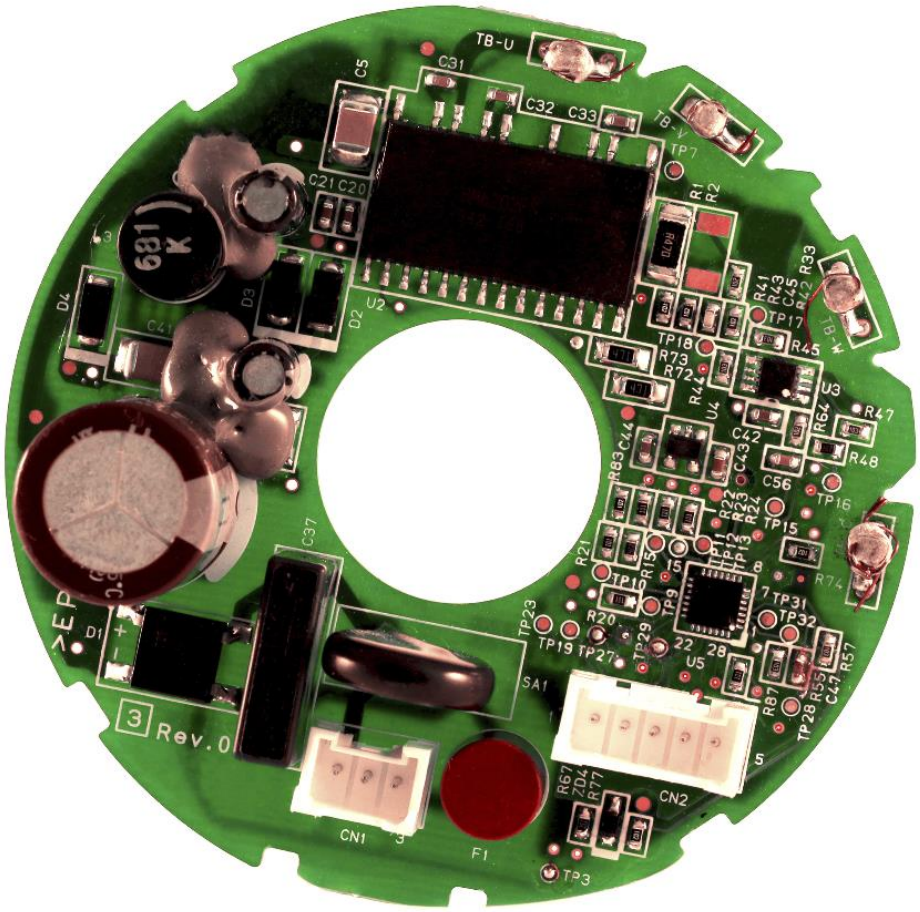
Deloitte.



Forvaltningsrevisjon | Etne kommune

IKT og informasjonstryggleik

August 2018

«IKT og informasjonstryggleik»

August 2018

Rapporten er utarbeidd for Etne 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 Etne kommune gjennomført ein forvaltningsrevisjon av IKT og informasjonstryggleik i kommunen. Føremålet med forvaltningsrevisjonen har vore å undersøkje om kommunane Etne og Vindafjord 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 Etne 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 Etne 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. 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 også 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.

Etne kommune har kome i gang med å førebu seg på komande krav og føringar innan IKT-området, og då særleg ny personvernlov (GDPR). Arbeidet er på eit relativt tidleg stadium, og revisjonen meiner difor at Etne kommune berre i avgrensa grad har arbeidd systematisk for å sikre at kommunen er tilstrekkeleg førebudd på komande krav og føringar innan IKT-området.

Etne kommune har styrande dokument for informasjonstryggleik. Desse er ikkje oppdaterte og blir i liten grad nytta. T.d. blir ikkje den formelle ansvars- og rolledelinga følgt i praksis, kontroll og etterprøving av informasjonstryggleiken finn berre stad i avgrensa grad, det blir ikkje sett akseptkriterium knytt til informasjonstryggleik, og etter det revisjonen kjenner til, blir det heller ikkje gjennomført tryggleiksrevisjonar. Kommunen har ikkje noko system som sikrar at oversikta over personopplysningar som kommunen handsamar er oppdatert og fullstendig, og heller ikkje noko system for å halde oversikta over kva databehandlaravtalar dei har inngått er oppdatert eller fullstendig. Det er difor risiko for at kommunen handsamar personopplysningar dei ikkje veit om, og at eksterne leverandørar behandlar personopplysningar på vegner av kommunen utan at kommunen veit om det.

På bakgrunn av desse svakheitene, meiner revisjonen at Etne kommune ikkje har eit styringssystem for informasjonstryggleik som er i samsvar med krav i regelverket.

Undersøkinga viser at dei fleste av respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller anna fortruleg informasjon i arbeidskvardagen. Likevel svara nesten 40 % av respondentane at dei 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 Etne 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 Etne 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

Samandrag		3
1.	Innleiing	7
2.	Om tenesteområdet	10
3.	Organisering av felles IKT-teneste i Etne og Vindafjord	12
4.	Rutinar for systemtilgjengelegheit	17
5.	Styringssystem for informasjonstryggleik	21
6.	Kompetanse om informasjonstryggleik	27
7.	Konklusjon og tilrådingar	38
Vedlegg 1 : Høyringsuttale		40
Vedlegg 2 : Revisjonskriterium		41
Vedlegg 3 : Sentrale dokument og litteratur		44
Vedlegg 4 : Supplerande informasjon		45

Detaljert innhaldsliste

Samandrag 3

1. Innleiing 7
   - 1.1 Bakgrunn 7
   - 1.2 Føremål og problemstillingar 7
   - 1.3 Avgrensing 7
   - 1.4 Metode 8
   - 1.5 Revisjonskriterium 9

2. Om tenesteområdet 10
   - 2.1 Organisering av informasjonstryggleiksarbeidet i Etne kommune 10
   - 2.2 Interkommunalt IKT-samarbeid mellom Etne og Vindafjord kommune 10

3. Organisering av felles IKT-teneste i Etne og Vindafjord 12
   - 3.1 Problemstilling 12
   - 3.2 Revisjonskriterium 12
   - 3.3 Mål og strategi for IKT-tenesta 13
   - 3.4 IKT-tenesta si rolle og ansvar 14
   - 3.5 IKT-tenesta si tilgang på kompetanse og kapasitet 15
   - 3.6 Systematisk arbeid for å førebu IKT-tenesta på komande krav og føringar 16

4. Rutinar for systemtilgjengelegheit 17
   - 4.1 Problemstilling 17
   - 4.2 Revisjonskriterium 17
   - 4.3 Kriterium for tilgjengelegheit 17
   - 4.4 Kontrollar av tilgjengelegheit og stabilitet i IKT-systema 18
   - 4.5 Oppleving av driftstryggleik i IKT-systema 18
   - 4.6 Organisering av IKT-brukarstøtte 19

5. Styringssystem for informasjonstryggleik 21
   - 5.1 Problemstilling 21
   - 5.2 Revisjonskriterium 21
   - 5.3 Styrande dokument for informasjonstryggleik 21
   - 5.4 Rutinar og ansvarsforhold knytt til informasjonstryggleik 22
   - 5.5 Kontroll og etterprøving av informasjonstryggleik 24

6. Kompetanse om informasjonstryggleik 27
   - 6.1 Problemstilling 27
   - 6.2 Revisjonskriterium 27
   - 6.3 Rutinar for opplæring i informasjonstryggleik 27
   - 6.4 Kjennskap til retningsliner og rutinar for informasjonstryggleik 28
   - 6.5 Etterleving av retningsliner og rutinar for informasjonstryggleik 34

7. Konklusjon og tilrådingar 38

Vedlegg 1 : Høyringsuttale 40

Vedlegg 2 : Revisjonskriterium 41

Vedlegg 3 : Sentrale dokument og litteratur 44

Vedlegg 4 : Supplerande informasjon 45

Figurar

Figur 1: Formell ansvarsorganisering for informasjonstryggleiken i Etne kommune 10
Figur 2: Formell organisering av felles IKT system i Etne og Vindafjord kommune 11
Figur 3: Når eg kontaktar IKT-tenesta får eg god hjelp (N=104) 15
Figur 4: Driftstryggleik i IKT-systema 19
Figur 5: Brukarstøtta for IKT 20
Figur 6: Handsaming av personopplysningar (N=107) 28
Figur 7: Tydelege og skriftlege retningsliner for handsaming av... 29
Figur 8: Teieplikt og tryggleiksinstruks 29
Figur 9: Kjennskap til eige ansvar og oppgåver knytt til informasjonstryggleik (N=106) 30
Figur 10: Viktigheita av informasjonstryggleik (N=107) 30
Figur 11: Opplæring av tilsette 31
Figur 12: Opplæring i informasjonstryggleik i Etne kommune 32
Figur 13: Mottatt opplæring 33
Figur 14: Kva gjer du vanlegvis når du i løpet av arbeidsdagen går frå PC-en du nyttar? (N=106) 34
Figur 15: Korleis oppbevarer du dokument (papir) med fortruleg informasjon? (N=105) 34
Figur 16: Fjerning av fortruleg informasjon frå møterom (N=107) 35
Figur 17: Avviksmelding (N=106) 35
Figur 18: Informasjonstryggleikspraksis - PC og passord 36
Figur 19: Informasjonstryggleik - dokumenthandsaming 36

Tabellar

Tabell 1: Svarprosent 8
Tabell 2: Sentrale mål og strategiar knytt til informasjonstryggleik i Etne kommune 22
Tabell 3: Rollar og ansvar knytt til internkontroll av informasjonstryggleiken i Etne kommune 22
Tabell 4: Oversikt over personopplysningar, Etne kommune 45

1. Innleiing

1.1 Bakgrunn

Deloitte har gjennomført ein forvaltningsrevisjon av IKT og informasjonstryggleik i Etne kommune. Prosjektet blei bestilt av kontrollutvalet i Etne kommune i møte 21. november 2017, sak 19/17.

Bakgrunnen for prosjektet er ein invitasjon frå kontrollutvalet i Vindafjord kommune om gjennomføring av felles forvaltningsrevisjon av IKT og informasjonstryggleik. Kommunane Etne og Vindafjord har felles IKT-avdeling.

1.2 Føremål og problemstillingar

Føremålet med forvaltningsrevisjonen har vore 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 har det vore eit føremål å undersøkje om Etne 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 Etne kommune sine styringssystem for informasjonstryggleik for å kartlegge rutinar og retningsliner, 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 Etne kommune har vi i tillegg intervjua leiaren ved tenestetorget og systemansvarleg for fagsystema innanfor pleie og omsorg. Totalt intervjua vi tre personar i samband med forvaltningsrevisjonen i Etne kommune.[1]

1.4.3 Spørjeundersøking

Revisjonen har gjennomført ei elektronisk spørjeundersøking blant eit utval tilsette i Etne kommune. Føremålet med spørjeundersøkinga var 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 210 tilsette, og etter fleire påminningar, kom det til sist 107 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 17 % (natur og næring) og 85 % (stab, støttefunksjonar og IKT). Total svarprosent var 51 %.

Tabell 1: Svarprosent

Tenesteområde	Svarprosent
Bustad og eigedom	27 %
Helse og omsorg	43 %
Kultur, idrett, fritid og reiseliv	50 %
Natur og næring	17 %
Oppvekst, skule og familie	53 %
Stab, støttefunksjonar og IKT	85 %
Totalt	**51 %**

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, og mindre faktafeil er retta opp i den endelege versjonen. Høyringsutkast av rapporten blei sendt til rådmannen for uttale, og rådmannen sin høyringsuttale er lagt ved den endelege 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, og eForvaltningsforskrifta. Kriteria er nærare presentert innleiingsvis under kvart tema, og i vedlegg 2 til rapporten.[3]

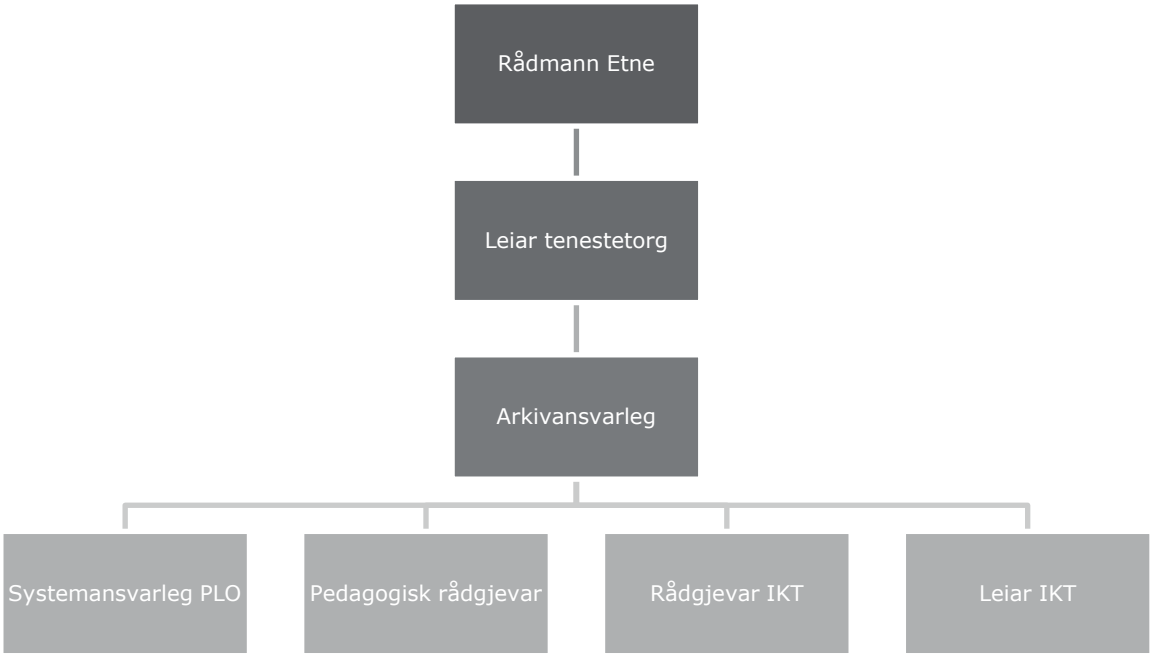
[2] RSK 001, sjå http://www.nkrf.no/rsk_001_standard_for_forvaltningsrevisjon
[3] I 2018 trer eit nytt og strengare regelverk knytt til personopplysningar i kraft (GDPR, sjå https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/).

2. Om tenesteområdet

2.1 Organisering av informasjonstryggleiksarbeidet i Etne kommune

Arbeidet med informasjonstryggleik i Etne kommune er formelt organisert som vist i figur 1 under. Det er rådmannen i kommunen som har det overordna ansvaret for informasjonstryggleik i kommunen. IKT-leiar det overordna ansvaret for bruken av IKT i kommunen.[4]

Figur 1: Formell ansvarsorganisering for informasjonstryggleiken i Etne kommune[5]



2.2 Interkommunalt IKT-samarbeid mellom Etne og Vindafjord kommune

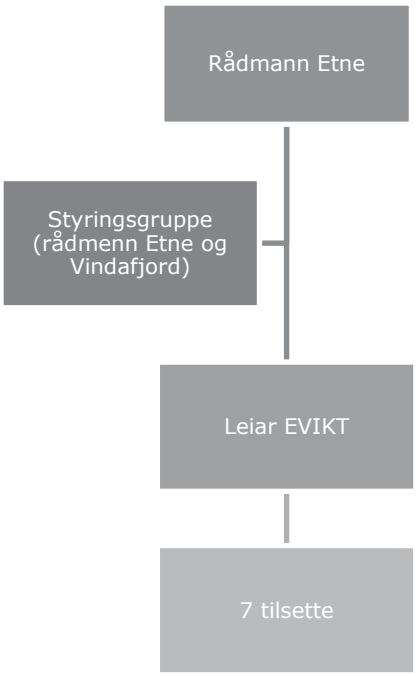
Den felles IKT-tenesta i Etne og Vindafjord kommune (EVIKT) er formelt organisert som vist i figur 2 under. Det er åtte tilsette i EVIKT, inkludert IKT-leiaren. Fire av desse i tillegg til IKT-leiaren arbeider primært med IKT-drift, og tre arbeider i hovudsak med brukarstøtte.

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. Avtalen, og ev. endringar i avtalen, skal vedtakast i kommunestyra 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 kommunen saka høyrer heime.[6]

[4] Organisasjon og ansvar for IKT i Etne kommune. Elektronisk dokument på Etne kommune sitt kvalitetsstyringssystem på kommuneforlaget.no.
[5] Oversikta er tilsendt i oversendingsbrev frå Etne kommune i samband med forvaltningsrevisjonen.
[6] 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[7]



[7] 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.[8] 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.[9] 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.

[8] *Meld. St. 27 (2015-2016) Digital agenda for Norge* gjev eit oversyn over regjeringa sin digitaliseringspolitikk.
[9] 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,[10] og i tenesteleveringsavtalen som regulerer tenestytinga i samarbeidet,[11] 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.[12]

For Etne kommune var nokre av måla med etableringa av EVIKT å oppnå «kostnadseffektivitet ved innkjøp, kvalitet, kompetanse, meir robust driftsteneste, god styring av IKT-funksjonane, betre tilbod til publikum og næringsliv og høve til samarbeid om tenester». I intervju kjem det fram at kompetansevinsten er oppnådd gjennom samanslåinga av IT-avdelingane i kommunane.

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 som er meint å styre utvikling av samarbeidet som skildra i samarbeidsavtalen. I første fase er det fokus på etablering av ei felles personalgruppe og felles driftsorganisasjon, samt etablering av hovudkontoret og felles vaktordning for kommunane. Andre 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.[13]

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.[14]

---

[10] 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.

[11] 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.

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

[13] Jf. samarbeidsavtala, skal samarbeidet evaluerast 1 år etter samlokalisering av driftsorganisasjonen. I kommunikasjon med Vindafjord kommune blir det opplyst 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.

[14] 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 underlagt 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 om at det er oppretta IKT-råd 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 tenesteleveringsavtalen; her går det mellom anna fram at EVIKT er databehandlar og at rådmennene i dei to kommunane er behandlingsansvarlege, jf. personopplysningslova mv.[15] 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.[16]

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 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

[15] Også i Vindafjord kommune sin nyleg utarbeida strategisk plan for informasjonstryggeik, går informasjonstryggleiksansvaret til EVIKT fram.
[16] Dette arbeidet er nærare skildra i kapittel 4.

aukar sannsynet både for at det dannar seg ulikheiter med omsyn til forventningar og ulike rolle- og ansvarsforståingar.

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

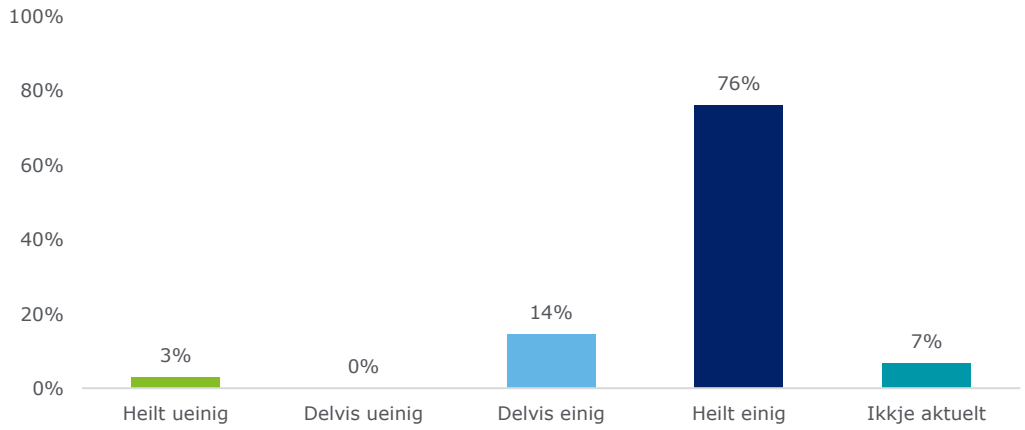
3.5.1 Datagrunnlag

EVIKT har i dag er åtte tilsette med variert erfaring og bakgrunn.[17] 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.[18] Vindafjord kommune er elles med KInS,[19] og både leiaren og tilsette i EVIKT har deltatt på seminar og kurs der. Det føreligg ingen formell opplæringsplan for tilsette i EVIKT.

I spørjeundersøkinga blei respondentane bedt 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 figur 3, seier 76 % av respondentane i Etne kommune seg «heilt einig» i påstanden, 14 % er «delvis einig», medan 3 % er «heilt ueinig».[20]

Figur 3: Når eg kontaktar IKT-tenesta får eg god hjelp (N=104)



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.

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.

[17] Utdanninga er som følgjer: fem med bachelorgrad i IKT, ein med mastergrad i IKT, ein fagarbeidar og ein lærling.
[18] Til dømes innanfor Microsoft- eller Cisco-system.
[19] Foreininga Kommunal informasjonssikkerhet.
[20] Meir om brukarane si oppleving av brukarstøtta under avsnitt 4.6.1.

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

Etne kommune opplyser at det er starta opp arbeid med å tilpasse seg nye krav og føringar på IKT-området. T.d. kjem det fram i intervju at det nyleg er sett ned ei gruppe som skal jobbe med å førebu kommunen på dei komande krava knytt til ny personvernlov (GDPR).[21]

Denne arbeidsgruppa arbeider utifrå eit mandat sett av rådmannen, og gruppa har våren 2018 arbeidd ut mot avdelingane i kommunen for å få oversikt over kva system som er i bruk der ein handsamar personopplysningar, og for å registrere kva arbeidsoppgåver der ein handsamar personopplysningar.

Gruppa har òg vurdert ulike styringssystem for informasjonstryggleik, og har no innstilt til rådmannen kva system dei ønskjer at kommunen skal kjøpe.[22]

Kommunen har oppnemnd leiaren for tenestetorget som kommunen sitt personvernombod. Det er ikkje avgjort om dette er ei varig løysing, og kommunen er mellom anna i samtalar med Vindafjord kommune om moglegheita for eit felles personvernombod.

Det går vidare fram i intervju at kommunen er med i eit samarbeid med fleire av kommunane på Haugalandet kalla «Nettverksgruppe - personvern».[23] Hovudmålet med arbeidet i gruppa er å førebu kommunane på GDPR, mellom anna gjennom opplæring av tilsette, utabeiding av personvernstrategiar, kartleggja personopplysningar i alle avdelingar, osb. Det er opp til kvar enkelt kommune å gjere sine eigne vurderingar og endringar for å vere i samsvar med GDPR, men samarbeidet gjev deltakarkommunane moglegheit til å utveksle erfaringar og få innspel til korleis ein kan arbeide meir aktivt med informasjonstryggleik.

Det kjem fram i intervju at Etne kommune fortsatt har eit stykke igjen før dei er tilstrekkeleg førebudd på komande krav og føringar på IKT-området. Leiaren for den felles IKT-tenesta fortel i intervju at han har forsøkt å få auka merksemd på dei komande krava , men at det har vore utfordrande å få i gang satsingar på dette i Etne kommune.

3.6.2 Vurdering

Revisjonen finn i sine undersøkingar at Etne kommune har kome i gang med å førebu seg på komande krav og føringar innan IKT-området, særleg gjennom deltaking i den interkommunale informasjonstryggleiksgruppa på Haugalandet, og arbeidsgruppa som førebur kommunen på GPDR. På revisjonstidspunktet var dette arbeidet fortsatt pågåande og på eit relativt tidleg stadium. Det er difor revisjonen si vurdering at Etne kommune i berre avgrensa grad har arbeidd systematisk for å sikre at kommunen er tilstrekkeleg førebudd på komande krav og føringar innan IKT-området.

[21] General Data Protection Regulation. Sjå: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/personvernregelverket/.
[22] Sjå også kapittel 5.
[23] Desse kommunane er med i Nettverksgruppe - personvern: Haugesund, Karmøy, Tysvær, Vindafjord, Etne, Bokn, Suldal, Sveio og Utsira.

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 paragrafens første ledd 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

Etne kommune har eit dokumentert internkontrollsystem for informasjonstryggleik.[24] Som del av internkontrollsystemet ligg det eit dokument kalla «sikring av tilgjenge», der det mellom anna går fram at det skal treffast tiltak for å sikre tilgang til personopplysningar der slik tilgjenge er naudsynt, og at sikringstiltaka også skal trygge tilgang til annan informasjon som er avgjerande for informasjonstryggleiken.

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.[25]

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 forbetring 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.

[24] Internkontrollsystem IT-tryggleik
[25] 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 unnatak – skal levere ei oppetid på i IKT-systema på 99,5 %.[26]

I intervju blir det opplyst at EVIKT har system for å gjere risikovurderingar knytt til endringar i IKT-systema.[27] 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 Etne 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 Etne 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 Etne 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 Etne 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

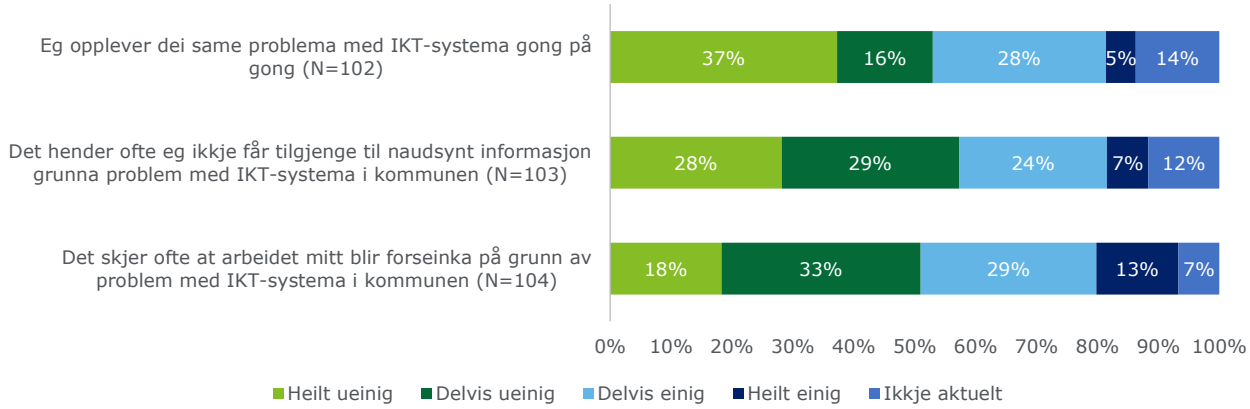
4.5.1 Datagrunnlag

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 4 under.

Svara indikerer at éin av tre av respondentane i Etne kommune opplever dei same problema med IKT-systema gong på gong. Vidare svara nesten like mange at dei er «delvis einig» eller «heilt einig» i påstanden om at dei ofte ikkje får tilgang til naudsynt informasjon på grunn av problem med IKT-systema i kommunen, og over 40 % at ofte opplever at arbeidet deira blir forseinka på grunn av problem med IKT-systema i kommunen.

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

Figur 4: Driftstryggleik i IKT-systema



Respondentane fekk også høve til å spesifisere om lag kor ofte dei opplever å bli forseinka i arbeidet sitt, og kor ofte dei ikkje får tilgang til naudsynt informasjon på grunn av problem med IKT-systema. 5 % svara at dei dagleg blir forseinka i arbeidet sitt grunna problem med IKT-systema i kommunen, 12 % at dei vekentleg opplever dette, og 36 % svara at dei månadleg opplever å ikkje få tilgjenge til naudsynt informasjon grunna problem med IKT-systema.

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 Etne 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 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, medan no er denne tenesta tilgjengeleg for begge kommunane. 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 utløyser bruk av vakttelefonen, og då særleg frå tilsette som jobbar på ukurante tidspunkt – t.d. barnevernet – som har behov for brukarstøtte utanfor ordinær arbeidstid.

Systemansvarleg for fagsystema i pleie og omsorg i Etne kommune fortel i intervju at ho som oftast tar kontakt med leverandøren direkte dersom det er problemstillingar knytt til fagsystemet. Kommunen har eit tenesteabonnement hos leverandøren, noko som gjer at ein kan be om utvida støtte. Vidare kjem det fram i intervju at ho sjeldan får telefonar frå tilsette knytt til fagsystema utanom arbeidstid. Dersom dei tilsette har problemstillingar knytt til fagsystem eller IKT utanom ordinær arbeidstid, opplever ho at dette blir løyst internt på avdelinga. Ho har sjølv størsteparten av ansvaret for fag- og IKT-systema innanfor

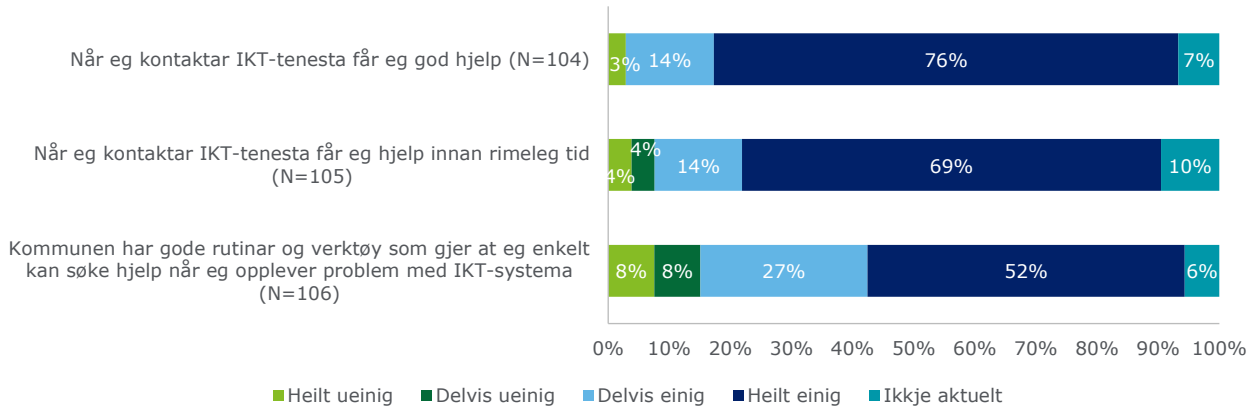
pleie og omsorg, medan IKT-tenesta støttar med oppgraderingar og liknande. Ho saknar noko meir støtte frå IKT-tenesta, men det er hennar erfaring at IKT-tenesta i liten grad følgjer opp fagsystema.

Leiaren for EVIKT meiner at dei tilsette i kommunen er nøgde med brukarstøtta, og får like god og effektiv hjelp no som før samanslåinga av IT-avdelingane i dei to kommunane. Han 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 eit stort fleirtal av respondentane var frå Vindafjord kommune.[28] 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 5:

Figur 5: Brukarstøtta for IKT



Langt dei fleste respondentane svara at dei er nøgde med hjelpa dei får frå EVIKT. Til saman 8 % av respondentane seier seg «delvis ueinig» eller «heilt ueinige» i påstanden om at dei får *hjelp innan rimeleg tid* når dei kontaktar IKT-tenesta, og 16 % er «heilt ueinig» eller «delvis ueinig» i at *kommunen har gode rutinar og verktøy som gjer at eg enkelt kan søke hjelp når eg opplever problem med IKT-systema.*

Respondentane i spørjeundersøkinga fekk moglegheit til å kome med ytterlegare kommentarar knytt til arbeidet til EVIKT; med få unntak var dei som nytta denne sjansen nøgde med brukarstøtta og EVIKT.

4.6.2 Vurdering

Revisjonen finn i sine undersøkingar at brukarstøtta til EVIKT 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.

[28] 76,3 % av respondentane er tilsett i Vindafjord kommune, medan 23,7 % er tilsett i Etne kommune.

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

Etne kommune har eit dokumentert styringssystem for informasjonstryggleik tilgjengeleg på internett gjennom kommunen sitt kvalitetssystem. Systemet inneheld ei rekkje styringsdokument, rutinar og retningsliner for informasjonstryggleik. Overordna er føremålet med styringssystemet å sikre at personvern blir ivaretatt i praksis, og at kommunen kan dokumentere samsvar mellom eigen praksis og regelverket.[29]

Tabell 2 presenterer sentrale mål og strategiar knytt til informasjonstryggleik i Etne kommune slik desse går fram i styringssystemet:

[29] Kommunen opplyser at dei vurderer å kjøpe eit IKT-verktøy for handsaming av personopplysingar.

Tabell 2: Sentrale mål og strategiar knytt til informasjonstryggleik i Etne kommune

Prosedyre/reglement	Samandrag
Tryggleiksmål og strategiar	Sikker og effektiv sakshandsaming av personopplysningar. Informasjonstryggleiken i kommunen skal kontinuerlig etterprøvast og forbetrast, og tilsette skal ha tilstrekkeleg kompetanse og opplæring på området. Tryggleiksstrategien skal ha tryggleiksmålet som utgangspunkt, og på overordna nivå skildre ansvars- og myndetilhøve, forholdet til partnarar og leverandørar samt organisatoriske og tekniske tryggingstiltak.
Hovudmål for informasjonstryggleik	Yte innbyggarane tenester med høg kvalitet og utnytta kommunen sine ressursar optimalt. Bruk av moderne informasjonsteknologi gjer det mogleg å løysa kommunale oppgåver best mogleg. Bruk av slik teknologi introduserer trugslar overfor dei opplysningane som blir handsama. Kommunen sitt overordna mål ved elektronisk handsaming av personopplysningar er sikker og effektiv sakshandsaming
Tryggleiksstrategi	Det er utforma sju tryggleiksstrategiar knytt til dokumenttryggleik, systemteknisk sikring, strategi for fysisk tryggleik, personelltryggleik, partnarar og leverandørar, og organisering av informasjonssystemet.

Dokumenta i styringssystemet blei lagt inn i kvalitetssystemet i desember 2017. I intervju kjem det fram at systemet opphaveleg blei utarbeidd for om lag 18 år sidan. Styringssystemet skal ha blitt revidert sidan den gong, men revisjonen har ikkje fått informasjon om på kva tidspunkt det har blitt revidert.

Vidare kjem det fram i intervju at styringssystemet for informasjonstryggleik ikkje eller berre i avgrensa grad blir nytta i det daglege informasjonstryggleiksarbeidet i kommunen. Det har heller ikkje vore tema i leiargruppa i kommunen.

Ifølgje EVIKT-leiar går det fram gjennom samtalar med tilsette og leiarar i kommunen at det er lite kunnskap knytt til innhaldet i styringssystemet for informasjonstryggleik i kommunen.

5.3.2 Vurdering

Etne kommune har styrande dokument for informasjonstryggleik. Delar av systemet er i samsvar med krav i regelverket, men fordi det ikkje har blitt oppdatert på fleire år, er også delar av systemet utdatert. Vidare kjem det fram i intervju at systemet ikkje eller berre i avgrensa grad blir nytta i det daglege informasjonstryggleiksarbeidet i kommunen. Basert på funna i undersøkingane, er det revisjonen si vurdering at Etne kommune sine styrande dokument for informasjonstryggleik ikkje er i samsvar med krav i regelverket.

5.4 Rutinar og ansvarsforhold knytt til informasjonstryggleik

5.4.1 Datagrunnlag

Ansvarstilhøve for informasjonstryggleik

Rolle- og ansvarsdelinga i kommunen, som skildra under overskrifta «organisasjon og ansvar for IKT i Etne kommune» i internkontrollsystemet for informasjonstryggleik, er vist i tabell 3.[30] Under same overskrift blir det skildra at rådmannen har det generelle ansvaret for IKT-aktiviteten i Etne kommune, og at stabssjefen er rådmannens faginstans i IKT spørsmål.

Tabell 3: Rollar og ansvar knytt til internkontroll av informasjonstryggleiken i Etne kommune

Rolle	Ansvar
Tryggleiksansvarleg	Den eller dei personar innan kommunen sin administrasjon som har ansvar for tryggleik, deriblant datatryggleiken kommunen. Ansvaret ligg hos Rådmann.
IKT-ansvarleg	Den person som har det overordna ansvaret for bruk av IKT innan kommunen. Ansvaret ligg hos IKT leiar

[30] I Etne kommune sitt internkontrollsystemet for informasjonstryggleik finn ein fleire ulike definisjonar av rollar og ansvar knytt til arbeidet med informasjonstryggleik.

Systemansvarleg	Den person som er ansvarleg for ein fagapplikasjon og som gir autorisert bruker den tilgangen i applikasjonen som brukaren er autorisert for. Ansvaret ligg hos einingsleiar.
Driftsansvarleg	Den person som er ansvarleg for drifta av IT-systemet og som gir den enkelte brukar tilgang til dei ressursar og applikasjonar på IT-systemet som brukaren er autorisert for. Ansvaret ligg hos Driftsansvarleg IKT.
Brukar	Den enkelte tilsette som er autorisert til å bruka IKT-systema i sitt daglege arbeid.

I intervju med leiaren for EVIKT kjem det fram at det ansvarshøva knytt til informasjonstryggleik har vore uklare i Etne kommune, men at det no er slik at dette ligg til tenestetorget og arkivtenesta. Leiaren på tenestetorget – som òg har ansvaret for arkivet – fortel i intervju at det ikkje er nokon formell ansvarsfordeling i kommunen knytt til personvern og informasjonstryggleik.

Rutinar for informasjonstryggleik

I styringssystemet for informasjonstryggleik i kvalitetssystemet i Etne kommune inngår det fleire rutine- og prosedyreskildringar. Mellom anna føreligg det ein *rettleiar til register med personopplysningar*, ei *sjekkliste for vurdering av kvaliteten på personopplysningar*, samt prosedyrar for *innhenting og kontroll av dei registrerte sitt samtykke*, for *innsyn ved handsaming av personopplysningar*, for *meldingar og konsesjonssøknadar til Datatilsynet*, og for *informasjonsplikt ved innsamling av personopplysningar*.

Det føreligg skriftlege rutinar for tilgangsstyring innan pleie- og omsorgsavdelinga.

Som nemnd over, blir styringssystemet for informasjonstryggleik ikkje eller berre i avgrensa grad nytta i det daglege informasjonstryggleiksarbeidet i kommunen. Det blir vidare fortalt i intervju at det er risiko for at det fins områder i kommunen der ein ikkje følgjer krav knytt til informasjonstryggleik.

Oversikt over personopplysningar og databehandlaravtalar

Revisjonen har mottatt oversikt over personopplysningar som blir handsama i kommunen sine fagmiljø og fagprogram. 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.[31]

I internkontrollsystemet for informasjonstryggleik i Etne kommune går det fram at det er *behandlingsansvarleg*[32] som skal halde oversikt over personopplysningar som blir handsama elektronisk i kommunen.

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.

Revisjonen har også mottatt ei oversikt over databehandlaravtalar frå kommunen. Oversikta inneheld ikkje fullstendig skildring av kva som er innhaldet i avtalane, kva år avtalane er inngått, eller kor lenge avtalane er gjeldande.[33]

I dokumentasjonen revisjonen har mottatt føreligg det ikkje skildringar av ansvarsdeling eller rutinar knytt til ajourhald eller rapportering på kva databehandlaravtalar som er inngått i kommunen.

EVIKT-leiar fortel i intervju at EVIKT verken har ansvar for eller oversikt over databehandlaravtalane inngått mellom kommunen og eksterne leverandørar; det er systemeigarane i kommunen som skal ha kontakt med eksterne leverandørar når det gjeld databehandlaravtalar.

I intervju kjem det elles fram at arkivtenesta på eige initiativ har starta praksis med å samle inn alle databehandlaravtalar i kommunen, men at det so langt ikkje er utarbeidd eller etablert rutinar for å at dei systemansvarlege skal levere databehandlaravtalane dei inngår til journalføring og oppbevaring på arkiv.

[31] Oversikta er attgjeve i tabell 4 i vedlegg 4.
[32] I dokumentet «Definisjonar» på kvalitetsstyringssystemet blir behandlingsansvarleg definert som «den som vedtar formålet med handsaminga av personopplysningar og kva hjelpemidlar som skal nyttast».
[33] Oversikta er attgjeve i vedlegg 4 på side 45.

5.4.2 Vurdering

Etne kommune har gjennom sitt internkontrollsystem formalisert rolle- og ansvarsdelinga for informasjonstryggleik. Undersøkingane avdekker at denne organiseringa ikkje eller berre i nokon grad blir følgt, og at det er til dels uklare ansvarstilhøve med omsyn til informasjonstryggleik i kommunen.

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. Etne 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.

Revisjonen finn vidare i sine undersøkingar at kommunen har ei dokumentert oversikt over kva personopplysningar dei handsamar. Kommunen har likevel ikkje noko system som sikrar at oversikta er oppdatert og fullstendig, og det er også uklart kven som er ansvarleg for å halde oversikta oppdatert. 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.

Etne kommune har heller ikkje noko 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 vegne 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.

5.5 Kontroll og etterprøving av informasjonstryggleik

5.5.1 Datagrunnlag

Etne kommune sitt internkontrollsystem for informasjonstryggleik inneheld ei rekkje prosedyrar for å føre kontroll og etterprøving av informasjonstryggleiken i kommunen, t.d. for tryggleiksrevisjonar, leiinga sin gjennomgang, risikovurdering og avvikshandsaming.

I intervju kjem det fram at slik kontroll og etterprøving ikkje eller berre i liten grad finn stad.

Leiinga sin gjennomgang

Ifølge dokumentasjonen, skal leiinga i Etne kommune med faste mellomrom gå gjennom tryggleiksmål og tryggleiksstrategi for Etne kommune med sikte på å vurdera om desse er i samsvar med behova i kommunen. Gjennomgangen skal danne grunnlag for endringar av tryggleiksmål og strategi.

Revisjonen har ikkje mottatt dokumentasjon på at leiinga sin gjennomgang blir gjennomført i Etne kommune.

Risikovurderingar av informasjonstryggleik

Ifølgje internkontrollsystemet for informasjonstryggleik skal behandlingsansvarleg halde oversikt over personopplysningar som blir handsama elektronisk i kommunen, og denne oversikta skal vere ein del av grunnlaget for risikovurderingar av informasjonstryggleiken.

Behandlingsansvarleg skal vidare fastsette kriterium for akseptabel risiko knytt til informasjonstryggleik.

Konsekvensane av brot på informasjonstryggleiken skal klargjerast ved hjelp av risikovurderingar. Resultatet av risikovurderinga skal samanliknast med fastlagde kriterium for akseptabel risiko. Resultatet vert nytta som ein del av grunnlaget for val av dei konkrete sikringstiltaka som må etablerast.

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.

Systemansvarleg for Profil fortel i intervju at ho ikkje har deltatt i risikovurderingar av tilgjenge i IKT-systema, og at ho ikkje har kjennskap til kven som eventuelt gjer slike vurderingar.

Avvikshandsaming

Det går fram av internkontrollsystemet for informasjonstryggleik at rapportering av avvik skal starte hos den tilsette som oppdagar avviket og deretter rapporterer til næraste ansvarleg leiar. Vidare prosess er iverksetjing av strakstiltak for å unngå følgeskadar, enten av den tilsette som oppdaga avviket eller av tilsett med ansvar for den delen avviket gjeld. Deretter følgjer korrigerande tiltak, med IT-driftsansvarleg som ansvarleg for systemteknisk avvikshandsaming og leiar for resultateininga som ansvarleg utførar for andre registerte avvik. Etter ei tid skal det gjerast ei vurdering av om korrigerande tiltak fungerer etter hensikta.

Kommunen har eit digitalt skjema for avviksrapportering. Det føreligg lenke til dette skjema i kvalitetssystemet.

I intervju med systemansvarleg for Profil går det fram at ein innan pleie- og omsorgseininga kan både føre avvik som skal inn i journalar i fagsystemet, og føre avvik på systemnivå i kommunen sitt kvalitetssystem. Det er ingen kopling mellom desse to systema. Avdelingsleiarane tar vekentleg ut avviksmeldingar frå fagsystemet for gjennomgang. Systemansvarleg for Profil har ikkje ansvar knytt til dei tilsette sine avviksmeldingar, verken i fagsystema eller i kvalitetssystemet.

Frå resultata i spørjeundersøkinga kjem det fram at dei fleste har fått informasjon om at dei skal melde avvik. 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. Og med omsyn til avviksmeldingspraksis, viser svara frå spørjeundersøkinga at dei færraste melder avvik knytt til informasjonstryggleik.

Revisjonen får opplyst at det i 2017 blei meldt 160 avvik i kvalitetssystemet i Etne kommune. Ingen av desse var knytt til informasjonstryggleik, etter det revisjonen kan sjå. So langt i 2018, viser statistikken frå kvalitetssystemet at det er meldt inn 132 avvik. Det går heller ikkje fram at nokon av desse er knytt til informasjonstryggleik.

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 fagsystemet innan pleie og omsorg i Etne kommune, blir det forklart at nytilsette får tilgang til fagsystemet ved at deira avdelingsleiar sender utfylt tilgangsskjema til EVIKT med skildring av kva tilgangar dei skal ha i fagsystemet. EVIKT sender deretter autorisasjonsskjema til systemansvarleg for fagsystemet; dette skjema inneheld kva rolle brukaren skal ha, og innan kva avdelinga vedkomande skal ha tilgang. EVIKT opprettar brukarnamn, og fagutviklingssjukepleiar opprettar tilgang i fagsystemet. Brukaren får tildelt eit brukarnamn og passord til fagsystemet, men må opprette eit eiget passord første gong dei loggar seg inn på fagsystemet. Ho fortel vidare at det i fagsystemet dei nyttar er mogleg å sette til og frå-dato for tilsettinga, og dimed også for tilgangane. Dette er noko dei nyttar ved tilsetting av sumarvikarar og frå vikarbyrå.[34]

5.5.2 Vurdering

Etne kommune har i internkontrollsystemet sitt for informasjonstryggleik dokumenterte prosedyrar for kontroll og etterprøving av informasjonstryggleik. Revisjonen avdekker i sine undersøkingar at slik kontroll og etterprøving av informasjonstryggleiken i avgrensa grad finn stad. Kommunen bryt slik med både sine eigne rutinar og retningsliner, samt sentrale krav i både POF og ISO27001:2013.

[34] Fagsystemet dei nyttar i pleie- og omsorgstenesta i Etne har ein funksjon der ein kan legge pasientar inn i eigne tilgangskategoriar der berre nokre få tilsette har tilgang til data. Dette har blitt nytta for pasientar som har uttrykt ønskje om eller behov for skjerming.

Etne kommune gjennomfører ikkje eller berre unntaksvis risikovurderingar knytt til informasjonstryggleik, og har difor manglande oversikt over kva risikoar kommunen står ovanfor i samband med handsaming av personopplysningar. Manglande risikovurderingar resulterer vidare i at kommunen ikkje har eit godt grunnlag for å vurdere å gjere eventuelle justeringar knytt til informasjonstryggleiken basert på endringar i trusselbilete. Kommunen bryt slik med POF § 2-4 anna ledd.

Kommunen set heller 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 kommunen bryt slik 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.

Etne kommune har eit etablert avvikssystem, men det blir ikkje meldt avvik knytt til informasjonstryggleik i dette. Revisjonen vil understreke at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta. Revisjonen meiner difor at Etne 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 punkt 9.3.

Når det gjeld tilgangskontroll, avdekker undersøkingane at Etne kommune og EVIKT har system for dette. Det kjem likevel fram at det er svakheiter i systema, som t.d. at det må meldast manuelt når tilsette slutter i kommunen eller bytter jobb internt i kommunen, noko som medfører ein viss auka 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.

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 anna 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 kommunen sitt internkontrollsystem for informasjonstryggleik går det fram at «kommunen sine medarbeidarar skal ha tilstrekkelig kompetanse og gjevast nødvendig opplæring slik at tilfredsstillande informasjonstryggleik blir oppretthalden». Vidare blir det skildra at det er Etne kommune sitt ansvar å syte for at dei tilsette har tilstrekkeleg kompetanse til å bruke informasjonssystema, samt å leggje til rette for vedlikehald og heving av denne kompetansen.

I internkontrollsystemet for informasjonstryggleik inngår det vidare eit dokument med tittel *Brukarkrav Etne*, som alle tilsette i kommunen er påkravd å lese og signere. Eit av punkta i dette dokumentet er «opplæring», der det går fram at ein skal gjennomgå naudsynt opplæring for å få tilgang til IKT-systema, og at dei tilsette sjølv er ansvarlege for å følgje gjeldande reglar innan dei aktuelle systema. Vidare i *Brukarkrav Etne* blir mellom anna retningsliner for bruk av kommunen sine informasjonssystem, internett og e-post skildra.

I intervju kjem det fram at kompetanse om informasjonstryggleig er eit område som ikkje har blitt prioritert i kommunen. Kommunen vurderer å kjøpe inn eit større kurs-opplegg på informasjonstryggleik for dei tilsette i kommunen, men dette har ikkje blitt gjort.

Vidare blir det fortalt at om lag 12 tilsette i kommunen deltok på eit 40-timars kurs knytt til lovverk, teieplikt og informasjonstryggleik i regi av studieforbundet AOF. I tillegg blir det opplyst at leiarar i

kommunen har fått kurs i informasjonstryggleik gjennom Nano-læring frå Nasjonalt senter for informasjonssikring (NorSIS).[35]

Det kjem òg fram i intervju at fleire tilsette har deltatt på eit dagskurs der ny personvernlovgiving var tema. Kurset er eit samarbeid mellom KS, KiNS, Datatilsynet, Senter for IKT i Undervisninga, Difi og Direktoratet for eHelse.[36]

Leiaren for EVIKT fortel om manglande kunnskap i nokre av einingane i kommunen når det gjeld rutinar knytt til informasjonstryggleik. Generelt opplever han at det er mangelfull oppfølging av rutinar for informasjonstryggleik i kommunen. Elles går det vidare fram i intervju at det ikkje er ei fast ordning på opplæring av nytilsette innan informasjonstryggleik, men at alle skal underteikne skjema om teieplikt ved tilsetting.

6.3.2 Vurderingar

Revisjonen meiner Etne kommune berre i avgrensa grad følgjer sine 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 innafor informasjonstryggleik, noko som aukar risikoen for brot både på regelverk som gjeld for handsaming av personopplysningar, og for informasjonstryggleika generelt.

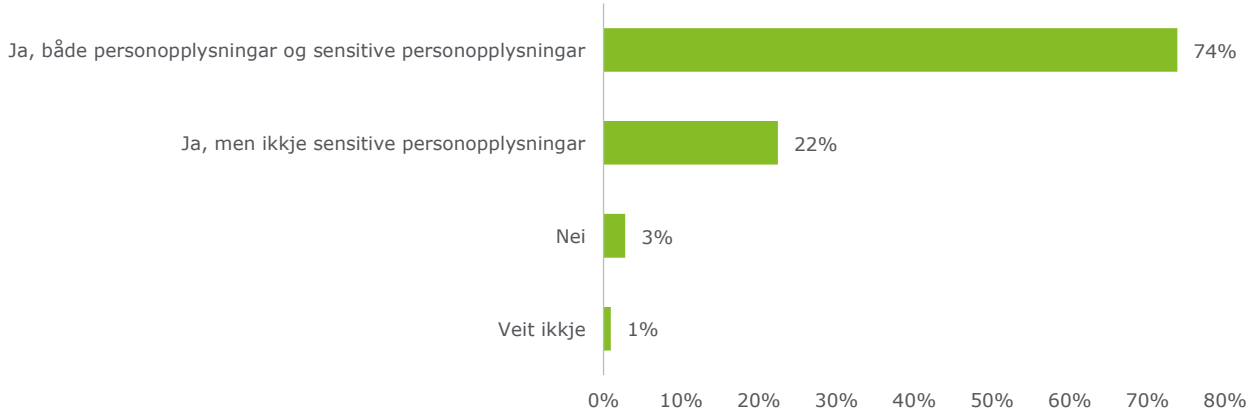
Det er revisjonen si vurdering at Etne kommune ikkje følger krava i POF 2-8 anna ledd, eller ISO27001:2013 punkt 7.2

6.4 Kjennskap til retningsliner og rutinar for informasjonstryggleik

6.4.1 Datagrunnlag

Langt dei fleste av respondentane i spørjeundersøkinga handsamar eller kjem i kontakt med personopplysningar i sitt arbeid (sjå figur 6). 83 % av respondentane svara at dei handsamar eller kjem i kontakt med anna fortruleg informasjon som følgje av sitt arbeid.

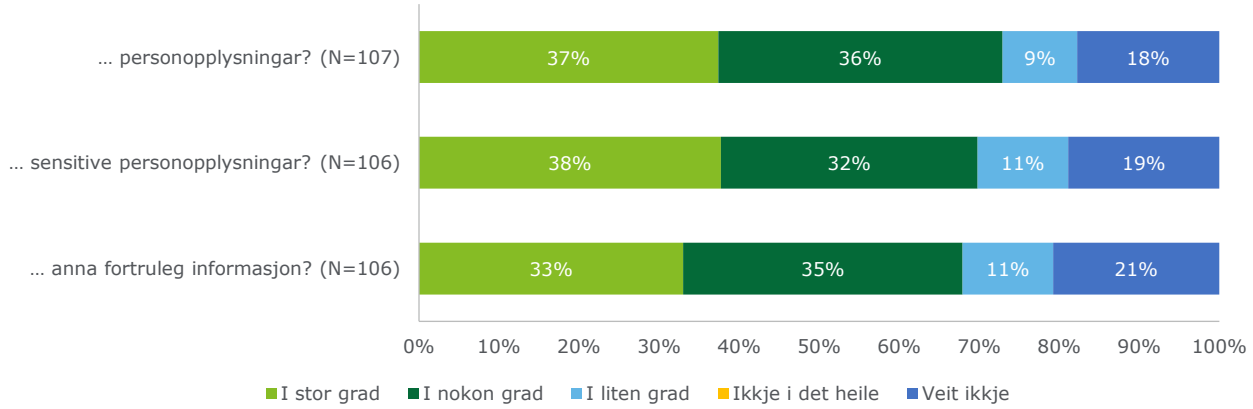
Figur 6: Handsaming av personopplysningar (N=107)



Vidare blei respondentane bedt om å svare på *i kva grad kommunen og/eller einingane vedkomande jobba i har tydlege og skriftlege retningsliner for handsaming av ulike typar opplysningar*. Som det går fram av figur 7, svara mellom 18 % og 21 % «ikkje veit», og mellom 9 % og 11 % «i liten grad».

[35] Sjå https://norsis.no/10250-2/
[36] Totalt deltok sju tilsette, mellom anna rådmannen, leiar og tilsette i pleie og omsorg, tilsette frå personalavdelinga, arkiv og IKT.

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

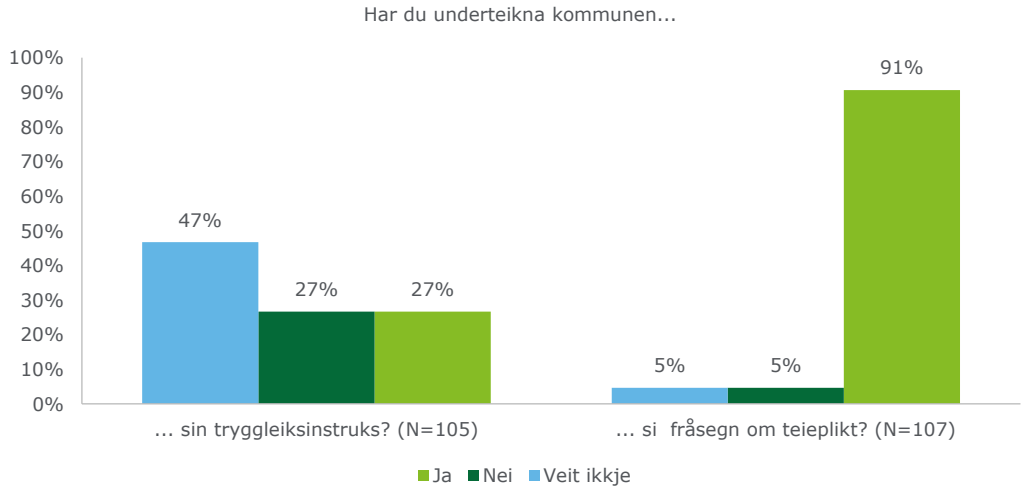


Respondentane blei så spurde om dei *veit kvar dei finn rutinar og retningsliner for handsaming av personopplysningar, sensitive personopplysningar og/eller anna fortruleg informasjon som gjeld kommunen og/eller deira eining*. På dette svara ca. 53 % «ja», 43 % «nei», og 4 % «har ikkje slike rutinar».

Dei 53 % av respondentane som svara «ja» fekk eit oppfølgingsspørsmål om *kvar Etne kommune og/eller eininga har tilgjengeleggjort informasjon om handsaming av denne typen opplysningar*. Av dei 37 som svara, viste fleire til enten kvalitetssystemet eller arkivplanen. Elles blei det vist til spesifikke fagsystem, e-postar, papirdokument, møte og regelverk. Tre av respondentane svara at dei likevel ikkje veit kvar dei finn dette, og to viste til at det ikkje er noko samordna system for dette i kommunen.

Svara som blir framstilt i figur 8, viser at om lag 5 % av respondentane ikkje har underteikna fråsegn om teieplikt, og at ca. 5 % ikkje veit om dei har gjort det. Om lag halvparten av respondentane veit ikkje om dei har underteikna tryggleiksinstruksen, og ca. 27 % seier at dei ikkje har underteikna på denne.

Figur 8: Teieplikt og tryggleiksinstruks

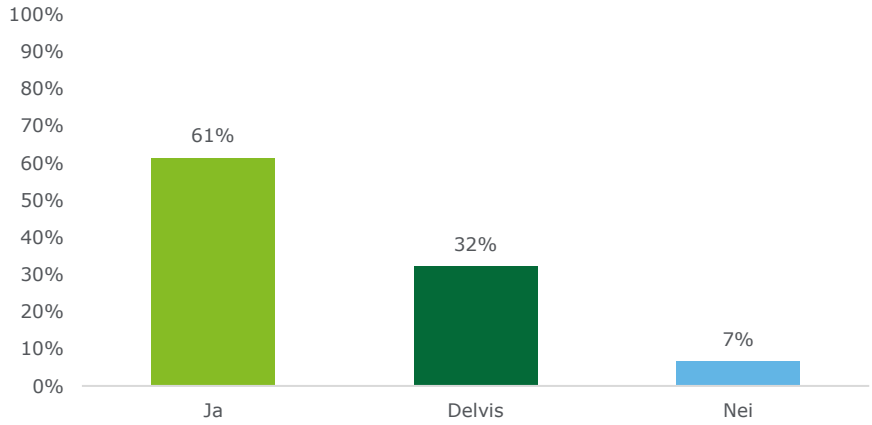


Dei som svara «ja» på at dei har underteikna på kommunen si fråsegn om teieplikt blei spurde om dei hugsar innhaldet i skjemaet. På dette svara 90,7 % av dei hugsar innhaldet.[37] På same vis blei dei som svara «ja» på at dei har underteikna kommunen sin tryggleiksinstruks spurde om dei hugsar innhaldet i denne. På dette spørsmålet svara éin av fem at dei ikkje hugsar innhaldet.[38]

[37] N=97
[38] N=27

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 32 % at dei delvis er kjend med eige ansvar og oppgåver knytt til informasjonstryggleik, medan 7 % ikkje er kjend med dette.

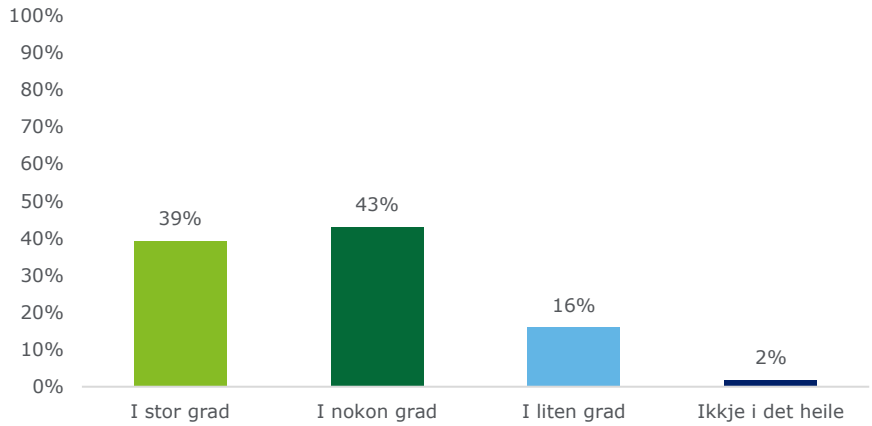
Figur 9: Kjennskap til eige ansvar og oppgåver knytt til informasjonstryggleik (N=106)



Dei som svara «ja» eller «delvis» på spørsmålet over, fekk eit oppfølgingsspørsmål på *kva oppgåver og ansvar dei har med omsyn til informasjonstryggleik.* Av svara som kom inn,[39] viser over 40 % til teieplikta og det å halde informasjon konfidensiell. Mange viser til overordna plikter på arbeidsplassen utan å gå nærare inn på dette, medan nokre er usikre eller meiner at det ikkje ligg nokre oppgåver eller ansvar knytt til informasjonstryggleik til deira stilling.

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 totalt 18 % av respondentane at deira leiar «i liten grad» eller «ikkje i det heile» har framheva viktigheita av informasjonstryggleik. 43 % svara at dette har blitt framheva «i nokon grad».

Figur 10: Viktigheita av informasjonstryggleik (N=107)

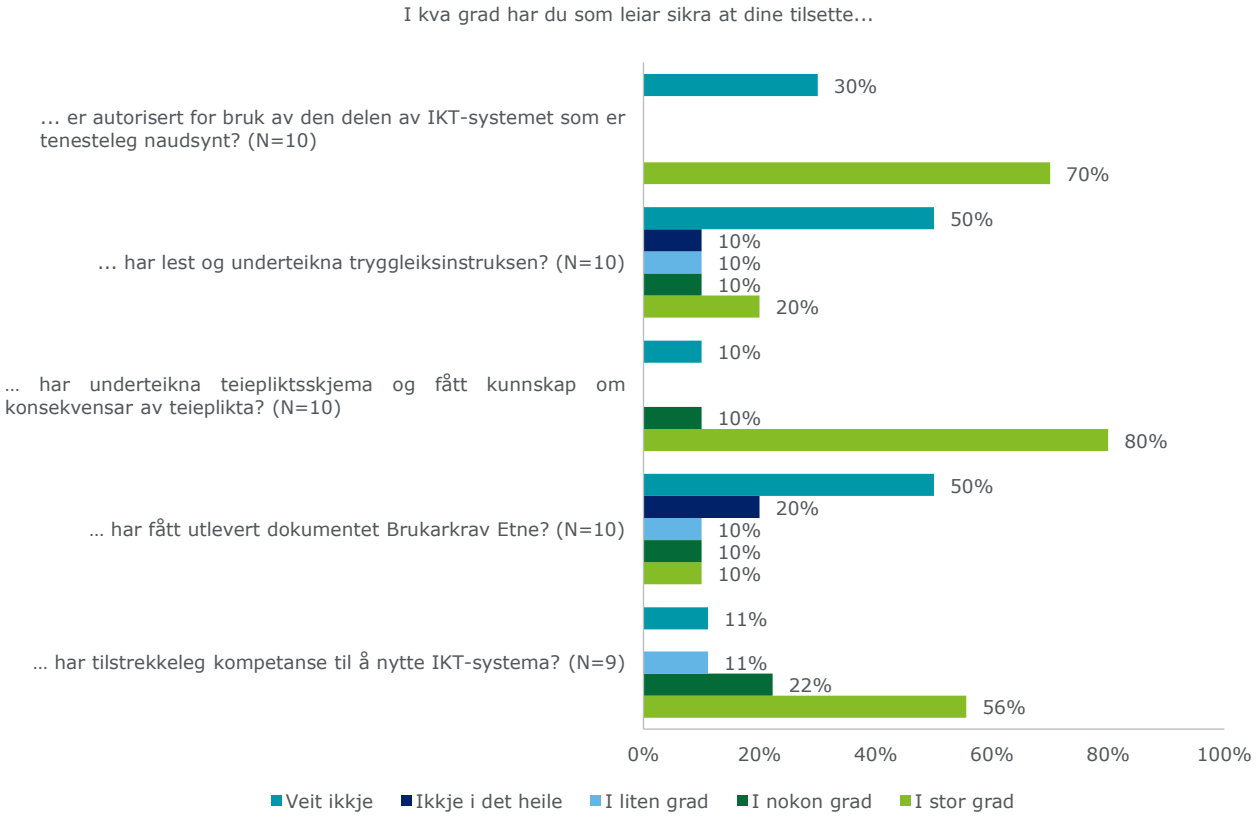


Dei som svara at dei har leiaransvar i kommunen, blei stilt ei rekkje spørsmål knytt til korleis dei sikrar at deira tilsette følger opp kommunen sine retningsliner for informasjonsstryggleik.[40] Som det går fram av figur 11 svara halvparten av leiarane at dei ikkje veit om dei har sikra at deira tilsette har lest og underteikna tryggleiksinstruksen og fått utlevert dokumentet *Brukarkrav Etne*. Vidare svara om lag ein av tre at dei ikkje veit om dei har sikra at dei tilsette er autorisert for bruk av den delen av IKT-systemet som er tenesteleg naudsynt. 20 % svara at dei «i nokon grad» eller ikkje veit om dei har sytt for at deira tilsette

[39] N=48
[40] Respondentane i spørjeundersøkinga som svara at dei er systemansvarlege fekk eit oppfølgingsspørsmål knytt til om dei har deltatt i opplæringa av andre brukarar. Av dei 3 som svara, har 2 av dei ikkje deltatt i opplæringa av andre.

har underteikna teiepliktskjema, medan over ein fjerdedel svara at dei «i liten grad» eller ikkje veit om dei har sikra om deira tilsette har tilstrekkeleg kompetanse til å nytte IKT-systema.[41]

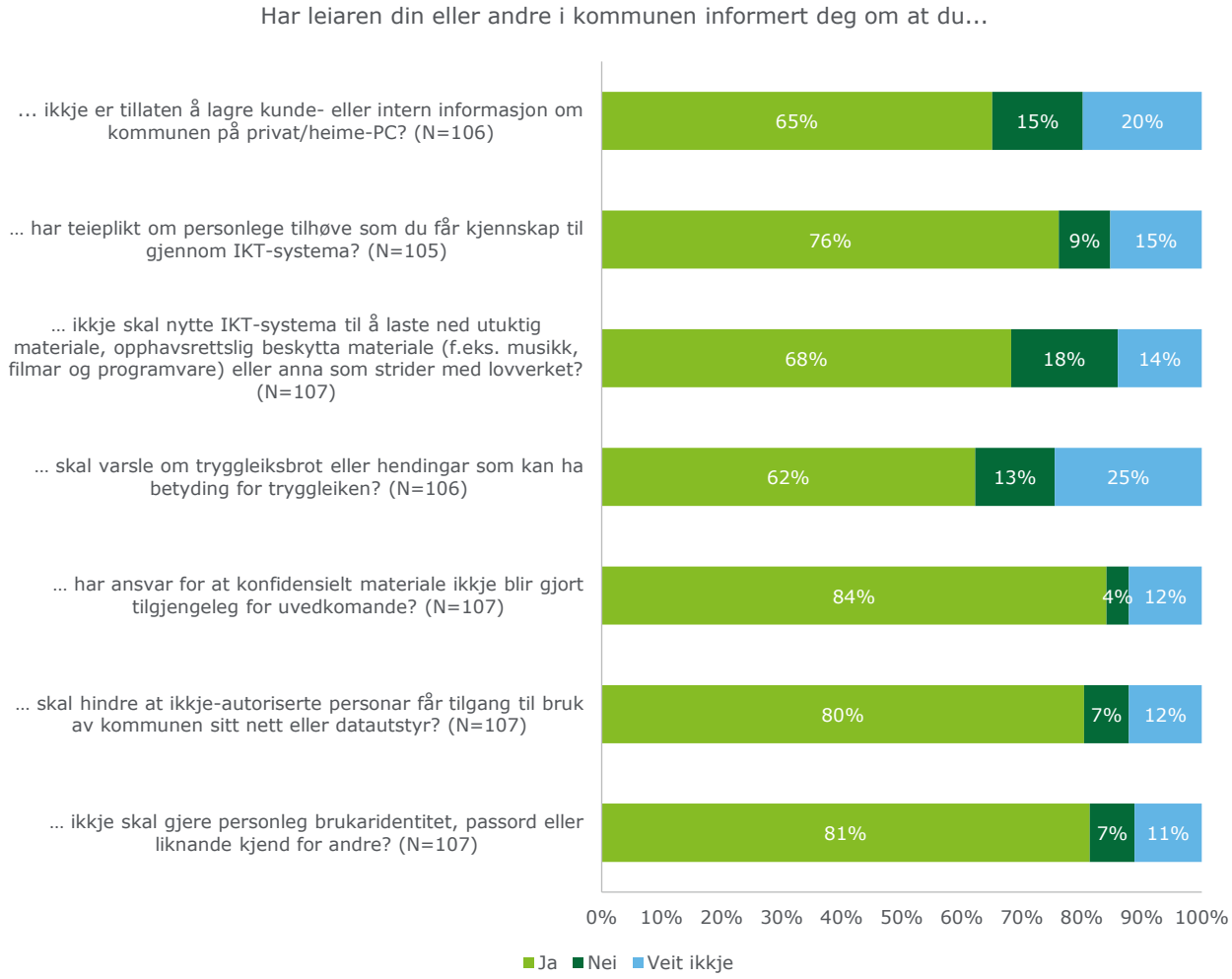
Figur 11: Opplæring av tilsette



Figur 12 viser respondentane sine svar på sju spørsmål om opplæring i informasjonstryggleik i Etne kommune. Mellom 11 % og 25 % svara at dei ikkje veit om dei har fått informasjon om dei ulike punkta som kommunen held fram som viktige for å vareta ein god informasjonstryggleik. Vidare svara 18 % av respondentane at dei ikkje har fått informasjon om at dei ikkje skal nytte IKT-systemet til å laste ned ututig materiale, materiale med opphavsrett eller annas om strider med lovverket, og 15 % har ikkje fått informasjon om at dei ikkje skal lagre kundeinformasjon på privat PC.

[41] Meir om tilsette si opplæring i informasjonstryggleik under avsnitt 6.4.1.

Figur 12: Opplæring i informasjonstryggleik i Etne kommune



Respondentane blei vidare spurt om dei veit *kven i kommunen dei skal kontakte ved spørsmål knytt til informasjonstryggleik og/eller handsaming av personopplysningar*. På dette spørsmålet svara over ein tredel av respondentane «nei».[42] Dei som svara «ja» på spørsmålet fekk eit oppfølgingsspørsmål der dei blei spurde om kven i kommunen dei kontaktar med slike førespurnader. Av dei 55 som svara på oppfølgingsspørsmålet, svara 44 % at dei ville ha kontakta næraste leiar, medan 31 % ville ha kontakta IKT-avdelinga eller IKT-leiaren. Vidare nemner nokre av respondentane at dei ville ha kontakta arkivtenesta/arkivansvarleg, personalleiar/personalavdelinga, rådmann og elles nokre namngjevne tilsette i kommunen.

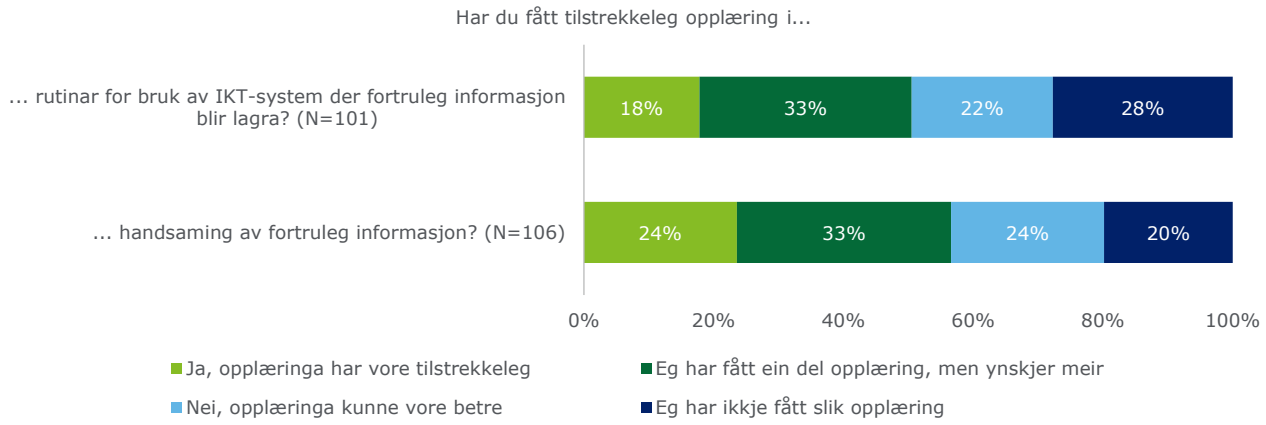
Vidare blei respondentane spurde om *dei er kjend med kva rutinar som gjeld for å melde avvik knytt til informasjonstryggleik.* På dette spørsmålet svara 57 % at dei ikkje har kjennskap til dette.[43] Dei som svara «ja» på spørsmålet blei bedne om å skildre *gjeldande avviksrutinar når prosedyrar ikkje blir følgde eller ein opplever potensielle eller faktiske trugslar mot informasjonstryggleiken.* I svara som kom inn[44] viser 70 % til at dei i denne situasjonen ville ha sendt inn avviksmelding; 17 % av desse spesifiserer at ein skal melde avvik gjennom kvalitetssystemet, medan dei andre respondentane viser generelt til «avviksskjema» eller at ein skal melde avvik i «avvikssystemet» eller i fagsystema. 18 % viser til at dei ville ha kontakta næraste leiar, medan 14 % er usikre på kva rutinar som er gjeldande.

Som det går fram av figur 13 svara 28 % av respondentane at dei ikkje har fått *opplæring i rutinar for bruk av IKT-system der fortruleg informasjon blir lagra.* 22% svara at opplæringa ikkje har vore tilstrekkeleg,

[42] N=106
[43] N=107
[44] N=30

og at opplæringa innan dette området i kommunen kunne ha vore betre. Ein av fem svara at dei ikkje har fått opplæring i handsaming av fortruleg informasjon, medan om lag ein fjerdedel svara at dei ikkje meiner denne opplæringa på dette området er god nok.

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 41 som svara på oppfølgingsspørsmålet, var det mange som svara at dei saknar ei generell opplæring i informasjonstryggleik, og mange etterlyser også faste gjennomgangar på dette. Fleire saknar ein grundig gjennomgang av Etne kommune sine rutinar og retningsliner på området, og ein del svara at dei ønskjer ei innføring i informasjonstryggleik ved bruk at IKT-systema, og då spesielt på tema knytt til konfidensialitet. Eit par av respondentane viser også til at dei saknar opplæring knytt til lovar og regelverk, som til dømes GDPR.

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 sakna i denne opplæringa. Av 33 respondentar svara mange at dei saknar ei generell opplæring, medan eit par ønskjer opplæring i meir effektive måtar å arbeide i systema. Nokre ønskjer opplæring i regelverk, teieplikt og korleis IKT-systema i kommunen står i forhold til kvarandre, medan ein del er usikre på kva opplæring dei har behov for på området.

6.4.2 Vurdering

Undersøkinga viser at dei fleste av respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller anna fortruleg informasjon i arbeidskvardagen. Likevel svara om lag éin av fem at dei ikkje veit om kommunen eller einingа har retningsliner for korleis å handtere slik type informasjon. Revisjonen merkar seg også at nesten 40 % 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 resultata frå spørjeundersøkinga at nesten halvparten av respondentane ikkje veit om dei har underteikna Etne kommune sin tryggleiksinstruks, og at av dei som har gjort det, hugsar om lag 20 % ikkje innhaldet. Vidare går det fram frå undersøkingane at retningsliner og krav til teieplikt, konfidensialitet og passordbruk er relativt godt kjend blant respondentane, men at dei i mindre grad er kjende med at dei ikkje skal nytte kommunen lagre intern informasjon om kommunen på privat PC, ikkje skal nytte IKT-systema til å laste ned utuktig eller opphavsrettslig beskytta materiale, og at dei skal varsle om tryggleiksbrot eller hendingar som kan ha betyding for tryggleiken.

Elles kjem det fram i spørjeundersøkinga at om lag 82 % av respondentane ikkje har fått tilstrekkeleg opplæring i bruk av IKT-systema der fortruleg informasjon blir lagra, og at ca. tre firedelar ikkje har fått tilstrekkeleg opplæring i handsaming av fortruleg informasjon.

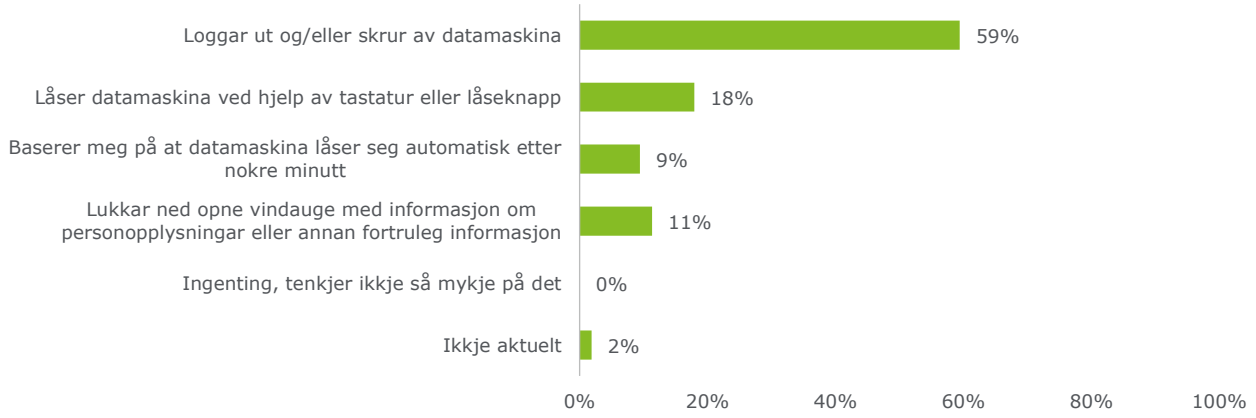
Basert på funna frå undersøkingane, er det revisjonen si vurdering at dei tilsette i Etne kommune ikkje har tilstrekkeleg kjennskap til eksisterande retningsliner og rutinar for informasjonstryggleik. Revisjonen meiner difor at kommunen bryt med POF § 2-8 anna ledd, og at det er risiko for at kommunen 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

Respondentane blei spurde om kvardagsrutinar når dei forlèt PC-en dei brukar. Svara på dette spørsmålet er presentert i figur 14 under:

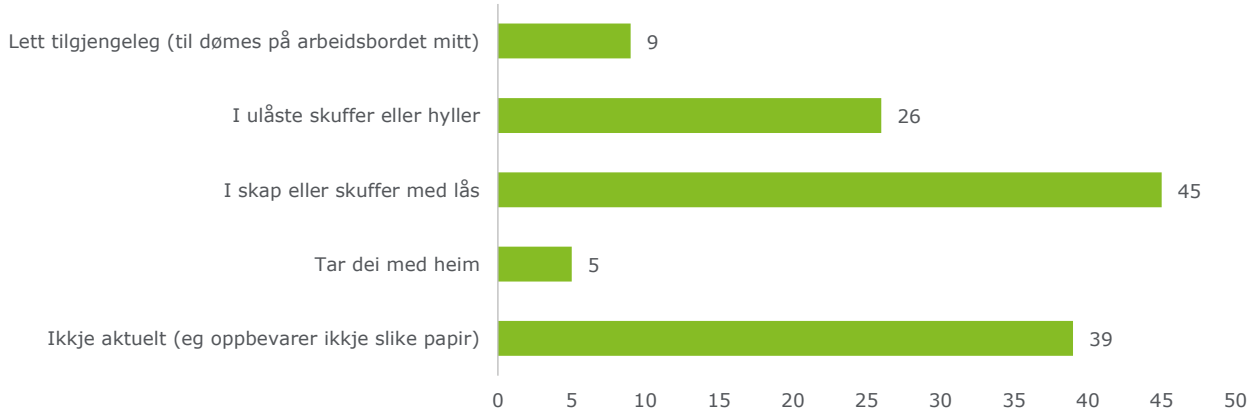
Figur 14: Kva gjer du vanlegvis når du i løpet av arbeidsdagen går frå PC-en du nyttar? (N=106)



Respondentane blei også spurde om dei *nokon gong har lånt ut brukarnamnet og passordet til andre*. Om lag 10 % svara «ja, men berre til IKT-avdelinga eller tilsvarande», rundt 8 % svara «ja», og 82 % «nei».[45]

På spørsmål om *korleis du oppbevarer papirdokument med fortruleg informasjon*, svara 26 av 105 respondentar at dei oppbevarer dokument med fortruleg informasjon i ulåste skuffer eller hyller, 9 at dei oppbevarer slike dokument lett tilgjengeleg, og fem at dei tek dei med heim.[46]

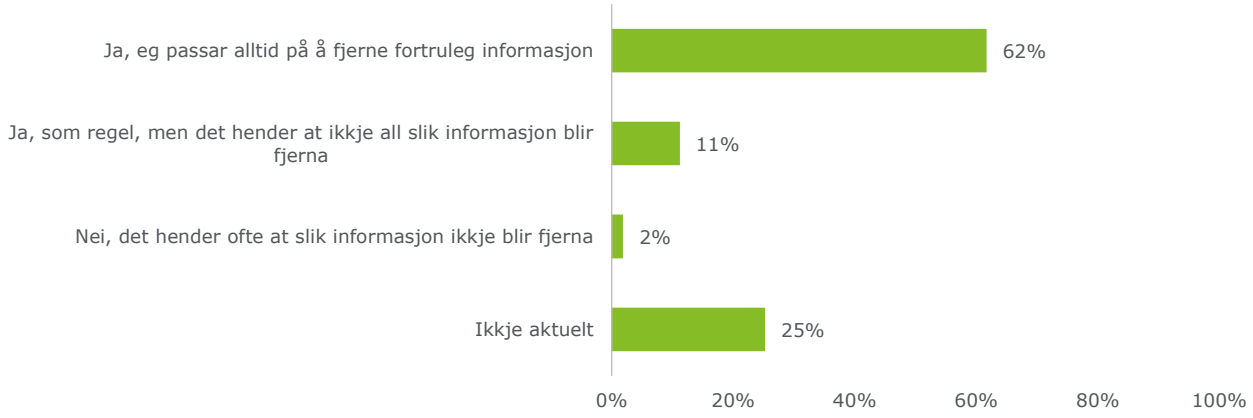
Figur 15: Korleis oppbevarer du dokument (papir) med fortruleg informasjon? (N=105)



Respondentane fekk vidare spørsmål om dei fjernar fortruleg informasjon frå møterom før dei forlèt det. Som vist i figur 16, svara 11 % at det hender at slik informasjon ikkje blir fjerna, medan 2 % svara at det skjer ofte at slik informasjon ikkje blir fjerna.

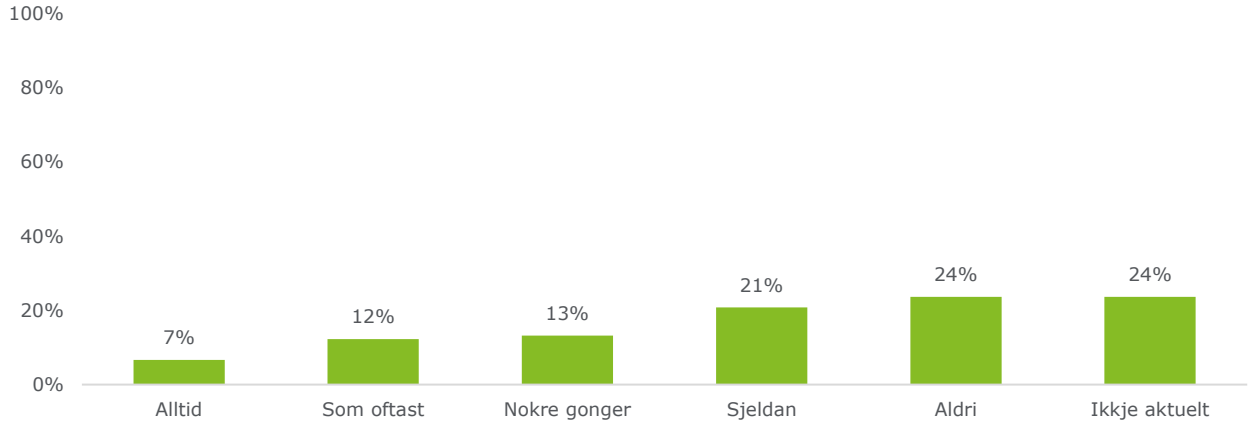
[45] Dei resterande 82 % svara «nei». N=107
[46] Respondentane hadde høve til å velje meir enn eit svaralternativ

Figur 16: Fjerning av fortruleg informasjon frå møterom (N=107)



Som vist i figur 17 svara om lag ein av fire at dei aldri melder avvik *dersom prosedyrar ikkje blir følgde eller når dei opplever potensielle eller faktiske trugslar mot informasjonstryggleiken.* Ein fjerdedel svara at dei sjeldan melder avvik ved slike hendingar, medan 24 % svarer at dette ikkje er aktuelt i deira arbeidskvardag.

Figur 17: Avviksmelding (N=106)



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 44 som svara, seier 15 at dei ikkje kjenner til rutinane for å melde avvik i kommunen. 10 av respondentane svarer at dei ikkje melder avvik då dei opplever at dei ikkje har tid til dette i arbeidskvardagen, 13 skriv at dei ikkje har opplevd slike tilfelle, og nokre viser til at ein ordnar opp i slike tilfelle internt.

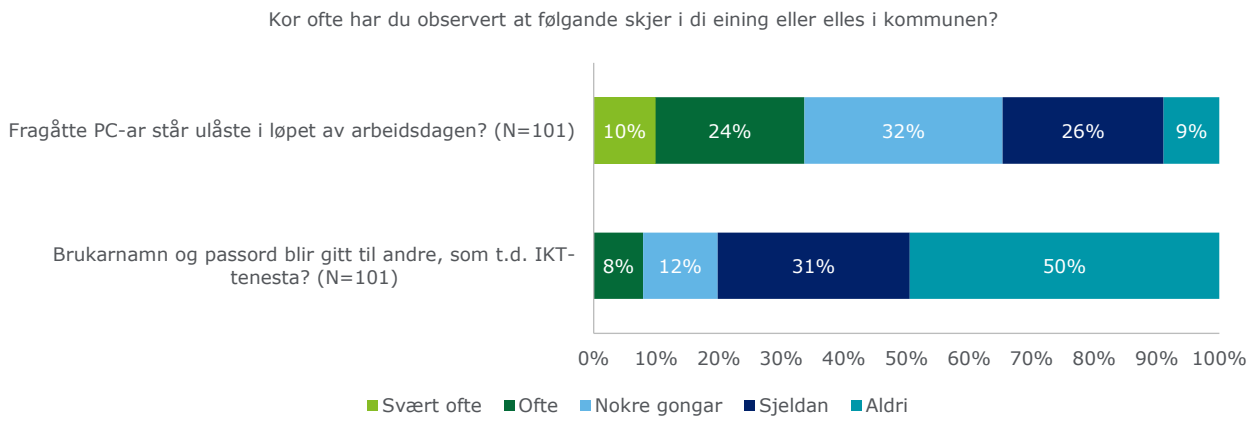
Respondentane som svara at dei «alltid», «som oftast», «nokre gonger» eller «sjeldan» melder avvik knytt til informasjonstryggleik fekk eit oppfølgingsspørsmål på om meldte avvik har blitt følgt opp. 29 % svara «delvis» og 17 % svara «nei» på dette spørsmålet.[47]

Andre sin informasjonstryggleikspraksis

Respondentane blei i spørjeundersøkinga bedt om å svare på to spørsmål knytt til kollegaar sin praksis knytt til informasjonstryggleik i samband med passord og PC. Svara som er presenterte i figur 18 viser at 34 % svarer at dei «ofte» eller «svært ofte» observerer fragåtte PC-ar som er ulåste, medan 32 % ser dette «nokre gonger». Svara knytt til om tilsette gjer frå seg passord og brukarnamn viser at 8 % «ofte» har observert at tilsette gjer frå seg dette til andre, medan 12 % svara at dei ser dette «nokre gonger».

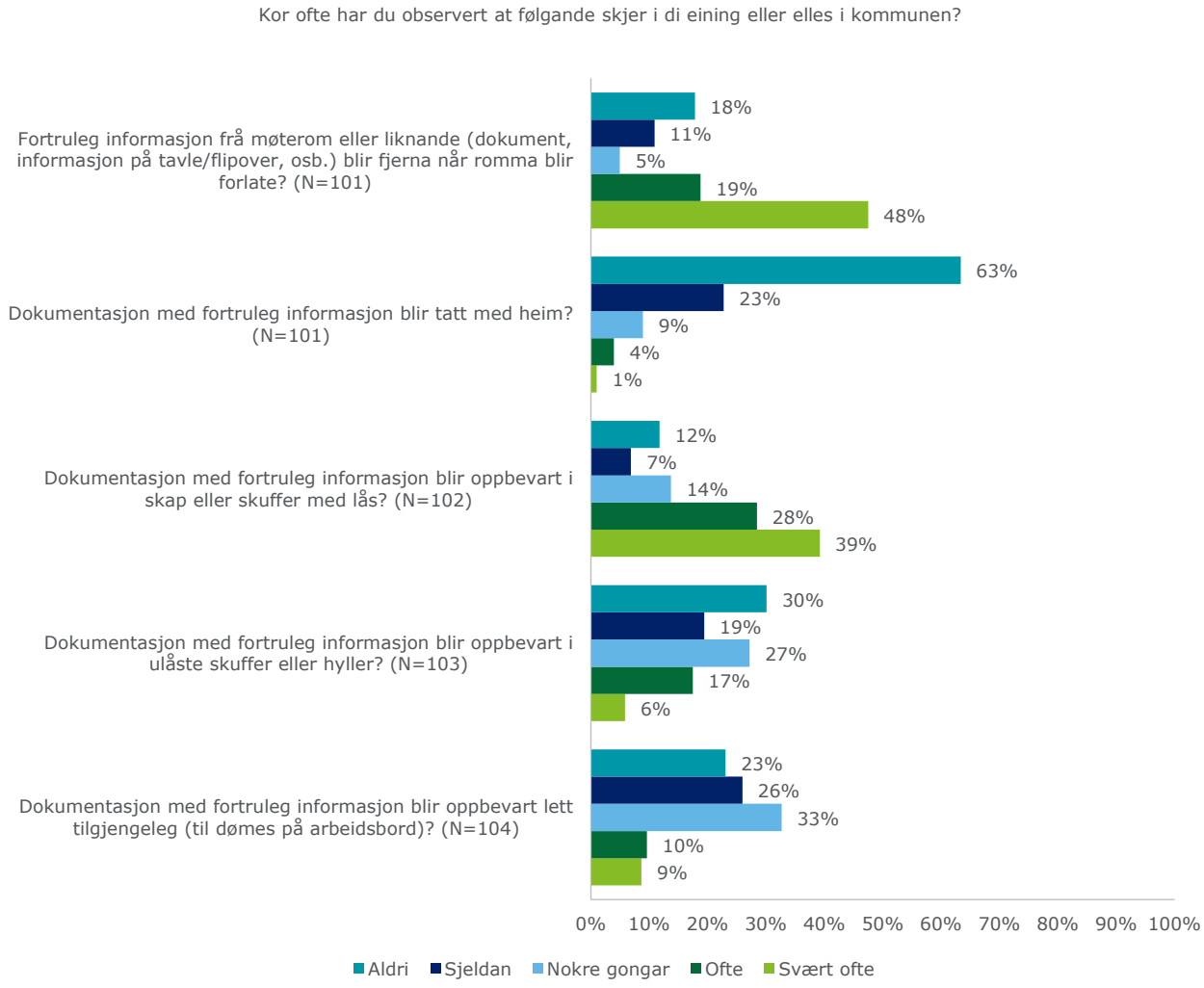
[47] 54 % svara «ja». N=48.

Figur 18: Informasjonstryggleikspraksis - PC og passord



Vidare fekk respondentane fem spørsmål knytt til kollegaar sin praksis knytt til dokumenthandsaming og informasjonstryggleik. Svara er presentert i figur 19 under:

Figur 19: Informasjonstryggleik - dokumenthandsaming



Som det går fram av figuren, svara 28 % av respondentane at fortruleg informasjon frå møterom «aldri» eller «sjeldan» blir fjerna når rommet blir forlate. 5 % av respondentane seier at det førekjem «svært ofte»

eller «ofte» at fortrulege dokument blir tatt med heim, medan 9 % seier at dei ser dette «nokre gongar». Vidare svarer 19 % av respondentane at dei «aldri» eller «sjeldan» observerer at fortulege dokument blir oppbevart i låste skap eller skuffer, medan 23 % svarer at fortruleg dokumentasjon «svært ofte» eller «ofte» blir oppbevart i ulåste skuffer eller hyller. Om lag ein av fem svarer at dei «svært ofte» eller «ofte» observerer at dokument med fortruleg informasjon blir oppbevart lett tilgjengeleg på til dømes arbeidsbord.

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 rett under 20 % av respondentane enten har delt passordet sitt med IKT-avdelinga eller andre, og at 20 % 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 vidare fram av spørjeundersøkinga at langt fleire «aldri» eller «sjeldan» meldar avvik enn dei som «alltid» eller «som oftast» gjer det, og vidare at det er knytt usikkerheit til korleis avvik skal meldast.

Når det gjeld dokumenthandsaming, viser undersøkinga at det i Etne 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 det er til dels uklåre rutinar og retningsliner for informasjonstryggleik i Etne kommune.

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 Etne 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. 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 også 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.

Etne kommune har kome i gang med å førebu seg på komande krav og føringar innan IKT-området, og då særleg ny personvernlov (GDPR). Arbeidet er på eit relativt tidleg stadium, og revisjonen meiner difor at Etne kommune berre i avgrensa grad har arbeidd systematisk for å sikre at kommunen er tilstrekkeleg førebudd på komande krav og føringar innan IKT-området.

Etne kommune har styrande dokument for informasjonstryggleik. Desse er ikkje oppdaterte og blir i liten grad nytta. T.d. blir ikkje den formelle ansvars- og rolledelinga følgt i praksis, kontroll og etterprøving av informasjonstryggleiken finn berre stad i avgrensa grad, det blir ikkje sett akseptkriterium knytt til informasjonstryggleik, og etter det revisjonen kjenner til, blir det heller ikkje gjennomført tryggleiksrevisjonar.

Kommunen har ikkje noko system som sikrar at oversikta over personopplysningar som kommunen handsamar er oppdatert og fullstendig, og heller ikkje noko system for å halde oversikta over kva databehandlaravtalar dei har inngått er oppdatert eller fullstendig. Det er difor risiko for at kommunen handsamar personopplysningar dei ikkje veit om, og at eksterne leverandørar behandlar personopplysningar på vegner av kommunen utan at kommunen veit om det.

På bakgrunn av desse svakheitene, meiner revisjonen at Etne kommune ikkje har eit styringssystem for informasjonstryggleik som er i samsvar med krav i regelverket.

Undersøkinga viser at dei fleste av respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller anna fortruleg informasjon i arbeidskvardagen. Likevel svara nesten 40 % av respondentane at dei 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 Etne 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 Etne 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 Etne 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. dei styrande dokumenta 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

ETNE KOMMUNE
RÅDMANNEN

Deloitte AS
Lars Hilles gate 30
5008 BERGEN

Etne, 29.08.2018

Dykkar ref.:	**Vår ref.:**	**Arkiv:**	**Sakshandsamar:**
	Arkivsaknr:17/1776 Journalpostnr:18/8052	N - 036.5	PAN

Høyringsuttale

Viser til utkast til rapport vedk. forvaltningsrevisjon - IKT og informasjonstryggleik - i Etne kommune.

Rådmannen tek utkast til rapport til etterretning og er allereie byrja å sjå på oppfølging av tilrådte tiltak i rapporten.

Med helsing

Pål Nygård
rådmann

Brevet er godkjent elektronisk og har derfor inga underskrift.

53 75 80 00 · Telefaks: 53 75 80 01 · E-post: post@etne.kommune.no · www.etne.kommune.no
5590 ETNE · Sjoarvegen 2 · Bankgiro · 3240.09.69808 · Org.nr.: 959 435 375

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.

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.

[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).

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

Kommunale dokument og avtaler

- Overordna samarbeidsavtale EVIKT
- Sak om vertskommunesamarbeid (EVIKT)
- Tenesteleveringsavtale EVIKT
- Organisasjonskart EVIKT
- Oversikt over personopplysningar
- Oversikt over databehandlaravtalar
- Diverse rutineskildringar for EVIKT
- Internkontrollsystem for IT-tryggleik (52 dokumenter)
- Spørjeundersøking evaluering EVIKT

Vedlegg 4: Supplerande informasjon

Tabell 4: Oversikt over personopplysningar, Etne kommune

Informasjon, formål	System	Heimel	Klassifisering	Sikrings-tiltak	Lagring og kommunikasjon	Register omfang	Konsesjon og arkivering	Systemeigar
Løn og personal	Visma Unique HMR	Personopplysnings-forskrift § 7-16d	Person-opplysningar	Tilgangsstyring	Lagra på kommunal server Internt kommunalt nettverk	ca. ?	Fritatt frå både konsesjons-og meldeplikt	Økonomi og personalavdeling a
Fagsystem Pleie og Omsorg	Visma Profil	Personopplysningsloven § 33 5. Ledd Helsepersonellov en §§ 26 og 39,	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone		Ingen konsesjons- plikt, men meldeplikt	Leiar PLO
Fagsystem Sosial	Visma Velferd	Personopplysningsloven § 33 5. Ledd Sosialtjenestelov en § 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	SystemX	Personopplysningsloven § 33 5. Ledd Helsepersonellov en §§ 26 og 39,,	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone		Ingen konsesjons- plikt, men meldeplikt	Leiar, helse
Fagsystem helsestastjon	SystemX	Personopplysningsloven § 33 5. Ledd Helsepersonellov en §§ 26 og 39,,	Sensitive person opplysningar	Sikker sone Tilgangssstyring	Lagra på kommunal server i sikker sone		Ingen konsesjons- plikt, men meldeplikt	Leiar, helse
Fagsystem barnehage	Visma barnehage	Personopplysnings-forskrift § 7-21	Person-opplysningar	Tilgangsstyring	agra på kommunal server Internt kommunalt nettverk		Unntatt både frå konsesjons- og meldeplikt	Styrar i barnehage
Fagsystem skule	WIS		Person-opplysningar	Tilgangsstyring	Lagra på kommunal server Internt kommunalt nettverk		Ingen konsesjons- plikt, men meldeplikt	Rektorar
Fagsystem kulturskule	Speed admin		Person-opplysningar	Tilgangsstyring	Skylagring Lagra på server i Norge		Ingen konsesjons- plikt, men meldeplikt	Leiar Kulturskulen
Sak/arkiv-system	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	Personalsaker ,jur. saker etc. varierande omfang	Ingen konsesjons- plikt, men meldeplikt	Leiar, tenestetorget

DATABEHANDLARAVTALAR FOR ETNE KOMMUNE

Databehandleravtale - IMDI-nett - Saksbehandlingssystem for busetting av flyktningar

Databehandler avtale KS FIKS - Meldingsformidler

Databehandleravtale - Telenor Objects, (trygghetsalarmar)

Databehandleravtale – INOSA

Databehandlaravtale for VOKAL frå Conexus

Databehandleravtale – Stafettloggen

Databehandleravtale - Insight

Databehandleravtale – Norkart

Databehandleravtale - Skånevik og Etne legekontor - HelseRespons

IPLOS data - Norsk Helsenett

Commfides virksomhetssertifikat

NaturData - Hjorterapport

Avtale – Ungdata

Avtale - Tilgang til Det sentrale folkeregister DSF via integrasjonsløysing

REVIDERT FDV AVTALE – GEODATA

TILLEGGSAVTALE - INFORMASJON OG METADATA - NORSK EIENDOMSINFORMASJON

DATABEHANDLINGSAVTALAR – NAV – bruk av Arena

DATABEHANDLERAVTALE NASJONALT LÅNEKORT

Deloitte.