utkast til konkurranse e.l.
Utsatt offentlighet	Offl. § 5	Utsatt offentlighet i særskilte tilfeller

Det er saksbehandlers ansvar å kontrollere at innkommende og utgående dokumenter avskjermes dersom det er hjemmel for dette.

Hjemler som påføres innkommende dokumenter er forslag for dokumentsenterets side. Dokumentsenteret leser ikke gjennom hele dokumentet. Det må saksbehandler selv gjøre og eventuelt korrigere påførte hjemler dersom dette er feil.

Figur 13 – Unnta dokumenter fra offentlighet[40]. Kilde: Spørreundersøkelse fra Rogaland Revisjon.



Over 80 prosent av de systemansvarlige i Sandnes kommune kjenner til lovbestemmelsene som regulerer hvilke dokumenter som skal unntas offentlighet. Dette er over 20 prosentpoeng høyere score en Stavanger kommune. Det er også flere som vet hvordan de unntar et dokument fra offentlighet i Public 360 i Sandnes. Ut i fra spørreundersøkelsen kan det se ut som om respondentene i undersøkelsen fra Sandnes både er sikrere på hvilke dokumenter som skal unntas, og hvordan man unntar et dokument fra offentligheten sammenlignet med respondentene i undersøkelsen i Stavanger kommune.

Begge kommunene bruker Public 360 og det er derfor interessant å se at respondentene fra Sandnes mener systemet er lett å bruke for å unnta et dokument fra offentlighet, men at dette ikke får like høy score i Stavanger.

OFFENTLIG JOURNAL

Offentlig journal er tilgjengelig på kommunens hjemmeside dagen etter registrering/ferdigstillelse i Public 360. Dette for at dokumentsenteret får tid til å foreta en kvalitetssikring av opplysningene. Saker som er unntatt innsyn er merket. Etter offentliggjøring blir dokumentene liggende på kommunens hjemmeside i 3 måneder. Via nettsiden er det mulig å be om innsyn i dokumentene.

Avdelinger/enheter som fører egne manuelle journaler er ikke med i offentlig journal på hjemmesiden til Sandnes kommune. Dette gjelder blant annet omsorg og helsestasjoner. Enheter som bruker Public 360 uten at postlisten publiseres til offentlig journal

[40] Respondenter som har svart alternativ 4-6, Sandnes N=27, Stavanger N=48-49.

på internett, må kunne fremlegge en offentlig journal på forespørsel, jfr. rutine for innsyn i Sandnes kommune.

Dokumenter fra brukermapper publiseres heller ikke på offentlig journal. Sandnes kommune har valgt dette først og fremst som en ekstra sikring mot at personsensitive opplysninger kommer på avveie. Innsyn i disse dokumentene vil i de aller fleste tilfellene reguleres av bestemmelsene om partsinnsyn i forvaltningsloven.

Revisjonen gjennomførte kontroll av alle journalførte saker på en gitt dato. Totalt ble 494 saker kontrollert. Av disse var om lag to tredjedeler unntatt offentlighet. De fleste saker var unntatt offentlighet etter offentlighetsloven § 25, og omhandlet ansettelser. Det var også flere saker som omhandlet tildeling av skoleplass og diverse søknader om dispensjoner som var unntatt etter offentlighetsloven § 13 og forvaltningsloven § 13.1. Revisjonen avdekket ingen feil i de sakene som ble kontrollert.

INNSYN

I kommunens arkivplan finnes det rutiner for innsyn i Sandnes kommune. Rutinen gir en oversikt over hvordan ledere, saksbehandlere og arkivarer ved dokumentsenteret skal håndtere innsynsbegjæringer fra publikum og presse.

Innsynsbegjæringer via offentlig journal behandles av dokumentsenteret. Ved innsynsbegjæring i et ugradert dokument foretas det en grundig kvalitetssjekk (offentlighetsvurdering) av innholdet i det bestilte dokumentet, selv om dokumenter står som ugradert. Dersom det ikke er noe i dokumentet som tilsier at det skulle vært unntatt offentligheten, sendes dokumentet til innsynsbegjærer på e-post, med blindkopi til ansvarlig saksbehandler.

Dersom det bes om innsyn i et gradert dokument videresender dokumentsenteret innsynsbegjæringen til ansvarlig saksbehandler. Rutinen er at dokumentsenteret også skal ta muntlig kontakt med saksbehandler for å informere om innsynsbegjæringen og opplyse om kravene til behandlingstid i lovverket. Dersom saksbehandler er fraværende, kontaktes leder for avklaring om hvem som skal behandle saken. Saksbehandler bes foreta en ny offentlighetsvurdering ut fra prinsippet om meroffentlighet. Dokumentsenteret og kommuneadvokat kan bistå ved behov. Saksbehandler gir tilbakemelding til innsynsbegjærer.

Innsynsbegjæringer fra andre postlister enn offentlig journal videresendes til aktuell enhet for videre behandling.

Hovedregelen er at du har rett til innsyn i de opplysningene som Sandnes kommune behandler om deg som enkeltperson. Du har også krav på å få informasjon om behandlingen. For å få innsyn i personopplysninger må tjenesten eller enheten som utfører behandlingen kontaktes.

Det ble i spørreundersøkelsen undersøkt hvor mange innsynsbegjæringer om personopplysninger det er kommet i fagsystemene. Her er det kun 26 prosent[41] som har mottatt innsynsbegjæring. 56 prosent[42] svarer at de har rutiner for håndtering av innsyn, samt rutine for retting og sletting av personopplysninger i fagsystemet. Det ble åpnet for at respondentene kunne legge igjen en generell kommentar i forhold til enhetens håndtering av innsynsbegjæringer. De fleste svarer her at de håndterer innsynsbegjæringer på en tilfredsstillende måte og at kommuneadvokaten kontaktes dersom de er usikre.

I tillegg til innsyn via offentlig journal har Sandnes kommune også flere løsninger for innsyn og fulltekstpublisering av dokumenter, for eksempel Open Gov Meeting[43] og Open Gov Cases[44]. Innsyn via disse løsningen har ikke blitt vurdert i prosjektet.

[41] N=27.
[42] N=27.
[43] Politiske dokumenter og vedtak som ligger til utvalgene.
[44] Dokumenter fra sakstypene Byggesak, Landbrukssak, VAR-sak, Plansak, Oppmåling og Miljøsak.

3.5 HACKING

Dette kapitlet fokuserer på følgende problemstilling:

Hva er risikoen for hacking, og hvordan beskytter kommunen seg mot det?

Til denne problemstillingen har vi utledet følgende revisjonskriterier, jfr. kapittel 2:

- Det skal være etablert betryggende systemer og prosedyrer for å sikre kommunen mot uønskede handlinger.

I kapittel 3.3 har vi undersøkt om Sandnes kommune har etablert et internkontrollsystem for å sikre informasjonssikkerheten. I dette kapittelet vil vi se mer på om de rutiner og systemer kommunen har er betryggende for å sikre kommunen mot uønskede handlinger. IT-sjefen peker på at det er sluttbrukeren som er den største risikoen for at et forsøk på hacking blir vellykket. Viktige tiltak er derfor opplæring og bevisstgjøring av ansatte. Sandnes kommune har de siste årene gjennomført nasjonal sikkerhetsmåned. Dette er et virkemiddel for å gjøre ansatte mer oppmerksomme på de ulike truslene som finnes, og tiltak som den enkelte kan gjøre for å høyne sikkerheten.

For å sikre seg mot hacking er det viktig å forstå hva angrepsflaten er. I forhold til trusselbilde pekes det på at ansatte er den største risikoen. Opplæring og kunnskap øker tryggheten og minsker faren. Kommunen er kjent med at de har blitt utsatt for to hacking-angrep de siste to årene. Ingen av angrepene har vært vellykket. Det er også en risiko for at kommune har blitt utsatt for hacking-angrep som ikke er kjent for dem. Siste året har det også vært om lag 10 hendelser der ansatte har gitt ut brukernavn og passord til andre.

I spørreundersøkelsen blant de systemansvarlige i Sandnes kommune svarer de fleste nei eller vet ikke på spørsmålene om det har forekommet uønskede hendelser. Men 22 prosent[45] svarer ja på spørsmålet om det har forekommet driftsstans som ble ansett som virksomhetskritisk.

På spørsmål om det har vært mistanke om uønskede hendelser, avvik eller sikkerhetsbrudd det siste året svarer 20 prosent[46] ja. I kommentarene til spørsmålet har en av respondentene kommentert at ansatte deler brukernavn og passord med andre ansatte som ikke har tilgang.

SIKKERHETSLØSNINGER

Sandnes kommune har på plass det som trengs av brannmurer, antivirus, innebygd sikkerhet i programvare (der det er aktuelt) og sikkerhets oppdateringer. Kommunen

[45] N=27.
[46] N=25.

har ingen programmer som overvåker systemet (som for eksempel en SIEM-løsning[47]). Kommunen har vurdert anskaffelse av sikkerhetsløsninger, men det er ikke prioritert i forhold til kapasitet og ressurser i IT-enheten. Et sikkerhetsovervåkingssystem vil gi et proaktivt vern mot stadig mer avanserte og komplekse trusler og angrep, og vil fungere som et kontrollsenter der sikkerhetsdata fra ulike kilder samordnes og analyseres. Per i dag opplyser IT-enheten at det ikke gjennomføres en systematisk overvåking av logger i systemet.

Brannmuren fremholdes som det viktigste forsvaret mot hacking av kommunens data. Sandnes kommune har en ny brannmur, og denne har ny funksjonalitet som er implementert. Dette gjør at sikkerheten er høynet.

Kommunens serverrom er flyttet til Green Mountain. Dette bidrar til et høyteknologisk serverrom med fokus på sikkerhet som adgangskontroll, strømaggregat, UPS[48], brannsikring, kjøling og bombesikring. Dette bidrar til fysisk og virtuell sikring av kommunens samlede data.

OPPGRADERING AV PROGRAM- OG MASKINVARE

Leverandørene kjenner sine fagsystemer best og er derfor i stor grad gitt ansvaret for drift og vedlikehold av løsningene som de leverer. Det er systemeier som har kontakt med leverandøren, og som har det funksjonelle ansvaret for IKT-løsningen, jfr. digital strategi. Dette innebærer at det er systemeier som har ansvaret for å vurdere utviklingsprosjekter for IKT-løsningen både økonomisk og funksjonelt. Det er systemeier som skal avklare om IKT-løsningen bør oppgraderes eller erstattes. På brukerstøtte sin portal[49] finnes rutine for oppgradering og endring av fagsystem. IT er kun involvert i større oppgraderinger av viktige systemer.

Sandnes kommune er medlem i HelseCERT. HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. Deres oppgave er å øke sektorens evne til å oppdage, forebygge og håndtere ondsinnede inntrengingsforsøk og andre uønskede IKT-hendelser.

Via medlemskap i HelseCERT får Sandnes kommune tidlig varsler av brudd og sikkerhetssvakheter. Kritiske oppdateringer tas med en gang, men det foretas en risikovurdering på enkelte systemer. Mindre viktige oppgraderinger i systemer som skal fases ut prioriteres ikke dersom risikoen blir vurdert som lav.

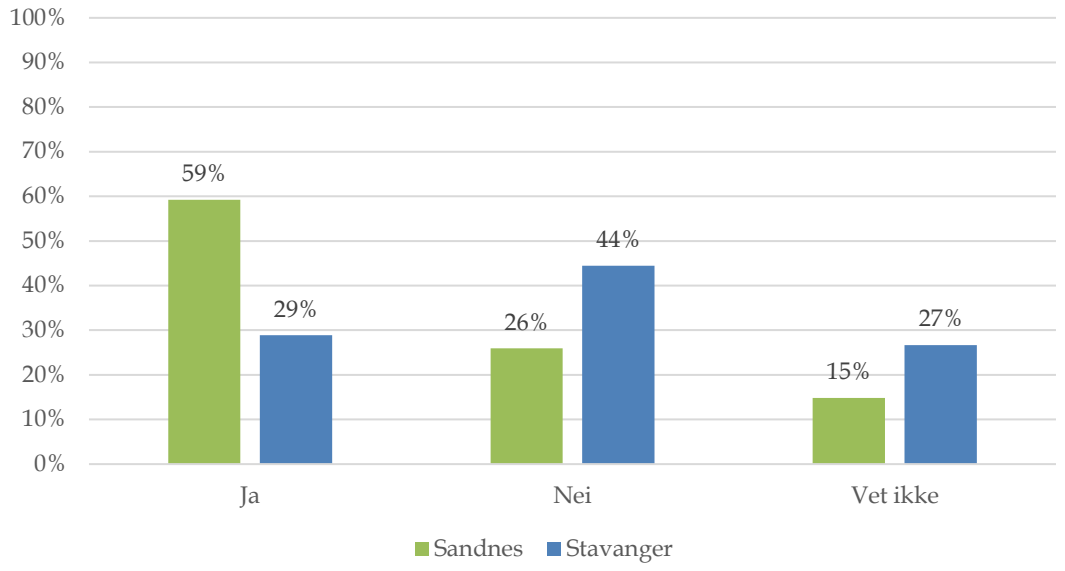
BRUKERKONTO

IT styre overordnet brukertilgang til kommunens nettverk, tilganger i den enkelte IKT-løsning gis av systemeier.

[47] Security Information and Event Manganement (SIEM).
[48] Uninterruptible power supply, UPS (avbruddsfri strømforsyning)
[49] Tilgjengelig for ansatte via Pulsen (intranett).

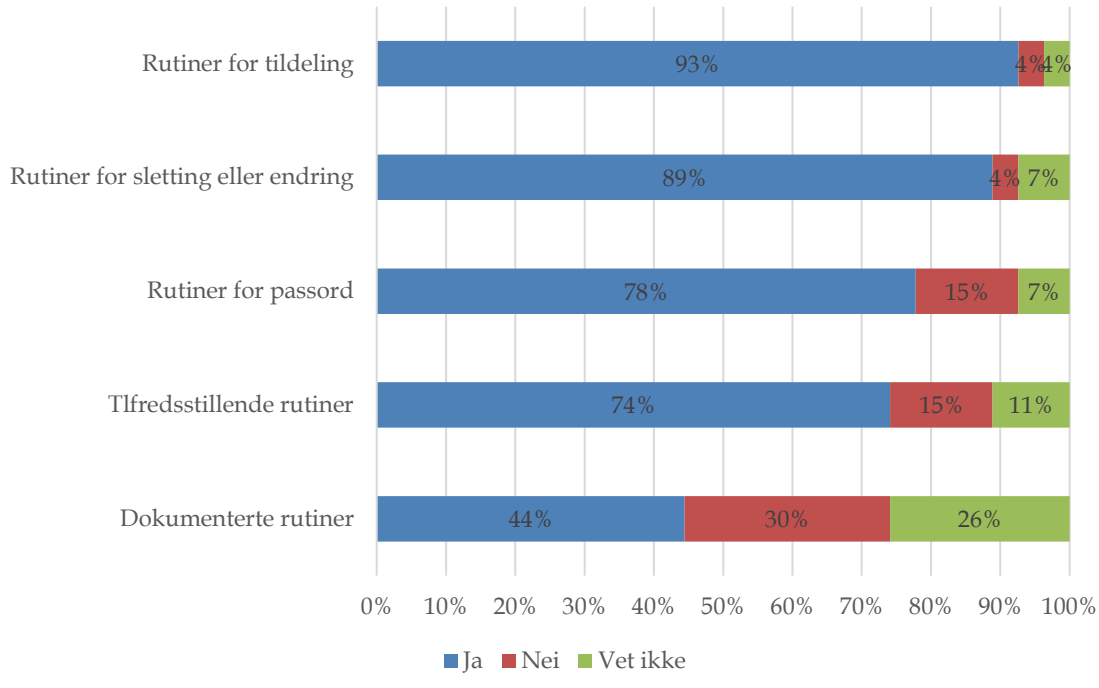
Systemeier er sikkerhetsmessig ansvarlig for IKT-løsningen og er blant annet ansvarlig for å etablere, endre og fjerne tilganger.

Figur 14 – Er det foretatt risikovurdering ifm. brukertilganger til fagsystemet?[50] Kilde: Spørreundersøkelse fra Rogaland Revisjon.



Langt flere systemansvarlige i Sandnes svarer at det er gjennomført risikovurdering i forbindelse med brukertilganger til fagsystemet.

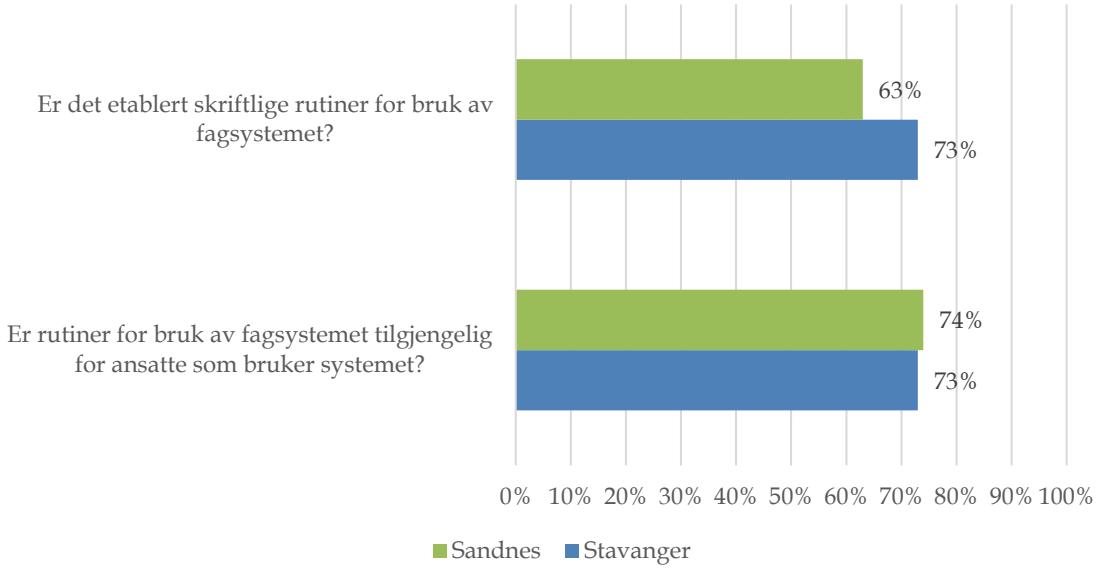
Figur 15 – Rutiner og prosedyrer for brukertilganger (N=27) Kilde: Spørreundersøkelse fra Rogaland Revisjon.



[50] Sandnes N=27, Stavanger N=45.

I svarene fra spørreundersøkelsen ser vi at de fleste har etablert rutiner for tildeling av brukertilganger i fagsystemene. De fleste har også etablert rutiner for sletting og endring av brukertilganger, mens noen færre har rutiner for passordbruk. 74 prosent svarer at rutiner og prosedyrer for administrering og kontroll av brukertilganger i fagsystemet er tilfredsstillende. Men svarene fra undersøkelsen viser at det er under halvparten som har dokumentert rutiner og prosedyrer for administrering av brukertilganger. Sammenlignet med svarene fra Stavanger kommune er bilde nokså likt, men Sandnes har noe høyere score på spørsmål om tilfredsstillende rutiner og rutiner for passord.

Figur 16 – Rutiner for bruk av fagsystemet[51]. Kilde: Spørreundersøkelse fra Rogaland Revisjon.



I Sandnes er det etablert skriftlige rutiner for bruk i noe mindre grad sammenlignet med Stavanger kommune. Men de rutinene som er etablerte er tilgjengelige for de fleste ansatte som bruker systemet.

IT-enheten har de siste årene foretatt en opprydning i antall administratortilganger. Antallet som har administratortilgang har blitt kraftig redusert. IT forsøker i størst mulig grad å ha rollebaserte tilganger, men siden IT-enheten har lav bemanning vil det kunne være personer som har flere tilganger fordi de kommer inn under flere roller.

Inaktive brukerkontoer blir automatisk slettet. Sandnes har også implementert et identitetsstyringsverktøy som er knyttet til lønns- og personalsystemet (HRM). På sikt er det ønskelig å knytte IDM-løsningen til fagsystemene slik at endringer i lønnssystemet blir direkte overført til fagsystemene.

[51] Antall som har svart ja på spørsmålene, Sandnes N=27, Stavanger N=45-46.

DIGITALISERING

Digitalisering, tingenes internett og gjenbruk av data medfører en høyere sikkerhetsrisiko. I forhold til personvernforordningen (GDPR) er viktig å lovhjemle formålet med behandlingen av alle aktiviteter som omfatter personopplysninger. Det skal også vurdere behov for risikovurdering. Sandnes kommune er bevisst på at kommunen blir mer sårbar som følge av økt digitalisering. Sikkerhet er derfor sentralt i arbeidet med digitalisering, blant annet som fast punkt på agendaen for digitaliseringskontoret sine møter.

3.6 OPPSUMMERING, VURDERING OG ANBEFALINGER

Sandnes kommune jobber aktivt for å bevisstgjøre medarbeiderne i forhold til informasjonssikkerhet og personvern, blant annet gjennom lederskolen, kurs for nyansatte samt at det er et tema på ledermøter.

Kommunen sier selv at de bruker lite ressurser og at de har utfordringer med å bistå, veilede og følge opp enhetene i forhold til informasjonssikkerhet og internkontroll. Dette kommer også fram via spørreundersøkelsen der om lag halvparten av de systemansvarlige svarer alternativ 1-3 på spørsmål om de har nok tid og ressurser til å utøve oppgaver som systemansvarlig. På tross av dette viser spørreundersøkelsen at de fleste er kjent med kommunens retningslinjer for informasjonssikkerhet og at rutinene i stor grad blir fulgt i det daglige.

Den største trusselen mot informasjonssikkerheten i Sandnes kommune er at ansatte ikke følger retningslinjer og prosedyrer. Dette kommer fram både i intervju med sikkerhetsansvarlig og IT-sjef, samt i ledelsens årlige gjennomgang av informasjonssikkerhet.

OPPFØLGING AV FORVALTNINGSREVISJON FRA 2010

I forvaltningsrevisjonen av elektronisk behandling av sensitive personopplysninger fra 2010 satte rådmannen opp fem forbedringspunkter som kommunen skulle ha fokus på. Kommunen har lykkes med å forbedre de fleste punktene. Men intervjuer av sikkerhetsansvarlig og spørreundersøkelse ut til systemansvarlige viser at kommunen fortsatt har utfordringer i forhold til tilstrekkelige ressurser.

INFORMASJONSSIKKERHET

Sandnes kommune har et styringssystem for informasjonssikkerhet som omfatter en digital strategi samt et internkontrollsystem for informasjonssikkerhet. Kommunen er i ferd med å implementere et nytt styringssystem for informasjonssikkerhet, SAKIS, som skal erstatte den tidligere informasjonssikkerhetshåndboken. I den tidligere informasjonssikkerhetshåndboken er sikkerhetsmål og -strategi definert. Ansatte har per i dag ingen mulighet til å finne kommunens retningslinjer og prosedyrer for informasjonssikkerhet da den tidligere sikkerhetshåndboken ikke lenger er tilgjengelig på intranett. Spørreundersøkelsen tyder allikevel på at retningslinjer og prosedyrer for informasjonssikkerhet er godt kjent blant de systemansvarlige. Sikkerhetsansvarlig i kommunen anslår at informasjonen fra sikkerhetshåndboken skal være overført til SAKIS innen 1. mars 2019.

Anbefaling:

- *Revisjonen anbefaler at Sandnes kommune påser at kommunens retningslinjer og prosedyrer blir tilgjengelig for ansatte på intranett så fort som mulig.*

Rådmannens ledergruppe har en årlig gjennomgang av informasjonssikkerhet. Gjennomgangen ser blant annet på avvik som er meldt i Compilo, egenkontroller, endringer i trusselbilde og ressurser for å ivareta internkontroll og informasjonssikkerhet.

Roller og ansvar knyttet til informasjonssikkerhet er definert i informasjonssikkerhetshåndboken. På intranett finner man organiseringen i grove trekk, men per i dag ligger det ikke ute informasjon som viser hvilke ansvar som ligger til de ulike rollene. Informasjonen som ligger i informasjonssikkerhetshåndboken er på noen områder utdatert som følge av nye personopplysningslov.

Risikovurderinger skal gjennomføres ved nye behandlinger av personopplysninger, og de skal danne grunnlaget for sikkerhetstiltak. Spørreundersøkelsen viser at det gjennomføres risikovurderinger i de fleste fagsystemene, og i langt større grad sammenlignet med Stavanger kommune.

Både sikkerhetsansvarlig og IT-sjef i Sandnes kommune peker på at kommunen bruker lite ressurser på arbeidet med informasjonssikkerhet. Spørreundersøkelsen avdekker også at de systemansvarlige i Sandnes kommune har for lite tid og ressurser til å utøve sine oppgaver som systemansvarlig. Sandnes har en desentralisert styringsmodell, jfr. digital strategi, der mye ansvar er delegert ut til virksomhetene. Det er også definert at IT-enheten i Sandnes ikke skal ha brukerkompetanse i det enkelte fagsystem, men gi brukerstøtte på et generelt nivå. Siden mye av ansvaret er delegert ned i organisasjonen er det viktig at de systemansvarlige har nok tid og ressurser til å utøve sine oppgaver for å sikre en forsvarlig informasjonssikkerhet.

Anbefaling:

- *Revisjonen anbefaler at kommunen sikrer at de systemansvarlige får tilstrekkelig tid og muligheter til å utøve sitt ansvar som systemansvarlig.*

Sandnes kommune har prosedyrer for informasjonssikkerhet. Ved større digitaliseringsprosjekter legges arkitekturprinsippene for digitalisering til grunn. Sikkerhetsprinsippene skal sikre at IT-løsninger blir etablert og driftet på en sikkerhetsmessig god måte. Konseptbeskrivelsen av oppvekst administrativt system følger arkitekturprinsippene, og digitaliseringssjefen i Sandnes kommune opplyser at konsekvenser og risikoer knyttet til løsningen vil bli analysert og dokumentert når kommunen har valgt leverandør.

Sandnes kommune bruker Compilo som kvalitets- og avvikssystem. Det er en systematisk gjennomgang av registrerte avvik på brudd på informasjonssikkerhet, både blant sikkerhetsansvarlig i kommunen, informasjonssikkerhetsforum og rådmannens ledergruppe.

Av avvikene som var meldt per oktober 2018 skyldes de fleste avvikene ansatte som ikke følger fastsatte prosedyrer.

IT-sjefen sier at de har blitt flinkere til å bruke Compilo for å melde tekniske feil, men at det i noen tilfeller ikke meldes men heller rapporteres direkte til rådmannens ledergruppe. IT bør rapportere alle feil i Compilo dersom kommunen ønsker å ha mulighet til å kunne ta ut en rapport som viser en fullstendig oversikt over avvik og tekniske feil som gjelder IT.

Kommunen har gjennomført egenkontroller av informasjonssikkerheten i enhetene i 2018. Det har ikke blitt gjennomført stedlig tilsyn, dette skyldes at det ikke har vært ressurser til både å gjennomføre kontroller og innføre GDPR til hele organisasjonen.

Den siste risikoanalysen som er gjennomført på bakgrunn av beredskapsplanen til IT viser behov for flere tiltak. IT-enheten har ikke hatt kapasitet til å utarbeide en plan for alle punktene som trenger oppfølging.

Anbefaling:

- *Revisjonen anbefaler at IT-enheten prioriterer å utarbeide en plan for oppfølging av risikoanalysen fra 2017/2018.*

ARKIVERING OG OFFENTLIGGJØRING

Arkivplanen til Sandnes kommune er blitt oppdatert etter tilsynsrapport fra Arkivverket. De systemansvarlige i Sandnes kommune har høy kunnskap om hva som regnes som arkivverdig materiale og mener praktiseringen av dokumentbehandling og arkivering i enhetene i stor grad er tilfredsstillende.

Arkivplanen er i mindre grad kjent blant de ansatte. Dette kan skyldes at arkivplanen ikke er et dokument, men består av en rekke dokumenter samlet i en portal på internett[52]. Undersøkelsen viser også at bare om lag halvparten er kjent med kommunens rutine for bruk og arkivering av e-post. E-post er et viktig kommunikasjonsmiddel i kommunen, og det er viktig at ansatte blir kjent med rutinen for arkivering av e-poster.

I Arkivverkets tilsynsrapport kom det fram at dokumentsenteret og IT-enheten ikke alltid involveres ved anskaffelser av nye systemer. I følge konstituert arkivsjef er det fokus på å sikre involvering. Også IT-sjef sier at dette er et fokus, og noe som presiseres i møter med enhetene. Opprettelsen av digitaliseringskontoret har bedret koordineringen av anskaffelser av de større digitaliseringsprosjektene.

Sandnes kommune har, etter pålegg fra Arkivverket, foretatt en ny gjennomgang av sine elektroniske systemer. Noe arbeid gjenstår og vil bli utført når nye Sandnes kommune bestemmer hvilke systemer den nye kommunen vil videreføre etter kommunesammenslåingen.

[52] Arkivplan.no

Informasjon om kommunens personvernombud finnes på kommunens hjemmeside. Rollen som personvernombud er tillagt kommunens forhandlingssjef som tidligere også hadde rollen som sikkerhetsansvarlig for den organisatoriske delen av informasjonssikkerhet i Sandnes kommune. Fra 2019 flyttes ansvaret for den organisatoriske delen av informasjonssikkerheten fra personvernombudet, og samles under området digitalisering og innovasjon. Dette fører til at det blir en sikkerhetsansvarlig i kommunen. Den tekniske delen av informasjonssikkerheten vil fortsatt utføres av IT.

Sandnes kommune har hatt stort fokus på innføringen av ny personvernforordning, og har kommet godt i gang med arbeidet med å registrere behandlinger i Draftit. Det gjenstår allikevel en kontroll av fullstendigheten av registreringene, både i forhold til tidligere behandlingsregister og skriftlige databehandleravtaler til behandlinger der det er påkrevd.

Anbefaling:

- *Revisjonen anbefaler at kommunen foretar en kontroll av registreringene i Draftit, både i forhold til hvilke systemer det er registrert behandlinger i forhold til og fullstendigheten i utfyllingen av skjemaene. Det må også kontrolleres at det foreligge nødvendige databehandleravtaler der det er påkrevd.*

Ansatte i Sandnes kommune kjenner i stor grad til lovbestemmelser som regulere hvilke dokumenter som skal unntas offentlighet. De er også i stor grad kjent med hvordan dokumenter unntas i Public 360. Kontrollen av offentlig journal avdekket ingen saker med sensitiv informasjon som ikke var unntatt offentlighet.

Kommunen har rutiner for innsyn, og det vurderes meroffentlighet dersom det bes om innsyn i et gradert dokument.

HACKING

Sandnes kommune har i liten grad implementert tekniske sikkerhetsløsninger som overvåker systemet, men benytter de innebygde løsningene som allerede finnes. IT-enheten gjennomfører heller ingen systematisk gjennomgang av logger i systemet, og kommunen bør vurdere å anskaffe et sikkerhetsovervåkingssystem.

Anbefaling:

- *Revisjonen anbefaler at kommunen vurdere om det er behov for et sikkerhetsovervåkingssystem som et proaktivt vern mot stadig mer avanserte og komplekse trusler og angrep.*

Det er systemeier som er ansvarlig for å etablere, endre og fjerne brukertilganger. I spørreundersøkelsen ble det undersøkt i hvor stor grad kommunen har rutiner og prosedyrer i forhold til brukertilganger til fagsystemet. Det er foretatt risikovurderinger i over halvparten av systemene, og de fleste systemene har rutiner for tildeling, sletting

og endring av tilgangene. Det er også rutiner for passord i de fleste systemene. Samtidig ble det kommentert under spørsmålet om mistanke om uønskede hendelser at ansatte har delt brukernavn og passord med ansatte som ikke har tilgang. Gjennomgang av registrerte avvik i 2018 avdekket også at det har vært flere tilfeller der ansatte har oppgitt brukernavn og passord til andre, som igjen har medført masseutsendelse av uønsket e-post fra kommunalt ansatte i Sandnes kommune. Passord og brukernavn på avveie vil kunne svekke både sikkerheten til kommunen og omdømme, og det bør derfor være et fokus i opplæringen av ansatte.

VEDLEGG

Om forvaltningsrevisjon

I kommunelovens § 77.4 pålegges kontrollutvalgene i fylkeskommunene og kommunene å påse at det gjennomføres forvaltningsrevisjon. Forvaltningsrevisjon innebærer systematiske vurderinger av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Lovens bestemmelser er nærmere utdypet i revisjonsforskriftens kapittel 3 og kontrollutvalgsforskriftens kapittel 5.

Revisjon i norsk offentlig sektor omfatter både regnskapsrevisjon og forvaltningsrevisjon, i motsetning til i privat sektor hvor kun regnskapsrevisjon (finansiell-) er obligatorisk.

Rogaland Revisjon IKS utfører forvaltningsrevisjon på oppdrag fra kontrollutvalget i kommunen. Arbeidet er gjennomført i henhold til NKRF sin standard for forvaltningsrevisjon, RSK 001. Les mer på www.rogaland-revisjon.no.

Prosjektleder for dette prosjektet har vært forvaltningsrevisor Linn Christin Rustøen og rapporten er kvalitetssikret av Ståle Opedal.

Revisjonskriterier

Revisjonskriteriene er krav eller forventninger som revisjonen bruker for å vurdere funnene i undersøkelsene. Revisjonskriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området, f.eks. lovverk og politiske vedtak. I dette prosjektet er følgende kriterier anvendt:

- Krav til informasjonssikkerhet i personopplysningsloven av 15. juni 2018 nr 38, og forskrift om behandling av personopplysninger av 15. juni 2018 nr 876.
- Datatilsynets veileder om internkontroll og informasjonssikkerhet. https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/
- Difis veileder om internkontroll i praksis – informasjonssikkerhet. https://internkontroll-infosikkerhet.difi.no/
- Lov om arkiv av 4. desember 1992 nr 126 og forskrift om offentleg arkiv av 15. desember 2017 nr 2105.
- For innsyn og offentliggjøring er lov om rett til innsyn i offentleg verksemd (offentleglova) av 19. mai 2006 nr 16 anvendt.
- Sandnes kommune sine egne planer og strategier, samt informasjon om informasjonssikkerhet til ansatte på kommunens intranettsider.

Informanter

Informantene har bidratt med informasjon muntlig i møter eller over telefon, eller skriftlig via e-post.

- Hilde Lofthus, kommunaldirektør for organisasjon
- Torunn S Nilsen, kommunaldirektør for økonomi
- Kari Ødegård Aas, IT-sjef
- Sigrun Homleid, forhandlingssjef og personvernombud
- Bjarte Våge, digitaliseringssjef
- Kjetil Lyse, rådgiver IT
- Rune Mangersnes, rådgiver organisasjon
- Bjarte Aanestad, konstituert virksomhetsleder dokumentsenteret

Vedlegg 1: Spørreundersøkelse

Sandnes kommune - informasjonssikkerhet, drift og sårbarhet

Spørreundersøkelsen er rettet mot systemansvarlige for fagsystemer i Sandnes kommune.

1) Hvilket tjenesteområde tilhører du?

- ○ Kultur og byutvikling
- ○ Levekår
- ○ Oppvekst barn og unge
- ○ Oppvekst skole
- ○ Teknisk
- ○ Organisasjon
- ○ Økonomi
- ○ Annet

2) Hvilken funksjon har du?

- ○ Leder/mellomleder
- ○ Medarbeider

3) Hvor mange fagsystemer er du systemansvarlig for?

- ○ 1
- ○ 2
- ○ 3
- ○ 4 eller flere
- ○ Jeg er ikke systemansvarlig

4) Som systemansvarlig for ett eller flere fagsystemer i Sandnes kommune:

	I liten grad 1	2	3	4	5	I stor grad 6
Har du fått tilstrekkelig opplæring i rollen som systemansvarlig?	○	○	○	○	○	○
Er du kjent med ditt ansvar og oppgaver som systemansvarlig?	○	○	○	○	○	○
Har du nok tid og ressurser til å utøve dine oppgaver som systemansvarlig?	○	○	○	○	○	○
Får du nødvendig støtte og bistand fra IT?	○	○	○	○	○	○

	I liten grad 1	2	3	4	5	I stor grad 6
Er du ansvarlig for opplæring av andre ansatte i fagsystemet du er systemansvarlig for?	○	○	○	○	○	○
Er opplæringen av nyansatte tilstrekkelig i fagsystemet du er systemansvarlig for?	○	○	○	○	○	○

5) Er det gjennomført risikovurdering i forhold til fagsystemet du er systemansvarlig for?

○ Ja
○ Nei
○ Vet ikke

6) I hvilken grad vil du si at risikovurderingen var tilstrekkelig?

○ 1 I liten grad ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 I stor grad ○ Vet ikke

Del 1: Informasjonssikkerhet

7)

8) Rutiner for informasjonssikkerhet

	I liten grad 1	2	3	4	5	I stor grad 6
Er du kjent med kommunes retningslinjer/prosedyrer for informasjonssikkerhet?	○	○	○	○	○	○
Er du kjent med kommunens sikkerhetsmål og -strategi?	○	○	○	○	○	○
Oppfatter du at rutiner for informasjonssikkerhet i kommune blir fulgt i det daglige?	○	○	○	○	○	○

9) Vet du hvor du finner retningslinjene for informasjonssikkerhet?

○ Ja
○ Nei

10) Hvor ofte søker du informasjon i retningslinjene for informasjonssikkerhet?

○ Daglig
○ Ukentlig
○ Sjeldnere
○ Aldri

11) Har det forekommet uønskede hendelser, avvik eller sikkerhetsbrudd det siste året i fagsystemet du er systemansvarlig for?

	Ja	Nei	Vet ikke
Uautorisert tilgang til kontorlokaler med arbeidsstasjoner og/eller skrivere?	○	○	○
Uautorisert bruk av fagsystemer?	○	○	○
Utilsiktet utlevering av personopplysninger?	○	○	○
Utilsiktet endring eller sletting av personopplysninger?	○	○	○
Tilfeller av virus eller tilsvarende trusler?	○	○	○
Elektroniske innbrudd eller forsøk på dette?	○	○	○
Driftsstans ansett som virksomhetskritisk?	○	○	○
Brudd på fastlagte prosedyrer eller rutiner?	○	○	○
Passord på avveie?	○	○	○

12) Har det vært mistanke om uønskede hendelser, avvik eller sikkerhetsbrudd det siste året?

○ Ja

○ Nei

13) Hvilke uønskede hendelser, avvik eller sikkerhetsbrudd har det vært mistanke om?

14) Brukertilganger og tilgangskontroll

	Ja	Nei	Vet ikke
Er det foretatt risikovurdering i forbindelse med brukertilganger til fagsystemet?	○	○	○
Er det etablert rutiner for tildeling av brukertilganger?	○	○	○
Er det etablert rutiner for sletting eller endring av brukertilgangene?	○	○	○
Er rutiner og prosedyrer for administrering og kontroll av brukertilganger i fagsystemet tilfredsstillende?	○	○	○
Er rutiner og prosedyrer for administrering av brukertilganger dokumentert?	○	○	○
Er det etablert skriftlige rutiner for bruk av fagsystemet?	○	○	○
Er rutiner for bruk av fagsystemet tilgjengelig for ansatte som bruker systemet?	○	○	○

	Ja	Nei	Vet ikke
Er det etablert rutiner for melding om uønskede hendelser, avvik eller sikkerhetsbrudd i fagsystemet?	○	○	○
Er det etablert rutiner for passordbruk?	○	○	○

15) Har du meldt avvik på brudd på informasjonssikkerheten i løpet av det siste året?

○ Ja
○ Nei

16) Ble avviket meldt i Compilo?

○ Ja
○ Nei
○ Annet

17) Ble håndteringen av avviket beskrevet og dokumentert?

○ Ja
○ Nei
○ Annet

18) Har du andre kommentarer angående informasjonssikkerhet?

Del 2: Behandling av personopplysninger og innsyn etter ny personopplysningslov (GDPR)

19)

20) Personvernforordning (GDPR)

	I liten grad 1	2	3	4	5	I stor grad 6
Har du fått tilstrekkelig opplæring i virksomhetens plikter og de registrertes rettigheter etter den nye personvernforordningen (GDPR)?	○	○	○	○	○	○
Vet du hvem som er personvernombud i Sandnes kommune?	○	○	○	○	○	○
Får du hjelp og veiledning av personvernombudet i kommunen dersom du har spørsmål som gjelder personopplysninger?	○	○	○	○	○	○

21) Har du registrert behandling av personopplysninger i Draftit?

☐Ja
☐Delvis
☐Nei
☐Ikke relevant

22) I hvilken grad sikrer de ansatte ved din enhet at kravene til behandling av personopplysninger blir ivaretatt?

○ 1 I liten grad ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 I stor grad

23) Innsyn i personopplysninger

	Ja	Nei	Vet ikke
Har det kommet innsynsbegjæring om personopplysninger i fagsystemet du er systemansvarlig for?	☐	☐	☐
Har dere rutiner for håndtering av innsyn, retting og sletting av personopplysninger?	☐	☐	☐

24) Hvordan vurderer du at innsynsbegjæringer blir håndtert i din enhet?

25) Har du andre kommentarer angående innsyn og personopplysninger?

Del 3: Arkivering og offentliggjøring

26)

27) I hvilke systemer arkiverer du dokumentene og sakene dine? Her er det mulig å sette flere kryss.

☐Public 360
☐Papirarkiver
☐Annet

28) Hvor ofte bruker du Public 360?

○ Daglig
○ Ukentlig
○ Sjeldnere

29) I hvilken grad

	I liten grad 1	2	3	4	5	I stor grad 6
Vet du hva som regnes som arkivverdig materiale?	☐	☐	☐	☐	☐	☐
Er rutiner for dokumentbehandling og arkivering kjent for de ansatte ved din enhet?	☐	☐	☐	☐	☐	☐
Er praktiseringen av dokumentbehandling og arkivering tilfredsstillende ved din enhet?	☐	☐	☐	☐	☐	☐
Kjenner du til innholdet i kommunens rutiner for arkivering (arkivplanen)?	☐	☐	☐	☐	☐	☐
Er du kjent med kommunens rutine for bruk og arkivering av e-post?	☐	☐	☐	☐	☐	☐

30) Vet du hvor du finner arkivplanen?

- ○ Ja
- ○ Nei

31) Hva mener du er årsaken til at praktiseringen av arkivrutinene ved din enhet ikke er tilfredsstillende?

32) I hvilken grad

	I liten grad 1	2	3	4	5	I stor grad 6
Kjenner du til lovbestemmelser som regulerer hvilke dokumenter som skal unntas offentlighet?	☐	☐	☐	☐	☐	☐
Vet du hvordan du unntar et dokument fra offentlighet i Public 360?	☐	☐	☐	☐	☐	☐
Er det enkelt for deg som bruker av Public 360 å unnta dokumenter fra offentlighet?	☐	☐	☐	☐	☐	☐

33) Hva er årsaken til at du ikke vet hvordan du unntar et dokument fra offentlighet i Public 360?

34) Hva er årsaken til at det er vanskelig for deg som bruker av Public 360 å unnta dokumenter fra offentligheten?

35) Har du andre kommentarer angående arkivering og offentliggjøring?

Rogaland Revisjon IKS

Regnskapsrevisjon **Forvaltningsrevisjon** **Selskapskontroll** **Andre tjenester**

Rogaland Revisjon IKS

Lagårdsveien 78
4010 Stavanger

Tlf 40 00 52 00
Faks 51 84 47 99

www.rogaland-revisjon.no