Rogaland Revisjon IKS

FORVALTNINGSREVISJON AV

INFORMASJONSSIKKERHET, DRIFT OG SÅRBARHET

STAVANGER KOMMUNE

FEBRUAR 2019

Forsidefoto: pexels.com

INNHOLD

SAMMENDRAG

BAKGRUNN OG FORMÅL

Prosjektets formål er å vurdere kommunens organisatoriske tiltak for informasjonssikkerhet, og er 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.

Stavanger kommune har et styringssystem for informasjonssikkerhet som omfatter en overordnet retningsgivende digitaliseringsstrategi, en IKT-strategi, håndbok for HMS/internkontroll, samt et internkontrollsystem med prosedyrer på intranett. Vi har i prosjektet vurdert Stavanger kommunes systemer og rutiner opp mot blant annet kravene i personopplysningsloven, personvernforordningen og veileder om internkontroll og informasjonssikkerhet fra Datatilsynet.

HOVEDINNTRYKK

Hovedinntrykket er at Stavanger kommune i stor grad har systemer og prosedyrer som ivaretar informasjonssikkerheten. Det er også flere tekniske løsninger som er implementert/skal implementeres som vil overvåke systemet og varsle om mulige trusler.

I Stavanger kommune er kommunalstyret for administrasjon kommunens IKT-utvalg. Dette sikrer at politikerne involveres i planer og retningslinjer for bruk av informasjonsteknologi. I kommunalstyret for administrasjon tas det også opp saker som omhandler brudd på informasjonssikkerhet, blant annet ble mediasaken angående sikkerhetsbrudd i renovasjonsappen behandlet i møte den 20.11.2018.

Det kommer fram i intervjuer at flere av kommunens egne rutiner for årlige gjennomganger og revisjoner ikke blir overholdt. Dette betyr ikke at informasjonen ikke er gyldig, men det gir en risiko for at kommunen ikke fanger opp viktige endringer i sine mål og strategier.

SYSTEMER OG RUTINER FOR Å IVARETA INFORMASJONSSIKKERHET

En av problemstillingene for prosjektet var å undersøke hvilke systemer og rutiner Stavanger kommune har for å ivareta krav om informasjonssikkerhet, og i hvilken grad kommunen etterlever kravene.

Sikkerhetsansvarlig i Stavanger kommune har i lengre tid arbeidet med en full revidering av informasjonen som ligger på intranettportalen. Målet er å få en lett tilgjengelig håndbok for informasjonssikkerhet. På grunn av arbeidet med ny håndbok har det ikke blitt prioritert å foreta en systematisk gjennomgang av sikkerhetsmål og -strategier fra

ledelsens side. Stavanger kommune har nå ansatt en ny sikkerhetsansvarlig i 100 prosent stilling. Dette gir økte ressurser, og direktør for støtte og utvikling sier at arbeidet med oppdatering av håndbok for informasjonssikkerhet vil bli prioritert.

Spørreundersøkelsen viser at de systemansvarlige i Stavanger kommune i stor grad er kjent med kommunens retningslinjer og prosedyrer, og at disse blir fulgt i det daglige.

Katastrofeplanen for IKT er fra 2015, og har ikke blitt revidert. Dette på tross av at det i planen står at den skal revideres årlig, samt at det skal gjennomføres årlige katastrofeøvelser. Siste beredskapsøvelsen IT var involvert i var fra februar 2017. Det er avdelingen selv som må stå for planlegging og gjennomføring av beredskapsøvelser innenfor eget ansvarsområde.

Stavanger kommune bruker i dag Synergi for registrering og behandling av avvik. Revisjonen avdekket at rutinen som er satt for avviksbehandling ikke følges. Avvik som omhandler brudd på informasjonssikkerhet blir ikke sendt som kopi til IT-sjef og sikkerhetsansvarlig i henhold til rutinen. Synergi er på vei til å fases ut, og revisjonen anbefaler at Stavanger kommune går nøye igjennom sine rutiner for avviksbehandling ved innføring av nytt avvikssystem.

ARKIVERING OG OFFENTLIGGJØRING

I prosjektet har det blitt undersøkt om krav til arkivering og offentliggjøring blir ivaretatt, og om de ansatte har kjennskap til regelverket.

Rogaland Revisjon gjennomførte en revisjon av kommunens arkiv i 2016. Denne rapporten viser til oppfølgingen av forvaltningsrevisjonsrapporten fra 2016. Spørreundersøkelsen viser at rutiner for dokumentbehandling og arkivering er godt kjent blant de systemansvarlige i kommunen. I forhold til tilsvarende spørsmål fra 2016 har antall respondenter som svarte 4 eller bedre (skala 1-6) økt med 20 prosentpoeng. Dette indikerer at kommunen har lykkes med sin oppfølging av rapporten fra 2016 der det blant annet ble iverksatt tiltak for å styrke arkivfunksjonen og bevisstheten om denne, sikre at arkivlovens bestemmelser blir etterlevd og styrke de ansattes kompetanse på arkivområdet.

Arkivplanen er i mindre grad kjent blant de systemansvarlige i kommunen. Arkivplanen ligger tilgjengelig på kommunens intranettside og består av mange enkeltdokumenter. I gjennomgangen av innledningen til arkivplanen (fra 2016) er det henvist til den tidligere arkivforskriften. I følge kommunens egne retningslinjer skal endringer i lover og forskrifter som har betydning for arkivarbeidet være grunnlag for oppdatering av arkivplanen.

Fra 2018 inkluderer personopplysningsloven EUs personvernforordning som gir offentlige virksomheter ytterligere plikter i forhold til behandling av personopplys-

ninger. Stavanger kommune har anskaffet en elektronisk løsning for registrering av behandlinger. Revisjonens gjennomgang av registreringer i Draftit, sammenlignet med tidligere registreringer over behandlinger som krevde konsesjon og meldeplikt, viser at det er flere mangler i hvilke behandlinger som er registrert. Personvernombudet i Stavanger kommune har ikke foretatt kontroller av fullstendigheten i registreringene. Alle registrerte behandlinger har status til gjennomgang, og det har ikke blitt angitt en overordnet vurdering av risiko i den elektroniske løsningen.

RISIKO FOR HACKING

Kontrollutvalget vedtok at revisjonsrapporten også skulle undersøke risikoen for hacking. Det er vanskelig å forutse hvilke former for dataangrep kommunen kan bli rammet av, og hvor utsatt kommunen er for hacking. Det viktigste verne for informasjonssikkerheten er tekniske løsninger som kan varsle om uregelmessig bruk av IT-systemet, samt prosedyrer.

I tillegg understreker sikkerhetsansvarlig at den største trusselen mot informasjonssikkerhet i Stavanger kommune er at ansatte ikke følger fastsatte prosedyrer. Dette nevnes også i den foreløpige risikoanalysen til Public Oppvekst. Opplæring og informasjon ut til de ansatte er derfor et viktig virkemiddel for å øke informasjonssikkerheten i kommunen.

I høst har Stavanger kommune hatt en e-post-kampanje ut til alle ansatte. Svarprosenten på kampanjen er noe lav (37 prosent), men svarene tyder på at de ansatte som har gjennomført kampanjen har blitt mer oppmerksomme på ulike former for IT-trusler.

ANBEFALINGER

Revisjonen anbefaler at Stavanger kommune:

- Prioriterer en full gjennomgang av rutiner og prosedyrer for informasjonssikkerhet som ligger på intranett.
- Reviderer katastrofeplanen for IKT årlig, og gjennomfører årlige katastrofeøvelser basert på katastrofeplanen.
- Gjennomgår sine rutiner for avviksbehandling ved innføring av nytt avvikssystem for å sikre at IT-sjef og sikkerhetsansvarlig er informert om hvilke avvik som meldes i forhold til brudd på informasjonssikkerhet. Gjennomgang av avvik bør være en del av den årlige gjennomgangen av sikkerhetsmål og -strategi.
- Går igjennom og oppdaterer arkivplanen slik at den er i henhold til dagens forskrift.
- Kontrollerer at registreringer av behandlinger av personopplysninger i Draftit er fullstendig. Behandlingene bør også gis en overordnet risikovurdering og status.

RÅDMANNENS KOMMENTAR

Rådmannen tar funn og anbefalinger til etterretning og vil iverksette de nødvendige tiltak i organisasjonen for å utbedre informasjonssikkerheten. Det er flere områder rådmannen vil følge konkret opp med tiltak og her kan blant annet nevnes revidering av katastrofeplan, innføring av nytt avviksbehandlingssystem (TQM), vurderer alternativ verktøy for protokoll over behandlingsaktiviteter og oppfølging av taushetserklæring og sikkerhetsregler.

Bystyret vedtok ibm HØP 2019-2022 å styrke sikkerhetssiden i kommunen. IT-avdelingen vil derfor fra 1. april 2019 få en ytterligere ressurs innen sikkerhet. Personvernombudsrollen vil overføres fra Støtte og utvikling v/IT-avdelingen til Strategi og styring. Bystyret vedtok også budsjettmidler til en ekstern gjennomgang av kommunens infrastruktur og arkitektur i et sikkerhetsperspektiv. En ekstern sikkerhetsgjennomgang av IKT-løsninger vil gi kommunen trygghet i at våre løsninger er tilstrekkelig organisatorisk og teknisk sikret - vi vil eventuelt få forslag til prosessendringer og forbedringstiltak.

Med hilsen

Per Kristian Vareide
rådmann

Kjersti Lothe Dahl
direktør støtte og utvikling

Roy Håland
saksbehandler

Vedlegg

Kopi til:

Dokumentet er elektronisk godkjent og sendes uten signatur

RAPPORTEN

1 INNLEDNING

1.1 FORMÅL OG PROBLEMSTILLINGER

Kontrollutvalget i Stavanger bestilte 19.09.2017 en forvaltningsrevisjon av IT-sikkerhet.

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 21.11.2017 ble følgende tillegg vedtatt:

- Hvor stor er risikoen for hacking?

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[1]
- Difi's veileder for internkontroll i praksis - informasjonssikkerhet[2]
- 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.

Metodisk er det benyttet intervju med sikkerhetsansvarlig i Stavanger kommune, IT-sjef og rådgiver på IT. Vi har også gjennomgått en rekke dokumenter fra Stavanger

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

kommune som strategier, politiske saker, arkivplan og prosedyrer 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 Stavanger kommune (95 respondenter). Undersøkelsen fikk en svarprosent på 52 prosent. Spørsmålene i undersøkelsen ligger i vedlegg 1. Revisjonen har også fått tilgang til svarene fra Stavanger kommune sin e-post-kampanje som ble gjennomført høsten 2018.

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 3, 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[3] 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[4] eller databehandleren, samt til de ansatte som utfører behandlingen av personopplysninger[5]. Kontaktopplysninger til personvernombudet skal registreres hos Datatilsynet via Altinn.

[3] Jfr. Datatilsynets veileder om behandlingsgrunnlag.
[4] Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
[5] 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 offentlege 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 KATASTROFEPLAN IKT FOR STAVANGER KOMMUNE

I henhold til Stavanger kommune sin katastrofeplan for IKT skal planen revideres årlig, under ledelse av sikkerhetsansvarlig og godkjennes i IT ledergruppen. Det skal også etableres rutiner for katastrofeøvelse basert på katastrofeplanen, og øvelse skal gjennomføres årlig hver høst.

2.1.5 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[6]:

- **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.

[6] Jfr. Politiet

2.1.6 REVISJONSKRITERIER

Ut fra gjennomgangen over er følgende revisjonskriterier lagt til grunn for å løse 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.
- Kommunen skal ha personvernombud.
- Akseptabelt risikonivå for sikkerhet skal dokumenteres.
- Kommunen skal foreta risikovurderinger og iverksette nødvendige sikkerhetstiltak.
- Det skal utarbeides prosedyrer for informasjonssikkerhet.
- Katastrofeplanen skal revideres årlig, og det skal gjennomføres årlige beredskapsøvelser.
- 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.
- 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.

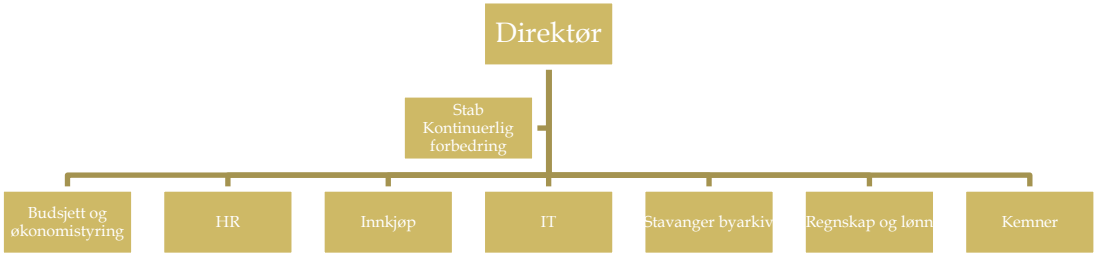
3.1 ORGANISERING, ROLLER OG REGELVERK

Dette kapittelet beskriver Stavanger 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 STAVANGER KOMMUNE

IT er i Stavanger kommune organisert under direktør for støtte og utvikling.

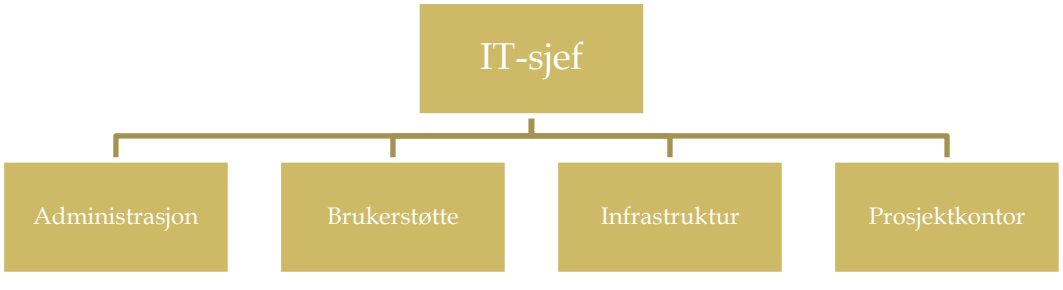
Figur 1 - Organisasjonskart for støtte og utvikling i Stavanger kommune. Kilde: Stavanger kommune.



IT drifter Stavanger kommune, Finnøy kommune, Forsand kommune og Rennesøy kommune, i alt over 9 000 PCer på administrasjonsnettet og over 6 000 PCer på undervisningsnettet. IT drifter også trådløst publikumsnett.

IT avdelingen består for tiden av 38 fast ansatte knyttet til brukerstøtte, infrastruktur- og systemdrift samt prosjekt, systemutvikling og administrasjon. 6 lærlinger i IKT-servicefag er også knyttet til IT.

Figur 2 - Organisasjonskart for IT i Stavanger kommune. Kilde: Stavanger kommune.



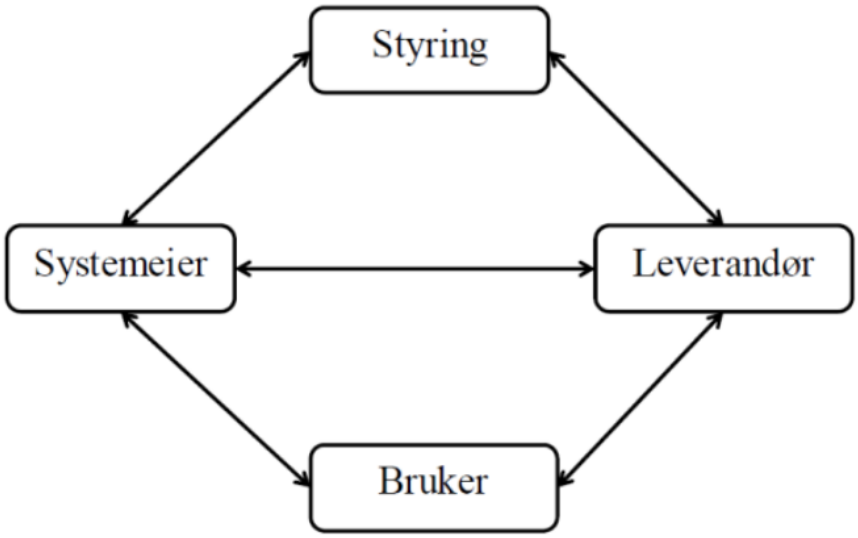
IT har følgende hovedoppgaver:

- Rådgivning til kommunenes ledelse og fagavdelinger i IT-relaterte spørsmål, samt styring/deltakelse i prosesser og IKT-prosjekter.
- Drift og videreutvikling av infrastruktur, IT-systemer og telefoniløsninger.
- Brukerstøtte og opplæring på IT-området for kommunens ansatte.
- Systemutvikling, tilrettelegging og rapportering for å optimalisere nytteverdien av IT-investeringer.
- IKT-sikkerhet og personvern.

3.1.2 Styringsmodell for IKT og rollebeskrivelser

Stavanger kommune har følgende overordnet styringsmodell for IKT:

Figur 3 – Overordnet styringsmodell for IKT i Stavanger kommune. Kilde: Stavanger kommune.



IKT-strategien for Stavanger kommune ble vedtatt i kommunalstyret for administrasjon 22.05.2018 i sak 16/18. Kommunalstyret for administrasjon er kommunens IKT-utvalg.

Rådmannen følger opp IKT-strategien og prioriterer utviklings- og driftstiltak gjennom handlingsplaner. Større satsninger innarbeides i handlings- og økonomiplan.

Det er etablert et rådgivende IKT-forum med representasjon fra systemeiere og IT-avdeling. IKT-forumet møtes tre ganger i året for å vurdere oppfølging av IKT-strategi og handlingsplaner.

STYRINGSROLLEN

Ivaretakelse av personvern og informasjonssikkerhet må, i følge rollebeskrivelsene til Stavanger kommune, sikres forankring i styringsrollen. Dette ivaretas gjennom en egen styringsgruppe for informasjonssikkerhet. Gruppen ledes av direktør for strategi og styring, og består av representanter fra de store tjenesteområdene. Styringsgruppen kan fatte vedtak i saker som angår informasjonssikkerhet.

SYSTEMEIER

Alle fagsystem skal ha en systemeier. Systemeier er den som har totalansvaret for det tjenesteområdet som systemet skal betjene. Systemeier tar normalt strategiske beslutninger og legger føringer for området.

Systemeier har:

- Overordnet juridisk og økonomisk ansvar for fagsystemet.
- Ansvar for driftsavtaler med IT eller eksterne leverandører.
- Sikkerhetsmessig ansvar for fagsystem, tilgangsstyring og data.
- Eieransvar i utviklings– og oppgraderingsprosjekt.
- Lederansvar i styringsgruppe i større utviklings– og oppgraderingsprosjekt.
- Ansvar for å utnevne systemansvarlig.
- Ansvar for å vurdere behov for opprettelse av brukerforum.

SYSTEMANSVARLIG

Systemansvarlig representerer brukersiden i organisasjonen og utpekes av systemeier. Vedkommende har på vegne av systemeieren det daglige og løpende ansvaret for fagsystemets «ve og vel».

Systemansvarlig har:

- Ansvar for å være kontaktperson mot leverandør av fagsystem og kontaktledd mellom IT og leverandør.
- Ansvar for å være kontaktledd mellom IT og brukersiden.
- Kjennskap til reglene for informasjonssikkerhet og har ansvar for oppfølging av lover og regler relatert til fagsystemet.
- Kjennskap til IT sine intranett sider og skal følge med på ITs driftsmeldinger.
- Solid kompetanse om fagsystemet.
- Ansvar for å gi opplæring og veiledning i bruk av fagsystemet.
- Rutiner knyttet til bruk av fagsystemet.
- Ansvar for å etablere og lede brukerforum med regelmessige møter. Det er systemeier som vurderer om det er behov for brukerforum.
- Dokumentert oversikt over integrasjoner til andre fagsystem og kontorstøttesystemer (for eksempel maler i Word).
- Ansvar for å ta imot ønsker/forslag til forbedringer fra brukerne av fagsystemet.

- Evne til å vurdere nødvendighet for oppgraderinger/forbedringer eventuelt nytt fagsystem.
- Ansvar for å holde seg oppdatert om teknologisk utvikling i markedet (med tanke på nye moduler og eventuelt fremtidig skifte av system).
- Ansvar for å melde endringer (oppgraderinger/forbedringer) i fagsystem til IT. Endringene skal meldes i god tid via IT Selvbetjening slik at IT kan gjennomføre endringene på en sikker og god måte i henhold til ITIL rammeverk[7].
- Hvis nødvendig plass sammen med IT i et endringsråd (CAB) ved endringer med høy risiko og kostnad.
- Ansvar for å melde og følge opp feil meldt til IT eller leverandør.
- Ansvar for å utarbeide testplaner og gjennomføre testing i forbindelse med endringer.
- Ansvar for å melde fra om nedetid, planlagt eller ved feilsituasjoner, til IT og brukersiden.
- Ved driftsproblem, som har innvirkning på fagsystem, ansvar for å videreformidle problemet til brukersiden.
- Ansvar for å administrere brukertilgang og tilgang til filområder.
- Kontroll på antall lisenser i henhold til avtale med leverandør.
- Sørget for at det finnes stedfortreder ved lengre fravær. Holde IT informert om navn på stedfortreder, også dersom systemansvarlig slutter i kommunen.

DRIFTSLEVERANDØR

IT-avdelingen skal være førstevalg som leverandør av driftstjenester for Stavanger kommune. Eksterne leverandører benyttes for sky- og ASP-løsninger.

Driftsleverandør har:

- Ansvar for at drifts- og forvaltningstjenester samsvarer med servicenivåavtalen (SLA).
- Ansvar for at infrastrukturens sikkerhetsmekanismer er implementert og fungerer i henhold til avklart sikkerhetsnivå.
- Koordinatoransvar for sentrale driftsoppgaver for å sikre effektiv økonomisk og stabil drift.
- Ansvar for rammeverk for drift og service innen IT-organisasjoner.
- Ansvar for å overvåke, påpeke og korrigere svakheter i systemløsninger.
- En rådgiverrolle overfor fagavdelinger og virksomheter i IKT-relaterte saker.

[7] Information Technology Infrastructure Library (ITIL) er et strukturert rammeverk for kvalitetssikring av leveranse, drift og support innen IKT-sektoren. Rammeverket brukes stadig mer også for andre tjenesteleveranser enn IKT. Jfr. Stavanger kommune sin IKT-strategi 2018-2021.

BRUKER

Alle som bruker IKT som et verktøy for å utføre nødvendige arbeidsoppgaver for kommunens innbyggere er brukere. Brukerne kan være representert i ulike brukerforum og kan komme med innspill og påvirke kommunens løsninger.

Bruker har:

- Ansvar for å benytte systemene i henhold til hensikt og formål, samt være med å definere arbeidsrutiner og retningslinjer for systemanvendelse og brukerstøtte.
- Ansvar for å melde feil eller brudd på serviceavtaler.
- Ansvar for å identifisere behov for forbedringer og melde dette til systemansvarlig.
- Tilstrekkelig kompetanse på alle system som skal benyttes.
- Ansvar for å etterleve lover, regler og lokale bestemmelser.

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, jfr. kapittel 2:

- Kommunen skal ha styringssystem for informasjonssikkerhet.

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

DIGITALISERINGSSTRATEGI 2014-2029 FOR STAVANGER KOMMUNE

Et av innsatsområdene i digitaliseringsstrategien er personvern og informasjonssikkerhet. Stavanger ønsker åpenhet og dialog internt og mellom kommunen og innbyggere/næringsliv. God informasjonssikkerhet og god internkontroll vil sikre at kommunen behandler personopplysninger lovlig, sikkert og forsvarlig.

Strategier:

- Vi jobber aktivt for åpenhet, samtidig som vi ivaretar personvern, taushetsplikt, informasjonssikkerhet.
- Vi gjennomfører grundige risiko- og sårbarhetsanalyser når nye tjenester tas i bruk.
- Vi har løsninger for sikker pålogging for innbyggere og næringsliv. Alle brukere av våre digitale løsninger skal være trygge på at opplysninger behandles forsvarlig.
- Vi har etablert internkontrollrutiner og gjennomfører selvpålagte revisjoner.

Digitaliseringsstrategien er et overordnet retningsgivende styringsdokument for hele kommunen. Stavanger kommunes styringsmodell gjelder for digitaliseringsarbeidet, og rollene tydeliggjøres og konkretiseres ytterligere i kommunens operative IKT-strategi.

Kommunalstyret for administrasjon er kommunens IKT-utvalg og skal vedta planer og retningslinjer for bruk av informasjonsteknologi. Rådmannen har ansvaret for å utvikle og gjennomføre strategien. Personvern og informasjonssikkerhet ivaretas gjennom en egen administrativ styringsgruppe for informasjonssikkerhet.

Hvert enkelt fagområde har ansvar for å se, ta i bruk og aktivt bidra i utviklingen av de muligheter som ligger i digitalisering innenfor eget tjenesteområde. IT-avdelingen har ansvar for å videreutvikle den tekniske infrastrukturen som grunnlag for videre digitalisering. De har også ansvar for utarbeidelse og oppfølging av IKT-strategien.

IKT-STRATEGI 2018-2021 FOR STAVANGER KOMMUNE

IKT-strategien for Stavanger kommune 2018-2021 ble vedtatt i kommunalstyret for administrasjon 22.05.2018 i sak 16/18. Strategien skal gi styringssignaler og retning for utvikling av IKT-løsningene i kommunen. IKT-strategien bygger opp under målene i digitaliseringsstrategien (2014-2029). Digitaliseringsstrategien henviser til IKT-strategien for konkretisering av rollene i styringsmodellen til kommunen. I revidering av IKT-strategien i 2018 ble det valgt å ta beskrivelsen av roller ut av strategien. Beskrivelsen av rollene er i stedet lagt tilgjengelig på intranettsiden til Stavanger kommune. Sammenhengen mellom digitaliseringsstrategien og IKT-strategien er illustrert i figuren under.

Figur 4 – «Det digitale huset» viser sammenhengen mellom IKT-strategien, delstrategier og digitaliseringsstrategien. Kilde: IKT-strategi 2018-2021 Stavanger kommune.

Målet for IKT-strategien er **«Gode og effektive tjenester for alle»**.

Stavanger kommunes IKT-arbeid skal preges av følgende:

- Åpenhet og transparens
- Smartere sammen
- Helhetlig arkitektur
- Integrerte løsninger
- Bærekraft og ny teknologi

Det er i planperioden valgt ut fire aktuelle innsatsområder:

1. Brukerorienterte tjenester
2. Prosess, kvalitet og kompetanse
3. Data og arkitektur
4. Personvern og informasjonssikkerhet

For forvaltningsrevisjonen av informasjonssikkerhet, drift og sårbarhet er innsatsområdene 3 og 4 mest aktuelle.

Innsatsområde 3: Data og arkitektur

- Sikre en god forvaltning av data.
- Sikre god håndtering av arkivverdig materiale.
- Legge til rette for enhetlig håndtering av masterdata.
- Integrere fagsystemer så langt det er mulig og fornuftig.
- Benytte standardiserte produkter, offentlige standarder og nasjonale felleskomponenter.
- Støtte opp om et sikkert «internett for alt» (Internet of Things, IoT).
- Videreutvikling av fremtidsrettet datasenter og driftsmodell.
- Ta i bruk ny teknologi.
- Benytte og vedlikeholde gode lokale, nasjonale og internasjonale nettverk for samarbeid og erfaringsutveksling.

Innsatsområde 4: Personvern og informasjonssikkerhet

- Ivareta informasjonssikkerheten og personvern fra start til slutt.
- Legge til rette for å gi innbyggeren innsyn og kontroll over egne data.
- Understøtte sikre tjenester for elektronisk kommunikasjon med innbyggerne.
- Sørge for rett sikkerhetsnivå og oppdaterte sikkerhetsrutiner.
- Gjennomføre organisatoriske tiltak for å ivareta personvern og informasjonssikkerhet.
- Bevisstgjøre og gi opplæring.
- Sikre moderne og effektive løsninger.

INTERNKONTROLLSYSTEM FOR INFORMASJONSSIKKERHET

Stavanger kommune har en overordnet administrativ styringsmodell som beskriver viktige styringsprinsipper og -verktøy. Under planer og strategier på intranett ligger håndbok for HMS/internkontroll som en del av det interne regelverket til kommunen, samt retningslinjer for informasjonssikkerhet i Stavanger kommune.

I tillegg er det etablert en egen portal på intranett knyttet til informasjonssikkerhet. Denne omfatter både strategier, overordnede prosedyrer, beskrivelse av organisering og ansvar og ulike tekniske prosedyrer knyttet til informasjonssikkerhet.

Systemansvarlige i Stavanger kommune svarer i spørreundersøkelsen at de er kjent med kommunens retningslinjer og prosedyrer[8], men at de sjelden søker informasjon i retningslinjene[9]. De fleste systemansvarlige svarer også at rutiner for informasjonssikkerhet blir fulgt i det daglige[10].

Informasjonssikkerhetsarbeidet styres av en styringsgruppe for informasjonssikkerhet som ledes av direktør for strategi og styring. Gruppen består av representanter for de store tjenesteområdene i Stavanger kommune. Styringsgruppen kan fatte vedtak i saker som angår informasjonssikkerhet. Revisjonen har mottatt møtereferat fra styringsgruppen for 2018. Det er kun avholdt et møte i 2018, og styringsgruppen har ikke sett behov for å avholde flere møter.

Internkontroll er strategier som inngår både i digitaliseringsstrategien og IKT-strategien til Stavanger kommune for å sikre at kommunen behandler personopplysninger lovlig, sikkert og forsvarlig. Stavanger kommune hadde i 2015 en forvaltningsrevisjon av internkontroll. En av anbefalingene til kommunen var å etablere tydelige føringer for hvordan internkontrollen skal integreres i den overordnede administrative styringsmodellen, og informasjon om hva som inngår i internkontrollarbeidet og hvilket ansvar ledere på ulike nivå har for internkontroll.

I løpet av 2017 har Stavanger kommune hatt et prosjekt *«Videreutvikling av system for sektorovergripende internkontroll»* som vil, sammen med tidligere gjennomførte tiltak, styrke rådmannens internkontroll og følge opp anbefalingene fra forvaltningsrevisjonsrapporten «*Internkontroll*». Prosjektet ble lagt fram for bystyret 15.01.2018, sak 6/18, og oppfølgingen av forvaltningsrevisjonsrapporten «*Internkontroll*» ble tatt til orientering. De mest sentrale oppgavene i tilknytning til iverksetting av anbefalte tiltak fra prosjektrapporten er å justere den administrative styringsmodellen ved å gjøre det tydeligere at internkontroll inngår i leders ansvar.

Stavanger kommune har anskaffet et nytt avviks-, varslings- og forbedringssystem. Etter planen vil implementeringen av systemet starte i begynnelsen av 2019. Systemet vil gi en helhetlig tilnærming til virksomhetsstyring og skal gi bedre risikostyring og internkontroll for ledere på alle nivå. Regelverk og prosessbeskrivelser for utøvelse av virksomhetsstyring og internkontroll i Stavanger kommune er under utarbeidelse, jfr. handlings- og økonomiplanen 2019-2022.

KATASTROFEPLAN IKT FOR STAVANGER KOMMUNE

Katastrofeplan IKT er fra 15.12.2015. Planen beskriver roller og ansvar hvis det oppstår en katastrofesituasjon for Stavanger kommune sine IKT-løsninger. Definisjonen av en

[8] 79 prosent svarte alternativ 4-6. N=48.
[9] 90 prosent svarte sjelden eller aldri. N=48.
[10] 70 prosent svarte alternativ 4-6. N=46.

katastrofesituasjon innen IKT er: «*Hele eller deler av IT infrastruktur, nettverksløsninger, eller sentrale IT-systemer er satt ut av drift. Kritikaliteten er avhengig av tidspunkt og varighet på hendelsen.*»

Katastrofeplanen skal revideres årlig, under ledelse av sikkerhetsansvarlig og godkjennes i IT ledergruppen, jfr. katastrofeplan IKT. Det skal også etableres rutiner for katastrofeøvelse basert på katastrofeplanen, og øvelse skal gjennomføres årlig hver høst.

PUBLIC OPPVEKST

I løpet av senhøsten 2018 og våren 2019 skal all ny elev-, barne- og PPT-dokumentasjon være digital. Per i dag oppbevares elev- og barnemapper i hovedsak på papir og minnebrikker. Public Oppvekst skal også sørge for at dokumentasjon kan brukes på tvers av skoler, barnehager, PPT og aktuelle fagavdelinger.

Prosjektet er en del av Stavanger kommunes digitale strategi som slår fast at Stavanger kommune skal gi innbyggerne og næringsliv et reelt digitalt førstevalg og at digitale verktøy skal bidra til høyere produktivitet og mer effektiv ressursbruk.

All rettighetsdokumentasjon tilknyttet alle barn i barnehage og grunnskole vil arkiveres i Public Oppvekst. Alle saker og dokumenter knyttes til barnets personnummer. Dette gjør det enkelt å gjenfinne dokumentasjon og håndtere framtidige innsyn i for eksempel elevmapper, karakterer og vitnemål raskt og effektivt.

Databasen til Public Oppvekst skal ligge i sikker sone. Brukere vil måtte logge seg på med to-faktor pålogging for å få tilgang til systemet. Deretter må de være opprettet som brukere i Public Oppvekst og de må være medlem av tilgangsgrupper for å få tilgang til saker og dokumenter som omhandler barnet eller eleven.

En risikoanalyse av Public Oppvekst er under utarbeidelse, men er ikke ferdigstilt siden systemet fortsatt utvikles og testes. Den foreløpige oppsummeringen viser at de største truslene mot at dokumentasjon på barn og elever blir lagret trygt i sikker sone er at rutiner ikke blir fulgt. Det står også at hvis det er gjentatte brudd på rutiner må tiltak som sanksjoner mot ansatte vurderes. Videre skal krav om sikker arkivering prioriteres foran effektivitetshensynet.

3.3 INFORMASJONSSIKKERHET I STAVANGER KOMMUNE

Dette kapitlet fokuserer på følgende problemstilling:

I hvilken grad etterlever kommunen kravene til informasjonssikkerhet?

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

- 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.
- Kommunen skal ha personvernombud.
- Akseptabelt risikonivå for sikkerhet skal dokumenteres.
- Kommunen skal foreta risikovurderinger og iverksette nødvendige sikkerhetstiltak.
- Det skal utarbeides prosedyrer for informasjonssikkerhet.
- Katastrofeplanen skal revideres årlig, og det skal gjennomføres årlige beredskapsøvelser.
- 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 evne 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 Stavanger 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 3.1 og 3.2).

3.3.1 MÅL OG STRATEGIER FOR INFORMASJONSSIKKERHET

I portalen for informasjonssikkerhet finner vi Stavanger kommunes sikkerhetsmål: *«Kommunen skal gjennom godkjent sikkerhetssystem muliggjøre samhandling og tilgang til informasjon mellom ulike deler av kommunen samt mellom kommunen og omverdenen. Sikkerhetssystemet skal tilrettelegge for effektiv informasjonstilgang for politikere og publikum.»*

Sikkerhetsstrategien skal definere hvilke tiltak på et overordnet plan som skal gjennomføres for å nå det definerte sikkerhetsmålet. Strategien sier blant annet at *«Det skal opprettholdes tilstrekkelig sikkerhet sett opp mot overordnede målsetting om å være en åpen og kommuniserende virksomhet.»*

Informasjonssikkerhetsleder har ansvaret for organisering, forberedelse og gjennomføring av ledelsens årlige gjennomgang. Hensikten med gjennomgangen er å kontrollere og revidere at sikkerhetsmål, -strategier og organisering av informasjonssikkerheten er i overensstemmelse med de til enhver tid gjeldende krav og behov. Avdelingens sikkerhetsansvarlige skal sammen med informasjonssikkerhetsleder identifisere tiltak gjennom innrapporterte avvik.

Spørsmålet i spørreundersøkelsen om kommunens sikkerhetsmål og -strategi var kjent fikk en score på 3,9 (der 6 var godt kjent). Det er færre som svarer at de kjenner til sikkerhetsmål og -strategi, enn de kjenner til retningslinjer/prosedyrer for informasjonssikkerhet (score 4,5).

I intervju med IT-sjef og sikkerhetsansvarlig kom det fram at kommunen ikke har gjennomført en årlig systematisk gjennomgang av kommunens sikkerhetsmål og -strategi. Årsaken skal være at kommunen i lenger tid har planlagt en full revidering av rutiner og prosedyrer for informasjonssikkerhet.

3.3.2 ORGANISERING OG ANSVAR FOR INFORMASJONSSIKKERHETEN

I overordnet sikkerhetsbestemmelse til Stavanger kommune finner vi disse roller og ansvar:

Rådmannen har overordnet ansvar for at kommunen vurderer sine sikkerhetsbehov og gjennomfører nødvendige sikringstiltak, og skal legge til rette slik at alle ledere kan ivareta sitt sikkerhetsansvar, og at medarbeidere får den nødvendige sikkerhetsforståelse og -kunnskap. Rådmannen har også ansvaret for at nødvendige konsesjoner foreligger for anvendelse av IT-systemet og/eller enkeltregistre.

Informasjonssikkerhetsleder skal på vegne av rådmannen ivareta den overordnede daglige oppfølgingen, og har blant annet ansvaret for å legge til rette for revisjon, ledel-

sens gjennomgang, gjennomføring av risikoanalyser, ajourføring av informasjonssikkerhetsprosedyrer og opplæring. Informasjonssikkerhetsleder inngår i rådmannens stab.

Informasjonssikkerhetsansvarlig er kontaktpersoner ved kommunens avdelinger overfor informasjonssikkerhetsleder og følger opp vedtatt informasjonssikkerhet i sin helhet for sin respektive avdeling. Dette innebærer avvikshåndtering, gjennomføring av risikoanalyser og -vurderinger, innføring og utarbeidelse av informasjonssikkerhetsprosedyrer og opplæring.

Ansvaret for den operative drift av IT-sikkerheten er tillagt IT-sjefen. IT-sjefens oppgaver er nedfelt i **IT-avdelingens** etablerte internkontrollsystem.

Systemeier skal ha tilsyn med vedlikehold og drift av systemet, samt systemets IT-sikkerhetsfunksjoner. Systemeieransvaret er normalt tillagt de respektive avdelinger i kommunen.

Behandlingsansvarlig (systemeier) skal sørge for rutiner og kontrolltiltak knyttet til behandlinger av personsensitiv informasjon. Behandlingsansvarlig har ansvaret for:

- at pålagte konsesjonskrav etterleves
- autorisasjon til IT-systemer
- tilgangskontroll

Alle **medarbeidere** har ansvar for å praktisere og etterleve vedtatte sikkerhetsbestemmelser og -tiltak, rapportere avvik og forstå konsekvensen ved brudd på sikkerhetsbestemmelsene.

Personvernombudet i Stavanger kommune er registrert personvern både i Stavanger, Finnøy og Rennesøy kommune. I Stavanger kommune har sikkerhetsansvarlig og personvernombudet vært tillagt samme person. Det er viktig at det legges til rette for ombudets uavhengighet for å unngå en interessekonflikt. Vi har blitt gjort kjent med at kommunen har opprettet en egen stilling som sikkerhetsansvarlig, og er i prosess for å få tilsatt i denne stillingen. Dette er besluttet som følge av at arbeidspresset ble for stort for en person å inneha begge rollene.

Beskrivelsen av ansvarsforhold er i noen grad mangelfull på kommunens intranettside da informasjonen ikke er oppdatert etter organisatoriske endringer. Det henvises også til konsesjon og meldeplikt. Den nye personopplysningsloven med personvernforordningen har avskaffet ordningen med meldeplikt og konsesjon jfr. Datatilsynet. Formålet med denne endringen er å flytte ansvaret for behandling av personopplysninger fra Datatilsynet til virksomhetene.

3.3.3 RISIKOVURDERING OG SIKKERHETSTILTAK

Den overordnede målsettingen til Stavanger kommune er å være en åpen og kommuniserende virksomhet. Sikkerheten skal være god nok for å tilstrekkelig opprettholde denne målsettingen, og avdelingene skal til enhver tid ha tilstrekkelig menneskelige ressurser.

Den overordnede sikkerhetsstrategien[11] sier også at risikovurdering- og analyser skal benyttes for å definere hvilke sikkerhetstiltak som må iverksettes knyttet til behandlingen av sensitiv informasjon. Gjennom rutiner og holdninger skal sikkerhet i alle ledd sikre tilgjengelighet, konfidensialitet, kvalitet og integritet i samtlige ledd ved behandlingen av sensitive informasjon.

For å opprettholde tilstrekkelig sikkerhet legges det i kommunens sikkerhetsstrategi vekt på bevisstgjøring gjennom følgende tiltak:

- Opplæring av nyansatte.
- Sikkerhetsfokus i forbindelse med risikovurdering ved innføring av nye IT-systemer.
- Opplæring i nye IT-systemer.
- Bevisstgjøring gjennom ledelse med ansvar for videreformidling.

Alle nyansatte i Stavanger kommune skal signere på sikkerhetsregler i tillegg til taushetserklæring. I styringsgruppen for informasjonssikkerhet ble det i september 2016 behandlet spørsmål om signering av sikkerhetsreglement skal ha en tilbakevirkende kraft for ansatte som ble ansatt før kravet om signert sikkerhetsreglement. Styringsgruppen vedtok at alle som er ansatt i Stavanger kommune skal signere sikkerhetsregler og taushetserklæring, og at kravet også gjelder ansatte som var ansatt før det var krav om signering av sikkerhetsregler. Sikkerhetsansvarlig i Stavanger kommune kan ikke bekrefte at alle har signert på sikkerhetsreglene, og viser til at det er virksomhetslederne sitt ansvar å følge opp. Rogaland Revisjons kontroll av sikker sone har signerte taushetserklæringer og sikkerhetsregler som ett av kontrollpunktene. Årets kontroll viser det ikke er avvik på signerte sikkerhetsregler ved de kontrollerte enhetene. Det var heller ingen avvik i kontrollerte enheter i 2017.

Stavanger har en prosedyre for sikkerhetskopiering for å sikre gjenoppretting av normal drift av alle informasjonssystemer, avbrudd eller feil, uten at kritiske data går tapt. Sikkerhetskopiering gjøres av servere, systemer og arbeidsstasjoner som IT-avdelingen har ansvar for. Kommunens IT-driftssenter ble i 2015 flyttet til Green Mountains fjellhall på Rennesøy. Etter flyttingen melder IT-avdelingen om mer oppetid på systemene. I handlings- og økonomiplanen for 2019-2022 er det i tillegg foreslått tiltak om å flytte langtidslagring fra Løkkeveien 51 til Green Mountains lokasjon på Rjukan. Dersom langtidslagringen flyttes til Rjukan vil alt være samlet hos Green Mountain, men man

[11] Jfr. Portal for informasjonssikkerhet, intranett Stavanger kommune.

vil skille produksjonsdata og backup på to fysisk uavhengige lokasjoner, noe som gir en ytterligere sikring av data.

Det er tjenesteområdene og sikkerhetsansvarlig som har ansvaret for opplæring i fagsystemene, og Stavanger kommune tilbyr også kurs i ulike systemer og har online kurs med fokus på informasjonssikkerhet og personvern. I tillegg benytter kommunen kurs via KS-læring. I høst har kommunen også gjennomført en e-post-kampanje med fokus på informasjonssikkerhet for alle ansatte i Stavanger kommune. E-post-kampanjen hadde en svarprosent på 37 prosent.

I spørreundersøkelsen ble de systemansvarlige spurt om de har fått tilstrekkelig opplæring i rollen som systemansvarlig. 66 prosent[12] sier de har fått tilstrekkelig opplæring. 75 prosent av respondentene svarer at de er kjent med sitt ansvar og oppgaver som systemansvarlig[13]. En del av ansvaret og oppgavene til de systemansvarlige er opplæring i fagsystemet. Dette spørsmålet får en score på 3,8[14]. Men hele 22,7 prosent av respondentene svarer at de i liten grad har ansvar for opplæring i fagsystemet. På spørsmål om opplæringen til nyansatte er tilstrekkelig i fagsystemet er også scoren 3,8[15]. Svarene kan tyde på at opplæringen i fagsystemene er på et gjennomsnittlig nivå, men at det kunne vært tydeligere kommunisert at systemansvarlig har ansvaret for opplæringen i fagsystemet.

Ved innføring av nye systemer finnes det rutine for bestilling. Bestiller skal fylle ut et elektronisk skjema i HP service manager der opplysninger om systemeier og systemansvarlig skal oppgis. Det skal også registreres om programmet behandler sensitive/taushetsbelagte opplysninger og om det er gjort en risikovurdering av programvaren. Det er tjenesteområdet sitt ansvar å vurdere om systemet som skal innføres behandler personopplysninger og vurdere om dette er i et omfang som krever risikovurdering.

Spørreundersøkelsen ble sendt ut til alle som er oppgitt som systemansvarlige i henhold til skjema i HP service manager[16]. På spørsmål om hvor mange fagsystemer den enkelte er systemansvarlige for, svarer hele 12,2 prosent[17] at de ikke er systemansvarlig. På spørsmål til sikkerhetsansvarlig og IT-sjef i Stavanger kommune om hvilke kontroller de har for kvalitetssikring av oversikten over systemansvarlige, er svaret at ansvaret ligger til tjenesteområdene.

[12] Respondenter som har svart 4-6. N=44.
[13] N=44.
[14] Svaralternativ 1-6. N=44.
[15] Svaralternativ 1-6. N=43.
[16] Listen over systemansvarlige er også tilgjengelig på intranett til Stavanger kommune.
[17] N=49. 12,2 prosent tilsvarer 6 respondenter.

SENSITIVE DATA

Rogaland Revisjon gjennomfører årlig en revisjon av informasjonssikkerheten til enheter som behandler sensitive data i sikker sone. Formålet med denne gjennomgangen er å sikre at:

- Enhetene følger kommunens rutiner og regler rundt informasjonssikkerhet, behandling og bruk av sensitive data og sensitiv dokumentasjon.
- Personopplysningslovens og -forskriftens krav om systematiske tiltak for behandling av personopplysninger etterleves.
- Ledelsen har jevnlige gjennomganger av sikkerhetsmål, -strategi og -organisering.
- Fagsystemene utvikles og forbedres jevnlig.
- Avvik rapporteres og tiltak er igangsatt.

Årets gjennomgang har avdekket flere avvik ute ved besøkene enn i de to foregående år. Avvikene var i stor grad knyttet til sensitiv informasjon sendt i e-post, faks eller lagret på datamaskin utenfor sikker sone. Revisjon av sikker sone har i 2018 blitt utvidet til å også inkludere enheter hvor avvik er avdekket de siste årene. Dette kan spille inn på omfang av avvik som er avdekket i år.

3.3.4 PROSEDYRER FOR INFORMASJONSSIKKERHET

Stavanger kommune har ulike prosedyrer som skal sikre tilfredsstillende informasjonssikkerhet.

Prosedyrer for brukerkonto beskriver fremgangsmåte for innmelding av nyansatte og opphørsskjema for brukere som skal avslutte sitt ansettelsesforhold til kommunen. Prosedyren sikre at det blir gitt riktig tilgang ved brukerdefinering. Det skal videre sikres at brukerkontoene som er definert er i bruk og at dermed ubenyttede brukerkontoer slettes. Prosedyren gjelder for alle brukere som er definert i systemer som administreres av IT-avdelingen.

Prosedyre for konfigurasjonskontroll skal sikre at utstyr og programmer fungerer sammen som forutsatt, og at man til enhver tid har en oppdatert oversikt over systemenes konfigurasjoner. Prosedyren skal også sikre at oppdateringer av maskin og programvare gjøres systematisk og kontrollert. Prosedyren gjelder innen IT-avdelingen og er begrenset til IT-arkitektur. Rutinen er at systemansvarlig for fagsystemet melder om behov for oppdateringer til IT-avdelingen.

Prosedyre for kryptering skal sikre at kryptering blir opprettet og vedlikeholdt i henhold til gjeldende krav. Alle nettverksforbindelser hvor det overføres sensitive data omfattes av prosedyren.

Prosedyre for fysisk sikring skal forhindre uautorisert adgang til informasjonssystemer og utstyr i IT-avdelingen.

Kommunen har også prosedyre for sikker avhending av utstyr.

De overordnede føringene for de tekniske løsningene for IT-sikkerheten er dokumentert i IT-sikkerhetspolicyen til Stavanger kommune. I sikkerhetspolicyen beskrives ulike sikkerhetsbarrierer som fysisk sikring, autorisasjon, tilgangskontroll, logging og annet. Tilgang for brukergrupper er også definert.

Hovedmålsetting for IT-sikkerhetsarkitekturen i Stavanger kommune er:
IT-avdelingen skal tilrettelegge, gjennom en klart definert IT-sikkerhetsarkitektur, for at Stavanger kommune skal ha et godt teknologisk fundament for ivaretakelse av personopplysninger. Som en overordnet integrert del av IT-sikkerhetsarkitekturen skal det etableres en helhetlig strategi som innbefatter IT-sikkerhetsorganisering, rutiner, prosedyrer og styringssystemer. Hovedmålsettingen for IT-sikkerhetsarkitekturen skal være i samsvar med de øverste mål og strategier for behandling av personopplysninger i Stavanger kommune.

Under punkt 4.15 om roller og ansvar i IT sikkerhetspolicyen står det at «*sikkerhetsansvarlig som er definert i sikkerhetsorganisasjonen er ansvarlig for informasjonssikkerheten inkludert IT-sikkerheten.*» Stavanger kommune presiserer at sikkerhetsansvarlig kun har en rådgivende funksjon mot tjenesteområdene. Tjenesteområdene er selv juridisk ansvarlig for den behandlingen de gjør av data. Det innebærer at de må ha innsikt i lover og regler, og etablere rutiner for internkontroll.

Katastrofeplan IKT beskriver roller og ansvar hvis det oppstår en katastrofesituasjon for Stavanger kommune sine IKT-løsninger. I møte med IT-avdelingen kom det fram at katastrofeplanen ikke har blitt revidert siden 2015. IT-sjefen er enig i at planen bør gjennomgås årlig i henhold til rutinen. Men sier samtidig at det ikke er store endringer som har skjedd siden planen ble utarbeidet i 2015 som ville ha påvirket innholdet i planen. I følge katastrofeplanen skal det årlig gjennomføres katastrofeøvelser basert på planen. Den siste øvelsen IT var involvert i var i februar 2017[18]. I referatet står det at det vurderes en ny øvelse senere våren 2017. Det ble ikke gjennomført en ny øvelse senere våren 2017, og i følge IT-sjef er det ikke gjennomført beredskapsøvelse i 2018. I følge beredskapssjef i Stavanger kommune er det avdelingene selv som er ansvarlig for gjennomføring av øvelser innenfor eget ansvarsområde.

3.3.5 AVVIKSHÅNDTERING

Stavanger kommunes prosedyre for avvikshåndtering har som formål å «*avdekke avvik, rapportere og foreta korrigerende strakstiltak, samt gi grunnlag for forebyggende tiltak og forbedring av prosedyren. Dette for å hindre gjentakelse av avviket. Avvik måles mot IT-sikkerhetspolicyen med tilhørende rutiner.*»

Den som oppdager et avvik innen eget eller andres arbeidsområde skal iverksette nødvendige strakstiltak og avviket skal rapporteres i avvikssystemet Synergi. Leder for

[18] Tabletop øvelse – Kommunikasjon, IT, Servicetorget og beredskap angående uønskede hendelser, 13.02.2017.

området hvor avvik har funnet sted sørger for ytterligere korrigerende tiltak for å gjenopprette normal tilstand. For å hindre gjentakelse av avviket skal forebyggende tiltak vurderes og eventuelt foreslås.

Iverksatte tiltak skal rapporteres til IT-sjef som skal evaluere iverksatte tiltak og overføringsverdi.

Som en del av kapitel 7.3.1 i håndbok for HMS/internkontroll inngår «*melding om brudd på regler for informasjonssikkerhet, personopplysninger og taushetsbelagt informasjon, klientforhold, straffesaker, helse, etnisitet, politiske, filosofiske, religiøse og seksuelle forhold.*» Alle ansatte skal melde om brudd på informasjonssikkerheten i avvikssystemet Synergi.

I intervju med IT-avdelingen opplyser de at det kun er ett avvik som gjelder brudd på informasjonssikkerhet til nå i 2018 som de har fått melding om. I gjennomgang av alle registrerte avvik på brudd på informasjonssikkerhet i Synergi i perioden 2016 til 30.09.2018 er det meldt om 108 avvik i 2016, 99 avvik i 2017 og 97 avvik til nå i 2018. Alle avvik som registreres i Synergi sendes til leder på det aktuelle arbeidssted for saksbehandling. I tillegg får lokalt verneombud på arbeidsstedet lesekopi av saken. Rutinen er også at alle saker som omhandler informasjonssikkerhet går som kopi til IT-sjef. Både IT-sjef og sikkerhetsansvarlig melder tilbake at de ikke får kopi av avvik som registreres i Synergi, heller ikke ved innlogging i Synergi.

Ved alvorlige brudd på personopplysningssikkerheten skal Datatilsynet gis melding innen 72 timer. Stavanger kommune har i 2018 meldt 7 avvik til Datatilsynet. Ved gjennomgang av avvik fra Synergi finner revisjonen ikke igjen alle avvikene. I følge sikkerhetsansvarlig registreres som regel ikke avvik som meldes til Datatilsynet i Synergi. Dette skyldes at den som melder avvik ikke er bevisst nok på at avviket også skal meldes inn i Synergi når det er meldt til Datatilsynet.

Fra mars 2017 til september 2018 er det meldt om 8 major incidents. Disse avvikene dokumenteres på sharepoint-siden til IT-avdelingen, og følges opp av IT. Dette er avvik av mer operasjonell form og driftsfeil.

Synergi er på vei til å fases ut, og IT-sjefen håper det nye systemet vil være et bedre system for varsling og oppfølging av avvik.

Om lag halvparten av de systemansvarlige[19] som svarte på undersøkelsen svarer at det er etablert rutiner for melding om uønskede hendelser, avvik eller sikkerhetsbrudd i fagsystemet. Nesten 30 prosent av respondentene svarer at det ikke er etablert rutiner.

[19] N=46.

Det er kun tre av respondentene som har meldt avvik på brudd på informasjonssikkerhet i løpet av det siste året. Av disse har to meldt og dokumentert avviket i Synergi.

3.3.6 SIKKERHETSREVISJON OG EGENKONTROLL

Ifølge Stavanger kommunes rutine for ledelsens gjennomgang skal sikkerhetsmål, -strategier og organisering av informasjonssikkerheten gjennomgås årlig for å kontrollere og revidere disse med de til enhver tid gjeldende krav og behov. IT-sjefen har også ansvar for at det gjennomføres og dokumenteres revisjon av IT-sikkerhetsarkitekturen årlig.

Stavanger kommune har i tillegg en årlig revisjon av informasjonssikkerheten i sikker sone som gjennomføres av Rogaland Revisjon.

Informasjonssikkerhetsleder er ansvarlig for å organisere årlig gjennomgang av informasjonssikkerheten i kommunen. Gjennom innrapporterte avvik skal det identifiseres hvilke tiltak som er iverksatt og planlagt iverksatt. Det skal utredes forslag til prioriterte tiltak med angivelse av økonomiske og organisatoriske konsekvenser. Oppfølgingen av vedtatte tiltak er det sikkerhetsansvarlig i avdelingen som har ansvaret for.

I følge IT-sjefen har det ikke blitt foretatt en systematisk årlig gjennomgang av rutiner og retningslinjer i Stavanger kommune de siste årene.

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, jfr. kapittel 2:

- 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.
- 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.

Etter omorganiseringen i Stavanger kommune ligger Stavanger byarkiv nå organisert under direktør for støtte og utvikling. Det vil ikke bli redegjort nærmere om organiseringen av Stavanger byarkiv i denne forvaltningsrevisjonsrapporten, men det henvises til forvaltningsrevisjonsrapporten om kommunens arkiv fra 2016. Fokuset i denne rapporten er arkivering av elektronisk informasjon, samt innsyn og offentliggjøring.

EARKIV 360

Stavanger byarkiv har anskaffet en frittstående arkivløsning, eArkiv 360. Den gir arkivet mulighet for å importere aktuelle dokumenter og historisk dokumentasjon fra ulike systemer og filområder til sikker langtidsarkivering og bevaring i et felles elektronisk system. Dette gir kommunen en mulighet for en sikker depotløsning for elektronisk informasjon.

3.4.1 FORVALTNINGSREVISJON AV KOMMUNENS ARKIV 2016

Rogaland Revisjon gjennomførte en forvaltningsrevisjonsrapport om kommunens arkiv i 2016. Rådmannen kom med en oppfølging av rapporten i august 2017[20], og kontrollutvalget ba om en ytterligere tilbakemelding høsten 2018.

[20] Kontrollutvalget i Stavanger kommune 19.09.2017, sak 45/17.

Forvaltningsrevisjonsrapportens konklusjon er at «*… kommunens arkivfunksjon er i det alt vesentlige ivaretatt på en tilfredsstillende måte ut fra krav i arkivloven og forskrift om offentlig arkiv.*» Det pekes likevel på utfordringer, og revisjonens anbefaling til kommunen var:

- Vurdere hvordan arkivfunksjonen kan styrkes ved å implementere denne i aktuelle strategiske digitaliseringsprosjekter i kommunen.
- Vurdere hvordan man sikrer at arkivlovens bestemmelser blir etterlevd.
- Vurdere hvordan man kan øke bevissthet, forståelse og aksept for arkivfunksjonen blant ledere og ansatte i kommunen.
- Vurdere hvordan man kan styrke ansattes kompetanse på arkivområdet, spesielt når det gjelder hva som skal unntas offentlighet og hvordan dette skal gjøres.

I behandlingen av forvaltningsrevisjonsrapporten ba bystyret rådmannen blant annet om å ha spesielt fokus på bestemmelsene om behandling av sensitiv informasjon i fokus og arkivering fra fagsystemer som ikke oppfyller kravene til Noark-standarden.

Stavanger byarkiv har iverksatt tiltak for å styrke arkivfunksjonen og bevisstheten om denne, sikre at arkivlovens bestemmelser blir etterlevd og styrke de ansattes kompetanse på arkivområdet.

For å sikre behandlingen av sensitive personopplysninger har blant annet nye lokaler i Arkivenes hus sikret at avvik i forhold til bygningsmessige og tekniske forhold er langt mer tilfredsstillende. Det arbeides også med implementering av andre systemer som skal sikre utsatt personsensitivt materiale. Public Oppvekst er et innovasjons- og digitaliseringsprosjekt som lager et fullelektronisk system for sikker behandling av dokumentasjon om barn i barnehage, elever i grunnskolen og for PP-tjenesten i sikker sone i Public 360.

3.4.2 ARKIVPLAN

Stavanger kommunes har gjennom sin arkivplan etablert rutiner for dokumentbehandling og arkivering i henhold til arkivforskriftens § 4. Arkivplanen er ikke et enkelt dokument, men består av en samling elektroniske dokumenter og rutinebeskrivelser. Alle dokumenter og rutinebeskrivelser er tilgjengelig for de ansatte på intranett. Nedenfor vises en oversikt over strukturen i arkivplanen til Stavanger kommune.

Figur 5 – Struktur på arkivplanen i Stavanger kommune. Kilde: Stavanger byarkiv.

Innhold	Arkivplan		
Innledning	Om bakgrunn, formål, innhold, struktur, oppdatering, arkivering, tilgjengelighet		
Delplaner	**1 Organisasjon**	**2 Rutiner**	**3 Arkiver**
Tema	Organisering av arkivansvaret og arkivarbeidet	Instrukser og rutiner for arkivarbeidet og dokumentbehandlingen	Hva arkivet omfatter og hvordan det er organisert og oppbevart
Arkivfag	1.1 Om arkivansvar og myndighet	2.1 Om instrukser og rutiner	3.1 Om arkiv og arkivorganisering
Gjeldende oversikter	1. 2.1 Organisering av arkivansvaret og arkivarbeidet 1.2.2 Arkivskapernes arbeidsområder og organisasjon	2.2.1 Lover og instrukser 2.2.1 Rutiner 2.2.3 Sikkerhet og innsyn	3.2.1 Organisering 3.2.2 Bestandsoversikt 3.2.3 Oppbevaring
Planer	1.3 Planer og strategier	2.3 Planer og strategier	3.3 Planer og strategier
Historikk	1.4 Aktuell historikk Utgåtte oversikter	2.4 Utgåtte oversikter	3.4 Utgåtte oversikter
Vedlegg (eks.)	1.5 Organisasjonskart	2.5.1 Avleveringslister 2.5.2 Kassasjonsplaner 2.5.3 Kassasjonslister 2.5.4 Bevaringsplaner	3.5.1 Arkivnøkler 3.5.2 Elektroniske system 3.5.3 Brukermanualer 3.5.4 Arkivoversikter

Arkivplanen skal til enhver tid være ajourført, jfr. arkivforskriften § 4. I planen står det at oppdatering av arkivplanen skal blant annet skje når:

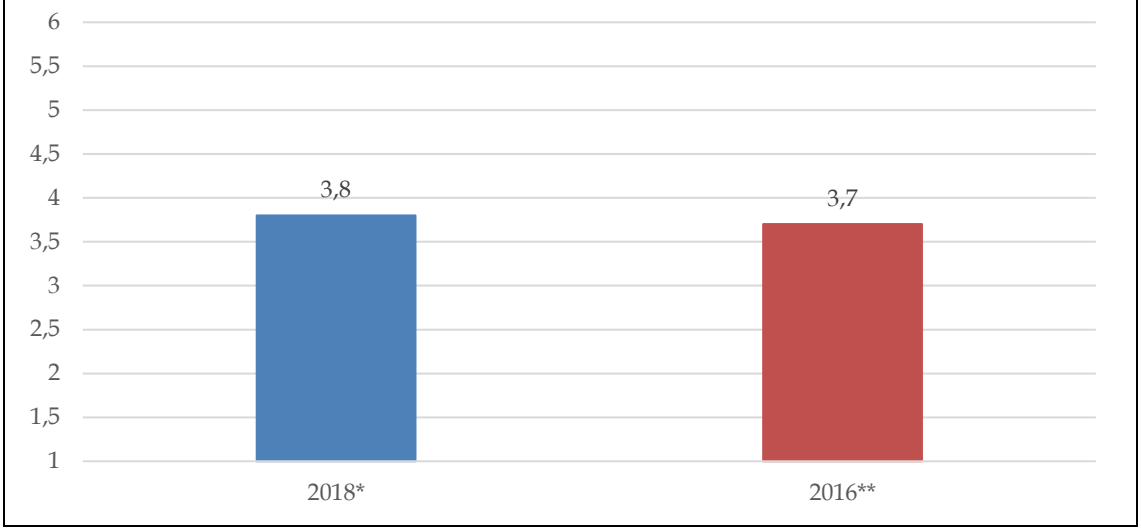
- *det skjer endringer i organisasjonen med betydning for arkivet, som eksempel når*
  - *det opprettes nye arkivskapere eller nye journalførende enheter.*
  - *arkivskapere blir nedlagt eller overført til andre organ.*
  - *kommunale oppgaver blir overført til andre organ.*
  - *saksområder endres internt med konsekvenser for arkivet.*
- *det skjer endringer i arkivarbeidet, som eksempel når*
  - *det er kommet nye lover og instrukser som har betydning for arkiv.*
  - *det er kommet endringer i lover, forskrifter som har betydning for arkiv.*
  - *det skjer endringer i rutiner som har betydning for arkivarbeidet.*
- *det skjer endringer med arkivmaterialet, som eksempel når*
  - *det opprettes nytt arkiv eller nye arkivdeler.*
  - *det blir tatt i bruk ny arkivnøkkel.*
  - *det blir tatt i bruk ny versjon av arkivnøkkelen med kodeendring.*
  - *det blir tatt i bruk nye datasystem for journalføring eller lagring av dokumenter.*
  - *oppdateringer av elektroniske arkivsystemer har betydning for arkiv.*

I innledningen til arkivplanen fra 2016 henvises det til den tidligere arkivforskriften, og revisjonen ser det naturlig å oppdatere arkivplanen med den nye forskriften.

I den nye forskriften om offentlig arkiv er det i § 4 tatt inn et krav om at arkivarbeidet blir omfattet av kommunens internkontroll. Dette kravet kommer i stedet for krav om arkivplanen, men er i prinsippet det samme kravet om at kommunen skal ha oversikt over arkivene, hvordan de er organisert, oversikt over regelverk og instrukser som gjelder for arkiv med mer. I følge arkivsjefen i Stavanger byarkiv gir arkivplanen denne oversikten.

Svarene fra spørreundersøkelsen som omhandler arkivering og offentliggjøring er sammenlignet med svarene som kom inn i forbindelse med forvaltningsrevisjonsrapporten av kommunens arkiv i 2016. Undersøkelsen som ble gjennomført i 2016 er ikke direkte sammenlignbar med undersøkelsen i denne rapporten. I 2018 er undersøkelsen kun sendt ut til systemansvarlige i Stavanger kommune, i 2016 ble undersøkelsen sendt ut til ledere, ansatte og administrativt personell/merkantilt personell for utvalgte virksomhetsområder[21].

Figur 6 – Kjenner du til innholdet i kommunens rutiner for arkivering (arkivplanen)? Kilde: Spørreundersøkelse fra Rogaland Revisjon.

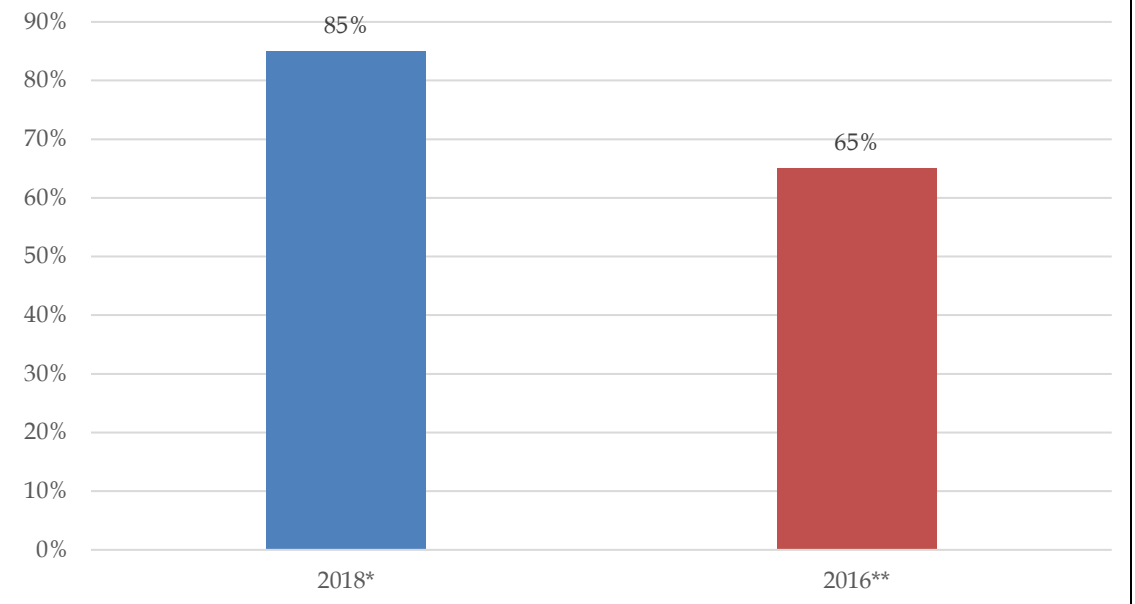


* Spørreundersøkelse ifm forvaltningsrevisjon av informasjonssikkerhet, drift og sårbarhet i Stavanger kommune, svaralternativ 1-6. N=49.
** Spørreundersøkelse ifm forvaltningsrevisjon av kommunens arkiv i Stavanger kommune 2016, svaralternativ 1-6. N=153.

Spørsmålet får omtrent samme score, og svarene indikerer at systemansvarlige i noe begrenset grad kjenner innholdet i kommunens arkivplan.

[21] Undersøkelsen ble sendt ut til 258 personer i kommunen, hvorav 154 personer svarte (59 prosent). De som fikk tilsendt undersøkelsen av rektorer, barnehagestyrere, virksomhetsledere på hjemmebaserte tjenester, virksomhetsledere på sykehjem, ledere og ansatte på byggesakskontoret, ansatte ved servicetorget og ansatte på personal- og organisasjon. I tillegg til ledere på ulike virksomheter har administrativt personell/merkantilt personell ved de utvalgte virksomhetsområdene mottatt undersøkelsen.

Figur 7 – Er rutiner for dokumentbehandling og arkivering kjent for de ansatte ved din enhet? Kilde: Spørreundersøkelse fra Rogaland Revisjon.



* Spørreundersøkelse ifm forvaltningsrevisjon av informasjonssikkerhet, drift og sårbarhet i Stavanger kommune, respondenter som har svart alternativ 4-6. N=48.
** Spørreundersøkelse ifm forvaltningsrevisjon av kommunens arkiv i Stavanger kommune 2016, respondenter som har svart alternativ 4-6. N=153.

I undersøkelsen for 2018 har antall respondenter som har svart at rutiner for dokumentbehandling og arkivering er kjent[22] for de ansatte økt fra 65 prosent til 85 prosent. Det er også en høy score på spørsmål om den systemansvarlige vet hva som regnes som arkivverdig materiale (76 prosent svarte alternativ 4-6). For å kartlegge de ansattes praktisering av rutiner har revisjonen inkludert et spørsmål som omhandler rutiner satt ut i praksis. På spørsmålet om praktiseringen av dokumentbehandling og arkivering er tilfredsstillende svarte 65 prosent[23] at praktiseringen var god. Dette kan tyde på at praktiseringen av rutinene er lavere enn kjennskapen til dem.

Det er lavere score på spørsmål om systemansvarlige kjenner til kommunens bruk og arkivering av e-post. Her var det 59 prosent av de spurte som svarte at de hadde god kjennskap til rutinen[24]. E-post er et viktig kommunikasjonsmiddel i kommunen, og det er viktig at ansatte blir kjent med rutinen for arkivering av e-poster. Stavanger byarkiv har en egen rutine for bruk og arkivering av e-post. Denne ligger tilgjengelig på intranett og er også innbakt i generelle arkivrutiner. I tillegg blir informasjon om arkivering av e-post tatt med i alle kurs om Public 360 og arkiv. Det er saksbehandler sitt ansvar å arkivere egne e-poster, og leder sitt ansvar og følge opp at virksomheten følger pålagte rutiner.

[22] Respondenter som har svart alternativ 4-6.
[23] Respondenter som har svart alternativ 4-6. N=48.
[24] Respondenter som har svart alternativ 4-6. N=49.

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.

Stavanger kommune oppgir i Riksarkivarens undersøkelse for 2018 at kommunen i stor grad[25] har dokumentert alle sine elektroniske systemer som inneholder arkivverdig informasjon i arkivplanen. Stavanger kommune svarer i undersøkelsen at de ikke[26] tar uttrekk fra avsluttede bevaringsverdige fagsystemer[27]. De oppgir også at de aldri har tatt uttrekk fra elektroniske systemer som inneholder bevaringsverdig informasjon, samtidig som det i neste spørsmål kommer frem at Stavanger kommune har kompetanse til å ta uttrekk fra systemer. Det er den enkelte virksomhet/systemansvarlig som har ansvaret for å ta nødvendige uttrekk fra et elektronisk system og avlevere dette til byarkivet. Dette har, i følge arkivsjefen, aldri blitt prioritert, antakelig på grunn av manglende kunnskap om dette i virksomhetene. Byarkivet har heller ikke hatt ressurser og kompetanse til å ta imot slike uttrekk, men er nå i ferd med å bygge opp en egen eArkiv-seksjon som kan veilede virksomhetene og motta og validere slike uttrekk. Arkivsjefen forventer at det blir tatt flere uttrekk av systemer i forbindelse med overgang til Nye Stavanger kommune, da mange systemer skal avsluttes i forbindelse med etablering av ny kommune.

3.4.3 PERSONOPPLYSNINGER

Protokoll over personopplysninger er ikke en ny oppgave for kommunene, og Stavanger 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.

[25] Svar 4 på spørsmål med svar alternativer 1-4 der 1= passer ikke i det hele tatt og 5= passer svært godt
[26] Svar 1 på spørsmål med svaralternativer 1-4 der 1= passer ikke i det hele tatt og 5= passer svært godt
[27] Bevaring av elektroniske arkivsystemer innebærer at det må tas uttrekk, som betyr at alle bevaringsverdige data og/eller elektroniske dokumenter må hentes ut i et format og med en struktur som er egnet for langtidsbevaring (depot).

I Draftit er det 62 registreringer til nå. Personvernombudet i Stavanger kommune opplyser at kommunen ikke er ferdig med å registre behandlinger i Draftit. Det er behandlingsansvarlig (systemeier) som har ansvaret for at protokollføring av alle behandlinger av personopplysninger blir gjennomført. Det har ikke blitt gjennomført kurs for de systemansvarlige i forhold til registrering av behandling av personopplysninger i Draftit. Men personvernombudet hjelper og veileder enheter som har behov.

I spørreundersøkelsen er det 34 prosent[28] som svarer at de har registrert behandling av personopplysninger helt eller delvis i Draftit. Men hele 45 prosent svarer at de ikke har registrert behandlinger. 30 prosent svarer at det ikke er relevant for dem å registrere behandling av personopplysninger i Draftit. 60 prosent[29] svarer at de har fått tilstrekkelig opplæring i virksomhetens plikter og de registrertes rettigheter etter den nye personvernforordningen. Men over 70 prosent svarer at de får hjelp og veiledning av personvernombudet i kommunen dersom de har spørsmål som gjelder personopplysninger[30].

Det er ikke laget en oversikt som viser om registreringene er fullstendige. Av listen som viser behandlinger som tidligere trengte konsesjon og meldeplikt finne revisjonen igjen kun 10 av 38 registreringer.

Registreringene i Draftit fremstår for revisjonen som ufullstendige både i forhold til den informasjonen som er registrert i Draftit og i forhold til antall behandlinger som er registrert. Draftit har en funksjonalitet der man kan angi en vurdering av risiko på hver registrering. Dette er ikke benyttet. Det er heller ikke satt en status for registreringene, noen som gjør at alle registreringene har status «til gjennomgang».

Personvernombudet i Stavanger kommune opplyser at flere brukere har hatt problemer med å forstå og gjennomføre en protokollføring i Draftit. Det vil derfor i løpet av 2019 bli bygget opp en ny protokoll i sharepoint, og Draftit vil bli faset ut i løpet av 2019.

Når nye aktiviteter, som omfatter behandling av personopplysninger, settes i gang har kommunen en rutine som skal følges. Denne omfatter blant annet at formålet for behandlingen skal være definert, og om nødvendig skal det foretas en risikoanalyse. Disse skal arkiveres i Public 360 og det registreres også i Draftit

For å sikre personvernet har personvernforordningen et krav om at alle nye løsninger skal ha innebygd personvern. Det skal også etableres databehandleravtaler med alle aktører hvor samspillet innebærer behandling av personopplysninger. I Stavanger kommune er det tjenesteområdene som har ansvaret for både innebygd personvern og databehandleravtaler. Personvernombudet hjelper ved behov.

[28] N=47.
[29] Respondenter som har svart alternativ 4-6. N=47.
[30] Respondenter som har svart alternativ 4-6. N=45.

3.4.4 OFFENTLIGHET OG INNSYN

Stavanger byarkiv har utarbeidet rutiner for å unnta et dokument fra offentligheten. Disse rutinene ligger tilgjengelig for de ansatte på intranett. I utgangspunktet unntas ikke saker fra offentligheten. Dersom det er nødvendig å skjerme innholdet i dokumenter og saker fra offentlighet kan dette enten gjøres av arkivet når saken opprettes, eller saksansvarlig kan gjøre det når saksnummeret blir tildelt. Dersom et dokument, vedlegg eller en sak skal graderes må saksbehandler velge rett hjemmel fra offentlighetsloven og skjerme de rette feltene. Det må også velges riktig tilgangsgruppe.

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

- Personlige forhold, offl. §13, fvl. § 13.1.
- Drifts- eller forretningsforhold, offl. §13, fvl. § 13.2.
- Interne dokumenter utenfra, offl. § 15.
- Organinterne dokumenter, offl. § 14.
- Rettspleielovene, offl. § 18.
- Økonomi-, lønns- eller personalforvaltning, offl. § 23.1.
- Økonomiske rammeavtaler, offl. § 23.2.
- Rikets sikkerhet, offl. § 24.
- Offentlige kontroll- eller reguleringstiltak, offl. § 24.1.
- Lovovertredelse, offl. § 24.2.
- Opplysninger som kan lette utføring av straffbare handling, offl. § 24.3.
- Ansettelsessak, offl. § 25. Unntaket gjelder ikke søkerliste. Opplysninger om en søker kan likevel unntas fra offentlighet dersom søkeren selv anmoder om dette.
- Besvarelser, offl. § 26.1.
- Utsatt offentlighet, offl. § 5.

Vurdering av offentlighet for inngående dokumenter gjøres i forbindelse med dokumentregistrering. Forhåndsvurdering om unntak skal bare gjøres når det er helt klart at det ikke er aktuelt å gi innsyn i konkrete opplysninger eller konkrete dokumenter. Offentlighetsvurderingen kan overprøves av ansvarlig saksbehandler som er ansvarlig for å vurdere og unnta egne dokumenter fra offentlighet.

Det er dokumentets innhold som avgjør valg av lovhjemmel og tilgangsgruppe. Dokumenter som unntas fra offentlighet skal også begrenses internt ved bruk av tilgangsgruppe og skjermes på offentlig journal.

I spørreundersøkelsen ble det undersøkt i hvilken grad de systemansvarlige kjenner til lovbestemmelsene som regulerer hvilke dokumenter som skal unntas offentlighet. Her

svarer 60 prosent[31] at de kjenner til de gitte lovbestemmelsene. Dette gir en gjennomsnittsscore på 3,9. Noen flere, 63 prosent[32], sier de vet hvordan de unntar et dokument fra offentligheten i Public 360. I kommentarer til dette spørsmålet ble det kommentert blant annet at en vet hvordan en unntar et dokument fra offentlighet i Public 360 i en aktuell saksgang, men at en er usikker på hva som på et generelt grunnlag kan unntas fra offentlighet. Det kommenteres også at en vet hvordan det gjøres, men at man ber om hjelp fra jurist når det er noe viktig for å være helt sikker. Det er også flere som kommenterer at de ikke har fått tilstrekkelig opplæring i hvordan de unntar dokumenter fra offentligheten. En kommenterer også at det er mye fokus på personvern, men savner fokus på konfidensielle opplysninger i anbud.

Spørsmålet om hvor enkelt det er for brukeren av Public 360 å unnta dokumenter fra offentligheten får en gjennomsnittsscore på 4[33]. Det kommenteres at det hadde vært enklere å unnta dokumenter hvis det ikke hadde vært så mange steg å gå igjennom for å få et dokument unntatt fra offentligheten. Andre kommentarer i forhold til arkiv var:

«Arkivloven og arkivsystemet er fokusert på «gammeldags» korrespondanse. Dagens kommunikasjonsstruktur er annerledes og ikke like hensiktsmessig å ha i Public. Mye bevaringsverdig bygningsmessig dokumentasjon passer ikke i inn/ut/notat strukturen.»

OFFENTLIG JOURNAL

Ingen av fagsystemene innen helse- og velferdssektoren er koblet opp mot den offentlige journalen som er tilgjengelig på hjemmesiden til Stavanger kommune. Dette skyldes at helse- og velferdssektoren har egne systemer som benyttes til saksbehandling og oppbevaring av dokumentasjon som er spesialdesignet for eget fagfelt. For innsyn i disse sakene må henvendelsen rettes direkte mot den enkelte virksomhet.

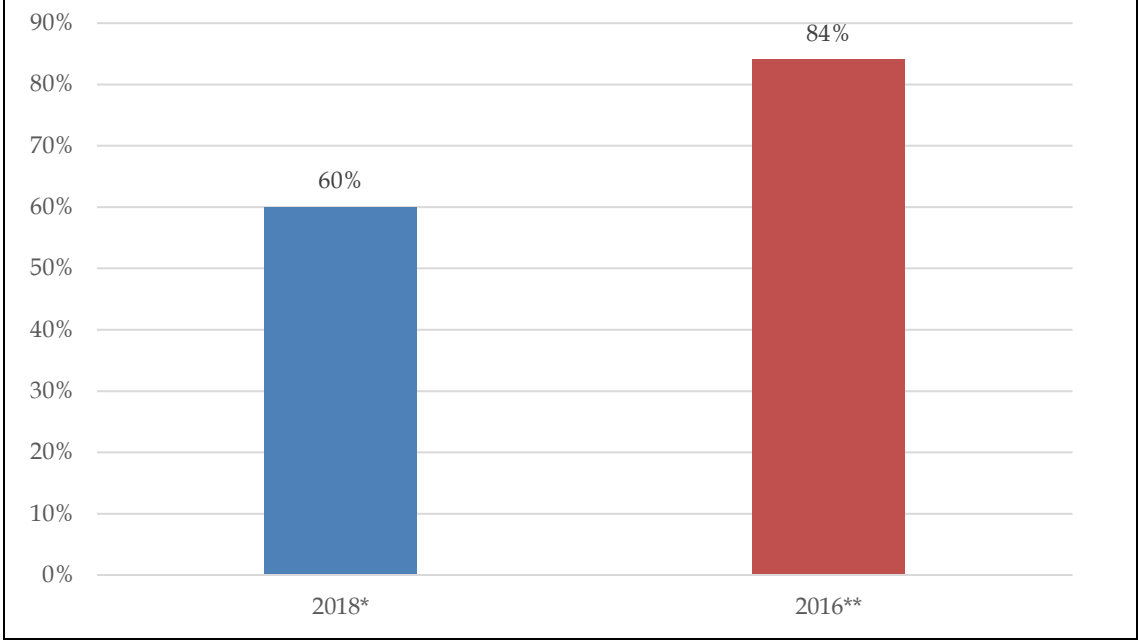
Revisjonen gjennomførte kontroll av alle journalførte saker på en gitt dato. Totalt ble 353 saker kontrollert. Av disse var om lag halvparten unntatt offentlighet. To saker ble undersøkt nærmere. Den ene saken gjaldt en jobbsøknad som ikke var avskjermet etter offentlighetsloven § 25. Årsaken til at denne søknaden ikke er avskjermet, slik som andre jobbsøknader, skyldes at søknaden ikke har kommet inn via kommunens integrasjon. Da blir det opp til arkivar (inngående søknader) og saksbehandler (utgående svarbrev) å selv registrere dokumentene og vurdere om de skal unntas fra offentlighet.

Den andre saken omhandlet oppfølging av gravid arbeidstaker. I denne saken framkommer både arbeidssted og navn på den gravide arbeidstakeren på postlisten selv om selve dokumentet er avskjermet. Stavanger byarkiv svarer at oppfølging av gravide arbeidstakere i henhold til rutinene ikke nødvendigvis er unntatt offentligheten. Helseopplysninger regnes i personvernforordningen som en sensitiv personopplysning, og

[31] Respondenter som har svart alternativ 4-6. N=48.
[32] Respondenter som har svart alternativ 4-6. N=49.
[33] N=48.

på hjemmesiden til NHO er graviditet listet opp som et eksempel på en sensitiv helse-opplysning.

Figur 8 – Kjenner du til lovbestemmelser som regulerer hvilke dokumenter som skal unntas fra offentlighet? Kilde: Spørreundersøkelse fra Rogaland Revisjon



* Spørreundersøkelse ifm forvaltningsrevisjon av informasjonssikkerhet, drift og sårbarhet i Stavanger kommune, respondenter som har svart alternativ 4-6. N=48.
** Spørreundersøkelse ifm forvaltningsrevisjon av kommunens arkiv i Stavanger kommune 2016, respondenter som har svart alternativ 4-6. N=144.

I forhold til forvaltningsrevisjonen av kommunen arkiv i 2016 er det en stor nedgang i respondentens kjennskap til lovbestemmelser som regulerer hvilke dokumenter som skal unntas fra offentlighet.

INNSYN

Det er innbyggerservice som administrerer mottak av begjæring om innsyn i offentlige dokumenter i Stavanger kommune. Dersom det bes om innsyn i dokumenter som er unntatt offentlighet, er det ansvarlig saksbehandler som skal behandle den (i Public 360). Stavanger kommune skal sikre at allmennheten kan få innsyn i saker og dokumenter. I dokumenter som er unntatt offentlighet kan det derfor vurderes om det kan innvilges delvis innsyn i stedet for å avvise kravet. Public 360 har elektronisk verktøy for å sladde dokumenter.

Innsyn i hvilke personopplysninger kommune har registrert på enkeltpersoner ligger til tjenesteområdene, og rutiner for innsyn må utarbeides for hvert enkelt fagsystem. Personvernombudet opplyser at kommunen er i gang med å utarbeide en felles rutine/system for hvordan innsyn kan behandles ute i tjenesteområdene.

Det ble i spørreundersøkelsen undersøkt hvor mange innsynsbegjæringer om personopplysninger det er kommet i fagsystemene. Her er det kun 24 prosent[34] som har mottatt innsynsbegjæring. Men 62 prosent[35] 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 god måte, men flere peker også på at innsynsbegjæringer er tidkrevende for enhetene. Noen kommenterer også at de savner en overordnet rutine for hvordan arbeidsflyten og dokumentflyten skal være dersom noen ber om innsyn i alt som finnes om dem i kommunen.

[34] N=45.
[35] N=45.

3.5 HACKING

Dette kapitlet fokuserer på følgende problemstilling:

Hvor stor er risikoen for hacking?

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 Stavanger 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. I intervju peker sikkerhetsansvarlig i Stavanger kommune på at den største faren for hacking ikke vil bli oppdaget før det er for sent, og at de største angrepene skyldes at medarbeiderne ikke følger fastsatte rutiner.

Stavanger kommune opplevde direktørsvindel i mai 2018. Hadde ansatte ved regnskapsavdelingen vært mer oppmerksom på direktørsvindel og fulgt fastsatte rutiner ville svindelen blitt avdekket før pengene ble utbetalt. Stavanger kommune har i ettertid gjennomgått rutinene og gjort ansatte enda mer bevisst på risikoen for svindel via internett. Rutinene er de samme, men dersom det kommer unntakshenvendelser om betalinger så skal disse nå løftes til øverste leder i regnskapsavdelingen. Stavanger kommune har valgt å være åpne om svindelen.

Stavanger kommune gjennomførte i høst en informasjonskampanje i forhold til informasjonssikkerhet til alle ansatte i kommunen. Undersøkelsen hadde en før- og etterundersøkelse. Det var vesentlig færre[36] som svarte på etter-undersøkelsen i forhold til før-undersøkelsen, og det er derfor vanskelig å trekke noen endelige konklusjoner. Men en ting som pekte seg markant ut er gjennomgående høyere svar på forståelsen av ulike IT-trusler som finnes. Dette gir en indikasjon på at informasjonskampanjen har bidratt til at ansatte er mer oppmerksomme på de ulike former for datakriminalitet som finnes. 87 prosent[37] svarte at de tenker mer på informasjonssikkerhet i det daglige nå enn før kampanjen. Det ble også kommentert ønske om å få samme opplæring en gang i halvåret for å bli mer bevisst på ord og begreper, og hvordan ansatte kan beskytte seg mot angrep.

I spørreundersøkelsen blant de systemansvarlige i Stavanger kommune svarer de fleste nei eller vet ikke på spørsmålene om det har forekommet uønskede hendelser. En av

[36] Basert på svar på spørsmål om ransomware og phishing per 2. november 2018. Om lag 2.350 svar på før-undersøkelsen, og 1.170 svar på etterundersøkelsen.
[37] N=1.220

respondentene peker på innbrudd som ble gjort fra hacker inn i fagsystemet som omfatter web-kalender og tømme-app (angrepet er også omtalt i media og ble tatt opp i kommunalstyret for administrasjon 20.11.2018 sak 7/18). Avviket er meldt til Datatilsynet og leverandøren har lukket sikkerhetshullet.

TEKNISKE LØSNINGER

IT-sikkerhetspolicy[38] beskriver de overordnede tekniske løsningene for IT-sikkerheten i Stavanger kommune. Revisjonen har ikke gått inn og vurdert de tekniske løsningene.

Stavanger kommune har delt sikkerhetsbarrierene inn i ytre og indre sikkerhetsbarrierer. Den ytre sikkerhetsbarrieren skal ha som funksjon og ivareta sikkerheten knyttet til eksterne forbindelser mellom interne nettsegmenter med ikke-personsensitive opplysninger. All ekstern kommunikasjon skal alltid skje gjennom den ytre sikkerhetsbarrieren. Den viktigste ytre sikkerhetsbarrieren er brannmuren.

Den indre sikkerhetsbarrieren skal sørge for å beskytte alle nettsegmenter med personsensitiv informasjon. I dette ligger det å gi brukere i nettverk med personsensitiv informasjon tilgang til ulike fellessystemer og informasjonstjenester med ikke-personsensitiv informasjon. Dette betyr også tilgang til ekstern kommunikasjon via den ytre sikkerhetsbarrieren. De viktigste indre sikkerhetsbarrierene er en logisk sikkerhetsbarriere applikasjon (brukergrupper, autentisering, definert skrivebord) og kryptering.

Samlet skal sikkerhetsbarrieren ivareta gjeldende sikkerhetspolicy i virksomheten. Kombinert danner dette grunnlag for en sonemodell (se figur under).

Figur 9 – Sonemodell i Stavanger kommune. Kilde: Stavanger kommune, IT sikkerhetspolicy.

Sensitiv sone:	Nettverksdel som behandler eller oppbevarer personsensitiv informasjon
Intern Sone:	Nettverksdel som ikke behandler eller oppbevarer personsensitiv informasjon. Dette inkluderer også de institusjoner som idag har fysisk delte nettverk.
Eksterne forbindelser:	Alle eksterne forbindelser, inkludert de spesielt sikrede sonene DMZ for ekstern informasjonsutveksling. Eksterne forbindelser er også definert mellom konsesjonsområder innad i virksomheten.

TOKONTO-PRINSIPPET

Alle brukere som skal ha adgang til systemer med personsensitiv informasjon tildeles to ulike kontoer for innlogging, en personsensitiv konto og en åpen konto (som gir tilgang til fagsystemer med ikke sensitiv informasjon og web-leser). Ved bruk av en logisk sikkerhetsbarriere applikasjon skal det ikke være mulig å flytte informasjon mellom disse kontoene. I rutinen opplyses det at det ikke gjøres unntak fra tokonto-prinsippet.

[38] Jfr. Portal for informasjonssikkerhet på Stavanger kommune sin intranettside.

VIRUSKONTROLL

All kommunikasjon som foregår mellom interne nettverk og eksterne nettverk sjekkes for virus. Dette gjelder spesielt e-post og vedlegg i e-post.

SIKKERHETSLØSNINGER

Fra sikkerhetsansvarlig har vi fått opplyst at Stavanger kommune i løpet av 2019 skal gå til anskaffelse av en SIEM-løsning, som samordner og analyserer sikkerhetsdata fra ulike kilder. Løsningen er et sikkerhetsovervåkingssystem som gir 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. Systemet bruker analyselogaritmer til å oppdage avvikende hendelsesmønster og advare om mulige trusler. Løsningen har også en løpende skanning av sårbarheter på alle relevante systemer.

For å sikre at SIEM-løsningen settes inn på de mest strategiske områdene foreslår rådmannen i handlings- og økonomiplanen for 2019-2022 midler til gjennomgang av IT-infrastrukturen. Gjennomgangen skal utføres av eksterne og skal avdekke sårbarheter og anbefale endringer i dagens rammeverk. I tiltaket står det at man ønsker å trygge informasjonssikkerheten gjennom for eksempel enhetlig behandling av alle systemer i kommunen.

I handlings- og økonomiplanen for 2019-2022 ble det vedtatt midler til automatisert kartlegging av elementer og sammenhenger i kommunens infrastruktur (uCMDB). Dette vil gi en kvalitetsheving og økt internkontroll av kommunens data.

OPPGRADERING AV PROGRAM- OG MASKINVARE

Systemeier for fagsystemene gir IT-avdelingen melding om behov for oppdateringer. Alle operative systemer hos IT blir oppgradert ukentlig.

Stavanger kommune er medlem i NorCERT og HelseCERT. NorCERT er den operative delen av Nasjonal sikkerhetsmyndighet (NSM). De håndterer alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon. 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.

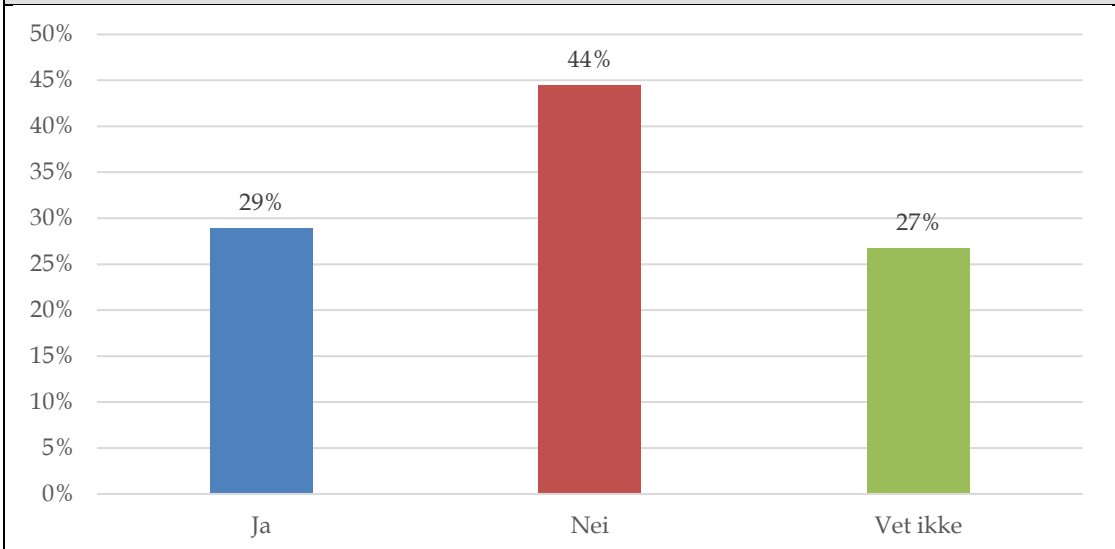
Via medlemskap i NorCERT og HelseCERT får Stavanger kommune tidlig varsler om brudd og sikkerhetssvakheter. IT-avdelingen håndterer rapporter fra NorCERT og HelseCERT systematisk og fortløpende. Det utføres tiltak som eksempelvis oppgraderinger dersom rapporten har avdekket sikkerhetshull i en programvare.

Stavanger kommune har fagsystemer som ikke er oppdatert med siste versjon. Dette kan medføre risiko for sikkerhetshull som kan utnyttes av kriminelle. IT-sjef opplyser at de fleste fagsystemene ikke er eksponert på internett, og at man da må være påkoblet Stavanger kommune sitt intranett[39] for å komme inn på fagsystemet og utnytte eventuelle svakheter.

BRUKERKONTO

I Stavanger kommune er det behandlingsansvarlig (systemeier) som har ansvaret for tilgangskontroll til fagsystemene. IT-avdelingen har ansvaret for etablering og oppfølging av tilgangskontrollrutiner i samarbeid med de andre systemeierne.

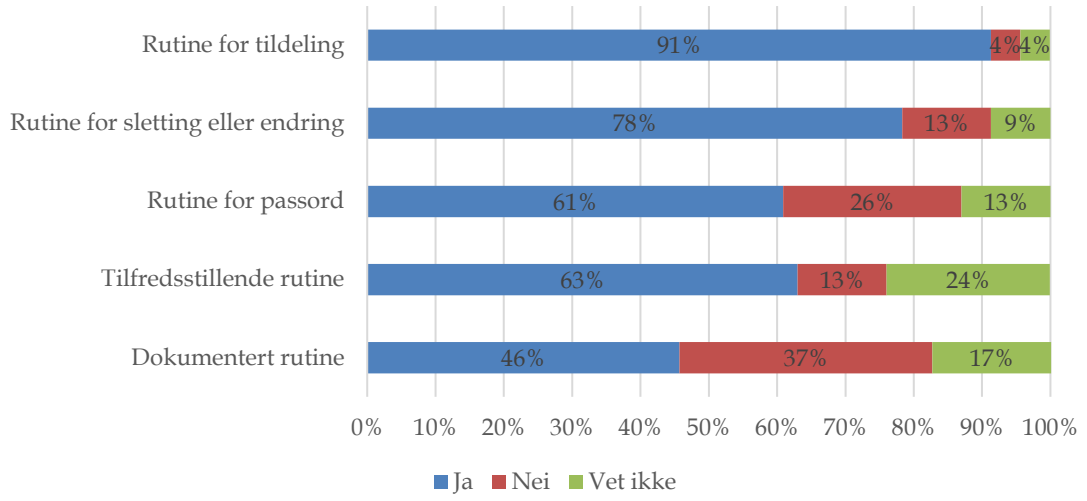
Figur 10 – Er det foretatt risikovurdering ifm. brukertilganger til fagsystemet? (N=45)
Kilde: Spørreundersøkelse fra Rogaland Revisjon.



Bare 29 prosent av de systemansvarlige svarer at det er foretatt risikovurdering i forbindelse med brukertilganger til fagsystemet.

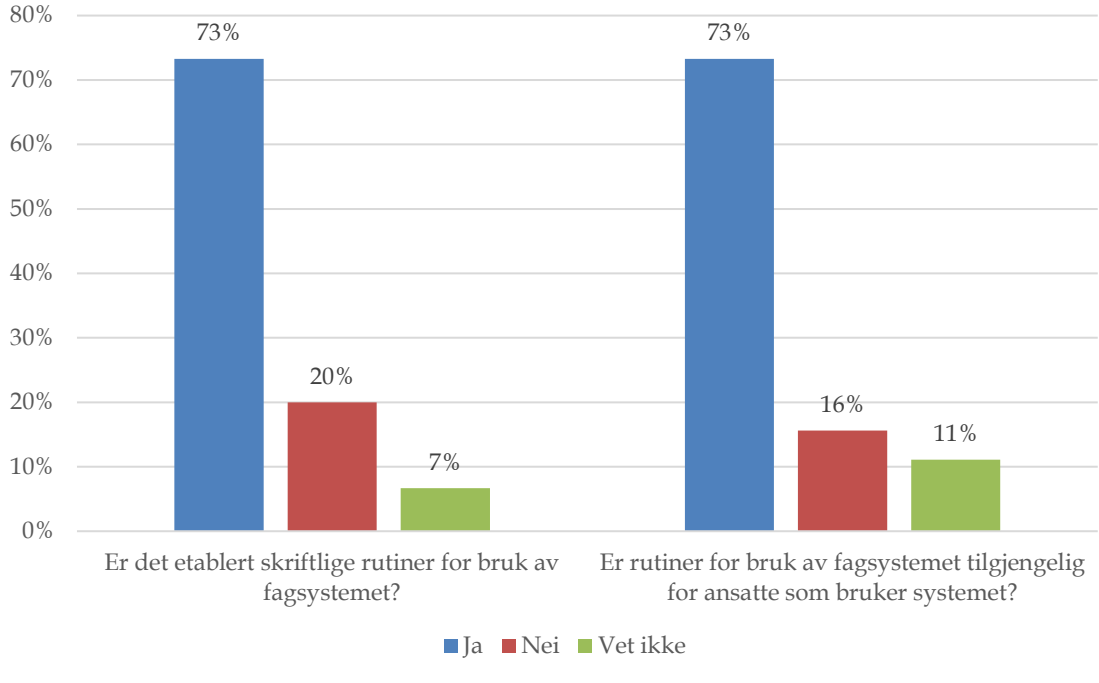
[39] Intranett er Stavanger kommunes interne nettverk og kun tilgjengelig for ansatte i kommunen.

Figur 11 – Rutiner og prosedyrer for brukertilganger (N=46) Kilde: Spørreundersøkelse fra Rogaland Revisjon.



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. 63 prosent svarer at rutiner og prosedyrer for administrering og kontroll av brukertilganger i fagsystemet er tilfredsstillende. Noe færre har etablert rutiner for passordbruk. Men svarene fra undersøkelsen viser at det er under halvparten som har dokumentert rutiner og prosedyrer for administrering av brukertilganger.

Figur 12 – Rutiner for bruk av fagsystemet (N=46) Kilde: Spørreundersøkelse fra Rogaland Revisjon.



Det er etablert skriftlige rutiner for bruk i de fleste fagsystemene. Rutinene er også tilgjengelige for de ansatte.

I IT-avdelingen har de som jobber med infrastruktur administratortilgang, men ikke alle har full administratortilgang til alle systemene. Det er IT-sjefen som må godkjenne administratortilganger til ansatte i IT-avdelingen, og tildelingen skjer manuelt. Endringer i tilganger skjer også manuelt.

Brukerkontoer til ansatte i Stavanger kommune styres gjennom lønns- og personalsystemet. Kontoer blir opprettet, men de aktiveres ikke før leder sender inn en tilgangsforespørsel. Fra den ansatte blir meldt inn må brukerkontoen brukes i løpet av de første 60 dagene før kontoen blir deaktivert. Når ansatte slutter skal leder sende melding om sperring av brukerkontoer. Dersom det ikke sendes en sluttmelding vil brukerkontoer uten aktivitet de siste 6 måneder automatisk bli deaktivert. Etter 2 år blir brukerkontoer automatisk slettet.

DIGITALISERING

Den raske digitale utviklingen på flere ulike fronter øker viktigheten for at anskaffelser gjøres i henhold til prosedyren. I forhold til GDPR[40] er det viktig å lovhjemle formålet med behandlingen av alle aktiviteter som omfatter personopplysninger. Det skal også vurderes behov for risikovurdering. Sikkerhetsansvarlig i Stavanger kommune sier at informasjonssikkerhet i forhold til digitalisering er noe som diskuteres internt for å sikre at all behandling av personopplysninger er lovhjemlet og at nødvendige risikovurderinger blir tatt.

[40] General data protection regulation.

3.6 OPPSUMMERING, VURDERING OG ANBEFALINGER

Stavanger kommune har i stor grad systemer og rutiner for å ivareta informasjonssikkerheten, men en del av retningslinjene og rutinene bærer preg av ikke å ha blitt revidert og oppdatert de siste årene. Svarene fra spørreundersøkelsen blant de systemansvarlige i Stavanger kommune viser jevnt over at retningslinjer og rutiner er kjent i organisasjonen.

Den største trusselen mot informasjonssikkerhet i Stavanger kommune er at ansatte ikke følger fastsatte rutiner og prosedyrer. Dette understrekes både av sikkerhetsansvarlig, og nevnes også i den foreløpige risikoanalysen til Public Oppvekst. Opplæring og informasjon ut til de ansatte er derfor et viktig virkemiddel for å øke informasjonssikkerheten i Stavanger kommune.

INFORMASJONSSIKKERHET

Stavanger kommune har et styringssystem for informasjonssikkerhet som omfatter en overordnet retningsgivende digitaliseringsstrategi, en IKT-strategi, håndbok for HMS/internkontroll, samt et internkontrollsystem for prosedyrer.

I digitaliseringsstrategien pekes det på viktigheten av en tydelig fordeling av roller og ansvar i digitaliseringsarbeidet for å sikre en handlekraftig gjennomføring av strategien. Det henvises til IKT-strategien for nærmere beskrivelse av roller og ansvar. I arbeidet med den nye IKT-strategien ble det valgt å legge disse beskrivelsene av roller og ansvar på intranett framfor å inkludere det i strategien, uten henvisning til intranettsidene. IKT-strategien burde henvist direkte til intranett slik at leseren av de ulike strategiene lettere kunne funnet frem til informasjonen. Når beskrivelsen av roller og ansvar er lagt på intranett vil det heller ikke være tilgjengelig for andre enn kommunens ansatte. IT-sjefen sier i intervju at det ikke vil bli utarbeidet en ny digitaliseringsstrategi når dagens strategi utløper, men heller inkludere den i IKT-strategien som rulleres oftere.

Stavanger kommune har prosedyrer for internkontroll for informasjonssikkerhet i form av portalen på intranett. Under overordnet sikkerhetsstrategi er sikkerhetsmål og -strategi definert.

Ved kontroll av rutinen for systematisk gjennomgang av sikkerhetsmål og -strategi fant vi at denne gjennomgangen ikke har blitt gjennomført de siste årene. I følge kommunen skyldes dette at det i lenger tid har vært planlagt en full revidering av prosedyrene for informasjonssikkerhet. Ifølge IT-sjef og sikkerhetsansvarlig er informasjonen som finnes på portalen fortsatt gyldig selv om portalen ikke er oppdatert med blant annet organisatoriske endringer og systematiske gjennomganger i henhold til rutinen.

Revisjonen kan heller ikke se at det har blitt gjennomført sikkerhetsrevisjon i form av egenkontroller i 2018. Det er imidlertid gjennomført revisjon av informasjonssikkerhet i sikker sone.

Anbefaling:

- *Revisjonen anbefaler at Stavanger kommune prioriterer en full gjennomgang av informasjonen som ligger på intranett.*

Rolle og ansvar knyttet til personvern og sikkerhet er definert i portalen for informasjonssikkerhet. Informasjonen er ikke oppdatert etter organisatoriske endringer, og er derfor noe mangelfull. Sikkerhetsansvarlig opplyser at dette vil bli oppdatert ved revidering av informasjonen som ligger på intranett. Informasjon om kommunens personvern ligger ikke i portalen for informasjonssikkerhet, men informasjonen er tilgjengelig på intranett.

Stavanger kommune har et stort fokus på tilgjengelighet av informasjon internt og eksternt. Integriteten og konfidensialitet til informasjonen blir blant annet ivaretatt via interne opplysningskampanjer om informasjonssikkerhet og personvern.

Det er ingen kontroll med at ansatte som ble ansatt før innføring av sikkerhetsregler signerer disse. Styringsgruppen for informasjonssikkerhet har vedtatt at signering av sikkerhetsregler skal gjelde alle ansatte i kommunen. I følge sikkerhetsansvarlig i Stavanger kommune er det den enkelte leder sitt ansvar å påse at alle ansatte har signert. Informasjon om sikkerhetsregler er imidlertid tilgjengelig på intranett i retningslinjer for informasjonssikkerhet. Det avholdes også nettbaserte opplysningskampanjer/kurs som inkluderer alle ansatte. I gjennomgangen av sikker sone har det heller ikke blitt avdekket avvik på signerte sikkerhetsregler de siste to årene.

Stavanger kommune øker sikkerheten på kommunens data ved å samle dem hos Green Mountain. Plassering av produksjonsdata og backup på to lokasjoner styrker sikkerheten ytterligere.

Stavanger kommune har utarbeidet ulike prosedyrer som skal sikre tilfredsstillende informasjonssikkerhet. Katastrofeplanen for IKT er fra 2015, og har ikke blitt revidert de siste årene. Det har ikke skjedd store endringer etter at planen ble innført og det er i følge kommunen ingen store endringer som burde vært fanget opp. Men IT-sjef erkjenner at de bør ha en årlig gjennomgang av planen i henhold til egne rutiner. Det er heller ikke gjennomført årlige katastrofeøvelser basert på katastrofeplanen.

Anbefaling:

- *Revisjonen anbefaler at katastrofeplanen for IT revideres årlig, og at det gjennomføres årlige katastrofeøvelser basert på katastrofeplanen.*

Stavanger kommune har etablert rutiner for håndtering og dokumentering av avvik i Synergi. Revisjonen har avdekket at IT-sjef og sikkerhetsansvarlig ikke får kopi av avvik som skyldes brudd på informasjonssikkerhet i henhold til rutinen. Per september 2018 har det blitt meldt inn 97 avvik som omhandler informasjonssikkerhet i Synergi. IT-sjef og sikkerhetsansvarlig bør jevnlig holde seg oppdatert på avvik som angår brudd på informasjonssikkerhet i Stavanger kommune. Synergi er på vei til å fases ut, og IT-sjefen håper det nye systemet vil være et bedre system for varsling og oppfølging av avvik.

I spørreundersøkelsen svarer 30 prosent[41] av respondentene at det ikke er etablert rutiner for avvik. Dette tyder på at det er behov for å presisere rutinen.

Anbefaling:

- *Revisjonen anbefaler at kommunen gjennomgår sine rutiner for avviksbehandling ved innføring av nytt avvikssystem for å sikre at IT-sjef og sikkerhetsansvarlig er informert om avvik som omhandler brudd på informasjonssikkerhet. Ved årlig gjennomgang av sikkerhetsmål og -strategi bør gjennomgang av avvik også være en del.*

ARKIVERING OG OFFENTLIGGJØRING

Rutiner for dokumentbehandling og arkivering er godt kjent blant de systemansvarlige som svarte på spørreundersøkelsen. I forhold til spørreundersøkelsen som ble sendt ut i forbindelse med forvaltningsrapport om kommunens arkiv i 2016 har antallet som svarer 4 eller bedre på i hvilken grad rutiner for dokumentbehandling og arkivering er kjent for de ansatte ved din avdeling økt med 20 prosentpoeng. Det er også en høy score på spørsmål om hva som regnes som arkivverdig materialet.

I oppfølgingen av revisjonsrapporten fra 2016 har Stavanger byarkiv iverksatt tiltak for å styrke arkivfunksjonen og bevisstheten om denne, sikre at arkivlovens bestemmelser blir etterlevd og styrke de ansattes kompetanse på arkivområdet. Spørreundersøkelsen blant de systemansvarlige viser en høy score på spørsmålet om kjennskap til dokumentbehandling og arkivering. Dette indikerer at de har lykkes med sine tiltak.

Gjennom spørreundersøkelsen kom det frem at de systemansvarlige i noe begrenset grad kjenner til innholdet i kommunens arkivplan. Arkivplanen gir en god oversikt over kommunens dokument- og arkivrutiner, og arbeidet med å forankre kjennskap til innholdet i arkivplanen hos de ansatte kan kommunen i stor grad ta tak i for å sikre at gjeldende praksis og nye rutiner i Public 360 blir integrert.

Arkivplanen henviser til den gamle arkivforskriften. I følge kommunens egne retningslinjer skal arkivplanen oppdateres med endringer i lover og forskrifter som har betydning for arkivarbeidet.

[41] N=46.

Anbefaling:

- *Revisjonen anbefaler at kommunen går igjennom og oppdaterer arkivplanen slik at den er i henhold til dagens forskrift.*

Stavanger kommune dokumenterer sine elektroniske systemer som inneholder arkivverdig informasjon i arkivplanen. Den enkelte virksomhet er ansvarlig for å ta uttrekk fra sine elektroniske systemer for langtidslagring av informasjon, men dette har ikke vært prioritert på grunn av manglende kunnskap. Stavanger byarkiv er i ferd med å bygge opp en egen eArkiv-seksjon som kan veileder virksomhetene og motta og validere slike uttrekk.

Registrering av behandlinger av personopplysninger i Draftit framstår som noe ufullstendig. Det bør gjøres en kontroll for å sikre at alle behandlinger av personopplysninger er registrert i Draftit, og at den informasjonen som er registrert på den enkelte behandling er fullstendig.

I Draftit finnes det også funksjonalitet hvor man kan angi en vurdering av risiko på hver registrering, dette er ikke lovpålagt jfr. personvernforordningen artikkel 30, men revisjonen anbefaler kommunen å ta i bruk denne funksjonaliteten i løsningen.

Anbefaling:

- *Revisjonen anbefaler at registreringer av behandlinger av personopplysninger i Draftit kontrolleres mot tidligere liste over behandlinger som krevde konsesjon og meldeplikt. Behandlingene bør også gis en overordnet risikovurdering og status.*

Gjennomgangen av offentlig journal avdekket to saker som revisjonen mener burde vært avskjermet. Den første saken gjelder en jobbsøknad som ikke var avskjermet. Grunnen til at denne søknaden ikke var avskjermet skyldes at søknaden ikke kom inn via kommunens integrasjon. Kommunen bør se på egne rutiner for arkivering av jobbsøknader som ikke kommer inn via kommunens integrasjon og sikre at disse søknadene også avskjermes på lik linje som andre søknader. Den andre saken omhandlet oppfølging av gravid arbeidstaker. Her burde navnet/arbeidsstedet til den gravide arbeidstakeren vært avskjermet i tillegg til dokumentet, på grunnlag av at graviditet er en sensitiv helseopplysning.

De fleste[42] systemansvarlig i Stavanger kommune svarer i spørreundersøkelsen at de kjenner til lovbestemmelsene som regulerer hvilke dokumenter som skal unntas offentlighet. I forhold til forvaltningsrevisjonen av kommunens arkiv i 2016 er dette en nedgang på over 20 prosentpoeng[43]. I de generelle kommentarene var det også flere som kommenterte at de var usikre på hva som skal unntas og at de manglet opplæring.

[42] 60 prosent svarte alternativ 4-6 på spørsmålet «I hvilken grad kjenner du til lovbestemmelsene som regulerer hvilke dokumenter som skal unntas fra offentlighet?» i undersøkelsen for 2018. N=48.
[43] 60 prosent svarte alternativ 4-6 på spørsmålet «I hvilken grad kjenner du til lovbestemmelsene som regulerer hvilke dokumenter som skal unntas fra offentlighet?» i undersøkelsen for 2016. N=144.

Dette kan, sammen med kontrollen av offentlig journal, tyde på at ansatte har behov for mer informasjon i forhold til hvilke dokumenter som skal unntas offentlighet.

Innsyn i hvilke personopplysninger kommune har registrert på enkeltpersoner ligger til tjenesteområdene. De fleste systemansvarlige svarer at de har rutiner for håndtering av innsyn, retting og sletting av personopplysninger i fagsystemet[44], og det kommenteres at innsynsbegjæringene håndteres på en god måte.

HACKING

Informasjonskampanjen til Stavanger kommune tyder på at de ansatte har blitt mer oppmerksomme på ulike former for IT-trusler som finnes. Det er vanskelig å forutse hvilke former for dataangrep kommunen kan bli rammet av. Det viktigste vernet for informasjonssikkerheten er derfor tekniske løsninger som kan varsle om uregelmessig bruk av IT-systemet, samt rutiner og prosedyrer. I tillegg er opplæring og informasjon ut til de ansatte viktig, da angrep ofte ikke vil få konsekvenser for kommunen så lenge den ansatte som blir utsatt for angrepet handler i tråd med fastsatte prosedyrer.

[44] 62 prosent svarte ja på spørsmålet «Har dere rutiner for håndtering av innsyn, retting og sletting av personopplysninger?». N=45.

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 og Elin Fagerheim Bjerke.

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/
- Difi's veileder om internkontroll i praksis – informasjonssikkerhet. https://internkontroll-informasikkerhet.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.
- Stavanger 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.

- Kjersti Lothe Dahl, direktør støtte og utvikling
- Roy Håland, personvernombud og sikkerhetsansvarlig
- Stein Ivar Rødland, IT-sjef
- Lars Holte, rådgiver IT
- Carl Rees Halvorsen, HR-/HMS-rådgiver i Støtte og utvikling
- Alf Magnar Thorsen, arkivsjef
- Kjetil Vagle, rådgiver Stavanger byarkiv – system og utvikling
- Kristoffer Ranaweera, rådgiver Stavanger byarkiv – system og utvikling
- Torstein Nielsen, beredskapssjef

Vedlegg 1: Spørreundersøkelse

Spørreundersøkelse - informasjonssikkerhet, drift og sårbarhet

Spørreundersøkelsen er rettet mot systemansvarlige for fagsystemer i Stavanger kommune.

1) Hvilket tjenesteområde tilhører du?

- Bymiljø og utbygging
- By- og samfunnsplanlegging
- Helse og velferd
- Oppvekst og utdanning
- Annet (stab-/støtteområde, innbygger-/samfunnskontakt)

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 Stavanger 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?						
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?			

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

15) Er det etablert rutiner for melding om uønskede hendelser, avvik eller sikkerhetsbrudd i fagsystemet?

○ Ja

○ Nei

- Vet ikke

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

- Ja
- Nei

17) Ble avviket meldt i Synergi?

- Ja
- Nei
- Annet

18) Ble håndteringen av avviket beskrevet og dokumentert?

- Ja
- Nei
- Annet

19) Har du andre kommentarer angående informasjonssikkerhet?

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

20)

21) 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 eller den nye personvernforordningen (GDPR)?						
Vet du hvem som er personvernombud i Stavanger kommune?						
Får du hjelp og veiledning av personvernombudet i kommunen dersom du har spørsmål som gjelder personopplysninger?						

22) Har du registrert behandling av personopplysninger i Draftit?

- ☐ Ja
- ☐ Delvis
- ☐ Nei
- ☐ Ikke relevant

23) 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

24) 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?	☐	☐	☐

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

26) Har du andre kommentarer angående innsyn og personopplysninger?

Del 3: Arkivering og offentliggjøring

27)

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

☐Public 360
☐Papirarkiver
☐Annet

29) Hvor ofte bruker du Public 360?

○ Daglig
○ Ukentlig
○ Sjeldnere

30) I hvilken grad

	I liten grad 1	2	3	4	5	I stor grad 6
Vet du hva som regnes som arkivverdig materiale?	☐	☐	☐	☐	☐	☐

	I liten grad 1	2	3	4	5	I stor grad 6
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?	☐	☐	☐	☐	☐	☐

31) Vet du hvor du finner arkivplanen?

- ○ Ja
- ○ Nei

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

33) 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?	☐	☐	☐	☐	☐	☐

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

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

36) 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