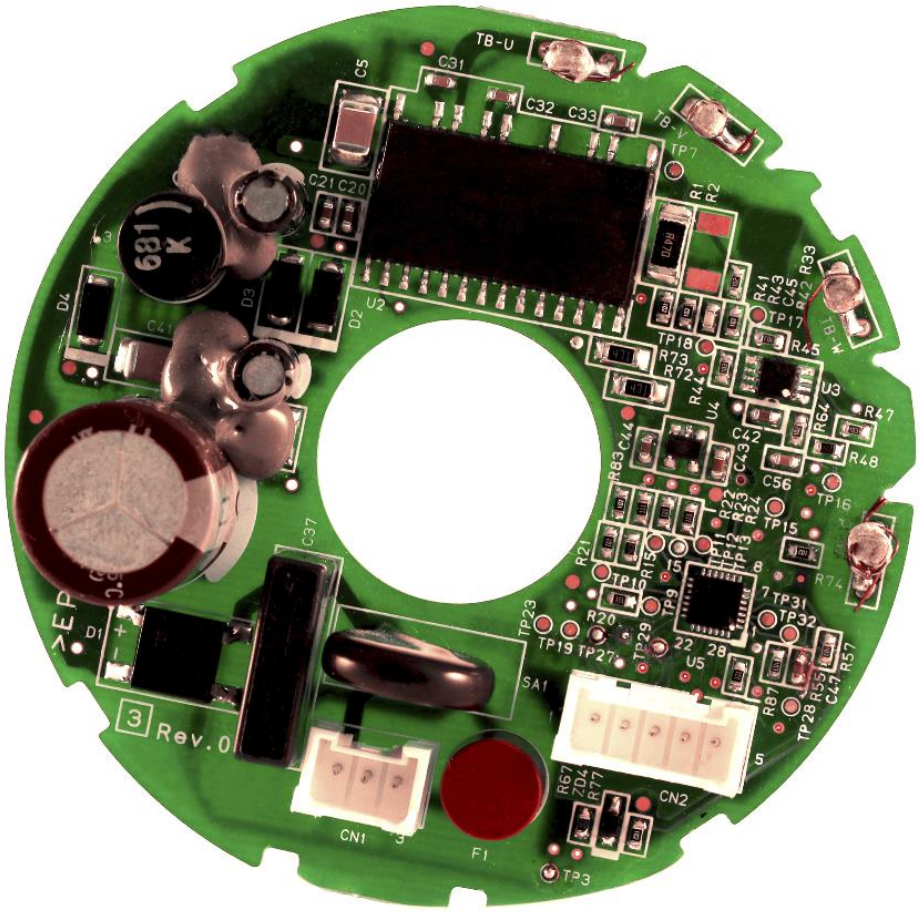
Deloitte.



Forvaltningsrevisjon | Vindafjord kommune

IKT og informasjonstryggleik

August 2018

«IKT og informasjonstryggleik»

August 2018

Rapporten er utarbeidd for
Vindafjord kommune av Deloitte AS.

Deloitte AS
Postboks 6013 Postterminalen, 5892
Bergen
tlf: 51 21 81 00
www.deloitte.no
forvaltningsrevisjon@deloitte.no

Samandrag

Deloitte har i samsvar med bestilling frå kontrollutvalet i Vindafjord kommune gjennomført ein forvaltningsrevisjon av IKT og informasjonstryggleik i Vindafjord kommune. Føremålet med forvaltningsrevisjonen har vore å undersøkje om kommunane Vindafjord og Etne har organisert si felles IKT-teneste (EVIKT) slik at den kan løyse tildelte oppgåver og etterleve sentrale føresegner. Vidare har det vore eit føremål å undersøkje om Vindafjord kommune har tilfredsstillande system og rutinar for informasjonstryggleik, og om etablerte standardar og gjeldande lover og reglar blir følgt innanfor dette området.

I prosjektgjennomføringa har revisjonen gjennomgått aktuell dokumentasjon frå Vindafjord kommune, gjort intervju med tre tilsette i kommunen, samt gjennomført ei elektronisk spørjeundersøking blant eit utval tilsette i kommunen.

Det er fastsett overordna mål for EVIKT, og både ansvaret og rolla til EVIKT er i hovudsak tydeleg definert og oppfatta. Av dei overordna måla, er det so langt berre kompetansemålet som blir vurdert som innfridd. Særleg ulikheiter i kommunane sine økonomiske rammar har gjort det utfordrande å nå målet om å standardisere driftsrutinar og fagprogram i kommunane. EVIKT har vidare tilgang på tilstrekkeleg kompetanse – anten internt eller gjennom rammeavtalar – og har i hovudsak tilstrekkeleg kapasitet til å skjøtte sine oppgåver. Brukarstøtta til EVIKT organisert på ein føremålstenleg måte med omsyn til tilgjengelegheit. Revisjonen merkar seg at det ikkje føreligg nokon operativ strategi for arbeidet til IKT-tenesta, og at EVIKT etterlyser både operative mål for arbeidet dei skal gjere, og meir langsiktig planlegging og strategisk arbeid frå eigarkommunane med omsyn til kvar dei vil med ei felles IKT-teneste.

Vindafjord kommune har gjennom arbeidet sitt med strategisk plan for informasjonstryggleik i relativt stor grad arbeidd systematisk for å sikre at kommunen er tilstrekkeleg førebudd på komande krav og føringar innan IKT-området, og då særleg knytt til ny personvernlovgiving (GDPR). Den strategiske planen for informasjonstryggleik tilfredsstilar nokre – men ikkje alle – krava til styringssystem for informasjonstryggleik. I planen blir rolle- og ansvarsdelinga knytt til informasjonstryggleik formalisert, men denne er i liten grad kjent i kommunen, og blir generelt ikkje praktisert. Fleire av rutinane for informasjonstryggleik i kommunen er vidare mangelfulle eller manglande. Revisjonen merkar seg særleg at kommunen ikkje har rutinar eller system som sikrar at oversikta over personopplysningar som blir handsama, eller at oversikta over inngåtte databehandlaravtalar, blir ajourført. Det er følgjeleg risiko både for at kommunen handsamar personopplysningar dei ikkje har oversikt over, og at eksterne leverandørar behandlar personopplysningar på vegner av kommunen utan at kommunen veit om det.

Revisjonen er merksam på at arbeidet med styringssystemet for informasjonstryggleik er pågåande, men på bakgrunn av desse svakheitene, meiner revisjonen at Vindafjord kommune ikkje har eit styringssystem for informasjonstryggleik som er i samsvar med krav i regelverket.

Undersøkinga viser at langt dei fleste respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller anna fortruleg informasjon i arbeidskvardagen. Likevel viser svara frå spørjeundersøkinga at nesten halvparten av respondentane berre delvis eller ikkje i det heile er kjende med kva oppgåver og ansvar som ligg til deira stilling med omsyn til informasjonstryggleik. Det er revisjonen si vurdering at dei tilsette i Vindafjord kommune ikkje har tilstrekkeleg kjennskap til retningsliner og rutinar for informasjonstryggleik. Kommunen bryt slik med forskriftskrav om opplæring av tilsette, og det er risiko for at kommunen som eit resultat av manglande kompetanse blant dei tilsette også bryt med andre krav i regelverket knytt til handsaming av personopplysningar, og for informasjonstryggleik i kommunen generelt.

Det er fastsett kriterium for tilgjenge i IKT-systema nytta i Vindafjord kommune. EVIKT overvakar systema som kommunen nyttar, og informerer at dei når målet om 99,5 % oppetid. Det er lite skriftleggjorte rutinar knytt til arbeidet med systemtilgjenge, og det blir ikkje utarbeidd rapportar om oppetid frå EVIKT til kommunen. Det er slik vanskeleg for kommunen å kontrollere tilgjenge og stabilitet i systema dei nyttar noko som gjer det vanskeleg for kommunen å sette i verk ev. tiltak for å betre tilgjenge og stabilitet. Ein stor del av respondentane i spørjeundersøkinga opplever jamleg problem med IKT-systema.

Revisjonen sine tilrådingar går fram i kapittel 7.

Innhald

Detaljert innhaldsliste

Figurar

Tabellar

1. Innleiing

1.1 Bakgrunn

Deloitte har gjennomført ein forvaltningsrevisjon av IKT og informasjonstryggleik i Vindafjord kommune. Prosjektet blei bestilt av kontrollutvalet i Vindafjord kommune i sak 19/17, 22.11.2017.

Bakgrunnen for forvaltningsrevisjonen er plan for forvaltningsrevisjon 2016-2020, der revisjon av IKT og informasjonstryggleik er blant dei prioriterte prosjekta. Vindafjord kommune bestilte forvaltningsrevisjonen under føresetnad om felles gjennomføring med Etne kommune. Dette blei avklart med kontrollutvalet i Etne kommune 20. november.

1.2 Føremål og problemstillingar

Føremålet med forvaltningsrevisjonen var å undersøkje om kommunane Vindafjord og Etne har organisert si felles IKT-teneste slik at den kan løyse tildelte oppgåver og etterleve sentrale føresegner. Vidare er det eit føremål å undersøkje om Vindafjord kommune har tilfredsstillande system og rutinar for informasjonstryggleik, og om etablerte standardar og gjeldande lover og reglar blir følgt innanfor dette området.

Med bakgrunn i føremålet har følgjande problemstillingar blitt undersøkt:

1. **I kva grad er IKT-tenesta for kommunane Etne og Vindafjord organisert slik at den kan løyse tildelte oppgåver og sikre at kommunane etterlever pålagde krav på IKT-området?**
   a) Har kommunen fastsett tydelege mål for IKT-tenesta?
   b) Har kommunen ein strategi for IKT-tenesta som er i samsvar med fastsette mål, krav og føringar?
   c) I kva grad er det tydeleg definert kva som er IKT-tenesta si rolle og ansvar?
   d) I kva grad har IKT-tenesta tilgang på tilstrekkeleg kapasitet og kompetanse til å ivareta sine oppgåver for begge kommunane?
   e) I kva grad blir det arbeidd systematisk for å sikre at kommunen er tilstrekkeleg førebudd på komande krav og føringar innan IKT-området?

2. **I kva grad er det etablert rutinar for å sikre systemtilgjengelegheit i IKT-systema?**
   a) Er det fastsett tydelege kriterium for tilgjenge til IKT-system?
   b) Er det etablert kontrollar for å sikre tilstrekkeleg tilgjengelegheit og stabilitet i IKT-systema?
   c) I kva grad opplever dei tilsette i kommunen at IKT-systema har tilfredsstillande driftstryggleik?
   d) Er brukarstøtta til IKT-tenesta organisert på ein føremålstenleg måte med omsyn til tilgjengelegheit?

3. **I kva grad har kommunen etablert styringssystem for informasjonstryggleik som tilfredsstillar krav i sentrale føresegner?**
   a) Er styrande dokument for informasjonstryggleik i samsvar med krav i regelverket?
   b) Er det etablert klåre rutinar og ansvarsforhold knytt til informasjonstryggleik?
   c) Har kommunen eit system for kontroll og etterprøving av informasjonstryggleik, og blir slik kontroll og etterprøving gjennomført?

4. **I kva grad har dei tilsette i kommunen tilstrekkeleg kompetanse om informasjonstryggleik?**
   a) Er det etablert rutinar for å gje tilsette i kommunen opplæring i informasjonstryggleik?
   b) I kva grad har dei tilsette i kommunen kjennskap til ev. retningsliner og rutinar for informasjonstryggleik?
   c) I kva grad blir ev. retningsliner og rutinar for informasjonstryggleik følgt?

1.3 Avgrensing

I undersøkingane av informasjonstryggleik har revisjonen primært fokusert på krav stilt til handsaming og sikring av personopplysningar. Personopplysningslova og personopplysningsforskrifta stiller strenge krav til handsaming og sikring av slike opplysningar, og ein lekkasje av denne typen informasjon kan få store konsekvensar, både for kommunen og personane som blir råka. Ein gjennomgang av rutinar på dette området vil likevel også kunne omfatte rutinar knytt til andre sensitive eller fortrulege opplysningar.

Revisjonen har ikkje gjennomført undersøkingar, testingar eller analysar av teknisk konfigurasjon, tryggingstiltak eller operative driftsrutinar.

1.4 Metode

Oppdraget er utført i samsvar med gjeldande standard for forvaltningsrevisjon (RSK 001).

Oppdraget er gjennomført i tidsrommet januar til august 2018.

1.4.1 Dokumentanalyse

Rettsreglar og kommunale vedtak har blitt gjennomgått og nytta som revisjonskriterium. Vidare har revisjonen gjennomgått Vindafjord kommune sine styringssystem for informasjonstryggleik for å kartlegge rutinar og retningslinjer, og vurdert desse opp mot krav i lovverk og standardar. Revisjonen har sett på både styrande og gjennomførande/kontrollerande dokumentasjon.

1.4.2 Intervju

Får å få supplerande informasjon til skriftlege kjelder har Deloitte intervjua utvalde personar som er involvert i IKT-arbeid og arbeidet med informasjonstryggleik. Vi har intervjua leiaren for den felles IKT-tenesta, og i Vindafjord kommune har vi i tillegg intervjua leiaren for eit nyleg avslutta informasjonstryggleiksprosjekt og systemansvarleg fagsystema innanfor pleie og omsorg. Totalt intervjua vi tre personar i samband med forvaltningsrevisjonen i Vindafjord kommune.[1]

1.4.3 Spørjeundersøking

Revisjonen har gjennomført ei elektronisk spørjeundersøking blant eit utval tilsette i Vindafjord kommune. Føremålet med spørjeundersøkinga har vore å kartleggje i kva grad dei tilsette har kjennskap til og følgjer etablerte rutinar knytt til informasjonstryggleik, å undersøkje korleis dei tilsette i kommunen opplever kompetansen og kapasiteten til brukarstøtta, samt kartleggje dei tilsette sine erfaringar med tilgjenge til IKT-systema.

Revisjonen fekk tilsendt ei oversikt over alle tilsette i kommunen, med deira e-postadresser og informasjon om kvar i kommunen dei arbeider. Eit tilfeldige utval tilsette frå alle einingane i kommunen fekk invitasjon til å svare på undersøkinga. Utvalet per eining blei vekta, slik at fleire tilsette i dei større einingane fekk invitasjon til å delta i undersøkinga. Spørjeundersøkinga blei sendt til 295 tilsette, og etter fleire påminningar, kom det til sist 115 svar.

Undersøkinga var anonymisert, slik at revisjonen ikkje veit kven som har svart. På bakgrunn av oversikta over kven undersøkinga blei sendt til, haldt saman med svara til respondentane på kor dei arbeider, er det likevel mogleg å anslå svarprosent innan dei ulike tenesteområda. Dette er presentert i tabell 1 under. Som det går fram av tabellen, varierer svarprosenten i dei respektive tenesteområda mellom 26 % (helse og omsorg) og 70 % (natur og næring). Total svarprosent var 39 %.

Tabell 1: Svarprosent

Tenesteområde	Svarprosent
Bustad og eigedom	40 %
Helse og omsorg	26 %
Kultur, idrett, fritid og reiseliv	33 %
Natur og næring	70 %
Oppvekst, skule og familie	37 %
Stab, støttefunksjonar og IKT	60 %
Totalt	**39 %**

Ei sannsynleg årsak til manglande svar i undersøkinga er at fleire av personane som fekk undersøkinga ikkje nyttar IKT-verktøy i sitt arbeid. For denne gruppa er temaet for undersøkinga mindre relevant, og i kombinasjon med at dei ikkje arbeider på kontor, kan dette forklare kvifor dei ikkje har svara. Fleire av dei

[1] Intervjuet med leiaren for IKT-tenesta var felles for dei to forvaltningsrevisjonane.

som har svara, sit på kontor og nyttar IKT-verktøy i arbeidet sitt, og for desse er undersøkinga meir aktuell. Følgjeleg er svarprosenten blant dei undersøkinga er relevant for sannsynlegvis høgare enn det som kjem fram i tabellen.

1.4.4 Verifiseringsprosessar

Oppsummering av intervju er sendt til dei som er intervjua for verifisering og det er informasjon frå dei verifiserte intervjureferata som er nytta i rapporten.

Datadelen av rapporten er verifisert av rådmannen. Mindre justeringar i datagrunnlaget er gjort basert på ny informasjon som kom fram i verifiseringa. Høyringsutkast av rapporten blei sendt til rådmannen for uttale, og rådmannen sin høyringsuttale er lagt ved rapporten (vedlegg 1).

1.5 Revisjonskriterium

Revisjonskriteria er dei krav og forventningar som forvaltningsrevisjonsobjektet skal bli vurdert opp mot. Kriteria er utleia frå autoritative kjelder i samsvar med krava i gjeldande standard for forvaltningsrevisjon.[2] I dette prosjektet er revisjonskriteria i hovudsak utleia frå personopplysningslova med forskrift, samt eForvaltningsforskrifta. Kriteria er nærare presentert innleiingsvis under kvart tema, og i vedlegg 2 til rapporten.[3]

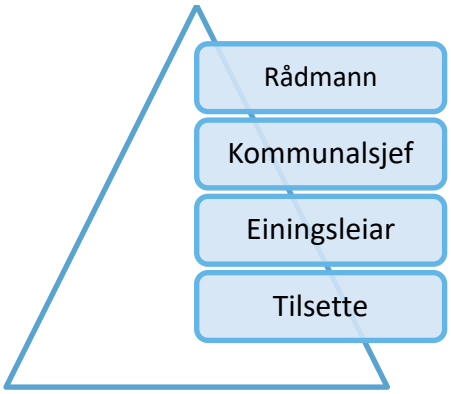
[2] RSK 001, sjå http://www.nkrf.no/rsk_001_standard_for_forvaltningsrevisjon
[3] I 2018 trer eit nytt og strengare regelverk knytt til personopplysningar i kraft (GDPR, sjå https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/).

2. Om tenesteområdet

2.1 Organisering av informasjonstryggleiksarbeidet i Vindafjord kommune

Arbeidet med informasjonstryggleik i Vindafjord kommune er formelt organisert som vist i figur 1 under. Rådmannen har det overordna ansvaret for informasjonstryggleiken i kommunen. Kommunalsjefane rapporterer til rådmannen i tryggleikssaker og er vidare ansvarlege for m.a. varetaking av informasjonstryggleiken, rett kompetanse hos einingsleiarane sine, iverksetting av kontrollar av tryggleiken i forvaltningsområda og betringsprosessar. Einingsleiarane rapporterer til sin kommunalsjef i tryggleikssaker, og er mellom anna ansvarlege for kompetanse og opplæring hos sine tilsette og at informasjonstryggleiken er varetatt og blir etterlevd i eininga. Den einskilde tilsett har ansvar for å følgje rutinar, rapportere avvik og rapportera til einingsleiar i tryggleikssaker.[4]

Figur 1: Formell ansvarsorganisering for informasjonstryggleiken i Vindafjord kommune



2.2 Interkommunalt IKT-samarbeid mellom Etne og Vindafjord kommune

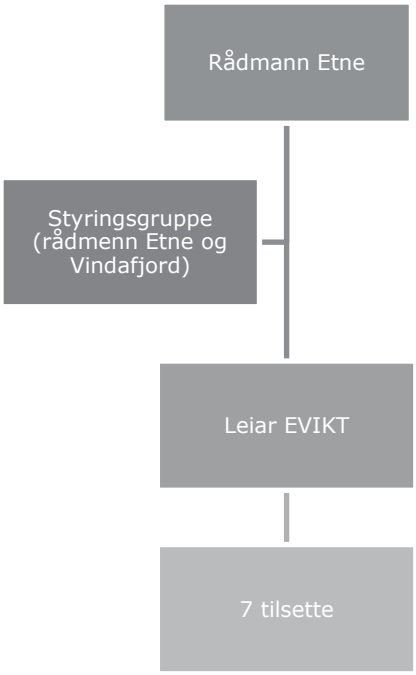
Den felles IKT-tenesta i Etne og Vindafjord kommune (EVIKT) er formelt organisert som vist i figur 2 under. Det er åtte tilsette i EVIKT, inkludert IKT-leiaren. Fire av desse i tillegg til IKT-leiaren arbeider primært med IKT-drift, og tre arbeider i hovudsak med brukarstøtte.

Begge kommunane er deltakarkommunar i samarbeidet, med Etne som vertskommune og Vindafjord som samarbeidskommune. Samarbeidet gjeld felles IKT-tenester og IKT-drift for kommunane og er regulert gjennom ei samarbeidsavtale som blei vedtatt i kommunestyra i Etne og Vindafjord kommune høvesvis 17.06.2014 og 28.10.2014. Etne kommune har ansvar for drifta av den felles IKT-tenesta, inkludert arbeidsgjevaransvar for dei tilsette i tenesta. Samarbeidsavtalen er det formelle grunnlaget for samarbeidet og for delegering av ansvar til vertskommunen. Avtala, og ev. endringar i avtala, skal vedtakast i kommunestyre i samarbeidskommunane.

Rådmennene i begge kommunane har fått delegert mynde frå kommunestyra til å treffe avgjersler som ikkje er av prinsipiell karakter. Rådmannen i Vindafjord skal vidaredelegere denne mynda til rådmannen i Etne kommune, som igjen skal delegere all mynde vidare til leiaren av EVIKT. Saker av prinsipiell art skal leggjast fram for politisk behandling i den kommune saka høyrer heime.[5]

[4] Sjå seksjon 5.4.
[5] Mynde og avgjerdsmynde etter samarbeidsavtalen mellom Vindafjord kommune og Etne kommune om Felles IKT Tenester blei overført frå 01.08.2014.

Figur 2: Formell organisering av felles IKT system i Etne og Vindafjord kommune[6]



[6] Oversikta er tilsendt i oversendingsbrev frå Etne kommune i samband med forvaltningsrevisjonen. Det kjem fram i intervju at denne organiseringa ikkje er gjeldande. Det eksisterer ikkje ei styringsgruppe slik som det er sett opp i dette organisasjonskartet.

3. Organisering av felles IKT-teneste i Etne og Vindafjord

3.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

I kva grad er IKT-tenesta for kommunane Etne og Vindafjord organisert slik at den kan løyse tildelte oppgåver og sikre at kommunane etterlever pålagde krav på IKT-området?

Under dette:

a) Har kommunen fastsett tydelege mål for IKT-tenesta?
b) Har kommunen ein strategi for IKT-tenesta som er i samsvar med fastsette mål, krav og føringar?
c) I kva grad er det tydeleg definert kva som er IKT-tenesta si rolle og ansvar?
d) I kva grad har IKT-tenesta tilgang på tilstrekkeleg kapasitet og kompetanse til å ivareta sine oppgåver for begge kommunane?
e) I kva grad blir det arbeidd systematisk for å sikre at kommunen er tilstrekkeleg førebudd på komande krav og føringar innan IKT-området?

3.2 Revisjonskriterium

Kommunal- og moderniseringsdepartementet sendte i september 2017 ut brevet *Digitalisering i kommunal sektor* til alle ordførarar og rådmenn. I brevet blir dei viktigaste nye tiltaka med relevans for den kommunale sektor i den statlege digitaliseringspolitikken gjennomgått.[7] Brevet viser også til *Digitaliseringsrundskrivet*, som er ei samanstilling av pålegg og anbefalingar knytt til digitalisering av offentleg sektor. *Digitaliseringsrundskrivet* har blitt sendt ut kvart år sidan 2009, og blei for fyrste gong sendt til kommunane i 2016. Rundskrivet trekk fram ei rekkje krav som er heimla i lov, og som difor også gjeld kommunane. Vidare oppmodar departementet kommunane til å gjere seg kjende med krava som blir stilt til dei statlege verksemdene og vurdere om nokon av desse anbefalingane er relevante for kommunen sitt digitaliseringsarbeid.

COBIT 5 er eit internasjonalt anerkjend rammeverk for styring av IKT-funksjonen i verksemder, utvikla av organisasjonen ISACA.[8] Rammeverket tek utgangspunkt i at IKT-funksjonen på ein effektiv og god måte skal underbyggje og bidra til at verksemda oppnår sine overordna mål. Med bakgrunn i dette har ein identifisert og definert ei rekkje mål og prosessar for IKT-funksjonen. Eksempelvis seier rammeverket at dersom det er eit overordna mål for verksemda å etterleve lovar og reguleringar må ein mellom anna sette følgjande mål for IKT-funksjonen:

- IKT-funksjonen skal sjølv etterleve, og hjelpe verksemda elles i å etterleve, lovkrav og reguleringar.
- IKT-funksjonen skal oppretthalde sikkerhet i informasjon, infrastruktur og applikasjonar.
- IKT-funksjonen skal handsame IKT-relatert risiko.
- IKT-funksjonen skal levere tenester i samsvar med verksemda sine behov.
- IKT-funksjonen skal ha påliteleg og nyttig informasjon til å fatte avgjersler.
- IKT-funksjonen skal etterleve interne retningsliner.

Vidare identifiserer rammeverket ei rekkje prosessar som verksemder kan implementere for å bidra til at desse måla blir nådd.

Sjå vedlegg 2 for utfyllande revisjonskriterium.

[7] *Meld. St. 27 (2015-2016) Digital agenda for Norge* gjev eit oversyn over regjeringa sin digitaliseringspolitikk.
[8] ISACA er ein internasjonal foreining som fokuserer på styring og kontroll innanfor IKT-sektoren.

3.3 Mål og strategi for IKT-tenesta

3.3.1 Datagrunnlag

Både i den overordna samarbeidsavtalen om felles IKT-system for Vindafjord og Etne kommune,[9] og i tenesteleveringsavtalen som regulerer tenestytinga i samarbeidet,[10] er det definerte mål for EVIKT. I den overordna avtalen er føremålet med samarbeidet definert som følgjer:

> Gjennom sentraliserte og standardiserte løysingar, krav til informasjonstryggleik, auka kompetanse og auka moglegheit for spesialisering, skal det etablerast effektiv drift med gode system for innmelding av brukarproblem og fokus på gevinstrealisering

Også standardisering av materiell og system er skildra som sentrale faktorar i arbeidet for å oppnå denne vinsten, sjølv om det òg blir peika på i avtalen at kommunane sine skilnader og ulike behov skal vurderast i dette standardiseringsarbeidet.

Tenesteleveringsavtalen skildrar føremålet med samarbeidet for EVIKT med tilvising til den overordna samarbeidsavtala, og målet vidare som:

> å fremme kommunenes tjenesteproduksjon gjennom målrettet bruk av informasjons- og kommunikasjonsteknologi, samt ivareta drift, service og utviklingsoppgaver.[11]

Eit mål for Vindafjord kommune med etableringa av EVIKT, var å betre kompetansemiljøet innan IKT, og å satse på utvikling av velferdsteknologi. Det går fram av intervjua at kommunen og EVIKT er nøgde med kompetansevinsten som er realisert gjennom samanslåinga. Vidare er EVIKT med i gruppa som arbeider med å føreslå og prøve ut ny velferdsteknologi, og EVIKT har òg deltatt i arbeidsgruppa som har utarbeidd den strategiske planen for informasjonstryggleik.

Leiaren for EVIKT opplever ikkje at det er sett klare operative mål for kva kommunane ønskjer å oppnå med EVIKT. Han etterlyser meir involvering frå rådmennene, og meiner at det er kommuneorganisasjonane sjølve som må ta styringa for kvar dei vil med den felles IKT-tenesta.

Han opplyser vidare at EVIKT har blitt ein rein driftsorganisasjon etter samanslåinga av IT-avdelingane i dei to kommunane, og at det er lite fokus frå kommunane knytt til langsiktig planlegging og strategisk arbeid med omsyn til EVIKT og arbeidet dei gjer.

Revisjonen har ikkje fått tilsendt nokon skriftleg strategi for arbeidet til EVIKT. Det næraste til ein strategi for EVIKT som revisjonen har fått tilsendt, er dei tre overordna fasane meint å styre utvikling av samarbeidet som skildra i samarbeidsavtala. I første fase er det fokus på etablering av ei felles personalgruppe og felles driftsorganisasjon, samt etablering av hovudkontoret og felles vaktordning for kommunane. Anna fase skal ha fokus på gjennomgang og standardisering av driftsrutinar og fagprogram, samt realisering av vinsten ved samanslåinga, medan ein i tredje fase skal vurdere, ut frå kriterium om m.a. datatryggleik og vinst, ei ev. etablering av eit felles dataserverrom.[12]

I intervju går det fram at første fase er ferdigstilt, medan dei neste to fasane er utfordrande å gjennomføre grunna til dels stor forskjell i driftsbudsjetta til dei to kommunane. Desse budsjettforskjellane gjer det vanskeleg å samordne val av IKT-system, noko som fører til lite samdrift av systema. Ei vidare utfordring knytt til ulikskap er at det er gjort investeringar for å betre situasjonen i Vindafjord kommune, noko som ikkje har vore mogelege i Etne kommune grunna økonomi. Dette fører til at kommunane ikkje får tatt ut alle vinstane ved den felles IKT-tenesta slik det var førespegla.[13]

---

[9] Overordna samarbeidsavtale mellom Vindafjord kommune og Etne kommune om Felles IKT Tenester (EVIKT). Eksemplara av avtalen som er tilsendt revisjonen frå begge samarbeidskommunane er ikkje datert eller signert, men det framkjem at avtalen er gjeldande frå 01.08.2014.

[10] TLA Tjeneste Leverings Avtale mellom Etne og Vindafjord IKT (EVIKT) og Etne og Vindafjord kommune. Dokumentet revisjonen har mottatt frå Vindafjord kommune er ikkje datert eller signert.

[11] Kommunen opplyser at tenesteleveringsavtalen er ein «kopi» av ein annan avtale, og vidare at det er eit arbeidsdokument som ikkje er vedtatt i kommunane.

[12] Jf. samarbeidsavtala, skal samarbeidet evaluerast 1 år etter samlokalisering av driftsorganisasjonen. Kommunen opplyser at dette so langt ikkje er gjort, men at det skal gjerast hausten 2018 i samband med ei politisk sak der kommunen skal ta stilling til om ein vil knytte seg til felles IKT-avdeling for heile Haugalandet, eller om ein vil fortsetje som no.

[13] Leiaren for EVIKT fortel i intervju at budsjettet er tredelt, med ein del for felles oppgåver, ein for drift av Etne kommune sine system, og ein for drift av Vindafjord sine system. Dei to kommunane er dermed ulike organisasjonar når det gjeld drift og system.

3.3.2 Vurdering

Revisjonen finn i sine undersøkingar at det føreligg overordna, skriftlege mål for EVIKT, men at det ikkje føreligg nokon styrande strategi for arbeidet til den felles IKT-tenesta.

Dei overordna måla er berre i nokon grad nådd. Av dei definerte måla, er det so langt berre kompetansemålet kommunen vurderer som innfridd. Frå intervju blir manglande målinnfriing dels forklart med manglande engasjement og involvering frå kommunane i EVIKT sitt arbeid, og dels med ulikheiter i kommunane sine økonomiske rammar. Sistnemnde har gjort det særleg utfordrande å nå målet om å standardisere driftsrutinar og fagprogram i kommunane.

Revisjonen merkar seg at EVIKT etterlyser operative mål for arbeidet dei skal gjere, og meir langsiktig planlegging og strategisk arbeid frå eigarkommunane med omsyn til kvar dei vil med ei felles IKT-teneste.

Revisjonen meiner manglande operative mål for tenesta aukar risikoen for at det ikkje er tilstrekkeleg tydeleg for dei involverte kva prioriteringar som bør gjerast på IKT-området. At det heller ikkje er nedfelt nokon strategi for EVIKT, medfører auka risiko for at det blir tatt avgjersler utan tilstrekkeleg konsekvensvurdering, noko som kan ha både uheldige og ikkje-planlagde utfall.

3.4 IKT-tenesta si rolle og ansvar

3.4.1 Datagrunnlag

I avtalane som regulerer IKT-samarbeidet mellom Vindafjord og Etne, er EVIKT si rolle og ansvar skildra. Mellom anna går det fram der at EVIKT skal vere organisert som eiga eining med IKT-leiar som einingsleiar, organisatorisk underliggjande rådmannen i Etne kommune.

Rådmennene i begge kommunane er EVIKT sine myndeorgan, og har høve til å vedta endringar i både tenestenivå, rollefordeling og ansvarsforhold. Jf. tenesteleveringsavtalen skal det i begge kommunane bli oppretta eit felles IKT-råd. Dette IKT-rådet er meint å fungere som ein samhandlingsarena for koordinering mellom deltakarkommunane og EVIKT. Det skal òg ha ein rådgivande funksjon overfor EVIKT-leiaren. Revisjonen har ikkje mottatt dokumentasjon eller opplysningar på at det er oppretta IKT-råd har i kommunane.

Det skal vere faste møtepunkt mellom rådmennene og EVIKT. I intervju kjem det fram at slike faste møtepunkt ikkje er etablert. Det er etablert faste møtepunkt mellom EVIKT og mellom anna IKT i skulane og i teknisk eining.

Oppgåvene som ligg til EVIKT er skildra punktvis i tenesteleveringsavtala; her går det mellom anna fram at EVIKT er databehandlar og at rådmennene i dei to kommunane er behandlingsansvarlege, jf. personopplysningslova mv.[14] Vidare i tenesteleveringsavtalen er ansvarsdelinga mellom systemansvarleg for fagsystema og EVIKT spesifisert, og det går fram kva ansvar EVIKT har med omsyn til datatryggleik. Det er òg skildra kva tenester EVIKT skal syte for at brukarane har tilgang til, som t.d. nettverk, sentral fillagring, printere, og tilgang til høvesvis intern sone og sikker sone. Det er også lista opp ei rekkje oppgåver som ligg til EVIKT med omsyn til praktisk tryggleiksarbeid (backup, antivirus, e-postvasking, mv.). Tenesteleveringsavtalen pålegg også EVIKT å drive driftsstøtte via telefon, web og e-post.[15]

Frå intervju kjem det fram at det opphaveleg ikkje var heilt avklart kva rolle, ansvar og mynde EVIKT skulle ha ovanfor kommunane. Dette har betra seg den seinare tida, og leiaren for EVIKT opplever at det i dag er tydeleg og klart kva rolle og ansvar EVIKT har; bestillinga frå kommunane med omsyn til kva tenester EVIKT skal levere er t.d. i avklart, og den interne ansvarsdelinga i EVIKT er også stort sett tydeleg.

3.4.2 Vurdering

Revisjonen finn i sine undersøkingar at EVIKT si rolle og ansvar er formalisert i avtaleverket som regulerer samarbeidet, at rolla og ansvaret til EVIKT i dag blir opplevd som tydeleg og avklart, og i hovudsak praktisert som skildra.

Revisjonen merkar seg likevel at enkelte av samarbeidsorgana og møtepunkta som skulle vore etablert, ref. dei styrande dokumenta for EVIKT, ikkje er det. Manglande eller mangelfulle møtepunkt og

[14] Også i Vindafjord kommune sin nyleg utarbeida strategisk plan for informasjonstryggeik, går informasjonstryggleiksansvaret til EVIKT fram. Dei ulike ansvarsrollane knytt til informasjonstryggleik i Vindafjord kommune blir skildra i avsnitt 5.4.1.
[15] Dette arbeidet er nærare skildra i avsnitt 4.6.1.

samarbeidsorgan mellom EVIKT på den eine sida og leiinga og brukargrupper i kommunane på den andre, kan redusere kvaliteten og frekvensen på kommunikasjonen mellom dei involverte aktørane, noko som aukar sannsynet både for at det dannar seg ulikheiter med omsyn til forventningar og ulike rolle- og ansvarsforståingar. Ei slik utvikling gjev vidare auka risiko for ytterlegare redusert samarbeidsklima mellom dei involverte aktørane og generell misnøye.

Overordna er det likevel revisjonen si vurdering at det i hovudsak er tydeleg definert kva som er EVIKT si rolle og ansvar, samtidig som det bør noterast at det hadde vore eit føremon om det blei etablert samarbeidsorgan og møtepunkt for dei involverte aktørane slik som planlagd.

3.5 IKT-tenesta si tilgang på kompetanse og kapasitet

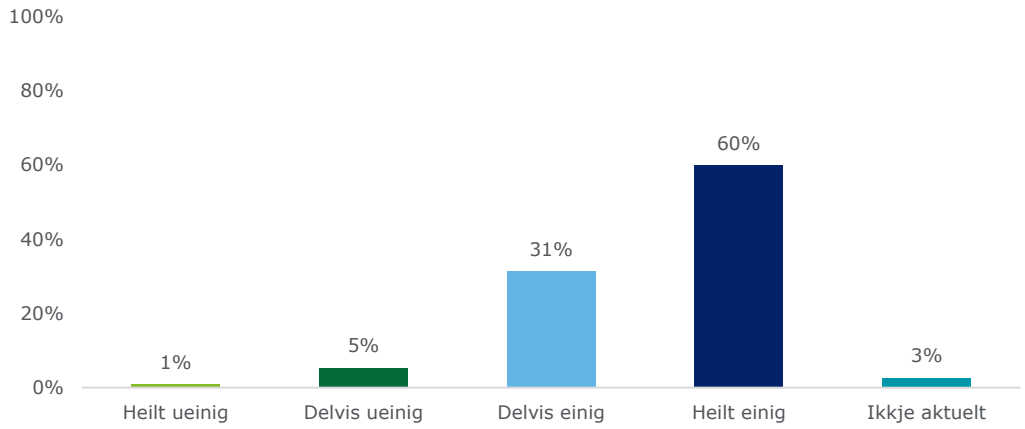
3.5.1 Datagrunnlag

EVIKT har i dag er åtte tilsette med variert erfaring og bakgrunn.[16] Leiaren for EVIKT meiner at dei tilsette i EVIKT har mykje og god kunnskap og erfaring.

Med omsyn til opplæring og kompetanseheving for dei tilsette i EVIKT, kjem det fram i intervju at fleire av dei får tilbod om kurs innan sentrale område for EVIKT kvart år.[17] Vindafjord kommune er elles med KInS,[18] og både leiaren og tilsette i EVIKT har deltatt på seminar og kurs der. Det føreligg ingen formell opplæringsplan for EVIKT.

I spørjeundersøkinga blei respondentane bedne om å seie seg einig eller ueinig i påstanden om at *når eg kontaktar IKT-tenesta får eg god hjelp.* Som det går fram av resultata presentert i tabell 2, seier 60 % av respondentane frå Vindafjord kommune seg «heilt einige» i påstanden, 31 % «delvis einig», og til saman 6 % er «delvis ueinig» eller «heilt ueinige».[19]

Tabell 2: Når eg kontaktar IKT-tenesta får eg god hjelp (N=112)



I intervju kjem det fram at områda der det kan oppstå utfordringar med omsyn til kompetanse i EVIKT, er i hovudsak knytt til ny teknologi som ein ikkje har nytta før. EVIKT-leiaren fortel at dei i slike situasjonar har tilgang til ekstern kompetanse gjennom rammeavtalar med IKT-konsulentar. Også på telefoniområdet leiger dei inn eksterne konsulentar. EVIKT har eigne midlar til å leige inn ekstern kompetanse, men kor mykje av desse midlane dei nyttar varierer frå år til år.

Leiaren for EVIKT fortel i intervju at det so langt ikkje har vore dømer på at den felles IKT-avdelinga ikkje har klart å løyse tildelte oppgåver. Det blir likevel òg peika på at EVIKT har relativt får tilsette, og at dette kan by på utfordringar, t.d. i prosjekt som involverer ny teknologi og som går parallelt i begge kommunane.

[16] Utdanninga er som følgjer: fem med bachelorgrad i IKT, ein med mastergrad i IKT, ein fagarbeidar og ein lærling.
[17] Til dømes innanfor Microsoft- eller Cisco-system.
[18] Foreininga Kommunal informasjonssikkerhet.
[19] Meir om brukarane si oppleving av brukarstøtta under avsnitt 4.5

3.5.2 Vurdering

Funna frå undersøkingane tyder på at EVIKT i hovudsak har tilgang på tilstrekkeleg kompetanse til å ivareta sine primære oppgåver knytt til brukarstøtte og drift av IKT-systema, og at EVIKT gjennom rammeavtalar har tilgang på ekstern ekspertise når det oppstår særlege kompetansebehov.

Funna frå undersøkingane tyder vidare på at EVIKT jamt over har tilstrekkeleg kapasitet, samtidig som revisjonen merkar seg at det i undersøkingane kjem fram at EVIKT på dette området er noko meir sårbar, t.d. i situasjonar der ny teknologi skal implementerast i begge eigarkommunane samtidig.

3.6 Systematisk arbeid for å førebu IKT-tenesta på komande krav og føringar

3.6.1 Datagrunnlag

Vindafjord kommune har pågåande fleire prosjekt knytt til komande krav og føringar på IKT-området. Mellom anna er det nedsett ei gruppe som arbeider med ny velferdsteknologi, der også EVIKT deltek. Vidare har kommunen nyleg avslutta eit prosjekt knytt til komande krav i høve ny personvernslov. Arbeidsgruppa har utarbeidd ein strategisk plan for informasjonstryggleik i kommunen. EVIKT har vore representert i denne arbeidsgruppa ved både leiar og ein tilsett.

Revisjonen har fått ettersendt det endelege planutkastet for ny strategi for informasjonstryggleik.[20] Her går det fram at kommunen skal opprette eit personvernombod, etablere eit utval for informasjonstryggleik, og innføre nye rutinar og kontrollsystem for å sikre informasjonstryggleiken i kommunen. Planen med tilhøyrande vedlegg blei godkjent av rådmannen i mars 2018, og har vore gjeldande sidan då.

Jf. planen er ansvaret for oppfølging av EU sin personvernforordning, The General Data Protection Regulation (GDPR), lagt til utvalet for informasjonstryggleik. Utvalet blei oppretta i mai 2018.

Prosjektleiar for arbeidsgruppa fortel i intervju at han har hatt mykje kontakt med rådmannen i samband med utarbeidinga av strategisk plan for informasjonstryggleik, og at det i arbeidet har blitt trekt opp klare ansvarsliner frå rådmannen til tilsette.

Rådmannen oppnemnde i juni 2018 eit personvernombod i kommunen.[21]

3.6.2 Vurdering

Revisjonen finn i sine undersøkingar at Vindafjord kommune førebur seg på komande krav og føringar innan IKT-området. Særleg sentralt er informasjonstryggleiksprosjektet som kommunen ferdigstilte tidleg i 2018, der dei gjennom ein strategisk plan for informasjonstryggleik har lagt planar for korleis å organiserer seg på ein måte som gjer at kommunen kan etterleve komande krav og føringar knytt til GDPR.

Det er revisjonen si overordna vurdering at Vindafjord kommune i relativt stor grad har arbeidd systematisk for å sikre at kommunen er tilstrekkeleg førebudd på komande krav og føringar innan IKT-området.

[20] Revisjonen fekk tilsendt endeleg utkast av strategisk plan for informasjonstryggleik for Vindafjord kommune 1. mars 2018

[21] Dette kom fram i samband med verifiseringsprosessen av rapporten. Sjå elles kapittel 5 og særleg seksjon 5.3.

4. Rutinar for systemtilgjengelegheit

4.1 Problemstilling

I dette kapittelet vil revisjonen svare på følgjande problemstilling med tilhøyrande underproblemstillingar:

I kva grad er det etablert rutinar for å sikre systemtilgjengelegheit i IKT-systema?

a) Er det fastsett tydelege kriterium for tilgjenge til IKT-system?
b) Er det etablert kontrollar for å sikre tilstrekkeleg tilgjengelegheit og stabilitet i IKT-systema?
c) I kva grad opplever dei tilsette i kommunen at IKT-systema har tilfredsstillande driftstryggleik?
d) Er brukarstøtta til IKT-tenesta organisert på ein føremålstenleg måte med omsyn til tilgjengelegheit?

4.2 Revisjonskriterium

Personopplysningslova § 13 stiller krav om at kommunen som behandlingsansvarleg av personopplysningar gjennom planlagde og systematiske tiltak skal syte for tilfredsstilande informasjonstryggleik, mellom anna med omsyn til *tilgjengelegheit*. POF § 2-12 stillar vidare krav om sikring av tilgjengelegheit, og i fyrste ledd av paragrafen kan ein lese at det «skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig».

Dette betyr at kommunen er forplikta til å ha system og rutinar som sikrar at informasjon er tilgjengeleg for dei som treng det, når dei treng det. Frå dette følgjer det at kommunen må syte for at systema der informasjonen lagrast, er tilgjengelege for dei som treng tilgang til den. Det er slik ikkje berre informasjonen som må sikrast med omsyn til tilgjengelegheit; også informasjonssystema må vere tilgjengeleg for at informasjonen kan vere det. For å sikre tilstrekkeleg systemtilgjengelegheit, er POF § 2-4 andre ledd om kriterium for akseptabel risiko forbundet med handsaming av personopplysningar relevant. Vidare stiller ISO27001:2013 kapittel 9 krav om overvaking av informasjonstryggleik for å kunne måle og evaluere og utbetre informasjonstryggleiksystemet.

Sjå vedlegg 2 for fullstendige revisjonskriterium.

4.3 Kriterium for tilgjengelegheit

4.3.1 Datagrunnlag

I Vindafjord kommune sin plan for informasjonstryggleik går det fram mål for systemtilgjenge. Der står det mellom anna at kommunen skal «sikre tilgjenge til opplysningane slik at dei med tenesteheimel kan bruke opplysningane når dei treng dei». Vidare blir det stilt krav til at kommunen skal utarbeide beredskapsplanar med mål om kortast mogeleg brot på tekniske system, og rutinar og retningsliner for praksis ved utilsikta stans i informasjonssystema. Revisjonen har ikkje fått tilsendt dokumentasjon på at det er utarbeidd slike beredskapsplanar.

Det er EVIKT som har ansvaret for datatryggleiken i Vindafjord. I tillegg til å sikre sentralt lagra data ved hjelp at backupløysingar, skal EVIKT også gjennomføre faste tryggleikskontrollar knytt til t.d. antivirus, innhaldskontroll og e-postvasking. I intervju fortel EVIKT-leiaren at dei tar utgangspunkt i malar frå Datatilsynet, og gjer det dei kan for å gjennomføre dei tryggingstiltaka dei meiner er nødvendige, t.d. knytt til brannmurar, soneoppdeling og e-postvasking. EVIKT involverer også leverandørar av IKT-system i å få til mest mogeleg sikre løysingar for kommunane.[22]

EVIKT har eigne internsider der mellom anna rutineskildringane for oppgåvene som skal gjerast kan leggjast inn. På tidspunktet rapporten blei skrive, var fire av 11 relevante rutinekategoriar tomme. Fleire av dei resterande kategoriane hadde korte og til dels ufullstendige rutineskildringar.

EVIKT-leiaren er i intervju open på at det er rom for betring når det gjeld skriftleggjering av rutinar i EVIKT. Med omsyn til rutinar for systemtilgjenge, blir det kommentert i intervju at EVIKT har lite formaliserte og skriftleggjorte rutinar.

[22] I vedlegget til strategisk plan for informasjonstryggleik er det lagt inn rutine for korleis EVIKT skal jobbe med tryggleikskopiering.

Kriterium for systemtilgjenge i EVIKT

I tenesteleveringsavtalen mellom EVIKT og kommunane Etne og Vindafjord går det fram fagsystema i kommunane normalt sett skal vere tilgjengeleg kontinuerleg. Vidare går det fram at EVIKT – med nokre unntak – skal levere ei oppetid på i IKT-systema på 99,5 %.[23]

I intervju blir det opplyst at EVIKT har system for å gjere risikovurderingar knytt til endringar i IKT-systema.[24] I desse vurderingane identifiserer EVIKT kva risikoen er for at ei endring vil ha påverknad på drifta av IKT-systema, og t.d. kor mange brukarar som vil som blir påverka, kor lang nedetida ev. kan bli, osb.

Leiaren for EVIKT fortel i intervju at det er lite ikkje-planlagt nedetid i kommunane sine IKT-system. Dette blir stadfesta i andre intervju.

4.3.2 Vurdering

Det er fastsett kriterium for tilgjenge i systema EVIKT drifter, og det er slik sett kriterium for tilgjenge i IKT-system som Vindafjord kommune nyttar. Vidare finn revisjonen i sine undersøkingar at EVIKT har system for å gjennomføre risikovurderingar knytt til IKT-systema.

Revisjonen registrerer at fleire av EVIKT sine rutineskildringar manglar eller er mangelfulle, og at det i intervju blir peika på at EVIKT har lite skriftleggjorte og formaliserte rutinar knytt til arbeidet med systemtilgjenge.

Overordna er det revisjonen si vurdering at det er fastsett tydelege kriterium for tilgjenge i IKT-systema nytta i Vindafjord kommune, men at kommunen med fordel kan gjere tiltak for å sikre auka skriftleggjering og formalisering av rutinane knytt til systemtilgjenge.

4.4 Kontrollar av tilgjengelegheit og stabilitet i IKT-systema

4.4.1 Datagrunnlag

EVIKT har verktøy som kontinuerlig overvaker oppetida i IKT-systema, og EVIKT-leiaren seier at dei når målet opp ei oppetid på 99,5 %, jf. tenesteleveringsavtalen.

Overvakingsverktøyet kan produsere rapportar for oppetid i nettverket om det skulle bli etterspurt. Kommunane har ikkje etterspurt tal knytt til dette, og EVIKT har ikkje rutinar for å hente ut slike rapportar.

4.4.2 Vurdering

EVIKT overvakar systematisk oppetida på nettverket dei driftar, og det er slik etablert kontrollar for å sikre tilgjenge og stabilitet i IKT-systema som Vindafjord kommune nyttar.

Revisjonen merkar seg at det ikkje er sett krav om rapportering på nedetid i avtalane som styrar arbeidet til EVIKT, og at EVIKT ikkje rapporterer på dette til kommunen. Manglande rapportering om nedetid gjer det vanskeleg for Vindafjord kommune å kontrollere tilgjenge og stabilitet i IKT-systema dei nyttar på ein systematisk måte, noko som gjer det vanskeleg for kommunen å få sett i gang ev. tiltak for å betre tilgjenge og stabilitet i IKT-systema.

4.5 Oppleving av driftstryggleik i IKT-systema

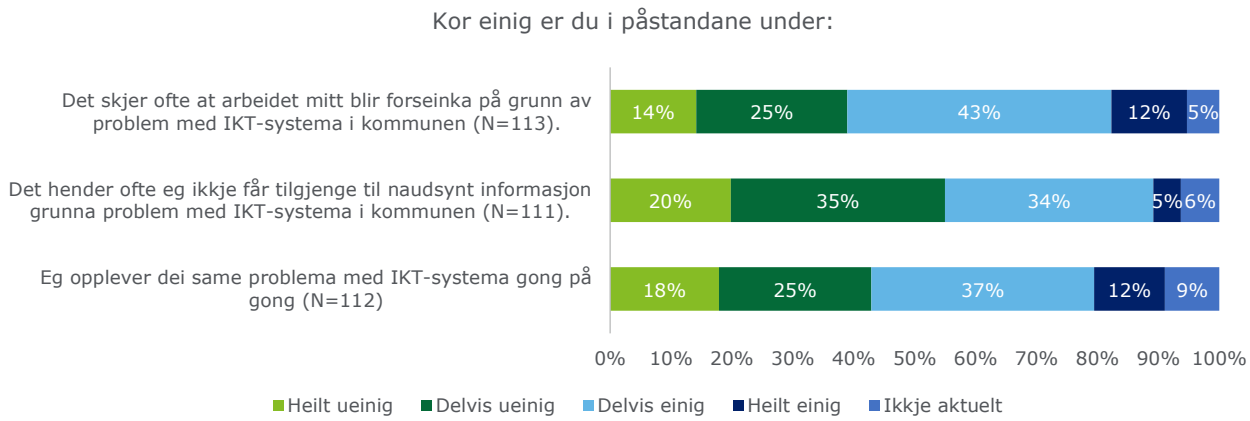
4.5.1 Datagrunnlag

Revisjonen nytta spørjeundersøkinga til å kartleggje i kva grad dei tilsette i kommunen opplever at IKT-systema har tilfredsstillande driftstryggleik. Svara er presentert grafisk i figur 3 under.

Som det går fram av figuren, opplever nesten halvparten av respondentane dei same problema med IKT-systema gong på gong; litt over ein tredel av dei spurte opplever ofte at dei ofte ikkje får tilgang til naudsynt informasjon på grunn av problem med IKT-systema i kommunen; og over halvparten av respondentane opplever ofte at arbeidet blir forseinka på grunn av problem med IKT-systema i kommunen.

[23] Unnataka er knytt t.d. knytt til brukarrelaterte feil, programfeil i fagsystema, o.l.
[24] Eit sokalla *change management system*.

Figur 3: Driftstryggleik i IKT-systema



Respondentane fekk også høve til å spesifisere om lag kor ofte dei opplever å blir forseinka i arbeidet sitt, og kor ofte dei ikkje får tilgang til naudsynt informasjon, på grunn av problem med IKT-systema. 20 % svara at dei vekentleg blir forseinka i arbeidet sitt grunna problem med IKT-systema i kommunen, medan over ein fjerdedel svara at dei månadleg opplever å ikkje få tilgjenge til naudsynt informasjon grunna problem med IKT-systema.

Vidare fekk respondentane høve til å kome med utfyllande kommentarar knytt til driftstryggleiken i IKT-systema. Av svara som kom inn, var det fleire som peika på at det stadig er problem med skrivarane i kommunen, og nokre som opplevde gjentakande utfordringar knytt til oppdateringar.

4.5.2 Vurdering

Ein stor del av respondentane i spørjeundersøkinga opplever jamlege problem med IKT-systema, får ofte ikkje tilgang til naudsynt informasjon grunna slike problem, og blir ofte forseinka i arbeidet sitt på grunn av problem med IKT-systema. Det er difor revisjonen si vurdering at dei tilsette i Vindafjord kommunen ikkje i tilstrekkeleg grad opplever tilfredsstillande drifstryggleik i kommunen sine IKT-system.

4.6 Organisering av IKT-brukarstøtte

4.6.1 Datagrunnlag

I tenesteleveringsavtalen er brukarstøtteoppgåvene til EVIKT spesifisert. Her går det fram at brukarstøtta skal vere bemanna måndag til fredag frå kl. 08:00 til kl. 15:30, og at alle feil på IKT systemet skal meldast til brukarstøtta, enten på telefon, EVIKT webapplikasjon eller per e-post. Det er fastsett svarfristar for førespurnader som kjem inn via webapplikasjon og e-post (sju arbeidstimar) og via telefon (fortløpande). Oppdatert kontaktinformasjon om brukarstøtta skal vere tilgjengeleg på EVIKT og kommunane sine respektive intranett. I intervju blir det stadfesta at brukarstøtta er organisert som skildra i avtalen.

I tillegg til den regulære brukarstøtta, har EVIKT ei vaktordning som omfattar system som omhandlar «liv og helse», i tillegg til andre system som har behov for, og forventningar om, høg oppetid. Vaktordninga skal nyttast ved kritiske feil og avbrot, og er bemanna måndag til fredag frå kl. 15:30 til kl. 22:00, laurdag frå kl. 10:00 til kl. 18:00 og søndag mellom kl. 14:00 og kl. 21:30. Vaktordninga er tilgjengeleg via telefon, og vaktnummeret er distribuert til einingane som er omfatta av ordninga. Leirane for EVIKT opplyser at vakttelefonen er døgnopen. Han fortel vidare at det før etableringa av EVIKT berre var Vindafjord kommune som hadde ein slik vakttelefon. Bemanninga av vaktordninga går på rullering mellom eit utval tilsette i EVIKT med nødvendig kompetanse.

EVIKT-leiaren fortel at det tidlegare i stor grad var legevakta som nytta ordninga med vakttelefonen, men at dei no nyttar vaktordringa mindre etter at systemet deira har blitt meir stabilt. Elles er det ofte utfordringar knytt til heimekontor som utløysar bruk av vakttelefonen, og då særleg frå tilsette som jobbar på ukurante tidspunkt – t.d. barnevernet – som har behov for brukarstøtte utanfor ordinær arbeidstid.

I intervju med systemansvarleg for helsefagsystemet i Vindafjord kommune, blir det opplyst at ordninga med vakttelefon har fungert godt, men at det er varierande praksis innan pleie- og omsorgseiningane når det gjeld kven dei kontaktar etter ordinær arbeidstid. Ho fortel at dei sjeldnare ringer direkte til henne no enn før når det er utfordringar med fagsystema eller PC-ar utanom ordinær arbeidstid, men ho har ikkje

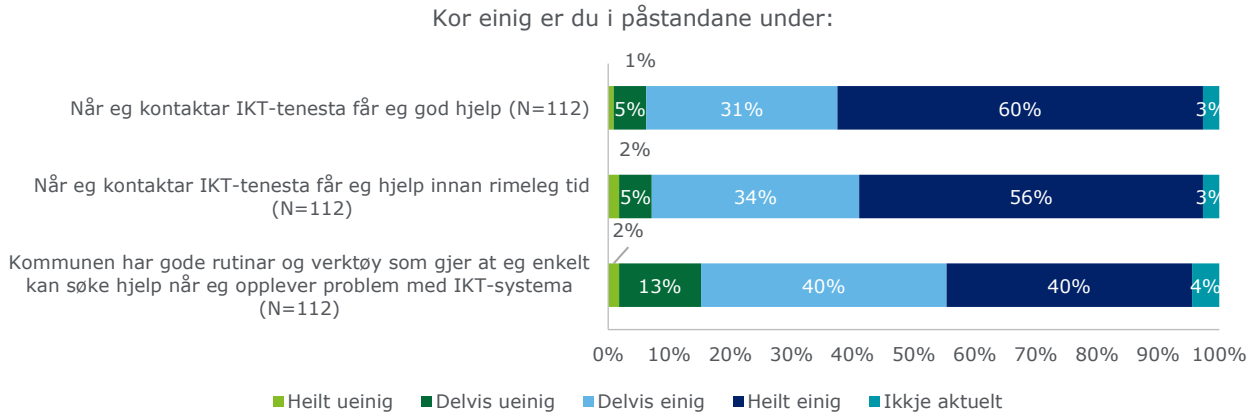
kjennskap til om dette er på grunn av at dei tilsette ringer vakttelefonen i staden. På tidspunkta når vakttelefonen er stengt, har det skjedd at ho har ringt direkte til dei tilsette i EVIKT.

Både leiaren for EVIKT og prosjektleiaren for informasjonstryggleiksplanen i Vindafjord kommune meiner at dei tilsette er nøgde med brukarstøtta, og får like god og effektiv hjelp no som før samanslåinga av IT-avdelingane i dei to kommunane. Leiaren for EVIKT viser i den samanheng til resultata i ei brukarundersøking som nyleg blei gjennomført i Vindafjord og Etne knytt til EVIKT sitt arbeid.

Revisjonen har fått tilsendt resultata frå brukarundersøkinga, der tre firdelar av respondentane var frå Vindafjord kommune. På spørsmål om kor nøgd eller misnøgd respondentane er med IKT-avdelinga si brukarstøtte og drift, svara langt dei fleste respondentane at dei enten er «fornøgd» (55,9 %) eller «svært fornøgd» (31,2 %). Brukarundersøkinga hadde òg spørsmål knytt til samanslåingsprosessen, og frå svara på desse spørsmåla går det fram at dei fleste respondentane er nøgde med IKT-avdelinga, også etter samanslåinga. Det kjem likevel fram i svara at fleire respondentar òg meiner det var betre då IKT også hadde kontortid i Vindafjord kommune, og at det var betre tidlegare, særleg knytt til mindre ventetid.

Også respondentane i spørjeundersøkinga gjennomført av revisjonen blei bedne om å ta stilling til fleire påstandar knytt til brukarstøtta frå EVIKT. Svara er presentert i figur 4:

Figur 4: Brukarstøtta for IKT



Svara tyder at langt dei fleste av respondentane er nøgd med hjelpa dei får av EVIKT, og med tida det tar før dei får hjelp. Vidare svara 80 % av dei er «delvis einig» eller «heilt einig» i at *kommunen har gode rutinar og verktøy som gjer at ein enkelt kan søke hjelp når ein opplever problem med IKT-systema*.

Respondentane i spørjeundersøkinga fekk moglegheit til å kome med ytterlegare kommentarar knytt til arbeidet til EVIKT; blant dei som nytta denne sjansen, var det fleire som ikkje var nøgde med brukarstøtta til EVIKT. Mellom anna var det respondentar som opplever at brukarstøtta ikkje alltid tar det ansvaret som er forventa frå brukarane, men t.d. skyv ansvaret for eit problem over på systemansvarleg for eit gitt fagsystem, på programleverandørar, eller på brukaren sjølv. Eit par av respondentane saknar plasseringa av IT-avdelinga i Ølen.

4.6.2 Vurdering

Revisjonen finn i sine undersøkingar at EVIKT si brukarstøtta for IKT jamt over blir opplevd som god, både av dei som blei intervjua og dei som svara på spørjeundersøkinga. Vidare er opningstid, bemanning og prosedyrar for både den regulære brukarstøtta og vakttelefonen for dei kritiske fagsystema formalisert. Revisjonen merkar seg at vakttelefonen er døgnopen, noko som avviker frå det som kjem fram i tilsendt dokumentasjon.

I sum vurderer revisjonen at brukarstøtta til EVIKT i hovudsak er organisert på ein føremålstenleg måte med omsyn til tilgjengelegheit. Revisjonen vil likevel anbefale kommunen å formalisere dei gjeldande opningstidene for vakttelefonen, for slik å redusere risikoen for misforståingar.

5. Styringssystem for informasjonstryggleik

5.1 Problemstilling

I dette kapittelet vil revisjonen svare på følgjande problemstilling med tilhøyrande underproblemstillingar:

I kva grad har kommunen etablert eit styringssystem for informasjonstryggleik som tilfredsstiller krav i sentrale føresegner?

Under dette:

a) Er styrande dokument for informasjonstryggleik i samsvar med krav i regelverket?
b) Er det etablert klåre rutinar og ansvarsforhold knytt til informasjonstryggleik?
c) Har kommunen eit system for kontroll og etterprøving av informasjonstryggleik, og blir slik kontroll og etterprøving gjennomført?

5.2 Revisjonskriterium

Personopplysningslova § 14 første ledd pålegg behandlingsansvarlege av personopplysningar å «etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller medhold av denne loven, herunder sikre personopplysningenes kvalitet». § 14 andre ledd i same lov slår fast at den behandlingsansvarlege skal dokumentere tiltaka, og at dokumentasjonen skal vere tilgjengeleg for medarbeidarane hos den behandlingsansvarlege og databehandlaren. Personopplysningsforskrifta kapittel 3 stiller krav til omfanget og rutinane i den påkravde internkontrollen.

Kapittel 2 i personopplysningsforskrifta stiller krav og føresegn knytt til informasjonstryggleik i verksemder som behandlar personopplysningar. Kapittelet pålegg mellom anna slike verksemder å:

- fastsette tryggleiksstrategi for verksemda (§ 2-3)
- gjennomføre risikovurderingar etter fastsette kriterier (§ 2-4)
- etablere klare ansvars og –myndigheitsforhold for bruk av informasjonssystem (§ 2-7)
- gjennomføre tryggleiksrevisjonar for å etterprøve at tiltak er sett i verk og fungerer (§ 2-5)
- behandle uønskte hendingar i informasjonssystemet som avvik (§ 2-6)
- foreta regelmessig gjennomgang på leiarnivå av tryggleiksmål og –strategi (§ 2-3)
- sikre at det ikkje vert overlevert personopplysningar elektronisk til andre verksemder dersom desse ikkje tilfredsstiller krava i tryggleiksføringane (§ 2-15)

Personopplysningsforskrifta § 2-8 andre ledd stiller krav om at «Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.» Frå dette kan ein utleie at kommunen må syte for at medarbeidarane får tilstrekkeleg opplæring til å følgje rutinane som er fastlagde

I tillegg er kommunen gjennom § 15 i eForvaltningsforskrifta forplikta å ha ein internkontroll basert på anerkjende standardar for styringssystem for informasjonstryggleik. Direktorat for forvaltning og IKT (Difi) er peika ut som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttast. Difi tilrår at offentlege verksemder baserer seg på ISO/IEC 27001:2013, som er ein internasjonal standard for styringssystem for informasjonstryggleik.

Sjå vedlegg 2 for fullstendige revisjonskriterium

5.3 Styrande dokument for informasjonstryggleik

5.3.1 Datagrunnlag

Vindafjord kommune viser til strategisk plan for informasjonstryggleik og delegeringsreglementet[25] som dei styrande dokumenta for informasjonstryggleik i kommunen. Delegeringsreglementet inneheldt det revisjonen kan sjå ikkje noko om informasjonstryggleik.[26]

[25] Politisk delegeringsreglement for Vindafjord kommune. Vedtatt av kommunestyret i sak 92/16 og supplert med vedtak i sak 29/17. Med rådmannen sin vidaredelegering datert 07.03.17 og supplert 05.07.2017 og Reglement for behandling av klagesaker i Vindafjord kommune. Vedtatt av kommunestyret 23.05.17, sak 030/17
[26] T.d. er det inga delegering av personopplysningsloven i reglementet.

Strategisk plan for informasjonstryggleik i Vindafjord kommune viser innleiingsvis til overordna føringar i lovverket knytt til informasjonstryggleik (personopplysningsforskriften), og definerer føremålet med å få på plass god informasjonstryggleik som å «stø opp om og sikre Vindafjord kommune si drift, ålmenn tillit og omdømme, ved å førebyggje og avgrense konsekvensane av uønskte hendingar».

Vidare blir det i strategisk plan for informasjonstryggleik vist til ulike hovudmål, strategiar, delmål, og delstrategiar. Desse er kortfatta presentert i tabell 3:

Tabell 3: Sentrale mål og strategiar i strategisk plan for informasjonstryggleik i Vindafjord kommune

Prosedyre/Reglement	Samandrag
Hovudmål	(1) rett forvalting av informasjon, (2) tilby innbyggjarane eit trygt og godt tenestetilbod kjenneteikna av god handsaming av sensitiv informasjon, (3) sikre tilgjenge til autoriserte brukarar og (4) trygge konfidensialitet.
Hovudstrategiar	Strategisk plan for informasjonstryggleik set seks overordna strategiar for å oppnå tryggleiksmåla dei har sett. Dette er mellom anna ansvarsfordeling, gjennomføring av ROS-analysar og utarbeiding av fysiske tryggingstiltak.
Delmål og -strategiar	Kommunen viser til fleire delmål med tilhøyrande strategiar innan avvikshandtering, risikovurdering og rapportering, beredskapsplanlegging, partnarar og leverandørar, fysisk tryggleik, og kontroll og oppfølging

Det går fram frå både tilsendt dokumentasjon og i intervju at arbeidet med å ferdigstille strategisk plan for informasjonstryggleik har føregått vinteren 2017/2018. Planen tredde som nemnd i kraft i mars 2018, og både den overordna delen og dei meir spesifikke vedlegga er no gjeldande. I intervju med prosjektleiar for planen, kjem det fram at nokre av rollane som er skildra i dokumentet ennå ikkje er etablerte.

Prosjektleiaren fortel vidare at Vindafjord kommune fram til no ikkje har hatt eit aktivt styringssystem for informasjonstryggleik. Kommunen har nytta og nyttar framleis kvalitetssystemet RiskManager, men har til no ikkje hatt klare ansvars- og rollefordelingar for kven som skal følgja opp informasjonstryggleiksfeltet. Vidare kjem det fram i intervjuet at det har vore varierande i kor stor grad leiarar eller andre tilsette i kommunen har følgt opp sine ansvarsområder knytt til informasjonstryggleik.

5.3.2 Vurdering

Gjennom den nyleg ferdigstilte og vedtekne strategiske planen for informasjonstryggleik har Vindafjord kommune eit styrande dokument for informasjonstryggleik. Planen oppfyller nokre – men ikkje alle – krava i regelverket; sjølv om den spesifisere overordna mål og strategi for informasjonstryggleiken i kommunen, viser den berre til eitt av fleire lovverk som stillar krav til informasjonstryggleik, og den manglar òg referansar til sentrale omgrep for informasjonstryggleik som konfidensialitet, integritet og tilgjengelegheit.

Revisjonen merkar seg elles at svara i spørjeundersøkinga tyder på at er styringssystemet berre til ein viss grad nytta i det daglege informasjonstryggleiksarbeidet i kommunen.

Revisjonen er merksam på at planen relativt nyleg blei vedteke, og at arbeidet med å utarbeide eit fullstendig styringssystem for informasjonstryggleik er pågåande. Basert på det som kjem fram i undersøkingane, er det likevel revisjonen si vurdering at Vindafjord kommune sine styrande dokument for informasjonstryggleik p.t. ikkje er i samsvar med krav i regelverket.

5.4 Rutinar og ansvarsforhold knytt til informasjonstryggleik

5.4.1 Datagrunnlag

Ansvarstilhøve for informasjonstryggleik

Rollar og ansvar knytt til informasjonstryggleik i Vindafjord kommunen er skildra i strategisk plan for informasjonstryggleik. Der går det fram at det overordna juridiske-, informasjonstryggleiks-, sakshandsamings, datahandsamings- og teiepliktsansvaret er lagt til rådmannen, og at rådmannen har delegert mykje av ansvarsoppfølginga til kommunalsjefar og einingsleiarar i kommunen. I tillegg er det tenkt at rådmannen skal utabeide eit mandat for utvalet for informasjonstryggleik.[27] Dette utvalet skal mellom anna årleg gjennomgå styringsdokumentasjonen, og følgje opp og ta avgjersler i saker knytt til informasjonstryggleik der utvalet er delegert avgjerdsmynde.

[27] Sjå avsnitt 3.6.1.

Elles følgjer ansvarstilhøve med omsyn til informasjonstryggleik den regulære lineorganiseringa i kommunen: einingsleiarane er ansvarlege for at dei tilsette er kjende med informasjonstryggleiksrutinar og at dette blir følgt opp og ivaretatt i eininga, medan den einskilde tilsette skal syte for å etterleve gjeldande rutinar og regelverk.

I strategisk plan for informasjonstryggleik er informasjonstryggleiksansvaret for følgjande stillingar/funksjonar definert: rådmann, kommunalsjef, einingsleiar, tilsette, utval for informasjonstryggleik, IT-sjef, arkivleiar, systemeigar, systemadministrator. I intervju kjem det fram at rollar og ansvar som skildra i strategisk plan for informasjonstryggleik fortsatt ikkje er etablerte i kommunen.

I intervju og frå resultata i spørjeundersøkinga, går det fram at ikkje alle tilsette i Vindafjord kommune er medvitne kva rolle og ansvar dei har med omsyn til informasjonstryggleik.[28] I intervju med seniorrådgjevaren, blir det likevel understreka at enkelte tilsette og leiarar følgjer opp sine ansvarsområde knytt til informasjonstryggleik.

Rutinar for informasjonstryggleik

Både frå tilsendt dokumentasjon og i intervju kjem det fram at Vindafjord kommune har mangla mykje av dei skriftlege rutinane som trengs for å sikre informasjonstryggleiken i kommunen. Prosjektleiaren understrekar likevel at dette ikkje betyr at kommunen har mangla alt av rutinar, og at kvalitetssystemet inneheld rutinar knytt til informasjonstryggleik for delar av kommunen.

Som ein del av arbeidet med strategisk plan for informasjonstryggleik har kommunen utarbeidd to vedlegg som inneheld rutinar og retningsliner for informasjonstryggleiksarbeid i kommunen, høvesvis *Retningsliner for alle tilsette i Vindafjord kommune* og *Tommelfingerreglar for tilsette i Vindafjord kommune*. Førstnemnde er ein del av introduksjonsprogrammet for nye medarbeidarar i kommunen, og inneheld føringar for grunnleggjande opplæring i informasjonstryggleik. Alle nytilsette skal stadfeste skriftleg at dei følgjer desse retningslinene. Føremålet med retningslinene er å bidra til korrekt handsaming av personopplysningar, og korrekt og sikker bruk av kommunen sine informasjonssystem.

Retningslinene listar fire moment som alle tilsette skal vere kjende med. Desse er: (1) tryggleiksorganisering, (2) mål og strategi for informasjonstryggleik, (3) tryggleikstiltak, og (4) rutinar for avvikshandsaming. Retningslinene inneheld elles mellom anna kortfatta rutineskildringar for teieplikt, låserutinar og tilgangskontroll, aktiv informasjonstryggleik, bruk av internett, bruk av kommunen sine dataverktøy, bruk av passord, mv. Det er òg ei kortfatta skildring av rutinar for avvikshandsaming for informasjonstryggleik.

I dokumentet *Tommelfingerreglar for tilsette i Vindafjord kommune*, er utvalde og overordna reglar for informasjonstryggleik kortfatta skildra. Her går det mellom anna fram rutinar for korleis passord skal handterast, at tilsette alltid skal låse PCane om dei forlét desse, at ein ikkje skal nytte berbar PC eller minnepinne til å lagre sensitive personopplysningar, og at bruk av internett skal avgrensast til føremål og omfang som toler å bli kjent.

Det nyleg etablerte utvalet for informasjonstryggleik har i oppgåve å oppdatere styringssystemet for informasjonstryggleik til kommunen, og det går fram frå tilsendt dokumentasjon kva rutinar og retningsliner dei har i oppgåve å utarbeide; mellom anna skal dei utarbeide detaljerte rutinar for systemeigarar og systemadministratorar, bruk av teknisk utstyr, opplæring av tilsette, tildeling av autorisasjonar og avviksmelding og –handtering.

Oversikt over personopplysningar og databehandlaravtalar

Revisjonen har mottatt kommunen si oversikt over personopplysningar som blir handsama i elektronisk.[29] Oversikta syner mellom anna kven som er systemeigar for dei ulike fagprogramma, kva type personopplysningar som blir handsama i systemet, heimel for handsaming, om opplysningane er sensitive, samt om opplysningane er konsesjons- eller meldepliktige. Det går ikkje fram av oversikta eller elles i tilsendt dokumentasjon kven som har ansvar for å oppdatere oversikta, eller kva som er rutinane for å melde inn kva personvernopplysningar som blir handsdama.

[28] Sjå 6.4.1 for nærare gjennomgang av data frå spørjeundersøkinga
[29] Oversikta er eit vedlegg til strategisk plan for informasjonstryggleik, og er attgjeven i tabell 5 i vedlegg 4.

I intervju med EVIK-leiaren går det fram at EVIKT har oversikt over dei personopplysningar som dei kjenner til at blir handsama i kommunen, men at dei ikkje er trygge på at oversikta er fullstendig. Det er t.d. ikkje noko rutine eller system for å halde oversikt over kva personopplysningar som blir handsama i einingane.

I intervju med kommunen går det fram at dei ikkje har tilgang på meir ajourførte opplysningar over personopplysningane som blir handsama i kommunen enn oversikta som blir laga av EVIKT. Kommunen fortel vidare at det er krevjande å få oversikt over kva opplysningar som kjem inn under personvernlovgjevinga.

Revisjonen har òg mottatt kommunen si oversikt over databehandlaravtalar inngått mellom Vindafjord kommune og eksterne partar.[30] Oversikta viser kva år databehandlaravtalane er inngått, med kva firma avtalane er inngått, kva system avtalane gjeld, og kva eining/avdeling i kommunen som eig systemet.

I dokumentasjonen revisjonen har mottatt føreligg det ikkje konkrete skildringar av ansvarsdeling eller rutinar knytt til ajourhald eller rapportering på kva databehandlaravtalar som er inngått i kommunen. I intervju kjem det fram at EVIKT verken har ansvar for eller oversikt over databehandlaravtalane inngått mellom kommunen og eksterne leverandørar. Det går vidare fram at det er systemeigarane i kommunen som har kontakt med eksterne leverandørar når det gjeld databehandlaravtalar opplyser EVIKT.

5.4.2 Vurdering

Gjennom strategisk plan for informasjonstryggleik har Vindafjord kommune formalisert rolle- og ansvarsdelinga knytt til informasjonstryggleik. Undersøkinga viser at dei formelle rollane og ansvaret ennå ikkje eller berre i avgrensa grad blir praktisert i kommunen, samt at fleire tilsette ikkje er medvitne kva ansvar som ligg til deira stilling når det gjeld informasjonstryggleik.

Revisjonen meiner difor at kommunen ikkje følgjer krava i POF § 2-7 første ledd, som seier at kommunen skal ha klare ansvars- og myndeforhold for bruk av informasjonssystemet. Vindafjord kommune er følgjeleg heller ikkje i samsvar med ISO27001:2013 punkt 5.3 som seier at ansvar og mynde for roller som er relevante for informasjonstryggleik skal vere tildelt og kommunisert.

Undersøkingane avdekker vidare at mykje av dei føreliggjande rutinane for informasjonstryggleik i Vindafjord kommune enten manglar eller er mangelfulle. Kommunen bryt slik med POF § 2-16 første ledd, som seier at rutinar for bruk av informasjonssystemet og anna informasjon med betyding for informasjonstryggleiken skal dokumenterast. Vindafjord kommune er slik heller ikkje i samsvar med ISO27001:2013 punkt 7.5 med underpunkt, som omhandlar dokumentering av styringssystemet for informasjonstryggleik.

Revisjonen finn at kommunen har dokumentert oversikt over kva personopplysningar dei handsamar, men undersøkingane avdekker òg at kommunen ikkje har system som sikrar at oversikta er oppdatert og fullstendig. Revisjonen merkar seg vidare at det ikkje er tydeleg kven som er ansvarleg for å halde oversikta over personopplysningar fullstendig; det kjem fram at tilsendt oversikt er frå EVIKT, men ifølgje EVIKT er det ikkje dei som er ansvarleg for halde oversikta fullstendig eller á jour.

Revisjonen meiner difor at det er risiko for at kommunen handsamar personopplysningar utanfor oversikta. På denne måten bryt kommunen med kravet om at det skal førast oversikt over personopplysningane som blir handsama, jf. POF § 2-4 første ledd, og det meir generelle kravet om å dokumentere all informasjon som har betyding for informasjonstryggleiken, jf. POF § 2-16. Manglande oversikt over kva personopplysningar som blir handsama, gjer i tillegg at kommunen bryt med POF § 3-1 tredje ledd a) til f), som stiller krav til kommunen om å ha systematiske rutinar for å kunne oppfylle sine plikter og dei registrerte sine rettar til ei kvar tid.

Undersøkingane avdekker vidare at Vindafjord kommune heller ikkje har system for å halde oversikt over kva databehandlaravtalar dei har inngått. Kommunen kan difor ikkje vere sikre på om dei har oversikt over kven som handsamar personopplysningar på vegner av kommunen. Det er difor risiko for at personopplysningar som kommunen har handsamingsansvar for, blir handsama av databehandlarar utan at kommunen kan halde oppsyn med om lov- og forskriftskrav blir etterlevd. Dette er eit brot på dokumentasjonskravet i POF § 2-16.

[30] Oversikta er attgjeven i tabell 4 på side 46 (vedlegg 4).

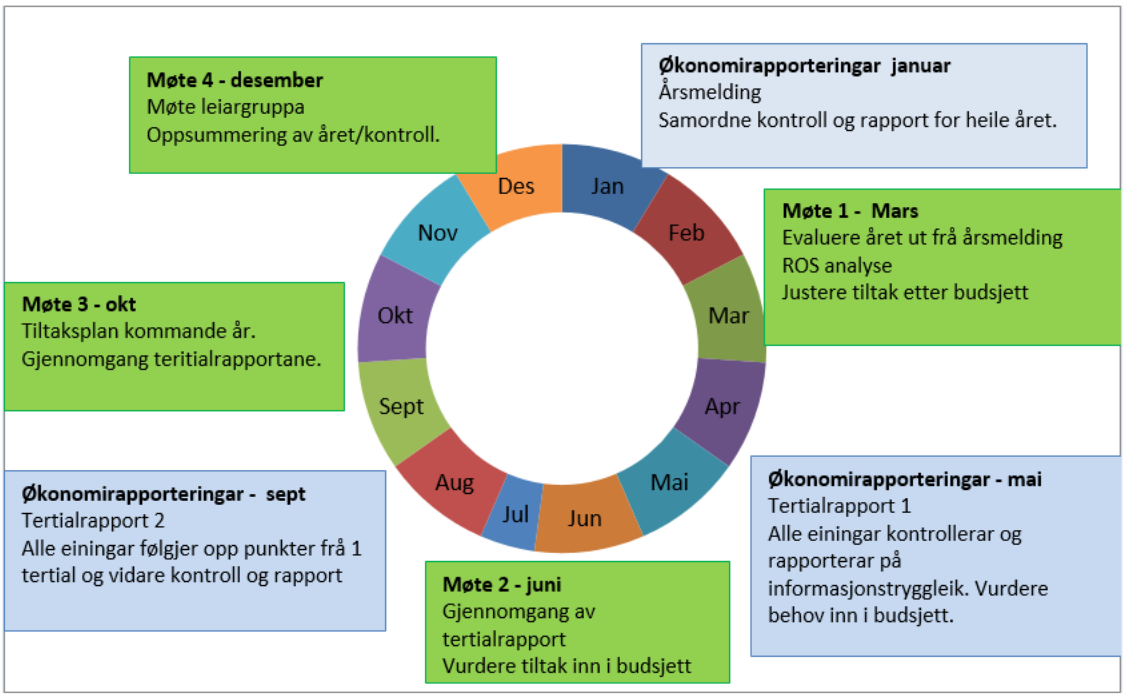
5.5 Kontroll og etterprøving av informasjonstryggleik

5.5.1 Datagrunnlag

I strategisk plan for informasjonstryggleik er det ein eigen del som omfattar kontroll og oppfølging av informasjonstryggleiken i kommunen. Her går det mellom anna utval for informasjonstryggleik har ein særskilt rolle når det gjeld kontroll og oppfølging av informasjonstryggleiken i kommunen. Utvalet skal mellom anna ha fire møter årleg og skal syte for at sjølve den strategiske planen og rutinearbeidet som skildra i gjennomføringsdelen av planen blir gjennomført.

Kontrollen skal gjennomførast i samsvar med årshjulet som vist i figur 5.

Figur 5: Årshjul for arbeidet til informasjonstryggleiksutvalet i Vindafjord kommune[31]



Vidare går det fram at leiinga i samarbeid med utvalet for informasjonstryggleik årleg skal gjere ein kontroll for å stadfeste at arbeidet med verksemda sine informasjonssystem på kvar kontrollstad er i samsvar med administrative og tekniske rutinar. Denne kontrollen og årlege revisjonen skal skje på desembermøtet i årshjulet.

Risikovurderingar av informasjonstryggleik

I strategisk plan for informasjonstryggleik går det fram at det er systemeigar som er ansvarleg for at det blir gjennomført risikovurderingar.

Vedlagt strategisk plan for informasjonstryggleik er eit rammeverk for risikoanalyse, med malar og eksempel for korleis ein kan gå fram i arbeidet med dei ulike fasane i ei risikovurdering som (1) identifikasjon av farar og uønskte hendingar, (2) vurdere sannsyn, (3) vurdere konsekvensar, (4) berekne risiko, (5) samanlikne med akseptkriteria og (6) vurdere risikoreduserande tiltak.

Det blir i vedlegget peika på at rammeverket er eit utkast som er utarbeidd av prosjektgruppa i kommunen, og at det må testast og evaluerast av utval for informasjonstryggleik.

I intervju kjem det fram at Vindafjord kommunen ikkje har jobba systematisk med risikovurderingar tidlegare. Det har blitt utført risikovurderingar gjennom eksterne dataselskap, men dette har ikkje vore gjort i tilstrekkeleg grad. Kommunen har ikkje formelle skriftlege risikovurderingar sett i system, og ev. risikovurderingar som har blitt uført er ikkje dokumentert.

[31] Kjelde: Strategisk plan for informasjonstryggleik

EVIKT har eit system knytt til risikovurderingar. EVIKT-leiaren fortel i intervju at dei m.a. gjer vurderingar av kva som kan påverke drifta og kor mange som blir påverka ved nedetid.

Avvikshandsaming

Det er kommunen sitt kvalitetssystem – RiskManager – som fungerer som avvikssystem. Her skal alle medarbeidarar melde avvik når dei oppdagar brot på tryggleikstiltak og/eller når oppgåver blir utført i strid med fastsette rutinar.

I strategisk plan for informasjonstryggleik går det fram korleis avvik skal bli handsama i kommunen. Alle tilsette har ansvar for å avdekke og melde brot på tryggleiksrutinar gjennom kvalitetssystemet. Hovudregelen er at alle avvik skal rapportrast tenesteveg til næraste leiar, og dokumentasjonen frå risikovurdering og avvikshandsaming skal lagrast i kvalitetssystemet. Om det blir oppdaga kritiske avvik skal dette rapporterast direkte til leiar for informasjonstryggleiksutvalet og melding skal sendast vidare til Datatilsynet innan 72 timar. Vidare skildrar dokumentet kva typar hendingar som krev at ein skriv avviksmelding.

Det går vidare fram frå dokumentasjon at kommunen som del av kontroll og oppfølgingsaktivitetane skal hente ut oversikt over avvik knytt til informasjonstryggleik kvart kvartal.

I intervju med systemansvarleg for helsefagsystema i kommunen, går det fram at avvik innan helse og omsorg skal registrerast manuelt både i fagsystemet og i kommunen sitt kvalitetssystem. Det er rutine på å ta ut oversikt over avvik og sende til leiargruppa kvart tertial, og ho opplever at det har vore ei nedgang i avviksmeldingar i 2017 til samanlikning med 2016. Ho fortel vidare at det tidlegare har skjedd at avvik ikkje blei handsama, men at dei dei seinare åra har hatt auka merksemd på nytten og viktigheita av å melde avvik.

Revisjonen får opplyst at det i 2017 blei meldt totalt 326 avvik i kvalitetssystemet i Vindafjord kommune, og at fem av desse var knytt til informasjonstryggleik.

Frå resultata i spørjeundersøkinga kjem det fram at dei fleste har fått informasjon om at dei skal melde avvik.[32] Som det går fram i avsnitt 6.4.1 svara likevel over halvparten av respondentane at dei ikkje er kjend med gjeldande rutinar for å melde avvik knytt til informasjonstryggleik. Fleire respondentar kommenterer også i eit ope kommentarfelt at det ikkje har vore tradisjon for å melde avvik gjennom kvalitetssystemet. Og med omsyn til avviksmeldingspraksis, viser svara frå spørjeundersøkinga at dei færraste melder avvik knytt til informasjonstryggleik.[33]

Tilgangskontroll

I intervju opplyser EVIKT-leiar at tilsette si tilgang til IKT-systemet blir styrt sentralt. Kommunen nyttar eit system for brukaradministrasjon som gjer at brukarar blir oppretta og deaktivert automatisk når dei blir tilsett eller slutter i kommunen, via ei kopling mellom lønnssystemet og EVIKT sine system.

Systemet er slik at det endringar i arbeidstilhøve i utgangspunktet automatisk skal føre til dei naudsynte endringane også i systemtilgangane. EVIKT-leiaren fortel at her er det litt utfordringar, då dei enno ikkje har fått implementert dei tekniske løysingane ferdig, og at det difor fortsatt må bli gjort endringar basert på manuelle beskjeder.

Tilgang til dei spesifikke fagsystema er det dei systemansvarlege ute i einingane som er ansvarlege for. I intervju med systemansvarleg for fagsystema innan pleie og omsorg, blir rutinane for tilgangsstyring i systema ho er ansvarleg for, skildra som følgjer:

- Når ein tilsett skal begynne å bruke fagsystema deira, sender avdelinga førespurnad på eit skjema om tilgang til systemansvarleg, og ho vidareformidlar til EVIKT. Når ho har lagt inn brukaren i systemet sitt, og IKT-tenesta har gitt tilgangar til sikker sone i IKT-systemet, kan vedkomande brukar begynne å bruke systemet.
- Når nokon sluttar, skal ho få tilsendt skjema frå avdelingane om dette, og ho stenger ned tilgangane i systema. Slike skjema blir òg vidaresendt til EVIKT, slik at dei kan stengje ned brukarkontoen sentralt.

[32] Som vist figur 12 på side 33.
[33] Sjå figur 17 på side 36.

- Systemansvarleg for pleie og omsorg skal også ha melding om tilsette skal ha utvida eller innskrenka tilgangar. Ho har vidare etablert ein eigen rutine for å kontrollere at tilsette ikkje har fleire tilgangar enn det som er naudsynt.

Systemansvarleg for pleie og omsorg har på eiget initiativ sett i verk tiltak for å betre tilgangsstyringa, særleg med omsyn til konfidensialitet. Ho peiker særleg på at skjemaa for tilgangar inneheld felt for namn og dato på dei som skal ha ulike tilgangar i fagsystemet, og at desse skjemaa blir gjennomgått i avdelingane og ajourført av systemansvarleg om lag annakvar månad.[34] Skjema med tilgangar som skal avsluttast blir vidaresendt til IKT for stenging.

5.5.2 Vurdering

Vindafjord kommune har i strategisk plan for informasjonstryggleik lagt grunnlag for kontroll og etterprøving av informasjonstryggleiken i kommunen. I undersøkingane finn revisjonen at dei ulike kontrollaktivitetane som er skildra i denne planen og/eller som bør inngå i ei oppfølging og kontroll av informasjonstryggleiken, berre i avgrensa grad blir praktisert i kommunen. Kommunen bryt slik med sentrale krav i både POF og ISO27001:2013.

Vindafjord kommunen gjennomfører ikkje eller berre i avgrensa grad risikovurderingar knytt til informasjonstryggleik, og har slik manglande oversikt over kva risikoar kommunen står ovanfor i samband med handsaming av personopplysningar. Dette medfører vidare at kommunen ikkje har eit godt grunnlag for å gjere eventuelle justeringar i informasjonstryggleikssystemet basert på endringar i trusselbilete. Kommunen bryt med dette med POF § 2-4 anna ledd.

Kommunen set ikkje akseptkriterium for risiko knytt til informasjonstryggleik, og har dimed ikkje grunnlag for å vurdere om risikoane for uønskte hendingar i handsaminga av personopplysningar er akseptable eller ikkje. Dette medfører at kommunen heller ikkje har noko grunnlag for å vurdere kor tid risikoreduserande tiltak må setjast i verk, og revisjonen meiner difor at kommunen bryt POF § 2-4 første ledd.

Etter det revisjonen kjenner til, gjennomfører heller ikkje kommunen tryggleiksrevisjonar, og kommunen har difor ikkje oversikt over kva tryggleikstiltak som fungerer og kva tryggleikstiltak som ikkje fungerer. Kommunen manglar med dette grunnlag for å gjere eventuelle justeringar og slik kontinuerlig forbetre informasjonstryggleiken. Basert på dette er det revisjonen si vurdering at kommunen bryt med POF § 2-5.

Vindafjord kommune har eit etablert avvikssystem, og det blir meldt avvik knytt til informasjonstryggleik i dette. Talet på informasjonstryggleiksavvik er lågt, og frå det som kjem fram i undersøkingane elles, har avviksmeldingspraksisen i kommunen forbetringspotensial. Revisjonen vil understreke at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta. Revisjonen meiner difor at Vindafjord kommune sin avvikspraksis ikkje er i samsvar med POF § 2-6 anna ledd og kapittel 10 i ISO27001:2013.

Undersøkingane tyder elles på at leiinga i kommunen ikkje eller berre i avgrensa grad følgjer opp informasjonstryggleiksarbeidet. Leiinga har slik ikkje grunnlag for å vurdere om avgjersler som blir tatt er i samsvar med behova for informasjonsteknologi og informasjonstryggleik. Leiinga har vidare heller ikkje grunnlag for å eventuelt justere kommunen sine tryggleiksmål og tryggleiksstrategi. Revisjonen meiner på denne bakgrunn at kommunen bryt med POF § 2-3 og ISO27001:2013 avsnitt 9.3.

Når det gjeld tilgangskontroll, avdekker undersøkingane at Vindafjord kommune og EVIKT har system for dette. Det kjem likevel fram at det er svakheiter i systema, som t.d. at det ikkje alltid vert meldt i frå når tilsette slutter i kommunen eller bytter jobb internt i kommunen. Dette medfører ein viss risiko for at tilsette manglar tilgang til naudsynt informasjon, og ein noko større risiko for at tilsette beheld tilgang til informasjon dei ikkje skulle hatt. Det er difor revisjonen si vurdering at Etne kommune bryt med personopplysningslova § 13 første ledd, og POF §§ 2-12 og 2-8 første ledd.

[34] Spesielt etter feriar er dei opptatt av å gå gjennom og avslutte tilgangar for sumarvikarar.

6. Kompetanse om informasjonstryggleik

6.1 Problemstilling

I dette kapittelet vil revisjonen svare på følgjande problemstilling med tilhøyrande underproblemstillingar:

I kva grad har dei tilsette i kommunen tilstrekkeleg kompetanse om informasjonstryggleik?

a) Er det etablert rutinar for å gje tilsette i kommunen opplæring i informasjonstryggleik?
b) I kva grad har dei tilsette i kommunen kjennskap til ev. retningsliner og rutinar for informasjonstryggleik?
c) I kva grad vert ev. retningsliner og rutinar for informasjonstryggleik følgt?

6.2 Revisjonskriterium

Personopplysningsforskrifta § 2-8 andre ledd stiller krav om at «Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.» Frå dette kan ein utleie at kommunen må syte for at medarbeidarane får tilstrekkeleg opplæring til å følgje rutinane som er fastlagde.

I tillegg er kommunen gjennom eForvaltningsforskrifta § 15 forplikta til å ha ein internkontroll basert på anerkjende standardar for styringssystem for informasjonstryggleik. Departementet har peika ut direktorat for forvaltning og IKT (Difi) som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttast, og Difi tilrår at offentlege verksemder baserer seg på ISO/IEC 27001:2013. Kapittel 7.2 i standarden seier at kommunen skal:

a) fastslå hvilken kompetanse som er nødvendig for personen(e) som utfører arbeid under organisasjonens styring, og som påvirker dens informasjonssikkerhetsprestasjon;
b) sikre at disse personene har kompetanse tilegnet gjennom passende utdanning, opplæring eller erfaring;
c) der det er relevant, treffe tiltak for å erverve nødvendig kompetanse og evaluere virkningen av tiltakene som er truffet; og
d) oppbevare relevant dokumentert informasjon som bevis på kompetanse.

I merknaden til punkt 7.2, står det at «Aktuelle tiltak kan for eksempel omfatte å sørge for opplæring, veiledning eller omplassering av nåværende ansatte eller innleie av eller kontraktinngåelse med kompetente personer.»

Sjå vedlegg 2 for fullstendige revisjonskriterium

6.3 Rutinar for opplæring i informasjonstryggleik

6.3.1 Datagrunnlag

I vedlegg til kommunen sin strategiske plan for informasjonstryggleig går det fram at det skal gjennomførast grunnleggande opplæring for alle tilsette i kommunen som handsamar personopplysningar, har tilgang til kommunen sine informasjonssystem, og/eller som nyttar PC eller mobile einingar tilhøyrande kommunen. Retningslinene skal vere ein del av opplæringa til nytilsette i kommunen. Alle tilsette skal vidare vere kjend med kva rollar og ansvar det er i kommunen knytt til informasjonstryggleik, kva mål og strategiar som er sett for området, kva tryggleikstiltak alle tilsette skal etterleve og kva som er kommunen sine rutinar for avvikshandsaming.

Dokumentet skildrar vidare korleis tilsette har rett og plikt til å gjennomgå naudsynt opplæring, og at det er næraste leiar som er ansvarleg for at dette blir gjennomført. Alle tilsette som nyttar fellessystema WebSak og Visma HRM skal ha fått grunnopplæring i desse systema innan ein månad etter jobbstart, og alle medarbeidarar skal ha opplæring i avvikshandsaming.

Prosjektleiaren for arbeidet med strategisk plan for informasjonstryggleik i Vindafjord kommune fortel i intervju at det per i dag er varierande praksis med omsyn til opplæring i informasjonstryggleik til nytilsette. Han opplyser vidare at dei retningslinene kommunen i dag har knytt til tilsetting av nye medarbeidarar, er at dei gjennomgår «krav til arbeidet», og får innføring i, og signerer på, teiepliktsskjema.

Systemansvarleg for fagsystema innanfor pleie og omsorg fortel i intervju at fleire av dei tilsette på området var på kurs i samband med introduksjon av *Norm for informasjonssikkerheit i helse- omsorgs- og sosialsektoren*. Ho fortel vidare at kommunen er med i Vestlandsløftet, eit bistandsprogram knytt til elektronisk meldingsutveksling mellom aktørane i helse- og omsorgstenestene. I samband med dette, har alle tilsette innan pleie- og omsorg deltatt på KOMP-iS-kurs.[35] I tillegg sender ho ut månadleg ut e-post til dei tilsette med stikkord knytt til informasjonstryggleik.[36]

Leiaren for EVIKT fortel om manglande kunnskap i nokre av einingane når det gjeld rutinar knytt til informasjonstryggleik. Generelt opplever han at det er mangelfull oppfølging av rutinar for informasjonstryggleik i kommunane.

Respondentane i spørjeundersøkinga som svara at dei er systemansvarlege fekk spørsmål *om dei har deltatt i opplæringa av andre brukarar*. 71 % svara «ja», og dei resterande 29 % svara «nei».[37] Dei som svara «ja» blei i eit oppfølgingsspørsmål bedne om å kort skildre kva opplæring dei har gitt. 15 svara på spørsmålet, og fleire av desse har gitt opplæring i bruk av dei aktuelle fagsystem dei er ansvarleg for. Nokre har òg gitt opplæring i oppbevaring av sensitive opplysningar og i reglar for e-post bruk.

6.3.2 Vurderingar

Revisjonen meiner Vindafjord kommune per i dag berre i avgrensa grad følgjer eigne retningsliner for å gje opplæring i informasjonstryggleik til sine tilsette. Dette gjer at det er høgare sannsyn for at dei tilsette ikkje har tilstrekkeleg kompetanse innanfor informasjonstryggleik, noko som aukar risikoen for brot på regelverket som gjeld for handsaming av personopplysingar og for informasjonstryggleiken generelt.

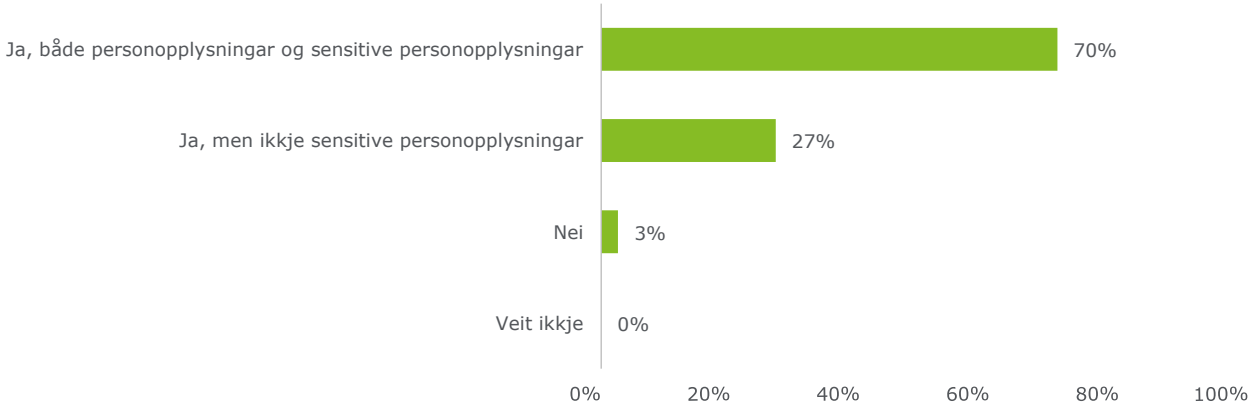
Det er revisjonen si vurdering at Vindafjord kommune ikkje fullt ut oppfyller krava i POF § 2-8 anna ledd, og heller ikkje ISO27001:2013 punkt 7.2.

6.4 Kjennskap til retningsliner og rutinar for informasjonstryggleik

6.4.1 Datagrunnlag

Som vist i figur 6, svara til saman 97 % av 115 respondentar i spørjeundersøkinga at dei *handsamar eller kjem i kontakt med enten både personopplysningar og sensitive personopplysingar, eller berre personopplysingar i sitt arbeid*. På spørsmål om dei kjem i *kontakt med eller handsamar anna fortruleg informasjon*, svara 88 % «ja».[38]

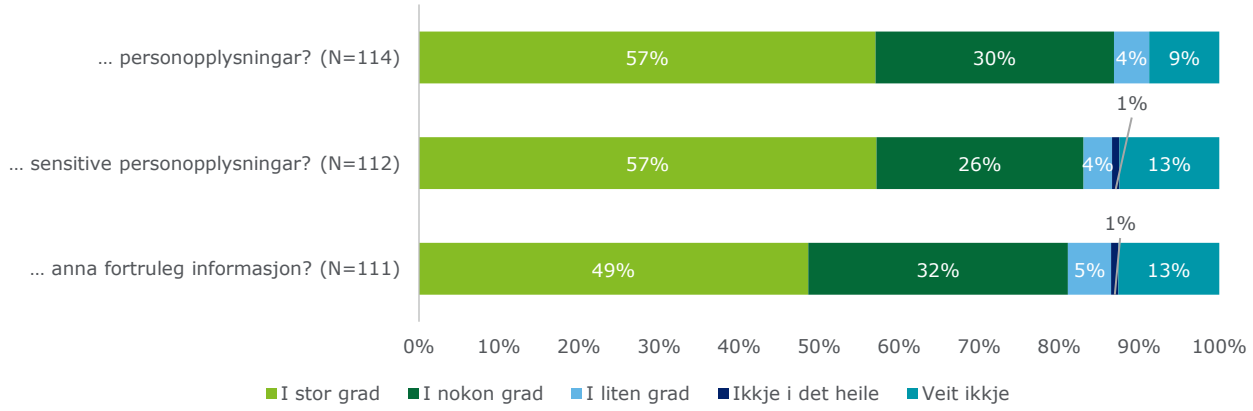
Figur 6: Handsaming av personopplysningar



Respondentane i spørjeundersøkinga blei bedne om å svare på *i kva grad kommunen og/eller einingа vedkomande jobba i har tydelege og skriftlege retningsliner for handsaming av ulike typar opplysningar*. Som det går fram av figur 7, svara mellom 9 % og 13 % «veit ikkje», og mellom 4 % og 5 % «i liten grad».

[35] KOMP-iS er eit kompetanseprogram for helse- og omsorgssektoren utarbeidd av Helse Sør-Øst.
[36] Revisjonen har fått tilsendt døme på ein slik e-post.
[37] N=21.
[38] N=112.

Figur 7: Tydelege og skriftlege retningsliner for handsaming av...

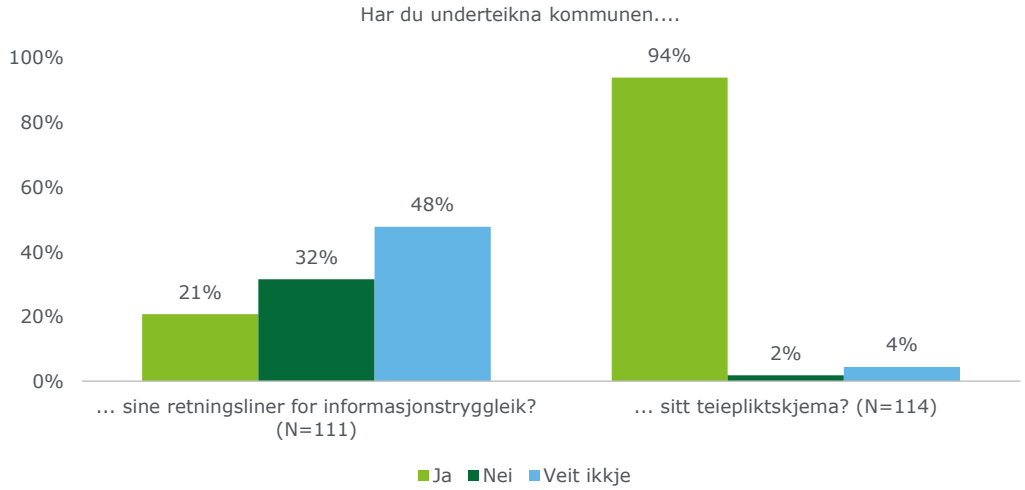


Respondentane blei så spurde om dei *veit kvar dei finn rutinar og retningsliner for handsaming av personopplysningar, sensitive personopplysningar og/eller anna fortruleg informasjon som gjeld kommunen og/eller deira eining*. På dette svara 78 % «ja», 20 % «nei», og 2 % «har ikkje slike rutinar».[39]

Dei som svara «ja» fekk eit oppfølgingsspørsmål om *kvar Vindafjord kommune og/eller eininga har tilgjengeleggjort informasjon om handsaming av denne typen opplysningar*. Fleirtalet av dei som svara, [40] svara at dei finn dette i kommunen sitt kvalitetssystem. Elles nemner respondentane fagsystem, handbok, informasjon ved tilsetting, informasjonsskriv, og permar og oppslag på arbeidsplassen.

Som vist i figur 8, har dei fleste av respondentane underteikna kommunen sitt teiepliktskjema, medan 21 % har underteikna kommunen sine retningsliner for informasjonstryggleik.

Figur 8: Teieplikt og retningsliner for informasjonstryggleik

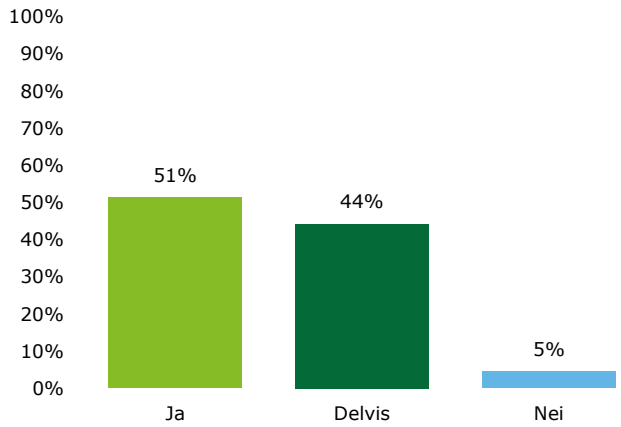


Dei som svara «ja» på at dei har underteikna kommunen sitt teiepliktskjema, blei spurde om dei hugsar innhaldet i skjema; 19 % svara «nei».[41] På same vis blei dei som svara at dei har underteikna kommunen sine retningsliner for informasjonstryggleik spurde om dei hugsa innhaldet i denne; her svara om lag ein tredel «nei».[42]

[39] N=113.
[40] N=72.
[41] N=108.
[42] N=24.

Respondentane blei vidare spurde om *dei er kjende med kva ansvar og oppgåver som ligg til deira stilling med omsyn til informasjonstryggleik i kommunen.* Som det går fram av figur 9, svara over halvparten at dei er kjende med eiget ansvar og eigne oppgåver knytt til informasjonstryggleik.

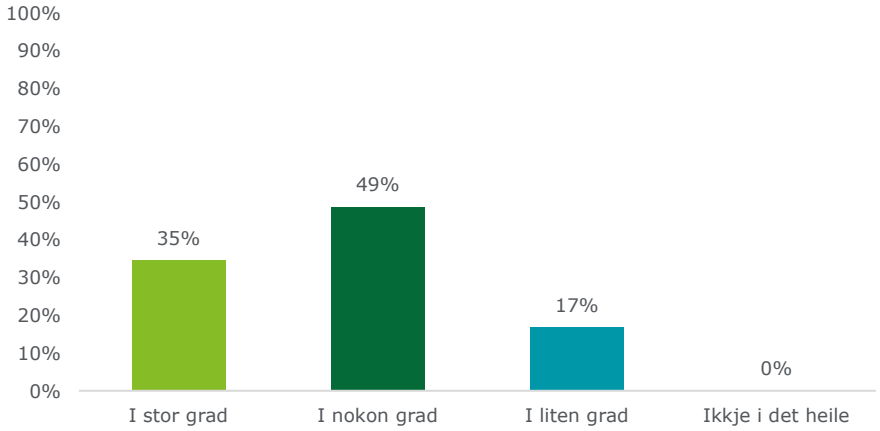
Figur 9: Kjennskap til eige ansvar og oppgåver knytt til informasjonstryggleik (N=111)



Dei som svara «ja» eller «delvis» på spørsmålet over, fekk eit oppfølgingsspørsmål på *kva oppgåver og ansvar dei har med omsyn til informasjonstryggleik.* Av dei 74 svara som kom inn, viser halvparten til sikker handsaming av fortruleg informasjon, og mange viser til teieplikta. Andre emne som er nemnt inkluderer mellom anna oppfølging av lov- og regelverk, bruk av PC og minnepenn, melde avvik og vern av passord. Fleire av svara var direkte knytt til den enkelte sine arbeidsoppgåver. Vidare svara nokre at dei er usikre på kva, eller om, dei har ansvar og oppgåver knytt til informasjonstryggleik i stillinga si, og nokre viser overordna til plikter og rutinar på arbeidsplassen utan å gå nærare inn på dette.

Svara på spørsmålet om *i kva grad har din næraste leiar framheva viktigheita av informasjonstryggleik* blir presentert i figur 10 under. Som det går fram av figuren svara om lag halvparten av respondentane «i nokon grad», og 17 % svara «i liten grad».

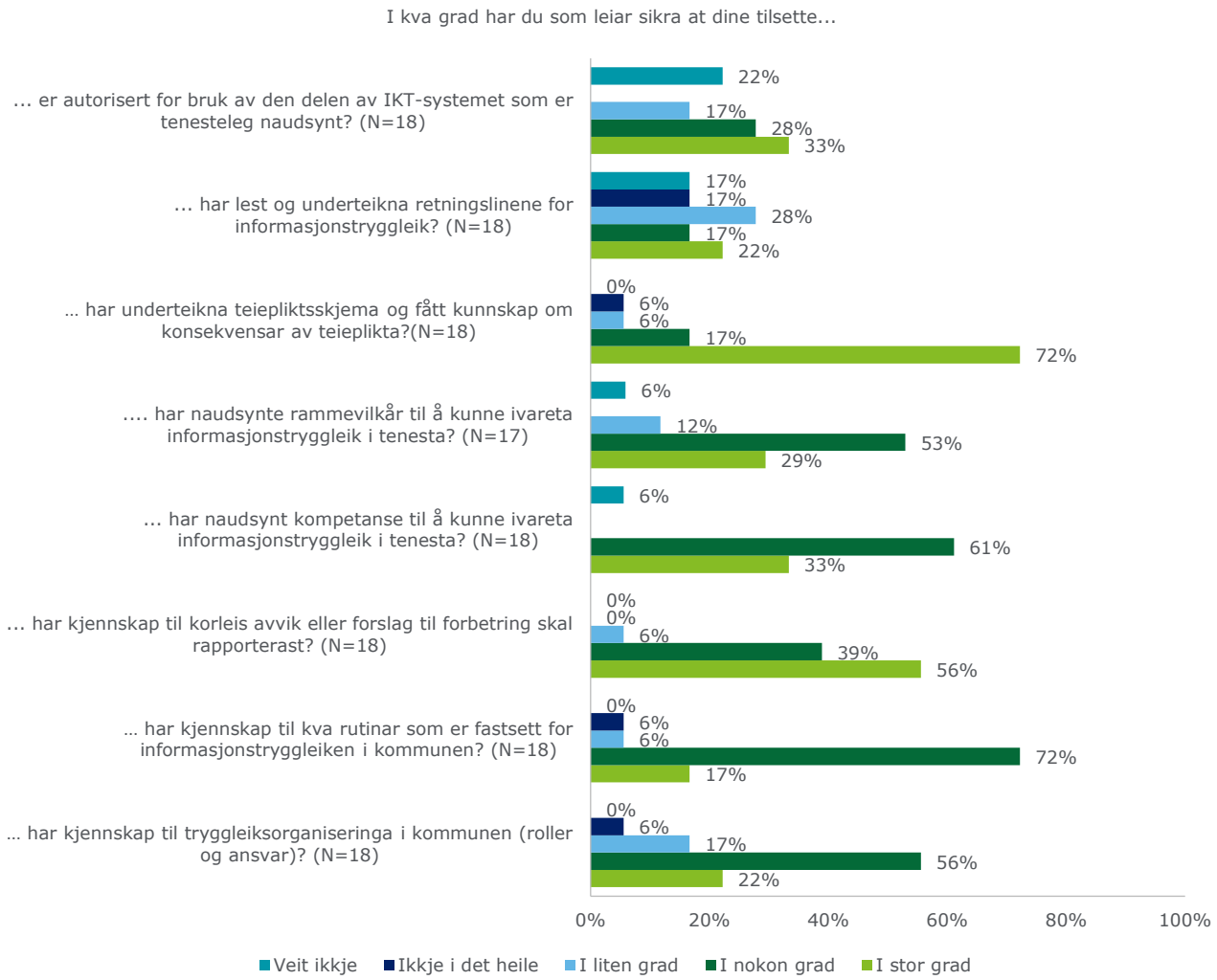
Figur 10: Viktigheita av informasjonstryggleik (N=113)



Dei som svara at dei har leiaransvar i kommunen, blei stilt ei rekkje spørsmål knytt til korleis dei sikrar at deira tilsette følger opp kommunen sine retningsliner for informasjonsstryggleik. Som det går fram av figur 11, varierer det i kva grad leiarane har sikra at deira tilsette har fått opplæring og informasjon; medan dei fleste sikrar at dei tilsette har underskrive og kjenner til konsekvensane av teieplikta (72 % «i stor grad»), svara over halvparten at dei berre «i nokon grad» har sikra at deira tilsette har naudsynt kompetanse, kjennskap til fastsette rutinar, kjennskap til tryggleiksorganiseringa og har naudsynte rammevilkår for å kunne ta i vare informasjonstryggleiken. På spørsmålet om leiarane har sikra at dei tilsette har kjennskap

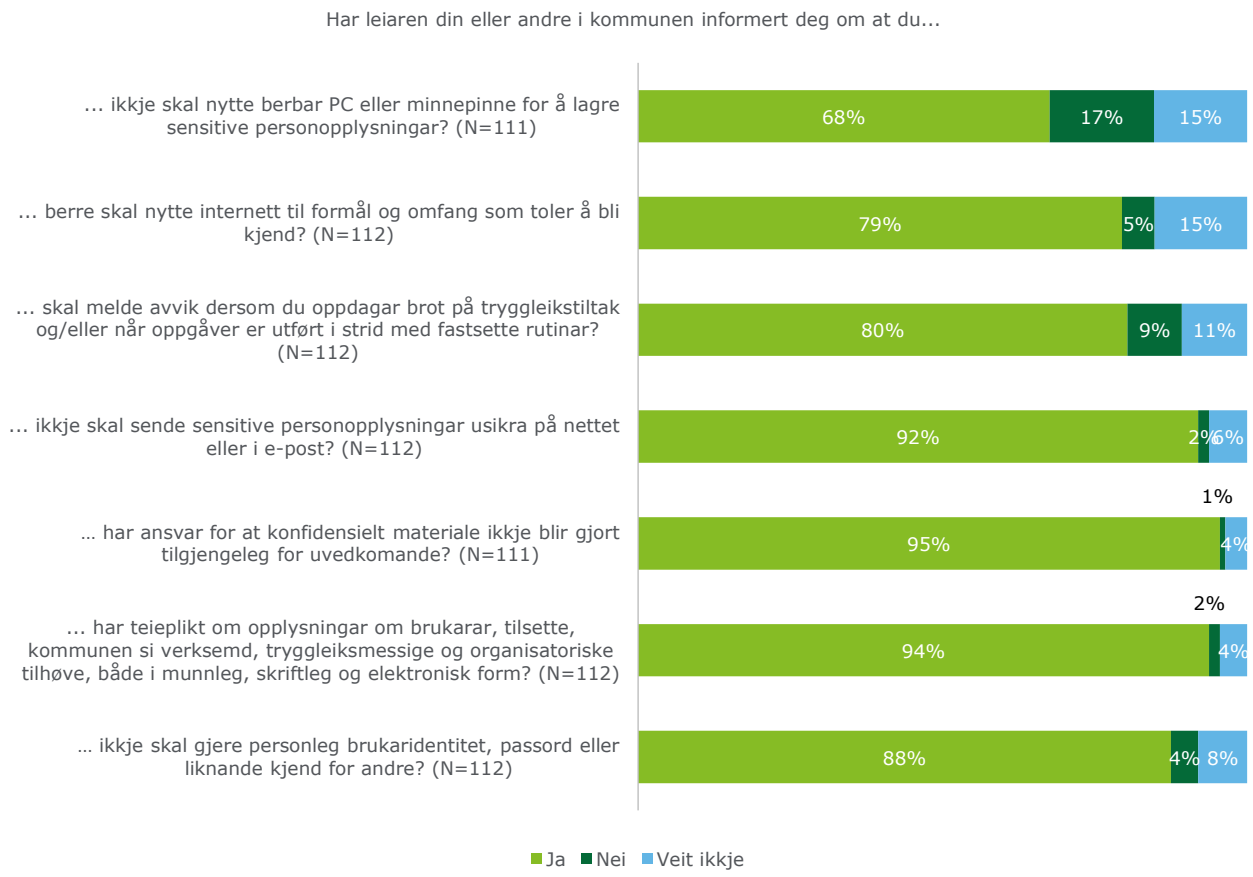
til avvikrapportering, svara over ein tredel at dei i «nokon grad» har gjennomført dette, og 45 % svara at dei «i liten grad» eller «ikkje i det heile» har sikra at dei tilsette har lest og underteikna retningslinene for informasjonstryggleik i Vindafjord kommune.

Figur 11: Opplæring av tilsette



Figur 12 viser respondentane som er tilsett i Vindafjord kommune sine svar på sju spørsmål om *kva deira leiar eller andre i kommunen har informert om knytt til informasjonstryggleik og bruk av kommunen sine IKT-system*. Svara indikerer at langt på veg dei fleste respondentane har fått informasjon om dei ulike punkta kommunen held fram som viktige for å vareta ein god informasjonstryggleik. Samtidig svara nesten ein tredel av respondentane at dei ikkje har fått informasjon, eller ikkje veit om dei har fått informasjon om, at ein ikkje skal nytte berbar PC eller minnepinne for å lagre sensitive personopplysningar.

Figur 12: Opplæring i informasjonstryggleik i Vindafjord kommune



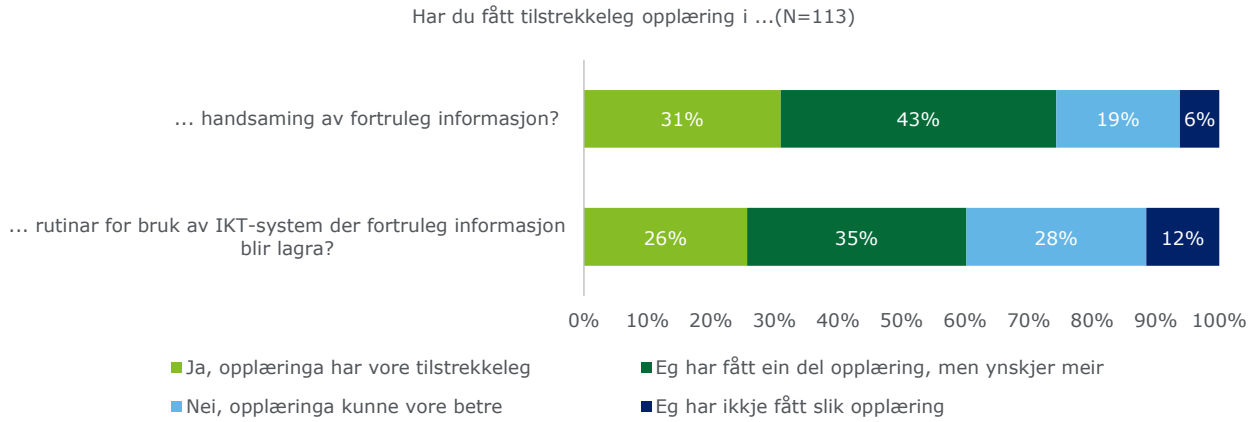
Respondentane blei vidare spurde om dei veit *kven i kommunen dei skal kontakte ved spørsmål knytt til informasjonstryggleik og/eller handsaming av personopplysningar.* Her svara 42 % «nei» og 58 % «ja».[43] Dei som svara «ja» fekk eit oppfølgingsspørsmål der dei blei spurde om *kven i kommunen dei kontaktar med slike førespurnader*. Om lag halvparten av dei 58 som har svara på oppfølgingsspørsmålet peikar på næraste leiar, medan ein fjerdedel nemner prosjektleiaren for strategisk plan for informasjonstryggleik. Om lag ein fjerdedel viser også til IKT–tenesta eller leiar for EVIKT, medan andre alternativ som blir nemnt er IKT-sjukepleiar, rådmann, arkivleiar, personalsjef og elles namngitte personar som jobbar i kommunen.

Vidare blei respondentane spurde om *dei er kjend med kva rutinar som gjeld for å melde avvik knytt til informasjonstryggleik;* her svara 56 % «nei» og 44 % «ja».[44] Dei som svara «ja», blei bedne om å skildre *gjeldande avviksrutinar når prosedyrar ikkje blir følgde eller ein opplever potensielle eller faktiske trugslar mot informasjonstryggleiken.* Av dei 39 svara som kom inn, viser 77 % til at ein kan melde avvik gjennom kommunen sitt kvalitetssystem. Vidare svara nokre at dei vil melde avvika inn til IKT brukarstøtta eller ta det opp med næraste leiar. Ein av respondentane svara at det manglar rutinar på avvikshandsaming.

Som det går fram av figur 13, indikerer svara til om lag to tredeler at dei ikkje har fått tilstrekkeleg opplæring i handsaming av fortruleg informasjon, og at om lag tre firedeler ikkje har fått tilstrekkeleg opplæring i rutinar for bruk at IKT-systema der fortruleg informasjon blir lagra.

[43] N=114
[44] N=114

Figur 13: Mottatt opplæring



Alle som svara at dei ynskjer meir opplæring i handsaming av fortruleg informasjon, fekk eit oppfølgingsspørsmål om *kva dei saknar innan informasjonstryggleiksopplæring*. Av dei 43 som svara er det gjennomgåande vist til at respondentane ønskjer ei generell opplæring i informasjonstryggleik, og ein gjennomgang eller repetisjon av kva som er gjeldane rutinar, reglar og retningsliner i kommunen. Fleire viser også til at dei ønskjer ei innføring i informasjonstryggleik ved bruk at IKT-systema, og då spesielt kva opplysningar som skal skjermast og ikkje. Eit par av respondentane nemner at det er mangelfulle system for å lagre personopplysningar innan deira eining, medan ein del er usikre på kva opplæring dei saknar.

Tilsvarande fekk alle som svara at dei ynskjer meir opplæring i rutinar for bruk av IKT-system der fortruleg informasjon er lagra, eit oppfølgingsspørsmål på *kva dei saknar i denne opplæringa*. Av dei 38 som svarar, er det mange som saknar grundig opplæring i dei fagsystema dei nyttar i kvardagen. Av dei same respondentane nemner også mange at det er mangelful informasjon knytt til byte og/eller oppgradering av fagsystem. Mange av respondentane er usikre på kva opplæring dei treng eller kva opplæring som er tilgjengeleg, medan fleire nemner at dei kunne tenke seg ei generell opplæring eller ein ny gjennomgang av systema som blir nytta i kommunen.

6.4.2 Vurdering

Undersøkinga viser at langt dei fleste respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller anna fortruleg informasjon i arbeidskvardagen. Likevel viser svara frå spørjeundersøkinga at rundt ein av ti ikkje veit om kommunen har retningsliner for å handtere slike opplysningar. Revisjonen merkar seg òg at nesten halvparten av respondentane berre delvis eller ikkje i det heile er kjende med kva oppgåver og ansvar som ligg til deira stilling med omsyn til informasjonstryggleik.

Elles indikerer spørjeundersøkinga at nesten halvparten av respondentane ikkje veit om dei har underteikna Vindafjord kommune sine retningsliner for informasjonstryggleik, og at av dei som har gjort det, hugsar nesten ein tredel ikkje kva som var innhaldet i retningslinene. Vidare går det fram frå undersøkingane at retningsliner og krav til teieplikt, konfidensialitet og passordbruk er relativt godt kjend blant respondentane, medan dei er mindre kjende med at dei ikkje skal nytte PC eller minnepenn for å lagre sensitive personopplysingar, ikkje skal nytte internett til formål som ikkje toler å bli kjend og at ein skal melde avvik dersom ein opplever brot på tiltak og oppgåver knytt til informasjonstryggleik.

Det kjem også fram i spørjeundersøkinga at nesten tre firedelar av respondentane anten ikkje har fått tilstrekkeleg opplæring i rutinar for bruk av IKT-systema der fortruleg informasjon blir lagra, og litt over to tredelar ikkje har fått tilstrekkeleg opplæring i handsaming av fortruleg informasjon.

Basert på funna frå undersøkingane, er det revisjonen si vurdering at dei tilsette i Vindafjord kommune ikkje har tilstrekkeleg kjennskap til eksisterande retningsliner og rutinar for informasjonstryggleik. Revisjonen meiner difor at kommunen bryt med POF § 2-8 anna ledd, og at det er risiko for at kommunen bryt med krav i regelverket som eit resultat av manglande kompetanse blant dei tilsette.

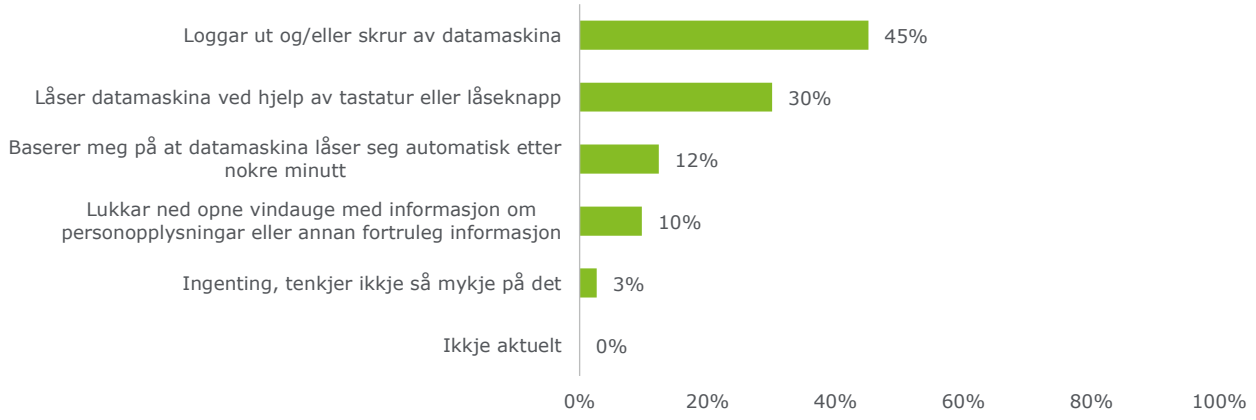
6.5 Etterleving av retningsliner og rutinar for informasjonstryggleik

6.5.1 Datagrunnlag

Eigen informasjonstryggleikspraksis

Respondentane blei spurde om kvardagsrutinar når dei forlèt PC-en dei brukar. Svara er presenterte i figur 14

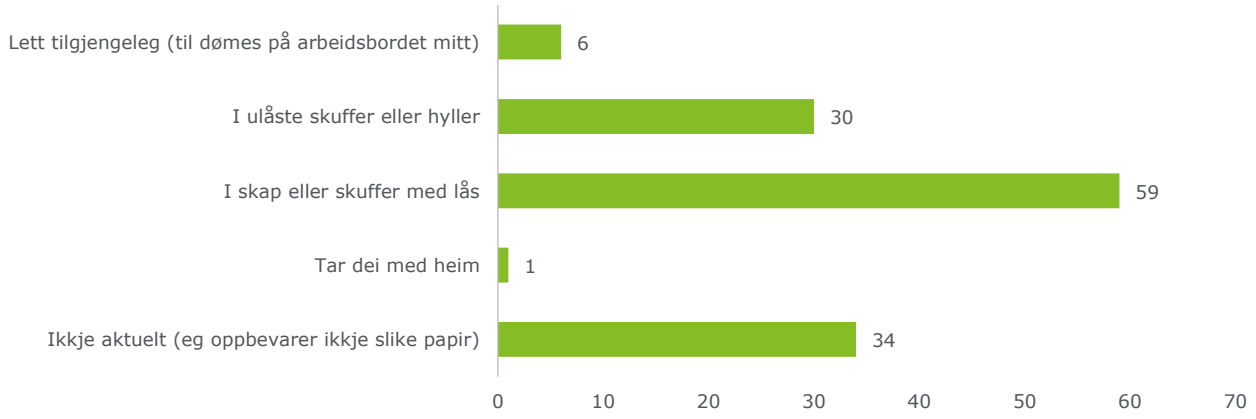
Figur 14: Kva gjer du vanlegvis når du i løpet av arbeidsdagen går frå PC-en du nyttar? (N=113)



Respondentane blei også spurde om dei *nokon gong har lånt ut brukarnamnet og passordet til andre*. Om lag 16 % svara «ja, men berre til IKT-avdelinga eller tilsvarande», rundt 4 % svara «ja», og 80 % «nei».[45]

På spørsmål om *korleis du oppbevarer papirdokument med fortruleg informasjon*, svara 30 av respondentane at dei oppbevarer dokument med fortruleg informasjon i ulåste skuffer eller hyller, 6 at dei oppbevarer slike dokument lett tilgjengeleg, og éin at vedkomande tek dei med heim (figur 15).[46]

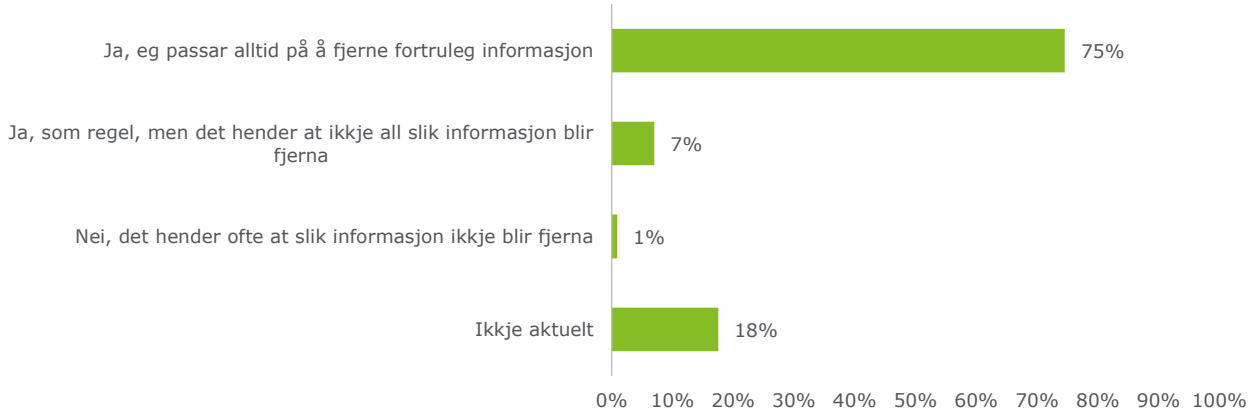
Figur 15: Korleis oppbevarer du dokument (papir) med fortruleg informasjon? (N=114)



Respondentane fekk vidare spørsmål om dei fjernar fortruleg informasjon frå møterom før dei forlèt det. Som vist i figur 16, svara 7 % at det hender at slik informasjon ikkje blir fjerna, medan 75 % svara at dei alltid passar på å fjerne fortruleg informasjon frå møterom.

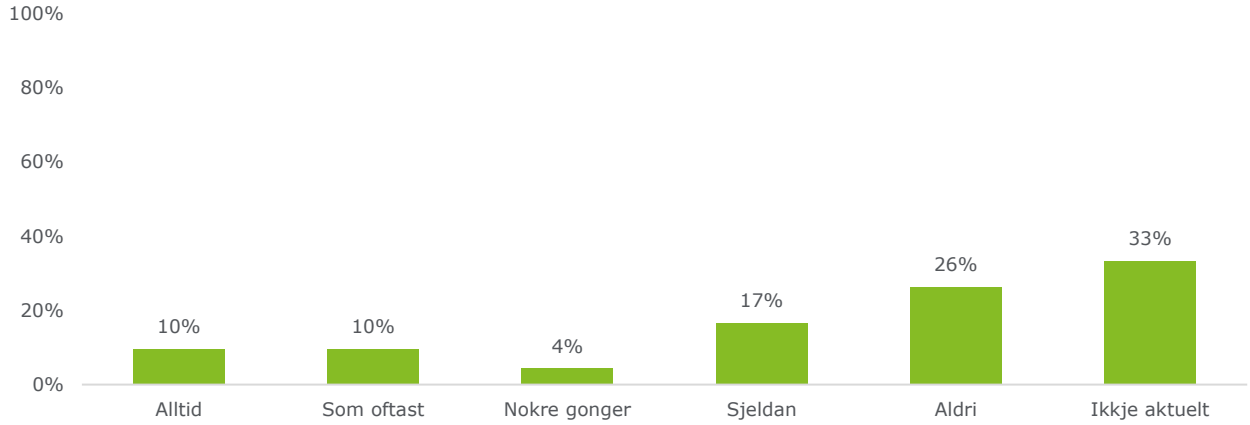
[45] N=114.
[46] Respondentane hadde høve til å velje meir enn eit svaralternativ.

Figur 16: Fjerning av fortruleg informasjon frå møterom (N=114)



Som vist i figur 17 svara over ein fjerdedel av respondentane at dei aldri melder avvik *dersom prosedyrar ikkje blir følgde eller når dei opplever potensielle eller faktiske trugslar mot informasjonstryggleiken.* 17 % svara at dei sjeldan melder avvik ved slike hendingar, medan ein tredel svara at dette ikkje er aktuelt i deira arbeidskvardag.

Figur 17: Avviksmelding (N=114)



Dei respondentane som svara «aldri» eller «ikkje aktuelt» fekk oppfølgingsspørsmål om kva som var årsaken til at dei *ikkje alltid melder avvik når prosedyrar ikkje blir følgde eller når du opplever potensielle eller faktiske trugslar mot informasjonstryggleiken.* Av dei 47 som svara, viser 22 respondentar til at dei ikkje i det heile eller sjeldan har opplevd avvik knytt til informasjonstryggleik. Om lag ein av fem svara at det ikkje er vanleg å nytte avvikssystemet då det mellom anna blir vurdert slik at avvikssystemet skal nyttast ved særdeles alvorlege tilfelle. Praksis er difor slik at ein som oftast melder frå til næraste leiar eller tar dette opp direkte med den eller dei det gjeld. Vidare blir det gitt tilbakemelding på at det ikkje er tid i kvardagen til å melde inn avvik gjennom avvikssystemet, at avviksmeldingar ikkje blir følgt opp av leiinga, og at det er uklåre rutinar på korleis og når ein skal nytte avvikssystemet.

Respondentane som svara at dei «alltid», «som oftast», «nokre gonger» eller «sjeldan» melder avvik knytt til informasjonstryggleik fekk eit oppfølgingsspørsmål på om meldte avvik har blitt følgt opp. 47 % svara «ja», 35 % svara «delvis» og 19 % svara «nei». [47]

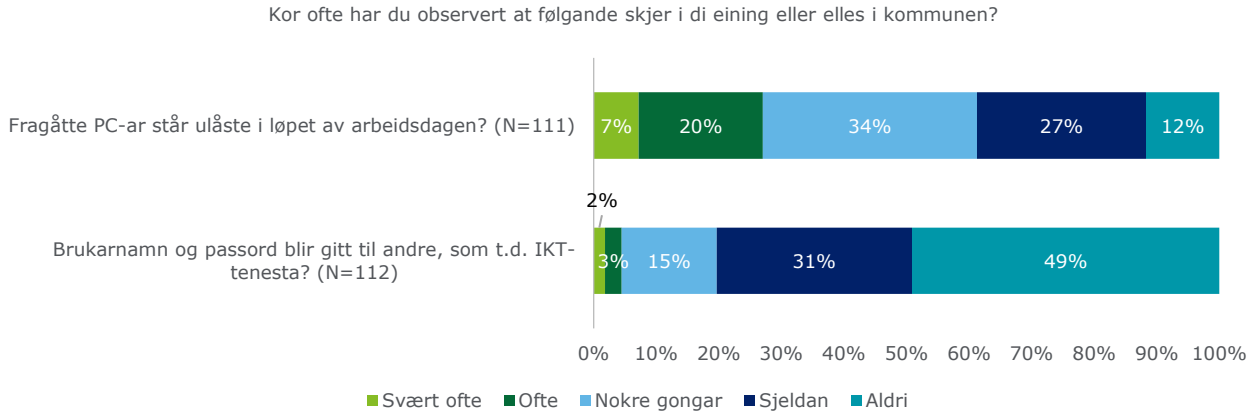
Andre sin informasjonstryggleikspraksis

Respondentane blei i spørjeundersøkinga bedne om å svare på ei rekkje spørsmål knytt til kollegaar sin informasjonstryggleikspraksis. Mellom anna blei dei spurde om *kor ofte dei har observert i deira eining eller elles i kommunen at fragåtte PC-ar står ulåste i løpet av arbeidsdagen*, og *kor ofte dei har observert at det*

[47] N=43

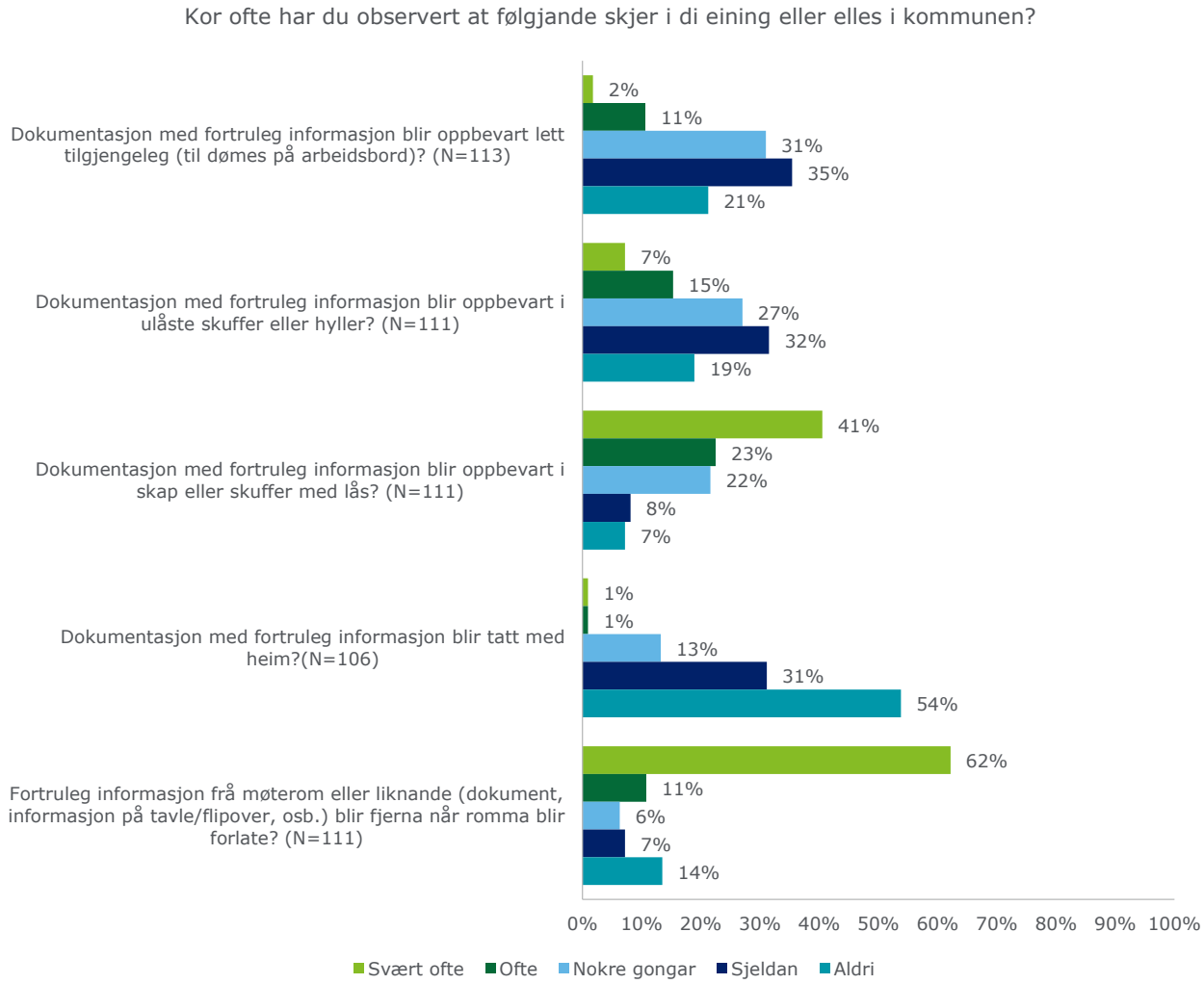
skjer i eira eining eller elles i kommunen at brukarnamn og passord blir gitt til andre, som til dømes IKT-avdelinga. Svara er presenterte i figur 18:

Figur 18: Informasjonstryggleikspraksis - PC og passord



Vidare blei respondentane spurde fem spørsmål knytt til kollegaar sin praksis knytt til informasjonstryggleik knytt til dokumenthandsaming. Svara er presentert i figur 19:

Figur 19: Informasjonstryggleikspraksis - dokumenthandsaming



Som det går fram av figuren, svara om lag ein femdel at informasjon og liknande på møterom «sjeldan» eller «aldri» blir fjerna når romma blir forlatne, og at 22 % av respondentane svara at fortruleg dokumentasjon «svært ofte» eller «ofte» blir oppbevart i ulåste skuffer eller hyller.

6.5.2 Vurdering

Undersøkinga viser mellom anna at ein relativt høg del av respondentane ikkje følger ein praksis for avlogging av datamaskina i samsvar med informasjonstryggleiksprinsipp. Vidare viser svara frå spørjeundersøkinga at 20 % av respondentane enten har delt passordet sitt med IKT-avdelinga eller andre, og at 5 % har observert at andre har gjort dette «svært ofte» eller «ofte». Revisjonen vil i den samanheng gjere merksam på at å dele passord med andre bryt med grunnleggjande prinsipp for informasjonstryggleik, også om det er IKT-tenesta ein deler passordet med.

Det går også fram av spørjeundersøkinga at langt fleire «aldri» eller «sjeldan» melder avvik enn dei som «alltid» eller «som oftast» gjer det, og vidare både at det er knytt usikkerheit til kva type avvik som skal meldast, og korleis avvik skal meldast.

Når det gjeld dokumenthandsaming, viser undersøkinga at det i Vindafjord kommune førekjem at fortruleg informasjon blir oppbevart i ulåste skap eller skuffer, eller lett tilgjengeleg.

Basert på funna frå undersøkinga, er det revisjonen si vurdering at dei tilsette i Vindafjord berre i noko grad følgjer etablerte retningsliner og rutinar for informasjonstryggleik.

7. Konklusjon og tilrådingar

Denne forvaltningsrevisjonen har undersøkt om kommunane Vindafjord og Etne har organisert si felles IKT-teneste (EVIKT) slik at den kan løyse tildelte oppgåver og etterleve sentrale føresegner, om Vindafjord kommune har tilfredsstillande system og rutinar for informasjonstryggleik, og om etablerte standardar og gjeldande lover og reglar blir følgt innanfor dette området.

Det er fastsett overordna mål for EVIKT, og både ansvaret og rolla til EVIKT er i hovudsak tydeleg definert og oppfatta. Av dei overordna måla, er det so langt berre kompetansemålet som blir vurdert som innfridd. Særleg ulikheiter i kommunane sine økonomiske rammar har gjort det utfordrande å nå målet om å standardisere driftsrutinar og fagprogram i kommunane.

EVIKT har vidare tilgang på tilstrekkeleg kompetanse – anten internt eller gjennom rammeavtalar – og har i hovudsak tilstrekkeleg kapasitet til å skjøtte sine oppgåver. Brukarstøtta til EVIKT er organisert på ein føremålstenleg måte med omsyn til tilgjengelegheit. Revisjonen merkar seg at det ikkje føreligg nokon operativ strategi for arbeidet til IKT-tenesta, og at EVIKT etterlyser både operative mål for arbeidet dei skal gjere, og meir langsiktig planlegging og strategisk arbeid frå eigarkommunane med omsyn til kvar kommunane vil med ei felles IKT-teneste.

Vindafjord kommune har gjennom arbeidet sitt med strategisk plan for informasjonstryggleik i relativt stor grad arbeidd systematisk for å sikre at kommunen er tilstrekkeleg førebudd på komande krav og føringar innan IKT-området, og då særleg knytt til ny personvernlovgiving (GDPR).

Den strategiske planen for informasjonstryggleik tilfredsstiller nokre – men ikkje alle – krava til styringssystem for informasjonstryggleik. I planen blir rolle- og ansvarsdelinga knytt til informasjonstryggleik formalisert, men denne er i liten grad kjent i kommunen, og blir generelt ikkje praktisert. Fleire av rutinane for informasjonstryggleik i kommunen er vidare mangelfulle eller manglande. Revisjonen merkar seg særleg at kommunen ikkje har rutinar eller system som sikrar at oversikta over personopplysningar som blir handsama, eller at oversikta over inngåtte databehandlaravtalar, blir ajourført. Det er følgjeleg risiko både for at kommunen handsamar personopplysningar dei ikkje har oversikt over, og at eksterne leverandørar behandlar personopplysningar på vegner av kommunen utan at kommunen veit om det.

Revisjonen er merksam på at arbeidet med styringssystemet for informasjonstryggleik er pågåande, men på bakgrunn av desse svakheitene, meiner revisjonen at Vindafjord kommune ikkje har eit styringssystem for informasjonstryggleik som er i samsvar med krav i regelverket.

Undersøkinga viser at langt dei fleste respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller anna fortruleg informasjon i arbeidskvardagen. Likevel viser svara frå spørjeundersøkinga at nesten halvparten av respondentane berre delvis eller ikkje i det heile er kjende med kva oppgåver og ansvar som ligg til deira stilling med omsyn til informasjonstryggleik.

Det er revisjonen si vurdering at dei tilsette i Vindafjord kommune ikkje har tilstrekkeleg kjennskap til retningsliner og rutinar for informasjonstryggleik. Kommunen bryt slik med forskriftskrav om opplæring av tilsette, og det er risiko for at kommunen som eit resultat av manglande kompetanse blant dei tilsette også bryt med andre krav i regelverket knytt til handsaming av personopplysningar, og for informasjonstryggleik i kommunen generelt.

Det er fastsett kriterium for tilgjenge i IKT-systema nytta i Vindafjord kommune. EVIKT overvakar systema som kommunen nyttar, og informerer at dei når målet om 99,5 % oppetid. Det er lite skriftleggjorte rutinar knytt til arbeidet med systemtilgjenge, og det blir ikkje utarbeidd rapportar om oppetid frå EVIKT til kommunen. Det er slik vanskeleg for kommunen å kontrollere tilgjenge og stabilitet i systema dei nyttar noko som gjer det vanskeleg for kommunen å sette i verk ev. tiltak for å betre tilgjenge og stabilitet. Ein stor del av respondentane i spørjeundersøkinga opplever jamleg problem med IKT-systema.

Basert på funna i undersøkinga, tilrår revisjonen Vindafjord kommune å setje i verk følgjande tiltak:

1. ferdigstille styringssystemet for informasjonstryggleik slik at det oppfyller alle krava i regelverket, og som del av dette:
    a. etablere eit system som sikrar at kommunen har fullstendig og ajourført oversikt over kva personopplysningar som blir handsama
    b. sikre at det blir gjennomført risikovurderingar av IKT-systema og behandlingar av personopplysningar opp mot fastsette akseptkriterium for informasjonstryggleik
    c. gjennomføre tilstrekkeleg kontroll og etterprøving av informasjonstryggleiken i kommunen sine system
2. utarbeide tilstrekkeleg med informasjon om informasjonstryggleik til dei tilsette, og sikre at dei tilsette får den naudsynte opplæringa for å kunne ivareta informasjonstryggleiken på ein tilfredsstillande måte
3. vurdere å utarbeide strategi og operative mål for EVIKT
4. etablere samarbeidsorgan og møtepunkt som planlagd, jf. samarbeidsavtale til EVIKT
5. formalisere gjeldande opningstider for vakttelefonen til brukarstøtta
6. utarbeide utfyllande rutinar for risikovurderingar av systemtilgjenge opp mot fastsette akseptkriterium
7. etablere system for tilstrekkeleg kontroll av systemtilgjengelegheit, samt rutine for rapportering om nedetid frå EVIKT til kommunen

Vedlegg 1: Høyringsuttale

VINDAFJORD KOMMUNE

Frode (NO - Bergen) Lovlie

Rådmannen
Saksh: Yngve Folven Bergesen
Tlf:
Dato : 29.08.2018
Vår ref: 18/19806
Dykkar ref:
Arkiv: K1 - 216

Forvaltningsrevisjonsrapport til høyring

Vi viser til epost frå 16.08.2018 med rapport frå forvaltningsrevisjon av IKT og informasjonstryggleik til høyring.

Vindafjord Kommune tar rapporten til etterretning, og har ingen kommentarar utover dette.

Med helsing

Yngve Folven Bergesen
Rådmann

Dokumentet vert sendt utan underskrift. Det er godkjent i samsvar med interne rutinar.

Postadr: Rådhusplassen 1 5580 Ølen
Sentralbord: 53 65 65 65
Organisasjonsopplysn: Org.nr: 988 893 226 Bankgiro: 3240.10.04172
Nettadresser: **www.vindafjord.kommune.no** Epost:postmottak@vindafjord.kommune.no

Vedlegg 2: Revisjonskriterium

Innleiing

Revisjonskriteria er utleia frå autoritative kjelder i samsvar med krava i gjeldande standard for forvaltningsrevisjon. I dette prosjektet er revisjonskriteria i hovudsak utleia frå personopplysningslova med føreskrifter (personopplysningsforskrifta [POF], eForvaltningsforskrifta, helseregisterlova, norm for informasjonstryggleik i helse-, omsorgs- og sosialsektoren [Norma] og sikkerheitslova).

Internkontroll og risikostyring

§ 23 i kommunelova omtalar administrasjonssjefen sine oppgåver og mynde. Her står det at administrasjonssjefen er den øvste leiaren for den samla kommunale administrasjonen, med dei unntak som følgjer av lov, og innanfor dei rammer kommunestyret fastset.

Vidare står det at administrasjonssjefen skal «sørge for at administrasjonen drives i samsvar med lover, forskrifter og overordnede instrukser, og at den er gjenstand for betryggende kontroll.» Dette inneber at ein må ha eit system for internkontroll på plass for å sikre forsvarleg sakshandsaming. Eit sentralt tiltak i internkontrollsystem vil vere at det blir gjennomført risikovurderingar av sentrale kommunale tenesteområder, og at det blir sett i verk risikoreduserande tiltak for dei områda der desse vurderingane avdekker risikoar.

Rammeverk for styring av IKT-funksjonen

COBIT 5 er eit internasjonalt anerkjend rammeverk for styring av IKT-funksjonen i verksemder, utvikla av organisasjonen ISACA.[48] Rammeverket tek utgangspunkt i at IKT-funksjonen på ein effektiv og god måte skal underbyggje og bidra til at verksemda oppnår sine overordna mål. Med bakgrunn i dette har ein identifisert og definert ei rekkje mål og prosessar for IKT-funksjonen. Eksempelvis seier rammeverket at dersom det er eit overordna mål for verksemda å etterleve lovar og reguleringar må ein mellom anna sette følgjande mål for IKT-funksjonen:

- IKT-funksjonen skal sjølv etterleve, og skal hjelpe verksemda elles i å etterleve, lovkrav og reguleringar.
- IKT-funksjonen skal oppretthalde sikkerhet i informasjon, infrastruktur og applikasjonar.
- IKT-funksjonen skal handsame IKT-relatert risiko.
- IKT-funksjonen skal levere tenester i tråd med verksemda sine behov.
- IKT-funksjonen skal ha påliteleg og nyttig informasjon til å fatte avgjersler.
- IKT-funksjonen skal etterleve interne retningsliner.

Vidare identifiserer rammeverket ei rekkje prosessar som verksemder kan implementere for å bidra til at desse måla blir nådd.

Sentrale føringar for digitalisering i kommunal sektor

Kommunal- og moderniseringsdepartementet sendte i september 2017 ut brevet *Digitalisering i kommunal sektor* til alle ordførarar og rådmenn. I brevet blir dei viktigaste nye tiltaka med relevans for den kommunale sektor i den statlege digitaliseringspolitikken gjennomgått.[49] Brevet viser også til *Digitaliseringsrundskrivet*, som er ei samanstilling av pålegg og anbefalingar knytt til digitalisering av offentleg sektor. *Digitaliseringsrundskrivet* har blitt sendt ut kvart år sidan 2009, og blei for fyrste gong sendt til kommunane i 2016. Rundskrivet trekk fram ei rekkje krav som er heimla i lov, og som difor også gjeld kommunane. Vidare oppmodar departementet kommunane til å gjere seg kjende med krava som blir stilt til dei statlege verksemdene og vurdere om nokon av desse anbefalingane er relevante for kommunen sitt digitaliseringsarbeid.

Informasjonstryggleik

Informasjonstryggleik handlar om trygging av informasjon med omsyn til *konfidensialitet*, *integritet* og *tilgjengelegheit*.

[48] ISACA er ein internasjonal foreining som fokuserer på styring og kontroll innanfor IKT-sektoren.
[49] *Meld. St. 27 (2015-2016) Digital agenda for Norge* gjev eit oversyn over regjeringa sin digitaliseringspolitikk.

Å sørgje for konfidensialitet inneber å hindre ikkje-autorisert innsyn i informasjon som ikkje skal vere tilgjengeleg for alle; å sørgje for integritet inneber å hindre ikkje-autorisert endring og sletting av informasjon; å sørgje for tilgjengelegheit inneber å sikre tilgang til informasjon ved behov for tilgang.

Personopplysningslova og -forskrifta

Regelverket knytt til informasjonstryggleik omfattar mellom anna persopplysningslova og -forskrifta. Jf. personopplysningslova § 13 første ledd, skal den behandlingsansvarlege[50] og databehandlaren[51] «gjennom planlagt og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.»

I kommunen er det rådmannen som er behandlingsansvarleg.[52] Databehandlarar er eventuelle tenesteleverandører til kommunen som behandlar personopplysningar, som til dømes leverandør av lønn- og personalsystem. Ved bruk av databehandlar skal det jf. personopplysningslova § 15 og personopplysningsforskrifta § 2-15, skrivast avtale med behandlingsansvarleg.

Kapittel 2 i personopplysningsforskrifta stillar utfyllande krav og føresegn knytt til informasjonstryggleik i verksemder som behandlar personopplysningar. Kapittelet pålegg mellom anna slike verksemder å:

- fastsette tryggleiksstrategi for verksemda (§ 2-3)
- gjennomføre risikovurderingar etter fastsette kriterier (§ 2-4)
- etablere klare ansvars og –myndigheitsforhold for bruk av informasjonssystem (§ 2-7)
- etablere fysiske og tekniske tiltak for informasjonstryggleik t (§§ 2-10 til 2-14)
- sørgje for at dei tilsette har tilstrekkeleg kunnskap om informasjonstryggleik (§ 2-8)
- gjennomføre tryggleiksrevisjonar for å etterprøve at tiltak er sett i verk og fungerer (§ 2-5)
- behandle uønskte hendingar i informasjonssystemet som avvik (§ 2-6)
- foreta regelmessig gjennomgang på leiarnivå av tryggleiksmål og –strategi (§ 2-3)
- sikre at det ikkje blir overlevert personopplysningar elektronisk til andre verksemder dersom disse ikkje tilfredsstiller krava i tryggleiksføringane (§ 2-15)

Personopplysningslova § 14 pålegg den behandlingsansvarlege å «etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller medhold av denne loven, herunder sikre personopplysningenes kvalitet», altså eit internkontrollsystem. Personopplysningsforskrifta kapittel 3 stiller utfyllande krav knytt til omfanget og rutinane i den påkravde internkontrollen.

Krav til styringssystem for informasjonstryggleik

Eit styringssystem for informasjonstryggleik er eit system som samlar prosedyrar, rutinar og dokumentasjon knytt til informasjonstryggleik. Kommunen er mellom anna gjennom eForvaltningsforskrifta § 15 forplikta til å ha ein internkontroll basert på anerkjende standardar for styringssystem for informasjonstryggleik:

> Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.
>
> Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

[50] Personopplysningslova § 2 fjerde ledd definerer behandlingsansvarleg som «den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes».
[51] Personopplysningslova § 2 femte ledd definerer databehandlar som «den som behandler personopplysninger på vegne av den behandlingsansvarlige».
[52] Jf. *En veiledning om internkontroll og informasjonssikkerhet* (Datatilsynet 2009, s. 11).

Direktorat for forvaltning og IKT (Difi) er peika ut som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttas. Difi tilrår at offentlege verksemder baserer seg på ISO/IEC 27001:2013, som er ein internasjonal standard for styringssystem for informasjonstryggleik.

Anna regelverk

I tillegg til krava i personopplysningsforskrifta og eForvaltningsforskrifta er det også fleire andre reglar knytt til informasjonstryggleik som er relevant for kommunen. Krava i desse regelverka er i nokon grad overlappande med krava til eit styringssystem for informasjonstryggleik.

I helseregisterlova er det gitt konkrete føringar knytt til handsaminga av helseopplysningar, og her kjem det mellom anna fram konkrete krav knytt til informasjonstryggleik (§ 16). Det er utarbeidd ein norm for informasjonstryggleik i helse-, omsorgs- og sosialsektoren (Norma), som stillar krav med utgangspunkt i både personopplysningsforskrifta og helseregisterlova. I Norma er det også innarbeidd ulike krav knytt til teieplikt og informasjonsrett etter særlovgiving for kommunehelsetenester, sosialtenester, psykisk helsevern, samt forvaltnings- og offentlegheitslov.

Kommunen er også omfatta av sikkerheitslova, og har som følgje av dette plikt til å ha forsvarleg informasjonstryggleik for informasjon som kan vere kritisk for å forhindre truslar som spionasje, sabotasje og terrorhandlingar. Desse krava kan vere relevante for kommunen for eksempel når det gjeld å beskytte vassforsyninga frå forureining av drikkevatn.

Vedlegg 3: Sentrale dokument og litteratur

Regelverk

- Justis- og beredskapsdepartementet: Lov om behandling av personopplysninger (personopplysningsloven). LOV-2000-04-14-31. Sist endret 01.10.2015.
- Kommunal- og moderniseringsdepartementet: Forskrift om behandling av personopplysninger (personopplysningsforskriften). FOR-2000-12-15-1265. Sist endret 01.01.2017.
- Kommunal- og moderniseringsdepartementet: Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). FOR-2004-06-25-988. Sist endret 01.07.2014.

Rettleiarar og standardar

- Datatilsynet: Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer. 2000.
- Datatilsynet: En veiledning om internkontroll og informasjonssikkerhet. 2009.
- Datatilsynet: Kommunens Internkontroll. Verktøy for rådmenn. 2012.
- Datatilsynet: Risikovurdering av informasjonssystem. 2015
- Helsedirektoratet: Norm for informasjonssikkerhet. Helse og omsorgstjenester. 2015.

Kommunale dokument og avtaler

- Overordna samarbeidsavtale EVIKT
- Sak om vertskommunesamarbeid (EVIKT)
- Tenesteleveringsavtale EVIKT
- Diverse rutineskildringar for EVIKT
- Organisasjonskart
- Oversikt over databehandlaravtalar
- Delegeringsreglement for Vindafjord kommune 2016-2019
- Introduksjon av nye medarbeidarar
- Spørjeundersøking evaluering EVIKT
- Strategisk plan for informasjonstryggleik med følgjande vedlegg:
    - Oversikt over personopplysningar (vedlegg til strategisk plan for informasjonstryggleik)
    - Utkast til rammeverk for risikoanalyse (vedlegg til strategisk plan for informasjonstryggleik)
    - Informasjonstryggleik – retningsliner for tilsette
    - Informasjonstryggleik – retningsliner for tilsette (tommelfingerreglar, kortversjon)
    - Avtaleskisse - Databehandleravtale
    - Rutine for tryggleikskopiering - Backup
    - Rutine for fysisk tryggleik

Vedlegg 4: Supplerande informasjon

Tabell 4: Vindafjord kommune sine databehandlaravtalar

År	Firma	System	Eining/avdeling
2011	Biblioteksystemer	Nasjonal lånekort	Vindafjord bibliotek
2011	ACOS	WebSak	Vindafjord kommune
2011	ACOS	Portalløsninger	Vindafjord kommune
2011	ACOS	CosDoc	Vindafjord kommune
2011	ACOS	Barnevern	Barnevern
2011	ACOS	Sosial-NAV	NAV
2012	Conexus	Vokal	Elevkartleggingsverktøy Web-basert
2013	Hove Medical System AS	System X	Ølen legekontor
2013	Hove Medical System AS	System X	Vikedal legekontor
2013	Hove Medical System AS	System X	Etne og Vindafjord legevakt
2013	Hove Medical System AS	System X	Fengselshelsetenesta
2013	Medilink Software AS	Medilink EDI	Ølen legekontor
2013	Medilink Software AS	Medilink EDI	Vikedal legekontor
2014	Hove Medical System AS	System X	Vindafjord helsestasjon
2014	Medilink Software AS	Medilink EDI	Etne og Vindafjord legevakt
2014	Medilink Software AS	Medilink EDI	Fengselshelsetenesta
2014	Medilink Software AS	Medilink EDI	Vindafjord helsestasjon
2014	Folkehelseinstituttet	Prøvetaking,analyse	Vindafjord kommune
2014	Visma	Visma Flyt skole	Vindafjord kommune
2016	Speedware ApS	Speedware administrasjonsprogram	Vindafjord kulturskule
2016	Norkart	KOMTEK-data og matrikkeldata. Gisline	Vindafjord kommune
2017	Integerings- og mangfoldsdirektoratet	IMDinett	Nasjonalt introduksjonsregister, Sakshandsamarsystem for busetjing
2017	Husbanken -region vest	Saksbehandling startlån mm	Vindafjord kommune
2017	Visma	Visma PPI	PPT Etne og Vindafjord

Tabell 5: Oversikt over personopplysningar i Vindafjord kommune

Formål	System	Heimel	Klassifisering	Sikrings-tiltak	Lagring og kommunikasjon	Konsesjon og arkivering	Systemeigar
Løn og personal	Visma Unique	Personopplysnings-forskrift § 7-16d	Person-opplysningar	Tilgangsstyring	Lagra på kommunal server Internt kommunalt nettverk	Fritatt frå både konsesjons-og meldeplikt	Økonomi og personalavdelinga
Rekrutterings-program	Visma Unique HRM	Lov om personoppl.§ 8, § 9, første ledd	Person-opplysningar	Tilgangsstyring	Lagra på kommunal server Skybasert pålogging for søkar	Fritatt frå både konsesjons-og meldeplikt	Økonomi og personalavdelinga
Fagsystem Pleie og Omsorg	ACOS Cosdoc	Personopplysningsl oven § 33 5. Ledd Helsepersonelloven §§ 26 og 39,	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone	Ingen konsesjons-plikt, men meldeplikt	Kommunalsjef
Fagsystem barnevern	ACOS Barnevern	Personopplysningsl oven § 33 5. Ledd Barnevernloven § 3-1 (jf. kap. 4)	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone	Ingen konsesjons-plikt, men meldeplikt	Einingsleiar barnevern
Fagsystem Sosial	ACOS Sosial	Personopplysningsl oven § 33 5. Ledd Sosialtjenesteloven § 3 (jf. kap. 4, 5 og 6	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone	Ingen konsesjons-plikt, men meldeplikt	Einingsleiar NAV
Fagsystem Lege	X-system	Personopplysningsl oven § 33 5. Ledd Helsepersonelloven §§ 26 og 39,,	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone	Ingen konsesjons-plikt, men meldeplikt	Kommunalsjef
Fagsystem helsestastjon	X-system	Personopplysningsl oven § 33 5. Ledd Helsepersonelloven §§ 26 og 39,,	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone	Ingen konsesjons-plikt, men meldeplikt	Kommunalsjef
Fagsystem barnehage	Visma barnehage	Personopplysnings-forskrift § 7-21	Person-opplysningar	Tilgangsstyring	Lagra på kommunal server Internt kommunalt nettverk	Unntatt både frå konsesjons- og meldeplikt	Stabsrådgjevar barnehage
Fagsystem skule	Visma Flyt	Lov om personoppl.§ 8, § 9, første ledd	Person-opplysningar	Tilgangsstyring	Skyapplikasjon. Arkivopplysningar lagra på kommunal server	Ingen konsesjons-plikt, men meldeplikt	Stabsrådgjevar Skule

					Internt kommunalt nettverk + sikker skypålogging		
Individuell opplærings-plan	Visma IOP	Lov om personoppl.§ 8, § 9, første ledd	Sensitive person opplysningar	Tilgangsstyring	Skylagring Lagra på server i Norge	Ingen konsesjons-plikt, men meldeplikt	Stabsrådgjevar Skule
Fagsystem kulturskule	Speed admin	Lov om personoppl.§ 8, § 9, første ledd	Person-opplysningar	Tilgangsstyring	Skylagring Lagra på server i Norge	Ingen konsesjons-plikt, men meldeplikt	Avdelingsleiar Kulturskulen
Fagsystem PP-tenesta	PPI	Personopplysningsloven § 33 5. Ledd Opplæringsloven § 13-5, 1. ledd, jf. § 5-6	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone	Ingen konsesjons-plikt, men meldeplikt	Einingsleiar PPT
Sak/arkiv-system	ACOS WebSak	Lov om personoppl.§ 8, § 9, første ledd, jfr. arbeidsm.l. § 20	Saksopp-lysningar som kan vere knytta til personar	System-funksjonar som sperrer mot innsyn	Lagra på kommunal server	Ingen konsesjons-plikt, men meldeplikt	Einingsleiar service og fellesavdeling
Elektronisk mottak av skjemaer/ søknader	ACOIS mottak	Lov om personoppl.§ 8, § 9, første ledd	Person-opplysningar	Tilgangsstyring	Lagra på kommunal server	Ingen konsesjons-plikt, men meldeplikt	Einingsleiar service og fellesavdeling
Formidlings-system. Sending og mottak av dokument	KS SVARUT		Person-opplysningar Sensitive personopp-lysningar	Tilgangsstyring. Sikker pålogging (nivå 4) for å hente dokument med sensitiv informasjon	Skybasert pålogging	Ingen konsesjons-plikt, men meldeplikt	Einingsleiar service og fellesavdeling

Deloitte.