Deloitte.

Forvaltningsrevisjon | Lindås kommune

Informasjonstryggleik

November 2017

«Forvaltningsrevisjon av informasjonstryggleik»

November 2017

Rapporten er utarbeidd for Lindås 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 Lindås kommune gjennomført ein forvaltningsrevisjon av informasjonstryggleik i Lindås kommune. Føremålet med forvaltningsrevisjonen har vore å undersøkje om kommunen har tilfredsstillande system og rutinar for informasjonstryggleik og om etablerte standardar og gjeldande lover og reglar vert følgt innanfor dette området.

I prosjektgjennomføringa har revisjonen gjennomgått aktuell dokumentasjon frå kommunen, gjort intervju med tre tilsette i kommunen og ein representant frå IKT Nordhordland (IKTNH), samt gjennomført ei elektronisk spørjeundersøking blant eit utval tilsette i kommunen.

Lindås kommune har eit styringssystem for informasjonstryggleik, men systemet er ikkje ferdigstilt. Det har ikkje vore oppdatert på fleire år, og vert berre i nokon grad nytta i informasjonstryggleiksarbeidet i kommunen. Styringssystemet formaliserer rolle- og ansvarsdelinga for informasjonstryggleik, men undersøkinga avdekker at denne organiseringa i praksis ikkje vert følgt, og at det er til dels uklare ansvarstilhøve med omsyn til informasjonstryggleik internt i kommunen, og mellom kommunen og IKTNH.

Lindås kommune har ikkje noko system som sikrar at oversikta over personopplysningar dei handsamar er oppdatert og fullstendig. Det er difor risiko for at kommunen handsamar personopplysningar utanfor oversikta. Det vert heller ikkje gjennomført risikovurderingar av systema kommunen brukar, noko som gjer det vanskelegare å vite kva risikoar for informasjonstryggleik kommunen er utsett for. Kommunen har heller ikkje noko oversikt over kva databehandlaravtalar dei har inngått, og kan difor ikkje vite om dei har oversikt over kven som handsamar personopplysningar på vegner av kommunen. Vidare har Lindås kommune dokumenterte rutinar og retningsliner for kontroll og etterprøving av informasjonstryggleik, men slik kontroll og etterprøving finn berre stad i avgrensa grad, og kommunen bryt slik med både sine eigne rutinar og retningsliner, samt sentrale krav i gjeldande regelverk.

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

Med omsyn til tilgjengelegheit i IKT-systema, kjem det fram i undersøkingane at IKTNH fastset kriterium for dette i systema dei driftar på vegner av Lindås kommune, men at Lindås kommune sjølv ikkje gjer dette. Vidare rapporterer ikkje IKTNH til Lindås kommune om nedetid i systema, noko som gjer det vanskeleg for Lindås kommune å kontrollere tilgjengelegheita og stabiliteten i IKT-systema på ein systematisk måte. Dette gjer det også vanskeleg for kommunen å setje i verk ev. tiltak for å betre tilgjengelegheit og stabilitet i IKT-systema.

Brukarstøtta for IKT i Lindås kommune vert jamt over opplevd som god av brukarane. Revisjonen merkar seg likevel at det ikkje er ei formalisert beredskapsvakt i brukarstøtta. Dette gir auka sårbarheit i brukarstøtta, noko som kan ha alvorlege konsekvensar for tilgjenge til naudsynt informasjon for dei tilsette i Lindås kommune, og slik for brukarane av kommunale tenester. Det kjem òg fram at organiseringa av brukarstøtte for fagsystema har manglar, mellom anna ved at det er knytt usikkerheit til kven som skal yte brukarstøtte til fleire av desse. Revisjonen si samla vurdering er difor at brukarstøttetenestene i Lindås kommune berre delvis er organisert på ein føremålstenleg måte.

Undersøkinga viser at langt dei fleste respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller annan fortruleg informasjon. Likevel indikerer svara i spørjeundersøkinga at over halvparten av respondentane berre delvis er kjende med kva ansvar og oppgåver dei har med omsyn til informasjonstryggleik. Revisjonen meiner at det er særleg alvorleg at nesten ein av fire av respondentane svarar at dei har delt passordet sitt, enten med IT-avdelinga eller andre. Dette bryt med heilt grunnleggjande prinsipp for informasjonstryggleik. Det er revisjonen si vurdering at dei tilsette i Lindås kommune ikkje har tilstrekkeleg kjennskap til eksisterande 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 som gjeld for handsaming av personopplysningar, og for informasjonstryggleika i kommunen generelt.

Revisjonen sine tilrådingar går fram i kapittel 6.

Innhald

Detaljert innhaldsliste

Figurar

Tabellar

1. Innleiing

1.1 Bakgrunn

Deloitte har gjennomført ein forvaltningsrevisjon av informasjonstryggleik i Lindås kommune. Prosjektet vart bestilt av kontrollutvalet i Lindås kommune i sak 05/17, 25. januar 2017.

Bakgrunnen for forvaltningsrevisjonsprosjektet er plan for forvaltningsrevisjon 2016-2020, der informasjonstryggleik var det første priorterte prosjektet.[1]

1.2 Føremål og problemstillingar

Føremålet med prosjektet har vore å undersøkje om kommunen har tilfredsstillande system og rutinar for informasjonstryggleik og om etablerte standardar og gjeldande lover og reglar vert følgt innanfor dette området.

Med bakgrunn i føremålet er det utarbeidd følgjande problemstillingar:

1. **I kva grad har Lindås kommune etablert eit styringssystem for informasjonstryggleik som tilfredsstiller krav i sentrale føresegner?**
   a) Er styrande dokument for informasjonstryggleik i samsvar med krav i regelverket?
   b) Er det etablert klare rutinar og ansvarsforhold knytt til informasjonstryggleik?
   c) Har kommunen eit system for kontroll og etterprøving av informasjonstryggleik, og vert slik kontroll og etterprøving gjennomført?
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) Er brukarstøtta til IKT-tenesta organisert på ein føremålstenleg måte med omsyn til tilgjengelegheit?
3. **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?

1.3 Avgrensing

Revisjonen har primært gått gjennom krav stilt til informasjonstryggleik knytt til personopplysningar. På dette området er det strenge krav gjennom personopplysningslova og personopplysningsforskrifta, og ein lekkasje av denne typen informasjon kan få store konsekvensar, både for kommunen og personane som vert råka. Ein gjennomgang av rutinar på dette området vil likevel også omfatte rutinar knytt til andre sensitive eller fortrulege opplysningar. Revisjonen har ikkje gjennomført testing eller analysar av teknisk konfigurasjon og tryggingstiltak.

1.4 Metode

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

Forvaltningsrevisjonen er gjennomført i tidsrommet februar til november 2017.

1.4.1 Dokumentanalyse

Rettsreglar og kommunale vedtak er vorte gjennomgått og nytta som revisjonskriterium. Vidare har revisjonen gjennomgått Lindås kommune sine styringssystem for informasjonstryggleik for å kartlegge rutinar og retningsliner, og vurdert desse opp mot krav i lovverk og standardar.

[1] Plan for forvaltningsrevisjon 2016-2020 vart vedteke av kommunestyret i sak 089/16, 15. desember 2016.

1.4.2 Intervju

For å få supplerande informasjon til skriftlege kjelder har revisjonen gjennomført fire intervju: tre tilsette i Lindås kommune som er involvert i informasjonstryggleiksarbeidet, og ein representant frå IKT Nordhordland (IKTNH).

1.4.3 Spørjeundersøking

Revisjonen har sendt ut ei elektronisk spørjeundersøking til eit utval tilsette i Lindås kommune. Føremålet med spørjeundersøkinga var å kartleggje i kva grad dei tilsette har kjennskap til og følgjer etablerte rutinar knytt til informasjonstryggleik.

Revisjonen fekk tilsendt ei oversikt over alle tilsette i kommunen, med e-postadressene deira og informasjon om kvar i kommunen dei arbeider. Eit tilfeldige utval tilsette ifrå alle einingane i kommunen fekk invitasjon til å svare på undersøkinga. Utvalet per eining vart vekta, slik at fleire tilsette i dei større einingane fekk invitasjon til å delta i undersøkinga. Totalt vart spørjeundersøkinga sendt til 359 personar, og etter fleire påminningar, kom det til sist 152 svar.

Undersøkinga var anonymisert, slik at revisjonen ikkje veit kven som har svart. På bakgrunn av oversikta over kven undersøkinga vart sendt til, haldt saman med svara til respondentane på kor dei arbeider, er det likevel mogleg å anslå svarprosent innan dei ulike einingane. Dette er presentert i tabell 1 under. Som det går fram av tabellen, varierer svarprosenten i dei respektive einingane mellom 10 % (anna stilling/eining innanfor oppvekst) og 100 % (stabsavdelinga). Total svarprosent var 42 %. Ei sannsynleg årsak til manglande svar i undersøkinga er at fleire av personane som fekk undersøkinga ikkje nyttar IKT-verktøy i sitt arbeid.[2] 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 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 under.

Tabell 1: Svarprosent

Eining	Respondentar	Inviterte	Svarprosent
Barnehage	6	16	38 %
Barnevern	8	9	89 %
Eining for funksjonshemma	15	43	35 %
Eining/avdeling innanfor personal, økonomi og organisasjon	3	12	25 %
Eining/avdeling innanfor samfunn og teknisk	22	38	58 %
Heimetenesta	14	51	27 %
Helsetenesta	7	13	54 %
Anna stilling/eining innanfor helse og omsorg	2	10	20 %
NAV	4	8	50 %
PPT	2	4	50 %
Sentraladministrasjonen	7	9	78 %
Sjukeheimstenesta	13	35	37 %
Skule	29	77	38 %
Anna stilling/eining innanfor oppvekst	1	10	10 %
Stabsavdelinga	5	5	100 %
Anna eining/avdeling	14	18	78 %
Total	**152**	**358**	**42 %**

[2] Svarprosenten blant tilsette som arbeider innanfor helse og omsorg eller skule og oppvekst, er lågare enn blant tilsette som arbeider på kontor (t.d. administrativt eller med sakshandsaming).

1.4.4 Verifiseringsprosessar

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

Rapportutkast vart sendt til rådmannen for verifisering og høyring. Det vart ikkje funne nokon faktafeil i samband med verifiseringsprosessen. I rådmannen si høyringsuttale vart det peika på mindre faktafeil. Revisjonen har kommentert desse i dei relevante avsnitta. Høyringsuttalen går fram av vedlegg 1 i rapporten.

1.5 Revisjonskriterium

Revisjonskriteria er dei krav og forventningar som forvaltningsrevisjonsobjektet skal verte vurdert opp mot. Kriteria er utleia frå autoritative kjelder i samsvar med krava i gjeldande standard for forvaltningsrevisjon.[3] I dette prosjektet er revisjonskriteria i hovudsak utleia frå personopplysningslova, personopplysningsforskrifta (POF), eForvaltningsforskrifta, helseregisterlova, norm for informasjonstryggleik i helse-, omsorgs- og sosialsektoren og sikkerheitslova. Kriteria er nærare presentert innleiingsvis under kvart tema, og i vedlegg 2 til rapporten.[4]

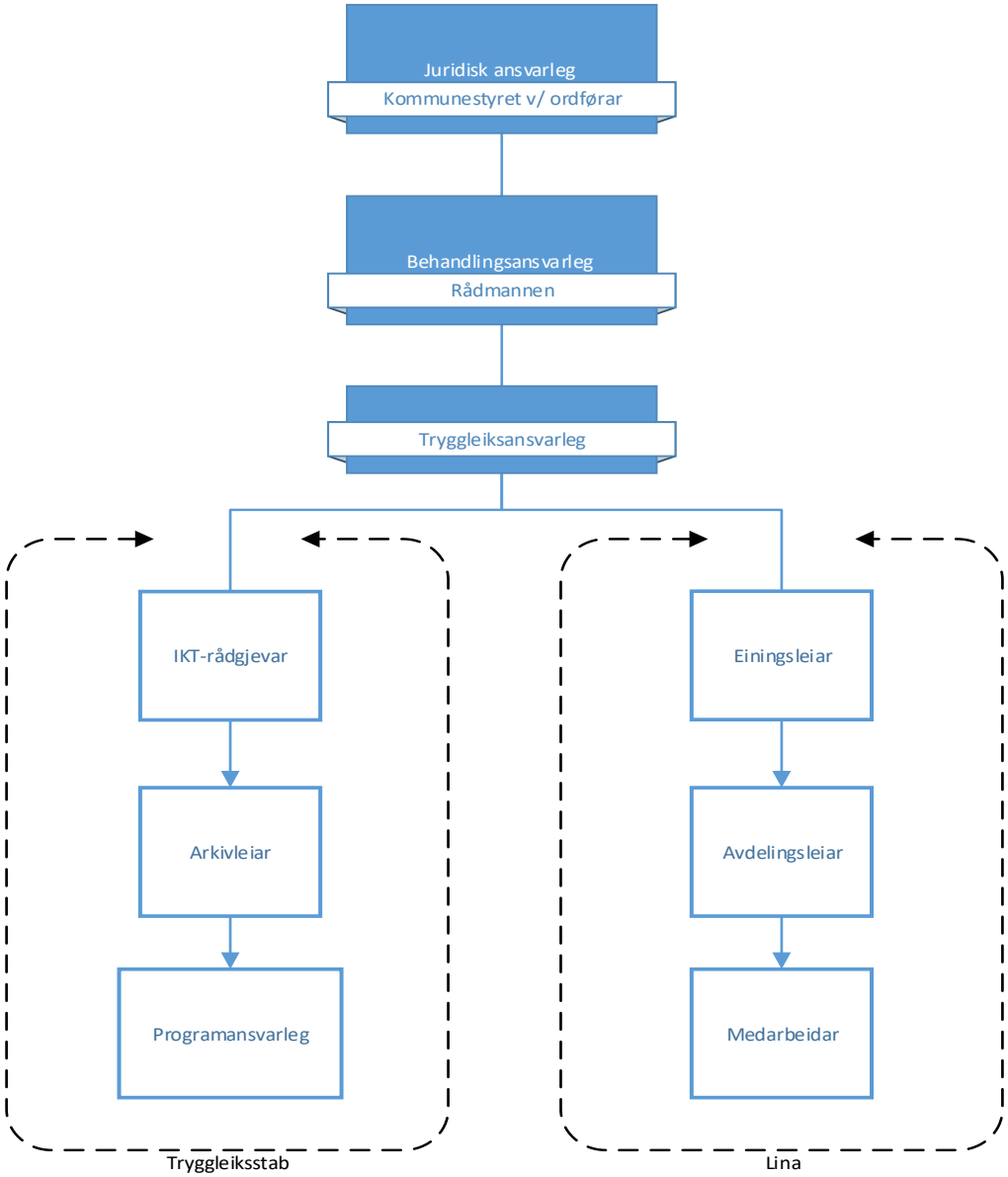
[3] RSK001, sjå http://www.nkrf.no/rsk_001_standard_for_forvaltningsrevisjon.
[4] I mai 2018 trer eit nytt og strengare regelverk knytt til personopplysningar i kraft (GDPR, sjå https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/).

2. Om tenesteområdet

2.1 Organisering av informasjonstryggleiksarbeidet i Lindås kommune

Arbeidet med informasjonstryggleik i Lindås kommune er formelt organisert som vist i figur 1. Rådmannen er behandlingsansvarleg, og skal vidaredelegere mynde for det daglege arbeidet til ein tryggleiksansvarleg. Tryggleiksansvarleg skal kunne trekkje på fagleg støtte frå ein tryggleiksstab bestående av IKT-rådgjevar, arkivleiar og dei programansvarlege. Informasjonstryggleiken skal ivaretakast i lina, frå einingsleiarane via avdelingsleiarane og til medarbeidarane. I dag er rolla som tryggleiksansvarleg delt mellom IKT-leiar og ein rådgjevar i rådmannen sin stab.

Figur 1: Formell organisering av informasjonstryggleiksarbeidet i Lindås kommune[5]



[5] Kjelde: Lindås kommune sitt styringssystem for informasjonstryggleik.

2.2 Interkommunalt IKT-samarbeid i Nordhordland

Lindås kommune er medlem i Interkommunale IKT-Tenester Nordhordland (IKTNH), eit interkommunalt samarbeid med åtte andre kommunar i Nordhordland.[6] Osterøy er vertskommune og ansvarleg for drifta av IKTNH.

Samarbeidet er regulert gjennom ein samarbeidsavtale frå 2011 og ein tenesteleveringsavtale frå 2013. Avtaleverket spesifiserer mellom anna at IKTNH er ansvarleg for IKT-brukarstøtte for medlemskommunane (sjå avsnitt 4.5).

Vidare er IKTNH databehandlar for ein del av personopplysningane som Lindås kommune er behandlingsansvarleg for. Dette er regulert gjennom ein databehandlaravtale frå 2015 (sjå avsnitt 3.4).

[6] Dei andre kommunane er Austrheim, Fedje, Masfjorden, Meland, Modalen, Osterøy, Radøy og Vaksdal.

3. Styringssystem for informasjonstryggleik

3.1 Problemstilling

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

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

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

3.2 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)

Vidare stiller § 15 i eForvaltningsforskrifta krav om at kommunar skal 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).

3.3 Styrande dokument for informasjonstryggleik

3.3.1 Datagrunnlag

Lindås kommune har eit dokumentert styringssystem for informasjonstryggleik (SiLk).[7] SiLk er tilgjengeleg på internett gjennom kommunen sitt kvalitetssystem, og er delt inn i ein styrande, ein gjennomførande og ein kontrollerande del. Føremålet med systemet er definert som å sikre «at det ikkje er fare for tap av liv og helse, økonomisk tap eller tap av omdømme og personleg integritet for einskildpersonar». SiLk skal sikre konfidensialitet, tilgjenge, og integritet, og det vert kortfatta vist til føremålet med handsaminga av helse- og personopplysningar innanfor ulike kommunaltenester.[8] Tabell 2 viser sentrale mål og strategiar knytt til informasjonstryggleik i SiLk.

[7] Styringssystemet for informasjonstryggleik i Lindås kommune.
[8] Det står at SiLk er bygd opp etter mønster av «Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren» (sjå https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet).

Tabell 2: Sentrale mål og strategiar i Styringssystem for informasjonstryggleik i Lindås kommune

Prosedyre/reglement	Samandrag
Tryggleiksmål og strategiar	SiLk inneheld mål for arbeidet med informasjonstryggleik. Kommunen ønskjer rask sakshandsaming av høg kvalitet, god tilgang på opplysningane, effektiv samhandling med andre forvaltningsnivå, og ivaretaking av personvernet. Det vert også vist til lovkrav kommunen er underlagt om handsaming av personopplysningar, samt til område som er regulert av tryggleiksordningar.
Sentrale delmål	SiLk inneheld fire delmål for handsaming av helse- og personopplysingar.
Hovudmål for informasjonstryggleik	Kommunen har definert eit hovudmål for informasjonstryggleik ved behandling av personopplysningar, samt to underpunkt om å etterleve styringssystemet og skapa tryggleiksmedvit i organisasjonen.
Tryggleiksstrategi	I SiLk er også kommunens strategi definert som «å utforme ein organisasjon med tryggleiksmedvit», som vert konkretisert i fire punkt. Kommunen skal også «sette tryggleikskrav til eksterne samarbeidspartar som handamar personopplysningar på kommunen sine vegne».

I Lindås kommune er det tilsett ein utviklingsrådgjevar som mellom anna har arbeidsoppgåver knytt til informasjonstryggleik. I intervju opplyser utviklingsrådgjevaren at det er han som i hovudsak har utarbeidd SiLk. I arbeidet med dette la han seg tett på *Norm for informasjonstryggleik i Helse- og omsorgstenester* (Norma), og nytta kommunen si eiga handbok om informasjonstryggleik. Årsaken til at Norma vart nytta, er ei vurdering om at denne femner om informasjonstryggleik breitt, og slik er relevant for fleire sektorar i kommunen.[9]

Det går fram av både intervju og dokumenta i SiLk at informasjonstryggleikssystemet ikkje er ferdigstilt. Det har heller ikkje har vore oppdatert sidan 2014-2015. I fleire intervju vert det peika på at det vil krevje mykje tid og innsats å få fullført og oppdatert SiLk, tid og innsats dei involverte opplever å ikkje ha til rådigheit.[10]

Utviklingsrådgjevaren meiner at den styrande delen av SiLk har ein viss verdi for informasjonstryggleiken i kommunen. Likevel kjem det fram i andre intervju og i svara i spørjeundersøkinga, at tilsette saknar og manglar tydelegare kunnskap også om den styrande delen i SiLk.

Når det gjeld dei gjennomførande og kontrollerande delane av SiLk, opplyser utviklingsrådgjevaren at dei begge er mangelfulle.[11] Også IKT-leiaren meiner dette, og peikar særleg på at den kontrollerande delen av SiLk ikkje, eller berre i liten grad, vert følgt.[12]

Generelt kjem det fram i intervju at SiLk ikkje vert opplevd å vere godt nok slik det er i dag: systemet er ikkje fullstendig, det er ikkje oppdatert, og sjølv dei delane som er ferdig utarbeidd er vanskelege å følgje i praksis. I intervju vert det sagt at desse svakheitene og manglane i SiLk utgjer den største utfordringa knytt til informasjonstryggleik i kommunen. Sjølv om nokre av dei intervjua ikkje trur det er særleg risiko knytt til informasjonstryggleik i kommunen, vert det understreka at det pga. manglande dokumentasjon t.d. av risikoar, er det usikkert kva som er den faktiske situasjonen med omsyn til informasjonstryggleiksrisikoar.

3.3.2 Vurdering

Gjennom SiLk har Lindås kommune styrande dokument for informasjonstryggleik. Sjølv om delar av SiLk er i samsvar med krav i regelverket, er ikkje systemet ferdigstilt, og at det ikkje har vore oppdatert på fleire år. Styringssystemet vert berre i nokon grad nytta i det daglege informasjonstryggleiksarbeidet i

[9] Utviklingsrådgjevaren fortel at han fekk bistand frå IKTNH på teknologi-sidan av SiLk. Han har ikkje fått noka opplæring i informasjonstryggleikssystem, men har vore på to kurs om Norma og deltatt på nokre seminar i regi av KInS (Kommunal Informasjonssikkerhet).
[10] Utviklingsrådgjevar fortel at han har prioritert å drive opplæring og endre haldningane til dei tilsette i kommunen med omsyn til informasjonstryggleik, framfor å ha alle dokument på plass. Sjå kapittel 5.
[11] T.d. peiker han på at SiLk manglar rutine- og prosedyreskildringar i den gjennomførande delen (sjå også avsnitt 3.4).
[12] Sjå også avsnitt 3.5.

kommunen. Basert på funna frå undersøkinga, er det difor revisjonen si vurdering at Lindås kommune sine styrande dokument for informasjonstryggleik ikkje er i samsvar med krav i regelverket.

3.4 Rutinar og ansvarsforhold knytt til informasjonstryggleik

3.4.1 Datagrunnlag

Interne ansvarsforhold knytt til informasjonstryggleik

SiLk spesifiserer ei rekkje roller i informasjonstryggleiksarbeidet i kommunen, og skildrar ansvarstilhøve mellom desse. Organiseringa av informasjonstryggleiksarbeidet slik det er definert i SiLk, skal sikre avklarte arbeids- og ansvarstilhøve for informasjonstryggleiken i kommunen.

Det overordna, juridiske ansvaret ligg til kommunestyret ved ordførar, medan rådmannen er behandlingsansvarleg. Rådmannen har delegert mynde for informasjonstryggleiksarbeidet til ein tryggleiksansvarleg. Tryggleiksansvarleg skal ha ein tryggleiksstab, som består av IKT-rådgjevar, arkivleiar og dei programansvarlege. Tryggleiksstaben skal vere ein ressursgruppe for tryggleiksspørsmål.[13]

Elles følgjer ansvarstilhøva lineorganiseringa; einingsleiarane har det daglege ansvaret for etterleving av SiLk, og medarbeidarar har mellom anna plikt til å setje seg inn i, og etterleve SiLk. Medarbeidarar har eit sjølvstendig ansvar for å be næraste leiar om råd dersom det er tvil om kva som er gjeldande praksis. Avdelings- og fagleiarar har same ansvar og oppgåver som andre medarbeidarar, med mindre noka anna er bestemt.

Tabell 3 presenterer kva stilling som har kva rolle og ansvar innanfor informasjonstryggleik.

Tabell 3: Ansvar og oppgåver i stillingar knytt til informasjonstryggleik slik dei går fram i SiLk

Stilling	Rolle knytt til informasjonstryggleik
Rådmann	Rådmann er behandlingsansvarleg, og bestemmer føremålet med og kva hjelpemidlar som skal nyttast i behandlinga av personopplysningar. Rådmannen skal sørgje «for at kommunen har tilfredsstillande informasjonstryggleik og at behandling av personopplysningar følgjer lov og forskrift». Behandlingsansvarleg inneber «eit sjølvstendig tilsyns-, tryggleiks- og kontrollansvar for det totale informasjonssystemet». Rådmannen har det overordna strategiske ansvaret, og skal avgjere korleis arbeidet med informasjonstryggleik skal organiserast og gjennomførast.
Tryggleiksleiar (tryggleiksansvarleg /informasjonssjef)	Tryggleiksleiar har fått delegert overordna operativt ansvar og avgjerdsmynde i informasjonstryggleik frå rådmannen, og rapporterer til rådmannen. Tryggleiksleiar skal ha ein stab med nøkkelpersonar innan tryggleiksspørsmål som ressursgruppe. Tryggleiksleiar skal m.a. fastsette krav til tryggleiksnivå for informasjonstryggleik, og utarbeide og halde à jour retningslinene.
Einingsleiar	Rådmannen har delegert det daglege ansvaret for etterleving av tryggleikssystemet til einingsleiarane. Einingsleiarane har ansvar for informasjonstryggleiken innanfor si eining og skal sørgja for at eininga gjennomfører naudsynte tryggleikstiltak i samsvar med overordna krav og retningsliner, samt at tilhøva vert lagt til rette for gjennomføring av tiltaka. Vidare har einingsleiarane oppgåver knytt til sikring av personopplysningar, og overfor dei enkelte medarbeidarar knytt til delegering, rapportering og avvikshandsaming.
Avdelings- og fagleiar	Avdelings- og fagleiar sitt ansvar og oppgåve er dei same som for andre medarbeidarar, med mindre anna er bestemt i delegering eller instruks frå einingsleiar.
Medarbeidar	Alle medarbeidarar skal underteikne teieplikt, sette seg inn i og etterleve SiLk. Dei skal kjenne prosedyrane for sine fagområde, og nytte avvikssystemet når prosedyrar ikkje vert følgt eller ved potensielle eller faktiske truslar mot informasjonstryggleiken. Alle medarbeidarar har eit sjølvstendig ansvar for å be næraste leiar om råd dersom det er tvil om gjeldande praksis.
IKT-rådgjevaren	IKT-rådgjevaren har det overordna operative ansvaret for at utstyr og programvare for informasjonsbehandling og kommunikasjon til ein kvar tid fungerer. IKT-rådgjevar har også ansvar for å utarbeide IKT-dokumentasjon, sikre sikker drift av nettet, gje rettleiing i tryggleiksspørsmål for dei elektroniske informasjonssystema, samt sette vilkår og godkjenne kravspesifikasjon, konsekvensutgreiingar og risikoanalyse saman med innkjøpar/programansvarleg ved nykjøp av informasjonssystem.
Arkivleiar	Arkivleiaren har overordna fagleg mynde for arkivverksemda i kommunen. Arkivleiar skal sjå til at informasjonstryggleik står sentralt i all arkiv- og dokumentbehandling, kontrollera at

[13] Sjå figur 1 på side 10.

	personopplysningar er fysisk og digitalt sikra, og hjelpe einingane i vurdering av personregistre med omsyn til konsesjon- og meldeplikt.
Programansvarleg	Det skal vere utpeikt ein programansvarleg for kvart fagsystem eller modular i desse. Vedkommande skal ha spesialkompetanse på sitt fagsystem, og ha utvida rettar som administrator. Programansvarleg skal kommunisere med IKT-rådgjevar i datatekniske saker og til sin einingsleiar ved organisatoriske og fysiske tilhøve, og har elles ansvar for å sjå til at medarbeidarar kan ivareta sitt personlege tryggleiksansvar i informasjonssystemet, sørgje for at reglar vert følgde, sørgje for tilgang til programvare, drive kontroll over systema, og gjennomføre opplæring i det aktuelle fagprogrammet.

I intervju kjem det fram at rollane og ansvarstilhøva skildra i SiLk berre i nokon grad vert følgt i praksis. Utviklingsrådgjevaren opplever at oppgåvene som går fram i den styrande delen i SiLk sannsynlegvis vert ivaretatt i kommunen, men han opplyser at dei ikkje kan vere sikre, då det manglar dokumentasjon på dette.

Vidare går det fram av intervju at SiLk manglar vesentlege delar av den skriftlege dokumentasjonen som fortel korleis tilsette skal handtere informasjonstryggleik.

Rolla «tryggleiksansvarleg» er i dag delt mellom IKT-leiaren og utviklingsrådgjevaren. Dette vart gjort munnleg av rådmannen, og er ikkje nedfelt i noko dokument eller stillingsskildring. IKT-leiaren opplever at rolla som tryggleiksansvarleg i liten grad er formalisert, noko som fører til usikkerheit om kva som faktisk ligg i ansvaret, særleg når det gjeld databehandlaransvaret.

IKT-leiar meiner at ansvaret må fordelast på fleire personar, og at den enkelte tenesteleiar må få ansvar og eigarskap til informasjonstryggleiksarbeidet. Det er ikkje realistisk å leggje opp til at ein informasjonstryggleiksansvarleg til ei kvar tid skal ha kontroll på alle helse- og personopplysningar i alle fagsystem åleine.

I intervju vert det referert til diskusjonar internt i kommunen om plasseringa av informasjons-tryggleiksansvarleg i organisasjonen. IKT-leiaren har sjølv bedt om at rolla vert lagt til eit anna stad enn hos ham, då han ikkje har kapasitet til å gjennomgå og vidareutvikle alle delane av styringssystemet.[14] Også utviklingsrådgjevaren fortel at kommunen manglar ressursar og kompetanse i arbeidet med informasjonstryggleik.

I intervju opplyser systemansvarleg for Visma Profil at rolla hennar i hovudsak går ut på å leggje til rette for at fagsystemet følgjer dei lovkrav og reglar som gjeld innan helse og omsorg, samt å leggje til rette for at brukarane veit føremålet med fagsystemet og har kompetanse til å bruke det. I tillegg inngår det i rolla som systemansvarleg eit ansvar for å ivareta informasjonstryggleikaspektet i fagsystemet.

Systemansvarleg for Visma Profil fortel vidare at det har vore gjort forsøk på å få til faste møte mellom dei systemansvarlege for dei ulike fagsystema, men at møta etter ei tid tok slutt. Ho er ikkje kjend med at kommunen har noka formell gruppe for systemansvarlege som arbeider med og sikrar lik utøving av informasjonstryggleik i kommunen. Ho er klar på at ei slik gruppe ville vore nyttig, men understrekar likevel at om det oppstår spørsmål eller utfordringar knytt til informasjonstryggleik, vert desse drøfta med utviklingsrådgjevaren og/eller IKT-leiaren, og at dei saman stort sett klarar å finne svar på utfordringane.

IKT-leiar kommenterer elles i intervju at det er vanskeleg å få oversikt over ansvarsdeling knytt til informasjonstryggleik, både internt i kommunen og mellom kommunen og IKTNH. Kommunen har ei sjølvstendig plikt knytt til informasjonstryggleik, sjølv om IKTNH tek hand om delar av dette på kommunen sine vegner. Utviklingsrådgjevar seier at kommunen tek større ansvar for dette no enn tidlegare, men at dei ikkje i tilstrekkeleg grad har ivaretatt sitt sjølvstendige ansvar for informasjonstryggleik.

Ansvarsfordeling mellom IKTNH og Lindås kommune knytt til informasjonstryggleik

IKTNH er driftsorganisasjon for alle kommunane i samarbeidet, og har ansvar for:

- Nettverk, kommunikasjon og tryggleik
- Serverpark

[14] Rådmannen har gjeve utviklingavdelinga i oppdrag å utarbeide eit prosjektmandat for arbeidet med å komplettere informasjonstryggleikssystemet.

- Drift av alle applikasjonar som er plassert i IKTNH sine datarom (ikkje SaaS-løysningar levert via nettet)
- Klienthandsaming (pc, nettbrett, mobil)
- Telefoni (fast og mobil)

I utgangspunktet er det kommunane sjølve som har ansvar for eigen informasjonstryggleik, men delar av dette ansvaret er gjennom avtale lagt til IKTNH. Dette gjeld i dei fysiske og tekniske dimensjonane i informasjonstryggleik, samt databehandlaravtalar med leverandørar som behandlar personopplysningar på vegner av kommunen gjennom system drifta av IKTNH. Med omsyn til den fysiske og tekniske sikringa, er det IKTNH som skal beskytte og varsle dersom noko skjer.

Når det gjeld den juridiske dimensjonen av informasjonstryggleiken, føreligg det ein generell databehandlaravtale mellom Lindås kommune og IKTNH ved Osterøy kommune.[15] Av denne går det fram at IKTNH er databehandlar og Lindås kommune er databehandlaransvarleg. Avtalen har tre vedlegg: eit IKT-reglement; dokumentasjon knytt til sikker sone som også inneheld skildring av oppbygginga av IKTNHs IKT-løysning; samt ei sjekkliste for databehandlar med 13 krav, mellom anna krav til tilgangstyring, hendingsregistrering, teieplikt og attenderapportering.

IKTNH opplyser å ha god kontroll på deira ansvar og oppgåver knytt til informasjonstryggleik. IKNTH opplyser òg å oppleve at dei og medlemskommunane stort sett har lik oppfatning av ansvarsfordelinga knytt til informasjonstryggleik. Likevel vert det presisert at denne ansvarsfordelinga ikkje alltid vert opplevd som avklart; til dømes kan det oppstå litt ueinigheit om kven som er ansvarleg i situasjonar der eit fagsystem går ned. Prosjektleiar viser til at sjølv om IKTNH har ansvar for at eit fagsystemet skal vere tilgjengeleg for kommunane, så kan problemet ligge hos dei som leverer og drifter fagsystemet.

Det er rådmennene i eigarkommunane som avgjer kva som skal vere IKTNH sine oppgåver. Dette kan dei gjere mellom anna i dei månadlege møta mellom IKTNH-leiar og rådmannsutvalet. IKTNH opplever kommunikasjonen med kommunane som god, og det vert mellom anna peika på at det er låg terskel for rådmennene å ta kontakt med leiar av IKTNH.

Frå IKTNH si side vert det sagt at det ikkje er nokon openbar informasjonstryggleiksrisiko for kommunane knytt til deira organisering. Likevel kunne den intervjua ønskje at det var noko meir konkret kva ansvar han og IKTNH har for informasjonstryggleiken i kommunane. Også IKT-leiaren i Lindås kommune opplever at ansvarsforholdet mellom kommunen og IKTNH ikkje er heilt tydeleg i tenesteleveringsavtalen når det gjeld informasjonstryggleiksarbeidet. Uklarheita gjeld likevel ikkje personopplysningar, då tenesteleveringsavtalen seier at IKTNH har ansvaret for persopplysningar dei handamar og at kommunen har ansvar for personopplysningar som vert handsama av andre.

Det går fram av intervju at systemansvarleg for Visma Profil samarbeider tett med IKNTH om drifta av fagsystemet,[16] og at det alltid er fokus på informasjonstryggleik, også når det gjeld underleverandørar som utfører arbeid. Systemansvarleg opplyser at ansvarsfordelinga mellom ho og IKTNH er tydeleg og avklart; IKTNH driftar systemet, medan systemansvarleg tek hand om innhaldet i det.[17]

Oversikt over personopplysningar som vert handsama

Revisjonen har mottatt kommunen si oversikt over personopplysningar som vert handsama i kommunen sine fagmiljø og fagprogram.[18] Oversikta synar mellom anna kven som er programansvarleg for kva fagprogram, kva informasjonstype som vert handsama, heimel for handsaminga, om det er sensitive opplysningar, samt om opplysningane er konsesjonspliktige eller meldepliktige. Det går fram av oversikta at det er tryggleiksleiar som skal oppdatere oversikta etter opplysningar frå leiarar for tenester, støttefunksjonar, avdelingar eller programansvarlege.

[15] Datert august 2015.
[16] IKTNH opplyser å drifte 43 fagsystem på vegner av kommunane i samarbeidet, og uttrykker at de har rimeleg god kontroll både desse og eigne system. Fagsystema IKTNH driftar for kommunane går fram av liste i vedlegg 3.
[17] Samstundes påpeiker ho at IKTNH har tilgang til kommunen sine fagsystem med administratorrettar, slik at det er ein teoretisk risiko for at dei kan gå inn og hente ut opplysningar. Systemansvarleg tek regelmessig ut rapport som viser kven som har vore inne i systemet og med kva grunngjeving, og ho har aldri opplevd at det har vore noko problem med IKTNH si tilgang.
[18] Oversikta vart sist oppdatert i desember 2016.

IKT-leiar meiner at oversikta er for generell når det gjeld kva personopplysningar kommunen handsamar, og han er ikkje trygg på at oversikta inneheld alle opplysningar som kommunen handsamar og som kan verte knytt til eit individ.[19] Utviklingsrådgjevaren – som har ansvaret for å halde oversikta oppdatert – meiner at dokumentet er rimeleg komplett, men også han seier han ikkje kan vere heilt sikker. Dei har ikkje noko system eller nedfelt ein rutine for å halde oversikta oppdatert og komplett.[20] Utviklingsrådgjevar påpeiker likevel at det ikkje er store endringar i kva fagsystem kommunen har eller personopplysningar kommunen handsamar.

I intervju går det fram at prosjektleiar i IKTNH meiner at Lindås kommune er om lag like gode til å handsame personopplysningar som dei andre kommunane i IKTNH.

Databehandlaravtalar

Tabell 4 viser seks dei seks databehandlaravtalar Lindås kommune har med eksterne partar som revisjonen har mottatt.

Tabell 4: Lindås kommune sine databehandlaravtalar

Avtalepartnar	År	Innhald
Alarm24	2017	Personopplysningar og pasientopplysningar knytt til tryggleiksalarm.
Vakt og alarm AS	2016	Personopplysningar og pasientopplysningar knytt til tryggleiksalarm.
Osterøy kommune IKTNH	2015	Generell databehandlaravtale mellom IKTNH og Lindås kommune.
NETS Norway AS (DNB)	2012	Personopplysningar knytt til fakturahandsaming.
NAV Hordaland	2012	Personopplysningar knytt til lov om sosiale tenester i NAV.
Ergo Group	2010	Likningsopplysningar.
Kommuneforlaget	2008	Avtalen angår ekstern tilgang til database i Lindås kommune.

Det vert opplyst at Lindås kommune ikkje har ei sentral oversikt over inngåtte databehandlaravtaler. Kommunen har heller ikkje følgt opp tredjepartsleverandørar eller eventuelle databehandlaravtaler IKTNH har inngått på vegner av kommunen. Følgjeleg har ikkje kommunen oversikt eller kontroll på dette området.[21]

Utviklingsrådgjevaren påpeiker at det er IKNTH som i hovudsak sikrar informasjonstryggleiken knytt til databehandlaravtalar. Likevel meiner både utviklingsrådgjevaren og IKT-leiaren at kommunen burde hatt eit eige system for databehandlaravtaler.[22]

IKT-leiaren opplyser at både IKTNH og Lindås kommune har kontakt med eksterne leverandører når det gjeld databehandlaravtalar. Frå kommunen er det primært IKT-leiar som er involvert i dette arbeidet. IKT-leiaren sikrar då at leverandørane tilfredstillar krava i regelverket, og signerer databehandlaravtaler på vegner av kommunen ved innføring nye fagsystem som omhandlar personopplysningar.

IKTNH oppgir å ha kontroll over databehandlaravtalane dei har med tredjepartar på vegner av medlemskommunane. Kommunane har moglegheit til å be IKTNH om å få sjå desse. Det vert understreka

[19] Systemansvarleg for Visma Profil opplever at kommunen har oversikt over kva personopplysningar som ligg i Visma Profil, men at kommunen kan bli betre på kvalitet og innhald. Ho viser til at kommunen nyleg har teke eit løft for å sikra rutinar rundt dokumentasjon i pasientjournal.

[20] Det har vore utfordringar knytt til å halde behandlingsoversikta over personopplysningar komplett. Som eit døme peiker utviklingsrådgjevaren på at Kemneren i Nordhordland nyttar tre ulike fagsystem i sitt arbeid – to eigd og drifta av staten og eit lokalt. Dette var ikkje utviklingsrådgjevaren informert om. Dei statlege fagsystema og personopplysningane i dei er ikkje i behandlingsoversikta til kommunen. Det er noko usikkerheit knytt til om stat eller kommune er behandlingsansvarleg for desse opplysningane. Utviklingsrådgjevar opplyser at kommunen ikkje har oversikt over kva personopplysningar som vert handsama i desse to systema, men at det skal verte kartlagt.

[21] Det kjem i intervju fram døme på hendingar der manglande oversikt over databehandlaravtalar og kva personopplysningar som vert handsama, førte til ein situasjon der informasjonstryggleiken vart skadelidande. Dei har rydda opp i situasjonen no.

[22] Dei føreslår at arkivsystemet eller kvalitetssystemet kan nyttast til dette, og/eller at databehandlaravtaler og leverandøren til avtalen kunne inngått som kolonnar i behandlingsoversikta.

at IKTNH berre har databehandlaravtale der IKTNH er databehandlaransvarleg. IKTNH er trygge på at databehandlaravtalene dei har dekker personopplysningane handsama av tredjepartar på deira vegne.

3.4.2 Vurdering

Gjennom SiLk har Lindås kommune formalisert rolle- og ansvarsdelinga for informasjonstryggleik. Undersøkinga avdekker at denne organiseringa i praksis ikkje vert følgt, og at det er til dels uklare ansvarstilhøve med omsyn til informasjonstryggleik både internt i kommunen, og mellom kommunen og IKTNH.

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

Revisjonen finn vidare i sine undersøkingar at Lindås kommune har dokumentert oversikt over kva personopplysningar dei handsamar. Kommunen har likevel ikkje noko system som sikrar at oversikta er oppdatert og fullstendig. Revisjonen meiner difor det er risiko for at kommunen handsamar personopplysningar utanfor oversikta. Kommunen bryt slik både med kravet om at det skal førast oversikt over personopplysningane som vert behandla, jf. POF § 2-4 først 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 vert handsama, gjer at kommunen òg 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 pliktar og dei registrertes rettar til ei kvar tid.

Kommunen har ikkje noko system for å halde oversikt over kva databehandlaravtalar dei har inngått. Kommunen kan difor ikkje vite om dei har oversikt over kven som handsamar personopplysningar på vegner av kommunen. Det er slik risiko for at personopplysningar som kommunen er behandlingsansvarleg for, vert handsama av databehandlarar utan at kommunen kan kontrollere om lov- og forskriftskrav vert følgt. Også dette er brot på dokumentasjonskravet i POF § 2-16.

3.5 Kontroll og etterprøving av informasjonstryggleik

3.5.1 Datagrunnlag

SiLK har som nemnd ein kontrollerande del.[23] Her går det mellom anna fram at «Rådmannen skal følgje opp at informasjonstryggleiken i kommunen vert tatt i vare». Det står vidare at det i tillegg til den daglege oppfølginga, skal utførast fem typar oppfølging:

1. tryggleiksrevisjonar
2. risikovurderingar i kommunen sine einingar
3. avvikshandsaming
4. leiinga sin gjennomgang
5. kontroll av kven som har hatt tilgang til eit behandlingsretta helseregister eller fagsystem.

Det går fram i intervju den kontrollerande delen av SiLk ikkje, eller berre i liten grad, vert følgt. Det manglar rutinar for dette arbeidet, og IKT-leiar peikar på at det er låg bevissthet om informasjonstryggleik i ulike delar av kommunen.[24]

Risikovurderingar av informasjonstryggleik

SiLk inneheld retningsliner for risikovurdering. Retningslinene introduserer omgrepa knytt til risikovurdering på eit overordna nivå (sannsyn og konsekvens), viser til relevant regelverk (utvalde paragrafar i personopplysningsforskrifta), og skildrar kort korleis ein kan gjennomføre vurderingsarbeidet. Retningslinene viser gjennomgåande til informasjonstryggleiksomgrep, t.d. i samband med

[23] Heile den kontrollerande delen er utarbeidd i august 2014, med unntak av det som omfattar «dokumentasjon», som er utarbeidd i juni 2015.
[24] Mellom anna peikar han på at det er mangelfulle behovsanalyser på informasjonstryggleik, det manglar rutinar om bruk av IT-løysingar i kvalitetssystemet, og det er vanskeleg å få oversikt over ansvarsdeling, både internt i kommunen og mellom kommunen og IKTNH.

trusselvurdering som peiker på mangelfull *tilgang*, manglande *integritet* og bristande *konfidensialitet* som truslar mot informasjonstryggleik.

IKT-leiaren i Lindås kommune fortel at det ikkje har vore gjennomført risiko- og sårbarheitsanalysar av kommunen sine fagsystem sidan han vart tilsett i 2016.[25] Han opplever at dette ein stor mangel, då slike analysar er eit sentralt vertkøy i arbeidet med å handsame risiko knytt til informasjonstryggleik. IKT-leiar fortel at det mellom anna har vore etterlyst slike analysar av det elektroniske pasientjournalsystemet (Visma Profil). Systemansvarleg for Visma Profil seier at dei ikkje har utført risikovurderingar av fagsystemet, og forklarar dette med at kommunen ikkje har rutinar for slike analyser.

I høyringsuttalen til rapporten går det fram at det nyleg har vorte gjort ROS-analysar av fagsystema som inngår i omsorgsteknologitenesta i kommunen, men at det ikkje er gjort ROS-analysar av dei fleste fagsystema til kommunen.

I intervju kjem det fram at det heller ikkje vert fastsett akseptkriterium for risiko knytt til informasjonstryggleiken i kommune.[26]

IKTNH gjennomfører ROS-analysar av eigne system og ansvaret dei har ovanfor medlemskommunane.

Tryggleiksrevisjon

Ifølgje SiLk skal rådmannen sjå til at tryggleiken vert ivaretatt ved å gjennomføre jamlege og minimun årlege tryggleiksrevisjonar. Dette skal skje etter ein godkjent plan for tryggleiksrevisjonar. Det går fram at tryggleiksrevisjonane sine resultat og konklusjonar skal dokumenterast. Det er vidare lista kva tema som skal vurderast i tryggleiksrevisjonane.[27]

Frå intervju kjem det fram at Lindås kommune ikkje har gjennomført nokon tryggleiksrevisjonar dei seinare åra. Det vert i intervju peika på at kommunen veit dette er noko dei burde gjere, men at det er vanskeleg å finne tid.[28]

IKTNH skal etter eigne rutinar gjennomføre årlege tryggleiksrevisjonar. I intervju opplyser prosjektleiar i IKTNH at det ikkje har vore gjort tryggleiksrevisjonar sidan har var tilsett i 2015.

Avvikshandsaming

Når det gjeld avvikshandsaming, går det fram av SiLk at det er einings- og avdelingsleiarar som har ansvar for informasjonstryggleiken i si eining. Avvik skal fortløpande meldast til næraste leiar, som har ansvar for å sette i verk nødvendige tryggleikstiltak. Dei kommunale einingane skal årleg gjennomgå sine tryggleiksrutinar og sin avvikstatistikk, for så å rapportere resultata til tryggleiksleiar. Mellom anna skal det kontrollerast at rutinar vert nytta og fungerer som meint, og at tidlegare meldte avvik er retta opp. Det skal settast i verk avviksbehandling dersom informasjonssystema vert nytta i strid med rutinane, ved brot på informasjonstryggleiken, eller ved mistanke om mangelfull tryggleik.

For vesentlege tekniske avvik, skal einingsleiarar rapportere til IKT-rådgjevar som i samråd med programansvarleg skal setje i verk tiltak. Ikkje-tekniske avvik som er vesentlege, skal meldast til tryggleiksansvarleg. Tryggleiksansvarleg skal så vurdere «avviket opp mot tryggleiksmåla til kommunen og eventuelt koma med framlegg om tiltak». I tilfelle avviket har medført ikkje-autorisert utlevering av personopplysningar der konfidensialitet er nødvendig, så skal det meldast ifrå til Datatilsynet.

Det vert opplyst i intervju at kommunen kjøpte KF Kvalitet i april 2013, men at avvikssystemet av tekniske årsaker ikkje vart integrert i kommunen sitt system før hausten 2015. I praksis vart avviksmodulen og KF Kvalitet-verktøyet tatt i bruk frå januar 2016. Heile kommunen nyttar no same avvikssystem.

---

[25] Nokre av leverandøren skal ha gjort slike analysar av produkta dei leverer.
[26] Sjå også avsnitt 4.3.
[27] T.d. plassering av ansvar og organisering av tryggleiksarbeidet, kvalitet på tryggleiksmål og tryggleiksstrategi, resultat av opplæring, forvaltning og bruk av helse- og personopplysningar, tilgang til helse- og personopplysningar og tiltak mot uautorisert innsyn, effekten av etablerte tryggleikstiltak og ivaretaking av informasjonstryggleik hos kommunikasjonspartnarar, databehandlarar og leverandører.
[28] Systemansvarleg for Visma Profil opplyser i intervju at det til ein viss grad vert gjort kontinuerlige evalueringar av fagsystemet i hennar daglege arbeid med det.

I perioden 1. januar 2016 til 16. juni 2017 vart meldt totalt 2229 avvik i Lindås kommune.[29] Av desse var 14 avvik meldt inn på områda «informasjonstryggleik» og «informasjonssikkerheit». Kommunen opplyser at det også kan vere avvik knytt til informasjonstryggleik i andre avvikskategoriar. Dei intervjua i kommunen er tydelege på at dei har ein veg å gå med omsyn til avviksmeldingar knytt til informasjonstryggleik.

IKTNH har eit eige avvikssystem som femner om både drifta av IKT-løysingane og personopplysningar.[30] Generelt melder kommunane avvik knytt til IKT-løysingane; det er sjeldnare at dei melder avvik knytt til personopplysningar. Lindås kommune er flinke til å melde avvik til IKTNH samanlikna med dei andre eigarkommunane.

Leiinga sin gjennomgang

Det går fram av den kontrollerande delen av SiLk at rådmannen saman med leiargruppe, IKT-rådgjevar og tryggleiksansvarleg skal «ha ein årleg gjennomgang av tryggleiksmål, strategi og organisering av informasjonssystema». SiLk fastset 12 punkt på kva gjennomgangen skal innehalde. Det er tryggleiksansvarleg som har ansvar for å organisere gjennomgangen.

I intervju med IKT-leiar i Lindås kommune kjem det fram at det ikkje har vore noko møte med leiinga om informasjonstryggleik i tida han har vore tilsett. IKT-leiar meiner dette er eit teikn på at informasjonstryggleik i avgrensa grad vert ivareteken i leiargruppa; leiinga har ikkje eit operativt fokus på informasjonstryggleik, men delegerer i stor grad ansvaret for dette arbeidet til dei tryggleiksansvarlege.[31]

Utviklingsrådgjevar opplever at informasjonstryggleiksarbeidet er betre forankra i leiinga no enn tidlegare, men opplyser om at det fortsatt er varierande korleis dette vert ivaretatt i lina.

Systemansvarleg for Visma Profil opplyser i intervju at leiinga i kommunen har vore involvert i arbeidet med informasjonstryggleik. Ho opplyser vidare at overordna rutinar har vorte førelagt rådmann til godkjenning (t.d. rutine for aktivitet i journal).

Dokumentasjon og aktivitetslogg

I SiLk sin kontrollerande del inngår rutinar for dokumentasjon og aktivitetslogg. Overordna vert det vist til at «[r]esultat frå arbeidet med informasjonssystemet skal dokumenterast i den utstrekning det er nødvendig for å oppnå tilfredsstillande informasjonstryggleik». SiLk spesifiserer kva type dokumentasjon som skal lagrast, og i kor lang tid ulike typar informasjon skal lagrast.[32]

Det går vidare fram i SiLk at det er IKTNH som er ansvarleg for aktivitetsloggen i nettverket, medan dei programansvarlege er ansvarlege for aktivitetsloggen til sine fagprogram. Delar av innhaldet i desse hendingsregistra er vidare spesifisert.

Det vert òg vist til POF § 2-16 om at både autorisert og ikkje-autorisert bruk av informasjonssystema skal verte lagra i minst tre månader. I den gjennomførande delen av SiLk, vert det stilt krav om at all autorisert bruk og forsøk på uautorisert bruk av informasjonssystema skal verte registrert og lagra i minimum 2 år. Føremålet med registreringane er å kunne spora utførte handlingar, noko som er nødvendig for å kunne avdekka og oppklara brot på informasjonstryggleiken.

IKTNH har eigne rutinar og prosedyrar knytt til hendingsregister og –handsaming.

---

[29] Avvika er gruppert på område (t.d. barnehage, eigedom, eller HMS), på område og avvikstype (t.d. sjukeheim – brot på interne rutinar eller HMS – inneklima), og på tenestestad (t.d. ein barneskule eller ein sjukeheim). Helse- og omsorg meldte inn 1453 av avvika. Dei andre store avviksgruppene er HMS (299), barnehage (144) og skule (112). Systemansvarleg for Visma Profil fortel at det har førekome informasjonstryggleiksavvik innanfor helse og omsorg. Eit alvorleg døme var uønskt innsyn i journal til slektningar/kollegaer utan grunngjeving. Systemansvarleg fortel at i slike tilfelle er avviket tatt opp med dei dette har gjeldt. Avdelingsleiarane skal regelmessig ta ut rapportar over kven som har vore inne i pasientjournalar, og følgje opp dersom nokon har vore inne utan legitim grunn.

[30] T.d. om ein PC vert stjålen, så vert det registrert og PC-en vert meldt ut av nettverket.

[31] IKT-leiar peikar òg på at leiargruppa etter regelverket skal fastsette risikomål, noko som ikkje er mogleg då dei ikkje gjennomfører ROS-analysar

[32] T.d. skal resultat frå leiargjennomgangar, risikoanalysar, eigenkontrollar og avviksbehandling, oversikt over område og utstyr med tilgangskontroll, oversikt over soner, data og program med tilgangskontroll, autorisering av brukarar og tidlegare utgåver av godkjende tekniske og administrative retningsliner og rutinar lagrast i fem år.

Tilgangskontroll

I den gjennomførande delen i SiLk skildrast prosedyrane for tilgangstyring. Ifølge prosedyren skal det berre gis autorisering og tilgang til personell som er underlagt instruksjonsmynde frå Lindås kommune, eller til dei som arbeider under instruksjonsmynde frå kommunen sine eventuelle databehandlarar. Vidare går det fram at «[a]utorisasjon kan berre bli gitt i den grad det er nødvendig i den tilsette sitt arbeid og er grunna i tenestlege behov. Det er berre slikt personell som kan gis tilgang til personopplysningar».

Det går vidare fram at kommunen skal ha eit autorisasjonsregister, der det som eit minimum skal gå fram:

- informasjon om kven som er tildelt autorisasjon
- til kva for rolle autorisasjonen er tildelt
- føremålet med autorisasjonen
- tidspunkt for når autorisasjonen ble gitt og eventuelt kalt tilbake
- informasjon om kva for verksemd den autoriserte er knytt til

Revisjonen har ikkje fått informasjon om at det er etablert eit slikt register.

Generelt meiner IKT-leiaren at tilgangstyring til IKT-systema er godt ivaretatt gjennom dei programvareløysingane som vert nytta i kommunen.[33] Tilgang til fagsystem er det systemeigarane som handterer, og også dette opplever IKT-leiaren at fungerer greitt; han har ikkje opplevd avvik der nokon har fått tilgang dei ikkje skal ha. Teknisk er det IKTNH som syter for tilgangsstyringa til kommunen sitt nettverk og dei ulike sonene.

IKTNH har eigne rutinar for brukarhandsaming.[34] Systemet for tilgangsstyring som IKNTH nyttar er designa slik at brukardatabasen er etablert og vedlikehalden på grunnlag av kommunane sine eigne fagsystem. Det er kommunen sitt ansvar å gje tilgangar til fagapplikasjonane som ligg på serverane. IKTNH gir brukaren rettigheitar for å komme inn på klienten. Tilsette i kommunen kjem ikkje inn i fagsystema utan at kommunen har gjeve den tilsette brukarnamn og passord. Fagapplikasjonane levert gjennom IKTNH sin infrastruktur er berre tilgjengeleg på klientar satt opp av IKTNH. I systemet kan ein spesifisere kva data ein brukar skal ha tilgang til, og kor tid ein brukar skal ha tilgang til kva type data. Vidare er det mogleg å leggje inn sluttdato, slik at kontoen til ein som skal slutte vert avslutta automatisk.[35]

Systemansvarleg for Visma Profil opplyser at kommunen nyleg har utarbeidd eit elektronisk skjema for tilgangstyring, noko som har betra dette arbeidet. Skjemaet må fyllast ut av næraste leiar. I Visma Profil har systemansvarleg utarbeidd profilar for dei ulike yrkesgruppene, slik at kvar brukar får tilgangen til delen av journalen som er nødvendig og relevant for si yrkesgruppe.[36] Ho fortel at det likevel skjer at det kjem førespurnader om å gje nokon tilgang til fagsystemet utan klare formål. Systemansvarleg følgjer då opp førespurnaden for å sikre at behovet for tilgangen er reelt, før det vert gitt tilgang. I SiLk går det, som nemnt over, fram at tilgang til helse- og personopplysningar berre kan gis til autorisert personell.[37]

Generelt opplever systemansvarleg for Visma Profil at dei har gode rutinar på tilgangsstyring for nytilsette. Det er vanskelegare med tilgangstyring når tilsette sluttar eller endrar jobb internt i kommunen. Ho fortel at dette er noko ho bruker mykje tid på, og som ho ser på som ein stor svakheit med tilgangsstyringa slik den er i dag.[38]

3.5.2 Vurdering

Lindås kommune har gjennom SiLk dokumenterte rutinar og retningsliner for kontroll og etterprøving av informasjonstryggleik. Revisjonen avdekker i sine undersøkingar at slik kontroll og etterprøving av

[33] Han viser her særleg til AD og VPN.
[34] Rutinen skal sikre korrekt inn- og utmelding av brukartilgang til nettverksressursar og fysiske lokasjonar, og inneheld ein tabell som viser ansvarstilhøve mellom kommunane og IKTNH.
[35] IKTNH har også ansvaret for tilgangsstyring til infrastrukturen i IKT-systema. I utgangspunktet har ingen utanfor IKTNH tilgang til dette. Tilgangar til leverandørar vert delt ut ved særskilte behov, og alltid assistert av IKTNH.
[36] T.d. har sjukepleiarar meir tilgang enn ufaglærte, og kommunepsykolog vil berre ha tilgang til sin pasientkategori.
[37] Med omsyn til journaltilgang, peiker systemansvarleg for Visma Profil på at det er vanskeleg å skjerme eksakt tilgang til dei journalane som tilsette faktisk treng tilgang til. Mange av einingane er store, og tilsette har tilgang til alle pasientane i det gitte geografiske området. Dette medfører at tilsette har tilgang til fleire journalar enn nødvendig.
[38] Ein gong i året forsøker systemansvarleg å sende ut rapportar til einingane med oversikt over tilsette med tilgang til fagsystemet, slik at dei kan sjå over om det er korrekt. Ei løysing som har vore diskutert er at lønnsavdelinga i kommunen sender melding til systemansvarleg når nokon sluttar, men det har ikkje vorte bestemt.

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.

Lindås kommunen gjennomfører berre unntaksvis risikovurderingar knytt til informasjonstryggleik, og har slik manglande oversikt over kva risikoar kommunen står ovanfor i samband med handsaming av personopplysningar. Manglande risikovurderingar gjer òg at kommunen ikkje har eit godt grunnlag for å gjere eventuelle justeringar i informasjonstryggleikssystemet basert på endringar i trusselbiletet. Kommunen bryt slik med POF § 2-4 andre ledd.[39]

Lindås kommune set heller ikkje akseptkriterium for risiko knytt til informasjonstryggleik, og har slik ikkje grunnlag for å vurdere om risikoane for uønskte hendingar i handsaminga av personopplysningar er akseptable eller ikkje. Av same årsak har kommunen heller ikkje noko grunnlag for å vurdere kor tid risikoreduserande tiltak må setjast i verk. Revisjonen meiner difor at kommunen bryt med POF § 2-4 første ledd.

Vidare gjennomfører ikkje Lindås kommune tryggleiksrevisjonar. Kommunen har difor ikkje oversikt over kva tryggleikstiltak som fungerer og kva tryggleikstiltak som ikkje fungerer. Kommunen manglar følgjeleg grunnlag for å gjere eventuelle justeringar og slik kontinuerlig forbetre informasjonstryggleiken. Revisjonen meiner difor kommunen bryt med POF § 2-5.

Kommunen har etablert eit avvikssystem, og det vert meldt avvik knytt til informasjonstryggleik i systemet. Talet på avvik knytt til informasjonstryggleik er lågt, og informantane er opne om at kommunen har ein veg å gå når det gjeld melding av avvik. Manglande avviksmeldingar aukar risikoen for at svakheiter i systemet ikkje vert retta.[40] Revisjonen meiner difor at Lindås kommune sin praksis på dette området ikkje er i samsvar med POF § 2-6 andre ledd og kapittel 10 i ISO27001:2013.

Undersøkinga avdekker vidare at kommunen si leiing berre i avgrensa grad følgjer opp informasjonstryggleiksarbeidet. Leiinga har difor ikkje grunnlag for å vurdere om avgjersler som vert tatt er i samsvar med behova for informasjonsteknologi og informasjonstryggleik. Leiinga har følgjeleg 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 kapittel 9.3.

Med omsyn til tilgangskontroll, finn revisjonen i sine undersøkingar at Lindås kommune og IKTNH har system for dette. Det kjem likevel fram at det er svakheiter i systema, som t.d. at det ikkje alltid vert meldt i frå når tilsette slutter i kommunen eller bytter jobb internt i kommunen, og at det kjem førespurnader om tilgang til fagsystem som ikkje er tilstrekkeleg grunngjeve. Sett i samanheng med uklarheitene i ansvarsdelinga mellom kommunen og IKTNH, meiner revisjonen at det både er risiko for at tilsette ikkje får tilgang til den informasjonen dei treng når dei treng den, og at det er risiko for at tilsette har eller kan få tilgang til informasjon dei ikkje skal ha tilgang til. Det er difor revisjonen si vurdering at Lindås kommune bryt med personopplysningslova § 13 første ledd, og POF §§ 2-12 og 2-8 første ledd.

[39] Revisjonen er merksam på at det nyleg har vorte gjort ROS-analysar av fagsystema som inngår i omsorgsteknologitenesta i kommunen. Revisjonen har ikkje gjort vurderingar av desse analysane, men har justert vurderinga noko.

[40] Denne delen av vurderinga er justert i samband med høyringsprosessen.

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) Er brukarstøtta til IKT-teneste organisert på ein hensiktsmessig og føremåltenleg 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

Den gjennomførande delen av SiLk inneheld rutinar for tilgjenge ved etablering og drift av informasjonssystemet. Der går det mellom anna fram at «kommunen må derfor sørge for at naudsynte helse- og personopplysningar er tilgjengelege også ved stopp i heile eller delar av det elektroniske informasjonssystemet.» Vidare vert det stilt krav til at kommunen skal kartleggje dei enkelte informasjonssystema med omsyn til kritikalitet for både kommunen og for brukarane. System med helse- og personopplysningar skal klassifiserast i fem ulike kategoriar (sjå tabell 5).[41]

Tabell 5: Klassifisering av system med helse og personopplysningar i SiLk

Klassifisering	Dømer
System der stopp av tenesta kan vere kritisk	Livstruande for pasient. Kritisk for kommunen si drift.
System der stopp av tenesta får alvorlege konsekvensar	Feilbehandling av pasient. Betydeleg meirarbeid for personell. Tapt effektivitet. Tapte inntekter for kommunen.
System der stopp av tenesta kan føre til svekking av pasienten sin tillit	
System der lengre stopp kan aksepterast	
System som ikkje er prioritert	

[41] System dei klassifiserte systema er avhengig av skal også kartleggjast, og få same klassifisering og nivå for akseptabel risiko som dei kritiske systema.

Det går fram i SiLk at for kvar klassifisering skal leiinga fastsette nivå for akseptabel risiko for tilgjenge, og som eit minimum ei maksimal avbrottstid. Kommunen skal etablere og minimum årleg teste naudprosedyrar for alternativ drift utan bruk av informasjonssystema og alternativ drift med delvis støtte frå informasjonssystema.

Frå intervju kjem det fram at rutinane for klassifisering av informasjonssystema ikkje vert systematisk gjennomført, og at det ikkje er sett nivå for akseptabel risiko for tilgjenge for systema. Det vert heller ikkje gjort årlege testing av naudprosedyrar.

I intervju vert det understreka at kommunen veit kva system som er mest kritiske, og prioriterer desse i situasjonar der system går ned. IKT-leiaren peikar t.d. på at systema innanfor helse og omsorg er kritiske; kommunen er heilt avhengig av å ha systemtilgjengelegheit på desse heile døgnet. Særleg viser han til at systemtilgjengelegheit på Visma Profil openbart er kritisk for kommunen. IKT-leiaren karakteriserer også telefonisentralen som eit kritisk system.

Utviklingsrådgjevar opplever at kommunen har god beredskap på det mest kritiske, med beredskapsplaner i helse- og omsorgssektoren, og med naudaggregat dersom straumen forsvinn.[42]

Kriterium for systemtilgjengelegheit i IKTNH

Tenesteleveringsavtale om drift/vedlikehald av IKT-løysinga garanterer ei tilgjengelege på >97 % frå leverandør av linesignal. I intervju opplyser IKTNH at akseptkriteriet for oppetid i netteverket er sett til 99,5 %.

IKTNH har ei oversikt over sine fagsystem og tenester fordelt på tre tenestenivåavtale-klasser.[43] Revisjonen har samanfatta oversikta i tabell 6:[44]

Tabell 6: IKTNH sine fagsystem og tenester fordelt på prioriteringsnivå og mål for gjennoppretting

Tenestenivåavtale-klasse (SLA)	Tal på fagsystem/tenester	Mål for gjenopprettingstid (RTO)[45]	Mål for gjenoppretting (RPO)[46]
Prioritet 1	13	48 timar	24 timar
Prioritet 2	40	7 dagar	24 timar
Prioritet 3	18	14 dagar	48 timar

I dette systemet er Visma Profil definert på tenestenivåavtale-klasse med prioritet 1, med eit tidsmål for gjenoppretting på 48 timer,[47] og eit kvalitetsmål for gjenoppretting på 24 timar.[48] IKTNH opplyser at dei har høgare beredskapsnivå for system der tilgjengelegheit er ein kritisk faktor.

4.3.2 Vurdering

IKTNH har fastsett kriterium for tilgjenge i systema dei driftar, og det er slik sett kriterium for tilgjenge i delar av IKT-systema som vert nytta i Lindås kommune. Lindås kommune sjølv har likevel ikkje fastsett kriterium for tilgjenge i IKT-systema sine, og kommunen bryt slik med eigne retningsliner, og med POF § 2-4 første ledd andre setning.

Basert på undersøkinga, meiner revisjonen at Lindås kommune berre delvis har fastsett tydelege kriterium for tilgjenge til IKT-systema.

---

[42] Han fortel òg at skulane opererer med lokale kopiar av elevmappene, slik at dei har tilgang på desse dersom nettverket bryt saman eller dei av andre årsakar ikkje får kopla seg på nettverket.
[43] Difi definerer ein tenestenivåavtale eller Service Level Agreement (SLA) slik: «Tenestenivåavtalen beskriv og regulerer ytingsnivået på den jamlege tenesta».
[44] Tabell over kritiske fagsystem og tenester er presentert i vedlegg 3.
[45] Mål for gjenopprettingstid (Recovery Time Objective) er «Den maksimale tiden som tillattes brukt etter et avbrudd for å gjenopprette en IT-tjeneste» (ITIL-ordliste og forkortelser på norsk).
[46] Mål for gjenoppretting (Recovery Point Objective) er den maksimale tidsperioden data kan vere tapt frå når tenesta vert gjeninnført (ITIL-ordliste og forkortelser på norsk).
[47] RTO.
[48] RPO.

4.4 Kontrollar av tilgjengelegheit og stabilitet i IKT-systema

4.4.1 Datagrunnlag

IKTNH leverer nettverkstenester til Lindås kommune. I tenesteleveringsavtalen mellom Lindås kommune og IKTNH går det fram at IKTNH skal arbeide for å oppnå høgast mogleg oppetid på tenester som vert leverte til kunden. Som ein del av dette arbeidet, skal IKNTH også loggføre all nedetid. Jf. avtalen, skal det verte utarbeidd ein månadleg rapport som syner tal og lengde på nedetidepisodane. Rapporten skal sendast til medlemskommunane.

I intervju med IKTNH, kjem det fram at dei ikkje rapporterer på nedetid til kommunane slik det står i tenesteleveringsavtalen. Det vert likevel peika på at kommunane har hatt eit snitt på over 99,9% oppetid sidan IKTNH vart skipa, og at det ikkje har vore ein månad som totalt sett har hatt ei oppetid på under 99,9 %.

4.4.2 Vurdering

IKTNH overvakar oppetida på nettverket, og det er slik etablert kontrollar for å sikre tilgjengelegheit og stabilitet i IKT-systema.

Likevel merkar revisjonen seg at IKTNH ikkje rapporterer til Lindås kommune om nedetid. Dette er ikkje i samsvar med tenesteleveringsavtalen mellom kommunen og IKTNH, og gjer det vanskeleg for Lindås kommune å kontrollere tilgjengelegheita og stabiliteten i IKT-systema dei nyttar på ein systematisk måte, og følgjeleg også vanskeleg å setje i verk ev. tiltak for å betre tilgjengelegheit og stabilitet i IKT-systema.

4.5 Organisering av IKT-brukarstøtte

4.5.1 Datagrunnlag

Det er IKTNH som er ansvarleg for den generelle IKT-brukarstøtte i Lindås kommune. Brukarstøtta til IKTNH er organisert slik at brukarane primært skal ta kontakt via ei nettside.[49] IKTNH opplyser å få førespurnader til brukarstøtta både frå nettsida, på e-post og over telefon. Dei som ringjer brukarstøtta får først høyre driftsmeldingar, før dei vert sett over til brukarstøtta. Det er fire tilsette og tre lærlingar i IKTNH som bemannar brukarstøtta.

Jf. tenesteleveringsavtalen mellom Lindås kommune og IKTNH er IKT-brukarstøtte ei bemanna teneste med servicetid frå måndag til fredag mellom kl. 07:30 og kl. 16:00. I IKTNH sin beredskapsrutine er brukarstøttefunksjonen nærare skildra. Der går det mellom anna fram at brukartelefon er open alle kvardagar mellom kl. 08:00 og kl. 15:30. Også i intervju med IKTNH vert det sagt at brukarstøtta har ordinær opningstid mellom kl. 08.00 og kl. 15.30. Utanfor normalt opningstid skal brukarane kontakte sin kommunale IKT-bestillar, som skal ta førespurnaden vidare til IKTNH. Pleie- og omsorgstenesta og legekontora kan kontakte IKTNH direkte. Dette er ikkje ei formell vaktordning, men basert på at tilsette deler på å vere tilgjengeleg på telefon også utanom arbeidstida.

I intervju opplyser prosjektleiar i IKTNH at ved kritiske eller andre alvorlege hendingar så er praksis i dag at den som oppdagar brotet tek kontakt med sin overordna, som så tek kontakt med rådmannen, som igjen tek kontakt med IKTNH sin leiar, som sender beskjed vidare til den i IKTNH som kan løyse problemet.

IKT-leiar i Lindås kommune opplever at ansvarsfordelinga mellom kommunen og IKTNH med omsyn til brukarstøtte er tydeleg og klar, at det fungerer bra og etter intensjonen, og at IKTNH har organisert brukarstøtta på ein føremålstenleg måte når det gjeld tilgjengelegheit. Det vert likevel peika på i intervju at manglande formalisert 24-timars vakt i brukarstøtta hjå IKTNH er eit risikomoment. Samtidig opplever dei intervjua i kommunen at IKTNH er fleksible, stiller opp når det er behov, og generelt gjer ein god jobb på brukarstøtte.

Systemansvarleg for Visma Profil opplyser at kommunen sjølv driv brukarstøtte for Visma Profil via e-post og telefon. Dei er tre tilsette i kommunen inkludert systemansvarleg sjølv som betener brukarstøtta for Visma Profil. Dei har fordelt ansvaret og oppgåvene knytt til dette mellom seg. Primært tek dei imot førespurnader på e-post. E-posten er betent mellom kl. 08.00 og 15.30 på kvardagar. I tillegg har systemansvarleg ein vakttelefon der ho vert varsla dersom Visma Profil ikkje er tilgjengeleg eller noko anna

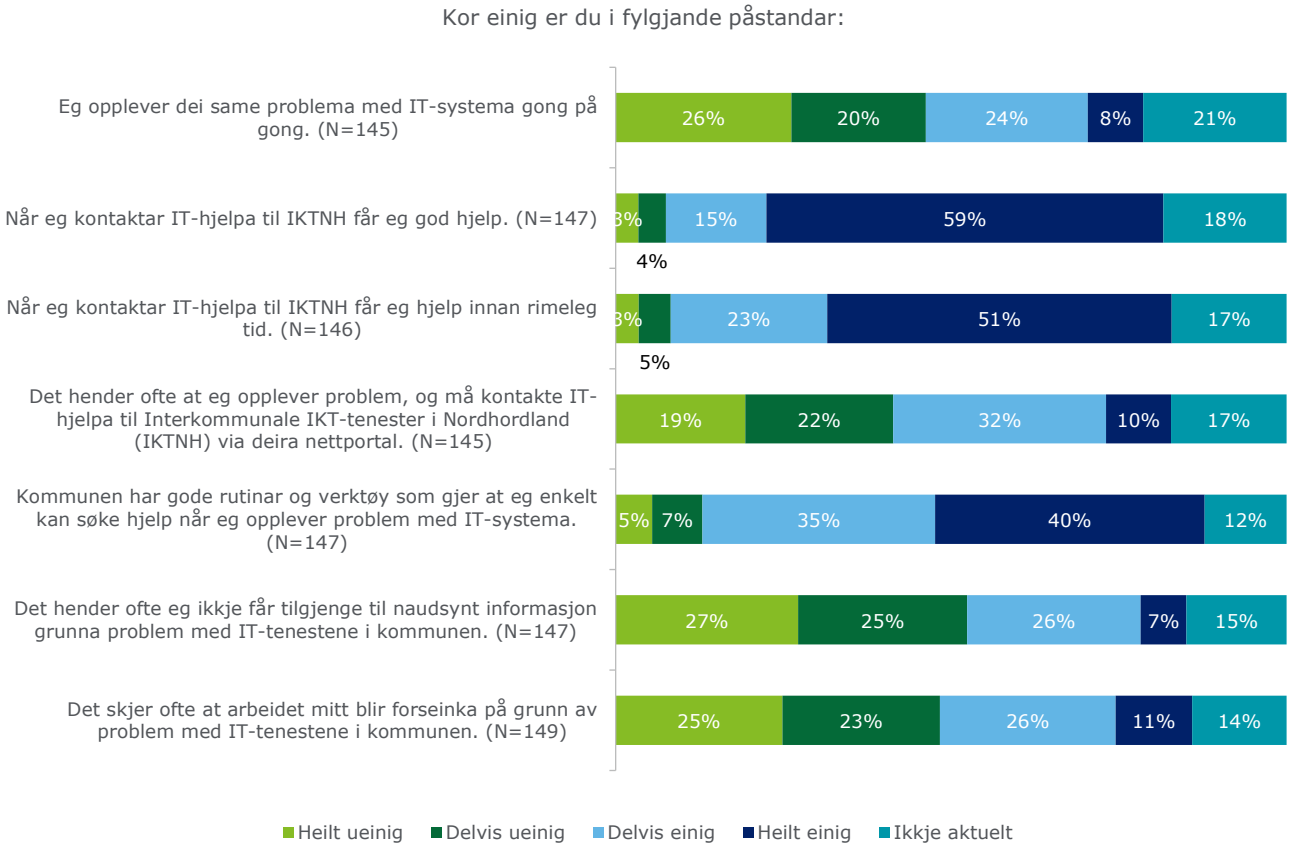
[49] Det er likevel opning for å ta kontakt med brukarstøtta også på telefon, dersom situasjonen tilseier det.

alvorleg har skjedd med systemet. Kommunen har ikkje nokon anna vakt på Visma Profil utanfor normal arbeidstid. Systemansvarleg opplyser å vere tilgjengeleg på telefonen alle dagar inkludert helgar og i feriar, fram til ca. kl. 22.00. Systemansvarleg fortel vidare at ordninga ikkje er formelt nedfelt noko stad, men at det i om lag 20 år har vore slik at systemansvarleg «alltid» er tilgjengeleg.[50] Systemansvarleg opplever at den uformelle brukarstøtta gjer systemet sårbart.

Når IKTNH vart etablert, var planen at dei skulle ta hand brukarstøtta også for Visma Profil. Dette har ikkje skjedd. Systemansvarleg støttar seg likevel på IKTNH i arbeidet med Visma Profil, t.d. når det vert meldt inn tekniske problem.[51]

Respondentane i spørjeundersøking fekk presentert ei rekkje påstandar knytt til IKT-tilgjenge og brukarstøtte. Svara er presentert i figur 2.

Figur 2: Brukarstøtta for IKT



Svara indikerer at om lag ein tredjedel av respondentane opplever dei same problema med IT-systema gong på gong. Langt dei fleste av respondentane er nøgde både med hjelpa dei får av IKTNH, og tida det tek før dei får hjelp.[52] Tre fjerdedelar av dei spurde svara at dei var «heilt» eller «delvis einig» i at kommunen har gode rutinar og verktøy som gjer at dei enkelt kan søke hjelp når dei opplever problem med IT-systema.

[50] Systemansvarleg estimerer at ho vert kontakta på telefonen ca. 10 gonger i året, og at det var fleire oppringingar på brukarstøtta før enn det er no.
[51] Dersom IKTNH må ha bistand frå Visma, tek dei direkte kontakt med Visma, men då i tett samarbeid med systemansvarleg. Systemansvarleg fortel at ho nyttar Visma sin support-funksjon flittig når det er utfordringar med innhaldet i programmet.
[52] Nesten tre fjerdedelar av dei spurde er «heilt» eller «delvis einig» i at dei får god hjelp når dei kontaktar IT-hjelpa til IKTNH. Likeeins svara om lag tre fjerdedelar at det er «heilt» eller «delvis einig» i at dei får hjelp frå IT-hjelpa til IKTNH innan rimeleg tid.

Svara indikerer elles at om lag ein tredel av respondentane ofte ikkje får tilgjenge til naudsynt informasjon grunna problem med IT-tenestene i kommunen. På oppfølgingsspørsmål om kor ofte dette skjer, svara 60 % sjeldnare enn månadleg, 28 % månadleg, 8 % vekentleg og 4 % dagleg.[53] Litt fleire opplever å verte forseinka i arbeidet sitt på grunn av problem med IT-tenestene i kommunen. På oppfølgingsspørsmål om kor ofte dette skjer, svara 44 % sjeldnare enn månadleg, 30 % månadleg, 17 % vekentleg og 9 % dagleg.[54]

Respondentane fekk også moglegheit til å kome med ytterlegare kommentarar knytt til IT-tenesta og tilgjenge til naudsynt informasjon. Av dei 43 respondentane som nytta sjansen, var om lag halvparten negative eller delvis negative til IT-tenesta og tilgjenge til naudsynt informasjon. Mellom anna vart det peika på at PC-ane låsar seg ofte og at fagsystema henger seg opp og at det er svakheiter knytt til innloggingsrutinar. Fleire meiner òg at programma dei nyttar er lite føremålstenlege, og opplyser at det er utfordringar med nettstabilitet, problem med Websak, og problem med skrivarar. I tillegg vert det kommentert at innkjøpa av system og utstyr ofte ikkje er forankra hjå brukarane. Vidare vert det meldt at det er uklart kven som har brukarstøtteansvaret for ulike fagsystem. Det vart òg etterlyst meir opplæring.

4.5.2 Vurdering

Revisjonen finn i sine undersøkingar at brukarstøtta for IKT i Lindås kommune jamt over vert opplevd som god, både av dei som vart intervjua og dei som svara på spørjeundersøkinga.

Revisjonen merkar seg òg at det er opplyst ulik opningstid for brukarstøtta i tenesteleveringsavtalen mellom Lindås kommune og IKTNH og kva som faktisk er tilfelle.

Undersøkinga viser at det ikkje er formalisert korleis eventuell brukarstøtte skal organiserast utanom arbeidstid. Dette gjeld både for den generelle brukarstøtta, og for brukarstøtta for dei ulike fagsystema. Sjølv om dette i hovudsak vert opplevd å fungere tilfredsstillande i dag, meiner revisjonen at ordninga er sårbar, spesielt for dei kritiske fagsystema.

[53] Berre respondentane som svara «delvis ueinig», «delvis einig», eller «heilt einig» i påstanden i førre spørsmål, fekk oppfølgingsspørsmålet. 83 svara.
[54] Berre respondentane som svara «delvis ueinig», «delvis einig», eller «heilt einig» i påstanden i førre spørsmål, fekk oppfølgingsspørsmålet. 89 svara.

5. Kompetanse om informasjonstryggleik

5.1 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?

5.2 Revisjonskriterium

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

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

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

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

Sjå vedlegg 2 for fullstendige revisjonskriterium.

5.3 Rutinar for opplæring i informasjonstryggleik

5.3.1 Datagrunnlag

I Lindås kommune si tryggleikstrategi går det fram at det aktivt skal leggjast til rette for og gjennomførast opplæringstiltak som fremjar det praktiske tryggleiksarbeidet. Også den gjennomførande delen av SiLk stiller krav til at det skal setjast i verk tiltak som syter for opplæring som gir dei tilsette tilstrekkeleg kunnskap til å ivareta informasjonstryggleiken. Det går vidare fram at denne kompetansebygginga må skje kontinuerleg og være tilpassa dei ulike rollane og brukargruppene, og at særskilte opplæringstiltak må vurderast for nytilsette og ved endringar i informasjonssystema eller i behandlinga av helse- og personopplysningar.

Kommunen opplyser at nytilsette vert informert om kor ein finn informasjon om informasjonstryggleik i *Sjekkliste for introduksjon* i Personalhandboka. Revisjonen har fått tilsendt sjekklista, og det går der fram at nytilsette i løpet av første veka skal få informasjon om mellom anna informasjonstryggleik, og at dei i løpet av første månaden skal få informasjon om KF-kvalitet, avviks- og skademeldingar, samt andre rutinepermar. Det er næraste leiar som har introduksjonsansvaret.

Utviklingsrådgjevaren fortel at han tilbyr opplæring i informasjonstryggleiksarbeid til tilsette i kommunen. Særleg har han hatt fokus på auke bevisstheita om teieplikta blant dei tilsette, samt å drive nytilsetteopplæring.[55] I intervju går det òg fram at systemansvarleg for Visma Profil tek opp haldningar og handsaming av informasjonstryggleik når leiargruppa i helse og omsorg har møte.[56] Det er avdelingsleiarane sitt ansvar å sikre at nytilsette får opplæring i informasjonstryggleik.

På kommunen sitt intranett har IKTNH gjort tilgjengeleg åtte e-læringsmodular basert på *Norm for informasjonstryggleik*.[57] Kommunen har ikkje sett krav til at tilsette skal gjennomføre desse. IKTNH presiserer i intervju at det er kommunen sitt eige ansvar å tilby og gjennomføre opplæring for sine tilsette i informasjonstryggleik, men at IKTNH ønskjer å bidra til opplæringstilbodet. Forutan dei nemnde e-læringsmodulane, har IKTNH planlagd å tilby e-læring i samband med oppdatering av operativsystemet på PC-ane som vert nytta i medlemskommunane.

IKT-leiar opplyser at det ikkje er etablert sentrale rutinar for å gje tilsette i kommunen opplæring i informasjonstryggleik.

Respondentane som svara at dei er programansvarleg fekk eit oppfølgingsspørsmål om dei har delteke i opplæringa av andre brukarar. Av dei 16 som svara, gjekk det fram at 63 % hadde delteke i opplæringa av andre brukarar og at 38 % ikkje hadde det.

Dei som svara «ja» vart bedne om å kort skildre opplæringa dei har gjeve i eit fritekstfelt. Av dei åtte som svara, går det fram at dei programansvarlege hadde gitt intern opplæring éin-til-éin eller saman med brukarstøtte og produsent. Vidare gjekk det fram at dei programansvarlege hadde gitt opplæring i bruk av systema dei er ansvarlege for. Det vart også nemnt at programansvarlege har gjeve opplæring i å handsame personopplysningar, fortrulege opplysningar og sensitive opplysningar.

5.3.2 Vurdering

Revisjonen meiner at Lindås 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 innanfor informasjonstryggleik, noko som aukar risikoen for brot både regelverket som gjeld for handsaming av personopplysningar, og for informasjonstryggleika generelt.

Det er difor revisjonen si vurdering at Lindås kommune ikkje følgjer krava i POF § 2-8 andre ledd, eller IS27001:2013 kapittel 7.2.

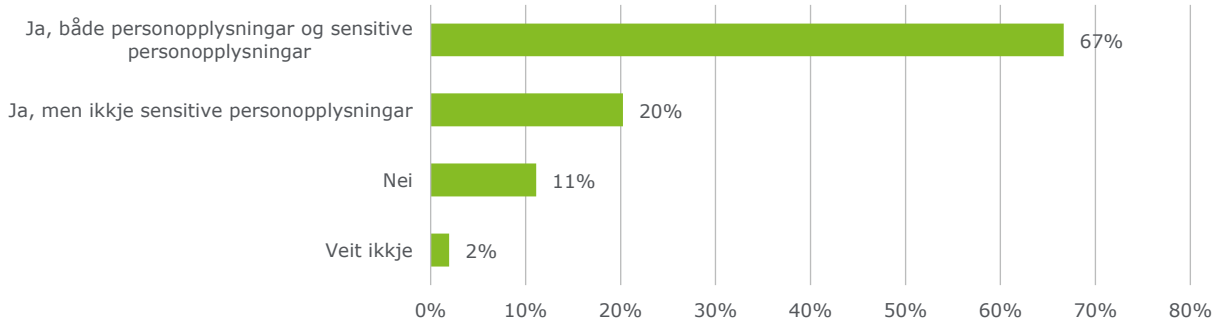
[55] Han opplyser elles at dei programansvarlege hadde kvartalsvise samlingar i 2009 og 2010 der informasjonstryggleik var ein del av agendaen.
[56] Systemansvarleg opplyser at etter ho fekk fleire arbeidsoppgåver ikkje har hatt så mykje tid til å vere så tett på avdelingane som før, slik at ho i dag har mindre oversikt over korleis det står til med omsyn til informasjonstryggleiken i praksis enn tidlegare.
[57] Følgjande modular er nemnd: Avvikshandsaming, Fysisk sikring av område og utstyr, Hendingsregistrering og oppfylging, Innsyn i hendingsregistre, Personvern og informasjonstryggleik, Retningsliner for dagleg informasjonstryggleik, Risikovurdering, og Skadebegrensing ved avvik.

5.4 Kjennskap til retningsliner og rutinar for informasjonstryggleik

5.4.1 Datagrunnlag

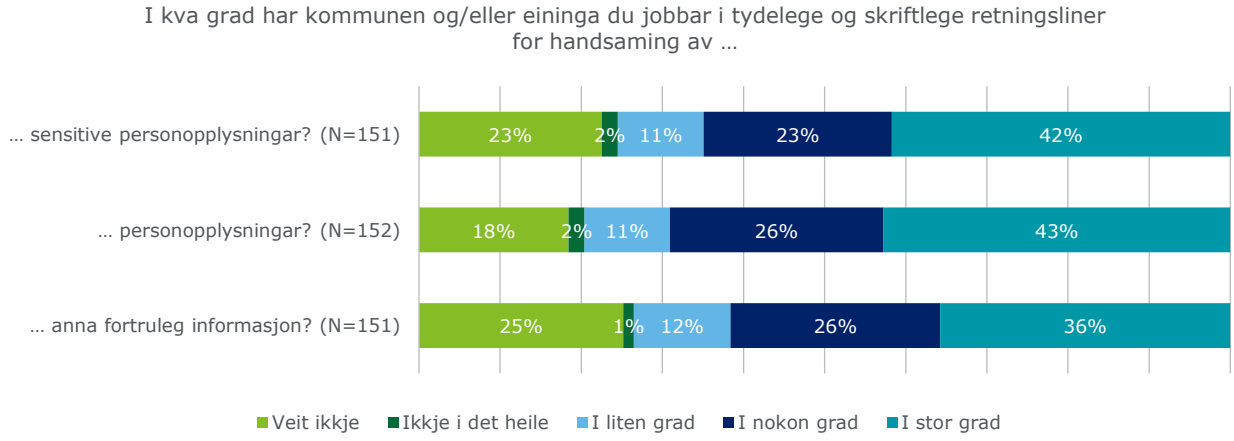
Om lag to tredjedelar av respondentane i spørjeundersøkinga handsamar eller kjem i kontakt med både personopplysningar og sensitive personopplysningar i sitt arbeid (sjå figur 3). Enda fleire svara at dei kjem i kontakt med «anna fortruleg informasjon» i sitt arbeid (79 %).[58]

Figur 3: Handsamar du eller kjem du i kontakt med personopplysningar i ditt arbeid? (N=153)



Respondentane vart spurde om *i kva grad kommunen og/eller eininga vedkommande jobbar i har tydelege og skriftlege retningsliner for handsaming av ulike typar opplysningar*. Som det går fram av figur 4, svara mellom 18 % og 23 % «veit ikkje», og mellom 11 % og 12 % «i liten grad» på spørsmåla.

Figur 4: Tydelege retningsliner for personopplysningar mv.



Respondentane vart vidare spurde om *dei veit kor dei finn rutinar og retningsliner for handsaming av personopplysningar, sensitive personopplysningar og/eller anna fortruleg informasjon som gjeld kommunen og/eller deira eining*. 56 % svara «ja» og 44 % «nei».[59]

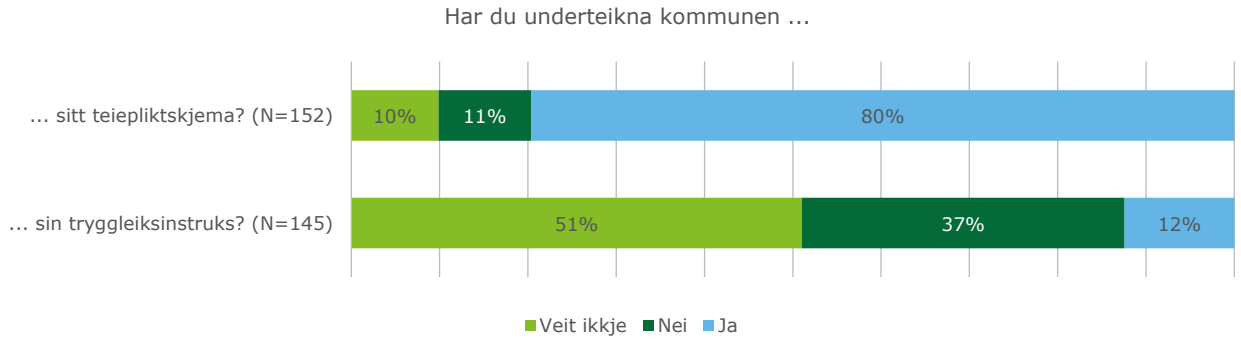
Dei som svara «ja», fekk eit oppfølgingsspørsmål der dei vart bedne om å skrive *kor kommunen og/eller eininga har gjort informasjon og rutinar om handsaming av personopplysningar, sensitive personopplysningar og/eller anna fortruleg informasjon tilgjengeleg*. Av dei 69 respondentar som svara på spørsmålet, viste over halvparten til enten kommunen sitt kvalitetssystem, intranettet eller nettsida. Vidare vart det vist til permar, papir, arkivskap eller liknande, samt ulike handbøker.[60] Nokre viste òg til ulike fag- og arkivsystem.[61]

[58] På spørsmålet svara 12 % «nei» og 8 % «veit ikkje».
[59] N=152.
[60] T.d. HMT-handboka og personalhandboka.
[61] Det vart elles vist til møter, kurs, samtalar, samt at det går fram av offentleglova.

Det går fram av intervju at IKT-leiar generelt opplever at konfidensialitet internt i kommunen er godt ivaretatt med mellom anna teiepliktserklæringar og sikker sone.[62] Utviklingsrådgjevar opplyser i intervju at kommunen har rutinar for teieplikt.

Som det går fram av figur 5, svara 80 % av respondentane at dei har underteikna kommunen si teiepliktskjema. 12 % har underteikna kommunen si tryggleiksinstruks, medan 51 % ikkje veit om dei har underteikna denne.

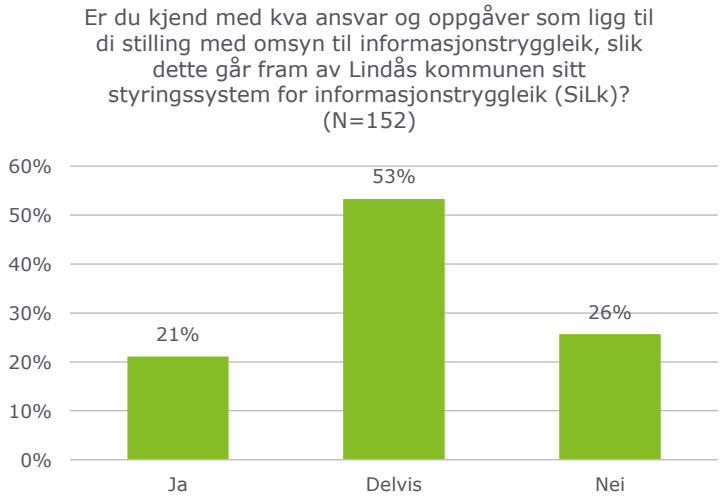
Figur 5: Teieplikt og tryggleiksinstruks



Dei som svara at dei har underteikna teiepliktskjemaet vart spurde om dei hugsar innhaldet i skjemaet; om lag ein tredjedel svara at dei ikkje hugsar innhaldet.[63] Tilsvarande fekk dei som svara at dei har underteikna tryggleiksinstruksen oppfølgingsspørsmålet om dei hugsar innhaldet i dette skjemaet; to tredjedelar svara her at dei ikkje hugsar innhaldet.[64]

På spørsmålet om *dei er kjend med kva ansvar og oppgåver som ligg til deira stilling med omsyn til informasjonstryggleik slik det går fram av styringssystemet for informasjonstryggleik*, svara om lag ein firedel «nei» (sjå figur 6).

Figur 6: Kjennskap til ansvar og oppgåver i SiLk



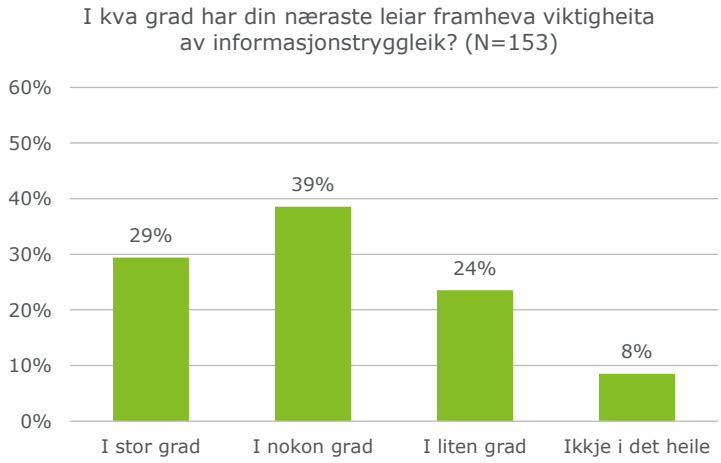
Dei respondentane som svara «ja» eller «delvis», vart spurde om *kva ansvar og oppgåver dei har med omsyn til informasjonstryggleik*. Av svara som kom inn,[65] viste om lag ein tredjedel til teieplikta, og om lag ein tredjedel svara at dei har ansvar for å sikre at personopplysningar og sensitive personopplysningar ikkje kommer på avvege. Elles svara respondentane t.d. ved å vise til skjerming av informasjon, fysisk

[62] IKT-leiar opplyser at dette særleg gjeld helse- og omsorgssektoren, medan skulesektoren ikkje har sikker sone.
[63] N=120.
[64] N=18.
[65] N=54.

sikring av dokument, og viktigheita av å melde avvik. Fleire av svara var direkte knytt til den enkelte respondents sine arbeidsoppgåver. Nokre svara at dei er usikre på kva ansvar dei har med omsyn til informasjonstryggleik, og nokre svara at dei ikkje kjenner til SiLk.

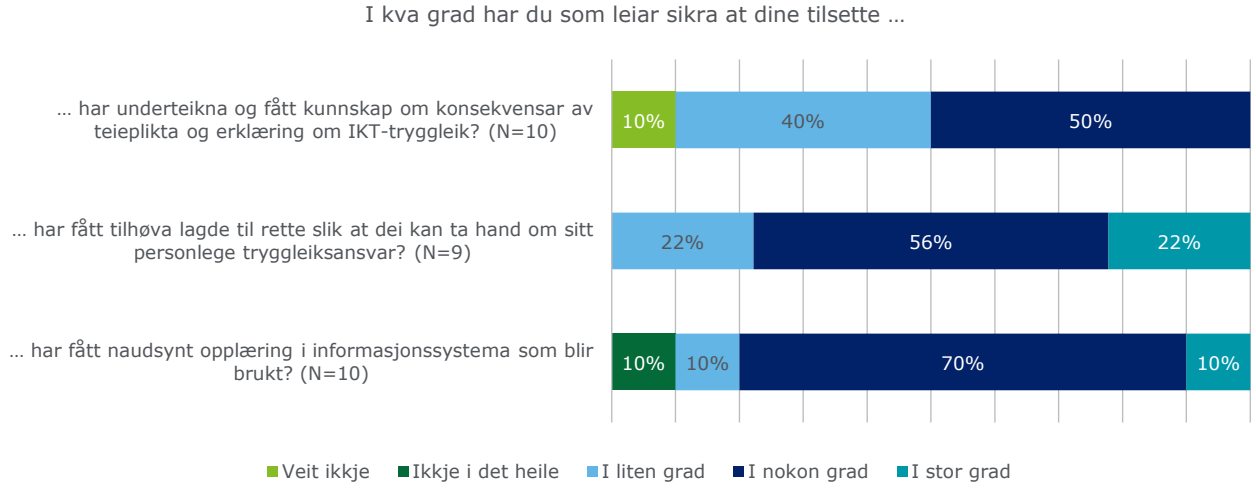
Svara på spørsmålet *i kva grad har din næraste leiar framheva viktigheita av informasjonstryggleik* er presentert i figur 7. Som det går fram der, svara nesten ein firedel «i liten grad» og 8 % «ikkje i det heile».

Figur 7: Viktigheita av informasjonstryggleik



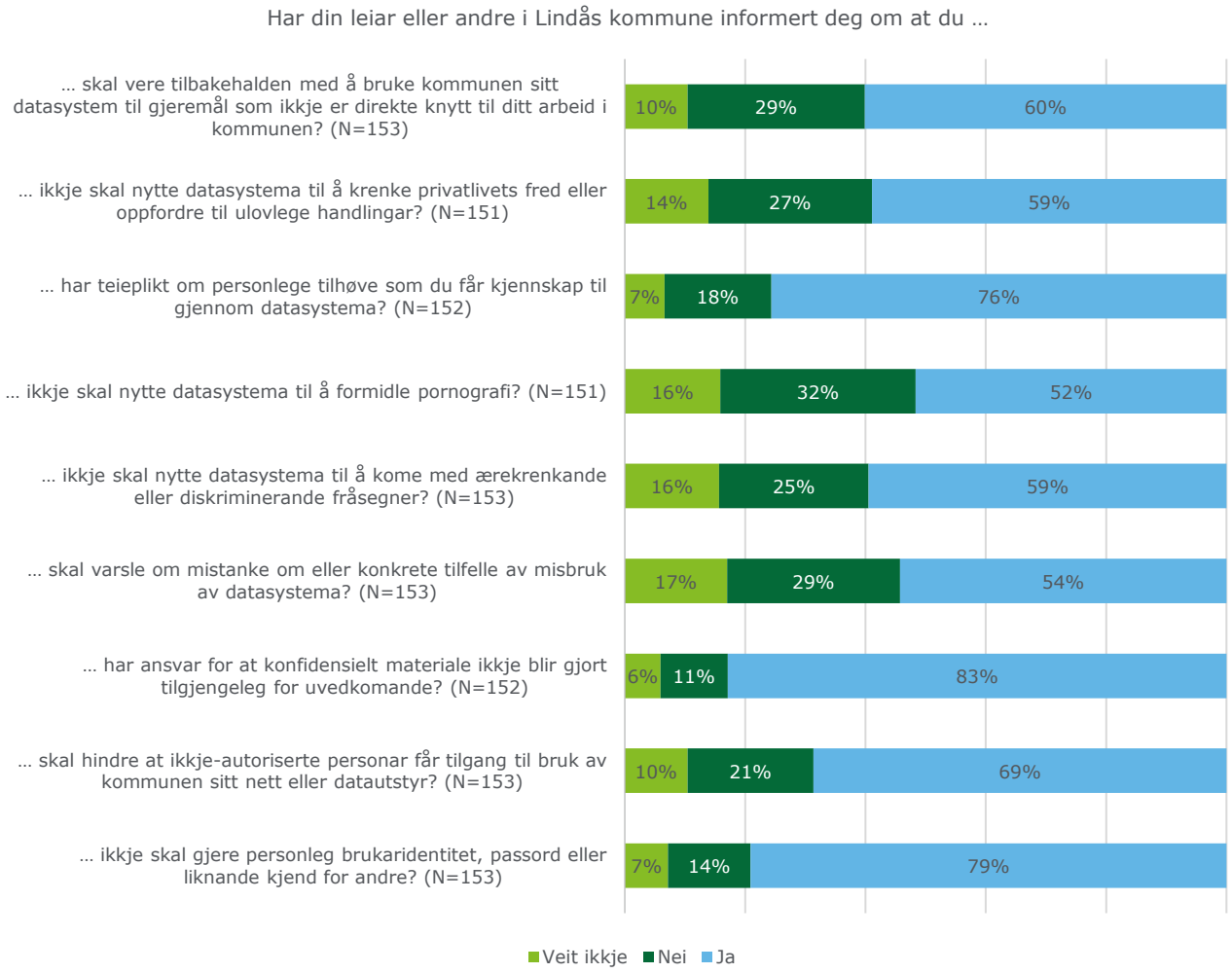
Einingsleiarane og dei avdelingsleiarane som opplyste at dei har fått delegert ansvar for informasjonstryggleik, vart stilt tre spørsmål knytt til kva dei som leiarar har gjort med omsyn til informasjonstryggleik. Som det går fram av figur 8, svara leiarane berre unntaksvis «i stor grad» på spørsmåla; dei fleste svara «i nokon grad» eller «i liten grad».

Figur 8: Opplæring av tilsette



Figur 9 visar respondentane sine svar på ni spørsmål om *kva deira leiar eller andre i kommunen har informert om knytt til informasjonstryggleik og bruk av kommunen sitt IKT-system*.

Figur 9: Kjennskap til rutinar og retningsliner for informasjonstryggleik



Svara tyder på at retningsliner og krav knytt til teieplikt, konfidensialitet, og passordbruk er relativt godt kjende blant respondentane. På den andre sida indikerer også svara at forbodet mot å nytte datasystema til å formidle pornografi, rutinar for varsling ved mistanke om misbruk av datasystema, og retningsliner mot bruk av datasystema til gjeremål som ikkje er direkte knytt til arbeidet, er relativt dårleg kjende.

Respondentane vart vidare stilt spørsmål om *dei veit kven i kommunen dei skal kontakte dersom dei har spørsmål knytt til informasjonstryggleik og/eller handsaming av personopplysningar*. Litt over halvparten svara «ja» (52%) og litt under halvparten «nei» (48%).[66] Respondentane som svara «ja» på spørsmålet, fekk eit oppfølgingsspørsmål der dei vart spurde om *kven* i kommunen dei skal kontakte. Om lag ein fjerdedel av dei 70 som svara, sa at dei skal kontakte sin næraste leiar eller overordna. Elles svarte fleire ved å vise til utviklingsrådgjevaren eller IKT-leiaren, enten med tittel eller med namn.[67]

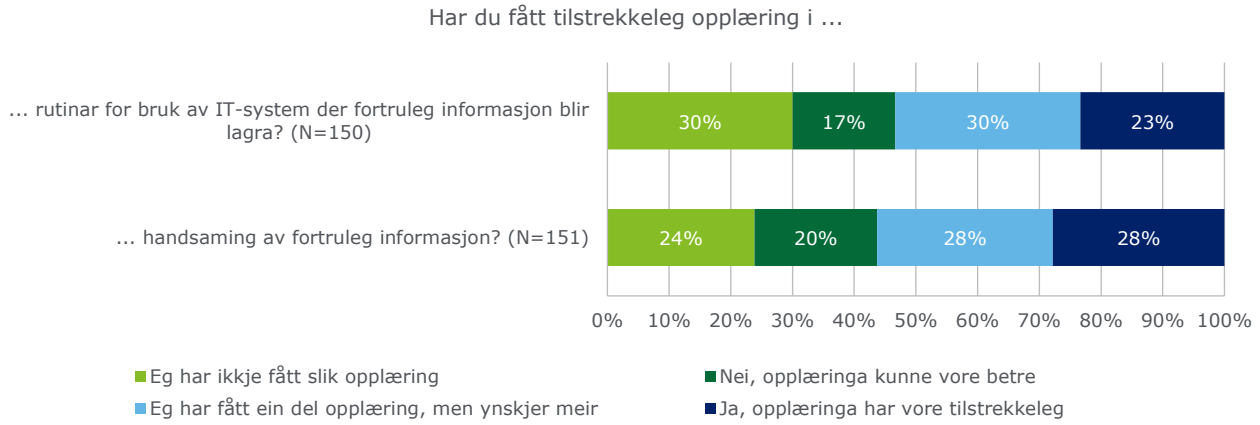
Vidare vart respondentane spurde om *dei er kjend med kva rutinar som gjeld for å melde avvik knytt til informasjonstryggleik*; 42 % svara «ja» og 58 % «nei».[68] Dei som svara «ja» vart bedne om å skildre avviksrutinane. I svara som kom inn vart det mellom anna vist til kommunen sitt avvikssystem,

[66] N=151.
[67] Resten av svara fordelte seg mellom å vise til administrasjon, dokumentsenter, arkiv, arkivar, personalavdelinga eller personalsjef, rådmann, systemansvarleg, dataansvarleg, HMT-ansvarleg, kundesenter, kommuneadvokat, samt IKTNH.
[68] N=151.

kvalitetssystem, intranett eller HMT-portal, og fleire svara at dei ville melde ifrå eller rapportere om avviket til sin næraste sjef, einingsleiar eller avdelingsleiar. Elles går det fram frå svara at nokre ville meldt avviket til enten IKT-avdelinga, personalavdelinga eller dokumentsenteret, og nokre ville meldt ifrå direkte til rådmannen.[69]

Som det går fram av figur 10, indikerer svara til om lag tre firedelar av respondentane at dei ikkje har fått tilstrekkeleg opplæring i rutinar for bruk av IT-system der fortruleg informasjon vert lagra, og at dei ikkje har fått tilstrekkeleg opplæring i handsaming av fortruleg informasjon.

Figur 10: Motteken opplæring



Alle som ikkje svara at dei har fått tilstrekkeleg opplæring i handsaming av fortruleg informasjon, fekk oppfølgingsspørsmål om kva opplæring knytt til informasjonstryggleik dei saknar. Av dei som 57 svara, vart det gjennomgåande vist til at respondentane saknar generell opplæring i informasjonstryggleik, opplæring i kva rutinar, retningsliner, instruksar, og system som gjeld for informasjonstryggleiksarbeid, samt repetisjon og oppfriskings- eller påminningskurs knytt til det same. Fleire saknar òg kurs i relevante lovverk, som t.d. forvaltningslova eller personvernforskrifta, eller når det skjer endringar i relevant lovverk.

Også opplæring knytt til avvikshandsaming vart nemnd som eit tema, i tillegg til generell opplæring i teieplikt. Generelt kjem det fram i svara at fleire er usikre på klassifisering og gradering av ulik type informasjon, og korleis elevinformasjon i elektroniske elevmapper skal sikrast og slettast.

Tilsvarande fekk alle som ikkje svara at dei har fått tilstrekkeleg opplæring i rutinar for bruk av IT-system der fortruleg informasjon vert lagra, eit oppfølgingsspørsmål om *kva opplæring knytt til bruk av IT-system dei saknar*. 52 respondentar svara på spørsmålet. Også her svara mange at dei saknar opplæring generelt, og nokon at dei saknar opplæring i dei fagsystema dei nyttar i kvardagen på jobb.[70]

5.4.2 Vurdering

Undersøkinga viser at langt dei fleste respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller anna fortruleg informasjon. Likevel viser svara frå spørjeundersøkinga at om lag éin av fem ikkje veit om kommunen har retningsliner for å handsame slike opplysningar. Revisjonen merker seg òg at over halvparten av respondentane i undersøkinga berre delvis er kjende med kva ansvar og oppgåver dei har med omsyn til informasjonstryggleik.

Vidare går det fram frå svara i spørjeundersøkinga at over halvparten av respondentane ikkje veit om dei har signert kommunen sin tryggleiksinstruks, og at to tredelar av dei som seier dei har signert han, ikkje hugsar innhaldet. Elles indikerer svara i spørjeundersøkinga at retningsliner og krav knytt til teieplikt, konfidensialitet, og passordbruk er relativt godt kjende blant respondentane, men at forbodet mot å nytte datasystema til å formidle pornografi, rutinar for varsling ved mistanke om misbruk av datasystema, og

[69] Også IKTNH vart nemnd, og ein respondent peika på at kommunen sitt avvikssystem er under omlegging, og at det difor er noko uklart for tida korleis ein skal melde avvik.
[70] I tillegg vart obligatoriske kurs, repetisjonar eller oppfrisking-kurs for alle tilsette, og/eller for alle nytilsette sakna, og fleire saknar opplæring i sikker lagring av opplysningar i mapper og på serverar.

retningsliner mot bruk av datasystema til gjeremål som ikkje er direkte knytt til arbeidet, er relativt dårleg kjende.

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

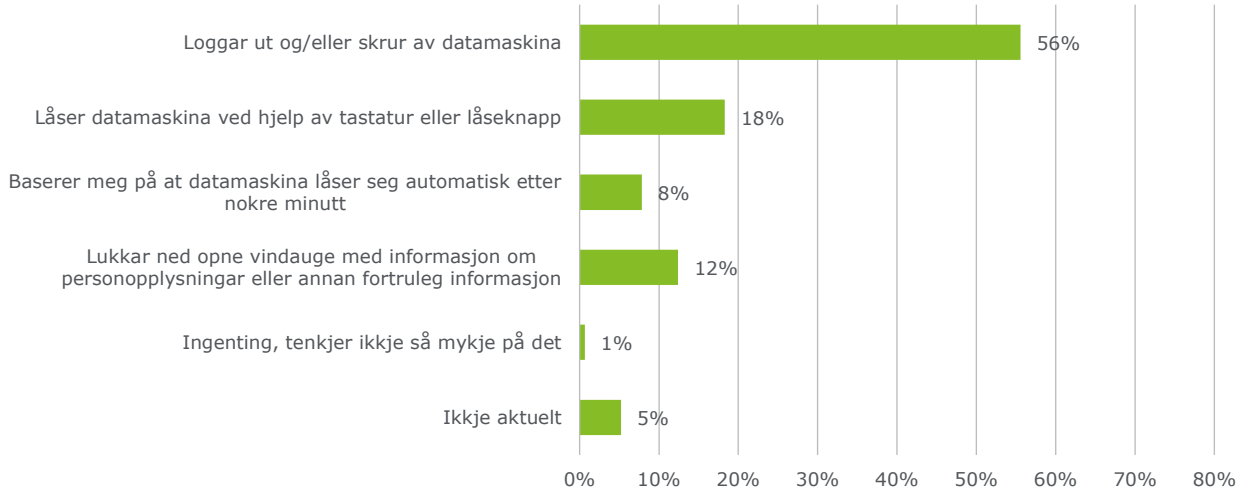
5.5 Etterleving av retningsliner og rutinar for informasjonstryggleik

5.5.1 Datagrunnlag

Eigen informasjonstryggleikspraksis

Respondentane vart spurde om *kva du vanlegvis gjer når du i løpet av arbeidsdagen går frå PC-en du brukar*. Svara er presentert i figur 11.

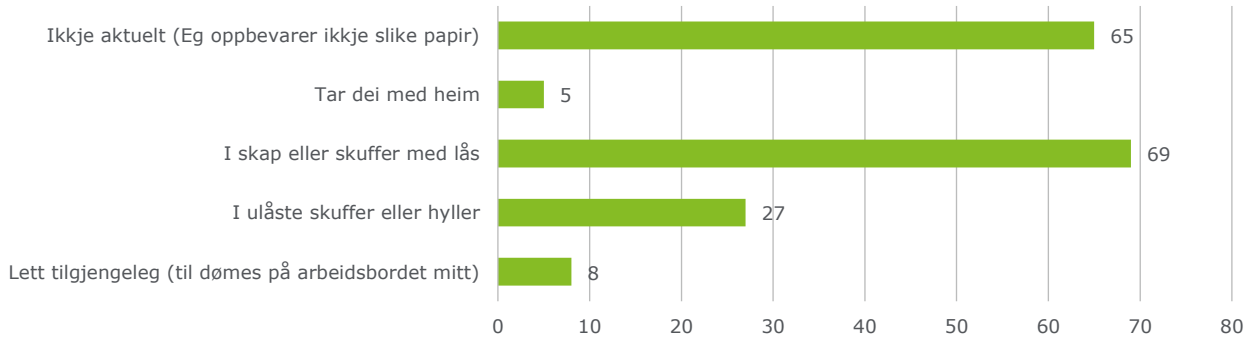
Figur 11: Kva gjer du vanlegvis når du i løpet av arbeidsdagen går frå PC-en du brukar? (N=153)



Respondentane vart òg spurde om dei *nokon gong har lånt ut brukarnamnet og passordet ditt til andre*. Nesten ein av fem svara «Ja, men berre til IT-avdelinga eller tilsvarande» (17 %), og 5,9 % svara «ja».[71]

Som vist i figur 12, svara 27 av respondentane at dei oppbevarer dokument med fortruleg informasjon i ulåste skuffer eller hyller, og 8 at dei ligg lett tilgjengeleg.[72]

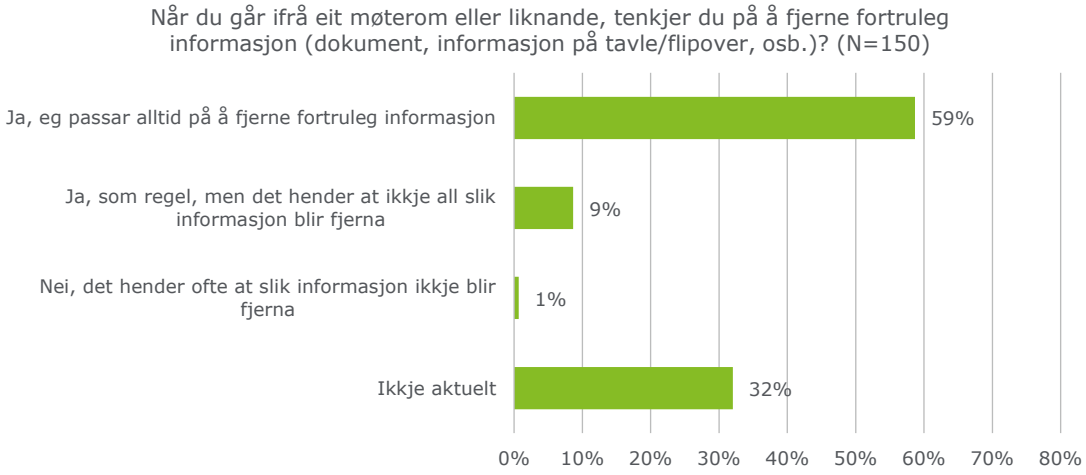
Figur 12: Korleis oppbevarer du dokument (papir) med fortruleg informasjon? (N=151)



[71] Dei resterande 77,1 % svara nei. 153 svara på spørsmålet.
[72] Respondentane hadde høve til å velje meir enn eitt svaralternativ.

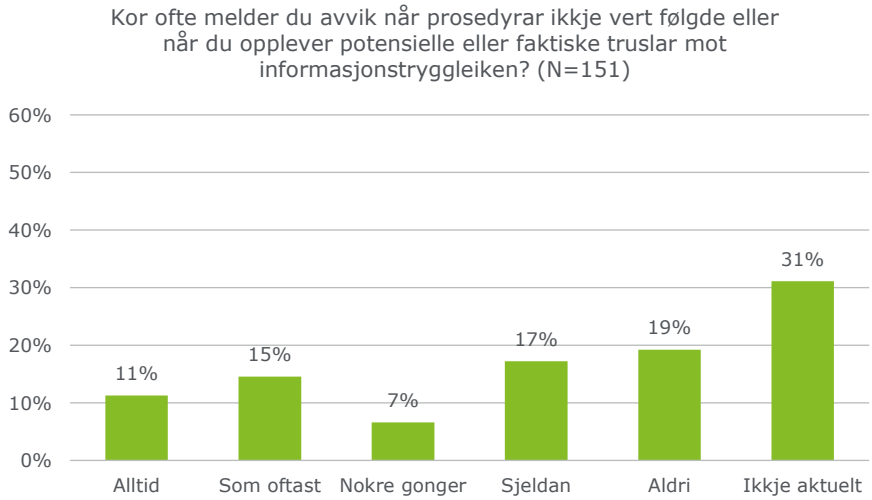
På spørsmål om *du tenkjer på å fjerne fortruleg informasjon som dokument, informasjon på tavle/flipover osb. når du går ifrå eit møterom eller liknande*, svara langt dei fleste der dette er aktuelt, at fortruleg informasjon enten alltid eller som oftast vert fjerna (sjå figur 13).

Figur 13: Fjerning av fortruleg informasjon frå møterom



19 % av respondentane meldar «aldri» og 17 % meldar «sjeldan» avvik *når prosedyrar ikkje vert følgde eller når du opplever potensielle eller faktiske truslar mot informasjonstryggleik* (sjå figur 14).

Figur 14: Avviksmelding



Alle som ikkje svara «alltid» eller «ikkje aktuelt» fekk oppfølgingsspørsmål om *kva årsaka/årsakene er til at du ikkje alltid melder avvik når prosedyrar ikkje vert følgde eller når du opplever potensielle eller faktiske truslar mot informasjonstryggleiken*. Flest svara at dei ikkje eller berre sjeldan har opplevd avvik knytt til informasjonstryggleik. Elles svara respondentane at dei ikkje har tid, ikkje veit kva som kvalifiserer som avvik, nokre veit ikkje at dei skal melde avvik, og ein del veit ikkje til kven dei skal melde avvik. Fleire svara at dei ikkje opplever at avviksmeldingar er forankra, tatt på alvor eller følgt opp av leiinga i kommunen.[73]

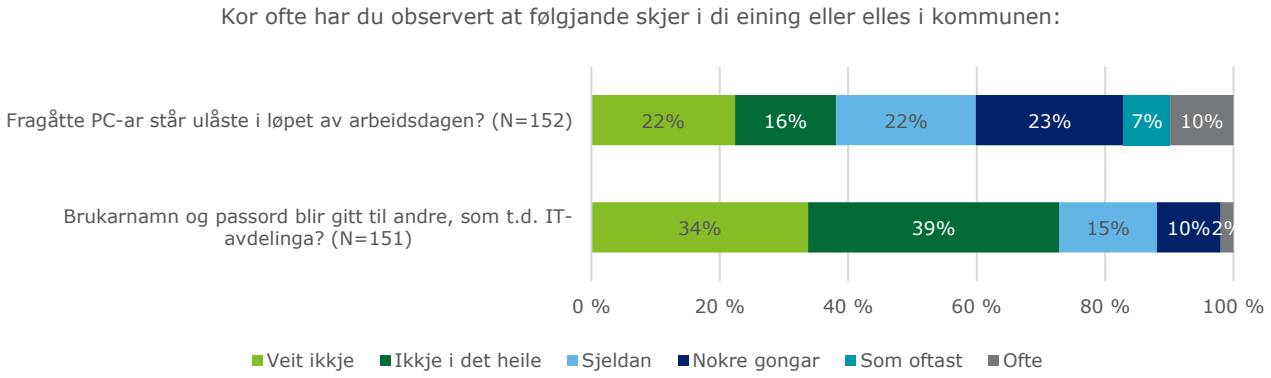
[73] I tillegg vart det nemnd at avvik vert meldt munnleg, og at årsaken til at ein ikkje meldar avvik er at det ikkje har skjedd nokon skade, at det vert mykje styr om ein melder avvik, at det var eit eingongstilfelle på eiga avdeling som dei sjølv retta opp, at det har lite læringseffekt for resten av organisasjonen, at ein i stadet tek det direkte opp med den det gjeld og får det rette opp.

Dei som svara at dei «alltid», «som oftast», «nokre gonger» eller «sjeldan» melder avvik knytt til informasjonstryggleik, vart spurde om meldte avvik har vorte følgt opp. 54 % svara «ja», 34 % «delvis» og 11 % svara «nei».[74]

Andre sin informasjonstryggleikspraksis

Respondentane vart i spørjeundersøkinga bedne om å svare på ei rekkje spørsmål knytt til kolleagers informasjonstryggleikspraksis. Mellom anna vart dei spurde om *kor ofte dei har observert i deira eining eller elles i kommunen at fragåtte PC-ar står ulåste i løpet av arbeidsdagen*, og *kor ofte dei har observert at det skjer i deira eining eller elles i kommunen at brukarnamn og passord vert gitt til andre, som til dømes IT-avdelinga*. Svara er presentert i figur 15:

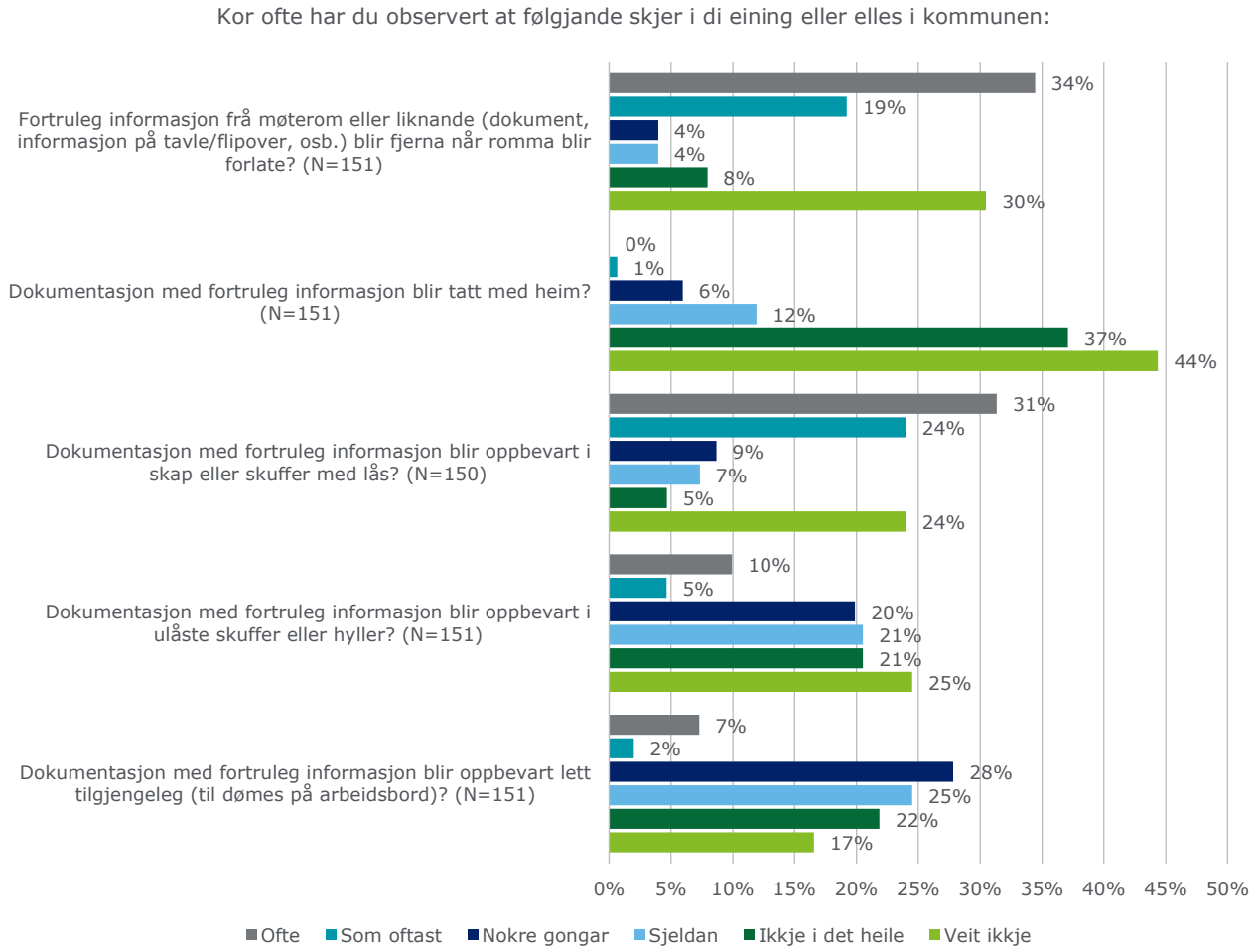
Figur 15: Informasjonstryggleikspraksis - PC og passord



Respondentane vart vidare spurde ei rekkje spørsmål knytt til kollegaers informasjonstryggleikspraksis med omsyn til dokumenthandsaming. Svara er presentert i figur 16:

[74] N=61.

Figur 16: Informasjonstryggleikspraksis - dokumenthandsaming



Som det går fram av figuren, har relativt mange av respondentane «som oftast» eller «ofte» observert at fortruleg informasjon frå møterom eller liknande vert fjerna når romma blir forlatne. Også når det gjeld oppbevaring av fortruleg informasjon, indikerer svara at dette som oftast vert låst ned i skap eller skuffer. Likevel tyder svara også på at dokumentasjon med fortruleg informasjon tidvis vert oppbevart i ulåst skap eller skuffer, eller lett tilgjengeleg på andre måtar.

5.5.2 Vurdering

Undersøkinga viser mellom anna at ein relativt høg del av respondentane ikkje følgjer ein praksis for avlogging av datamaskinen som er i samsvar med informasjonstryggleiksprinsipp. Vidare viser svara frå spørjeundersøkinga at heile 23 % av respondentane enten har delt passordet sitt med IT-avdelinga eller andre, og at 12 % har observert at andre har gjort dette. Det går òg fram i spørjeundersøkinga at fleire «aldri» eller «sjeldan» melder avvik knytt til informasjonstryggleik når slike avvik skjer, enn dei som «alltid» eller «som oftast» gjer det.

Når det gjeld dokumenthandsaming, viser spørjeundersøkinga at det førekjem at fortruleg informasjon i Lindås kommune vert oppbevart i ulåste skap eller skuffer, eller lett tilgjengeleg.

Basert på funna frå undersøkinga, er det revisjonen si vurdering at dei tilsette i Lindås kommune berre i nokon grad følgjer etablerte retningsliner og rutinar. Revisjonen meiner vidare at det er særleg alvorleg at nesten ein av fire av respondentane har delt passordet sitt, enten med IT-avdelinga eller andre. Dette bryt med heilt grunnleggjande prinsipp for informasjonstryggleik.

6. Konklusjon og tilrådingar

Denne forvaltningsrevisjonen har undersøkt om Lindås kommune har tilfredsstillande system og rutinar for informasjonstryggleik, og om etablerte standardar og gjeldande regelverk vert følgt innanfor dette området.

Lindås kommune har eit styringssystem for informasjonstryggleik, men systemet er ikkje ferdigstilt. Det har ikkje vore oppdatert på fleire år, og vert berre i nokon grad nytta i informasjonstryggleiksarbeidet i kommunen. Styringssystemet formaliserer rolle- og ansvarsdelinga for informasjonstryggleik, men undersøkinga avdekker at denne organiseringa i praksis ikkje vert følgt, og at det er til dels uklare ansvarstilhøve med omsyn til informasjonstryggleik både internt i kommunen, og mellom kommunen og IKTNH.

Lindås kommune har ikkje noko system som sikrar at oversikta over personopplysningar dei handsamar er oppdatert og fullstendig. Det er difor risiko for at kommunen handsamar personopplysningar utanfor oversikta. Det vert heller ikkje gjennomført risikovurderingar av systema kommunen brukar, noko som gjer det vanskelegare å vite kva risikoar for informasjonstryggleik kommunen er utsett for. Kommunen har heller ikkje noko oversikt over kva databehandlaravtalar dei har inngått, og kan difor ikkje vite om dei har oversikt over kven som handsamar personopplysningar på vegner av kommunen.

Vidare har Lindås kommune dokumenterte rutinar og retningsliner for kontroll og etterprøving av informasjonstryggleik, men slik kontroll og etterprøving finn berre stad i avgrensa grad, og kommunen bryt slik med både sine eigne rutinar og retningsliner, samt sentrale krav i gjeldande regelverk.

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

Med omsyn til tilgjengelegheit i IKT-systema, kjem det fram i undersøkingane at IKTNH fastset kriterium for dette i systema dei driftar på vegner av Lindås kommune, men at Lindås kommune sjølv ikkje gjer dette. Vidare rapporterer ikkje IKTNH til Lindås kommune om nedetid i systema, noko som gjer det vanskeleg for Lindås kommune å kontrollere tilgjengelegheita og stabiliteten i IKT-systema på ein systematisk måte. Dette gjer det også vanskeleg for kommunen å setje i verk ev. tiltak for å betre tilgjengelegheit og stabilitet i IKT-systema.

Brukarstøtta for IKT i Lindås kommune vert jamt over opplevd som god av brukarane. Revisjonen merkar seg likevel at det ikkje er ei formalisert beredskapsvakt i brukarstøtta. Dette gir auka sårbarheit i brukarstøtta, noko som kan ha alvorlege konsekvensar for tilgjenge til naudsynt informasjon for dei tilsette i Lindås kommune, og slik for brukarane av kommunale tenester. Det kjem òg fram at organiseringa av brukarstøtte for fagsystema har manglar, mellom anna ved at det er knytt usikkerheit til kven som skal yte brukarstøtte til fleire av desse. Revisjonen si samla vurdering er difor at brukarstøttetenestene i Lindås kommune berre delvis er organisert på ein føremålstenleg måte.

Undersøkinga viser at langt dei fleste respondentane handsamar eller kjem i kontakt med personopplysningar, sensitive personopplysningar eller annan fortruleg informasjon. Likevel indikerer svara i spørjeundersøkinga at over halvparten av respondentane berre delvis er kjende med kva ansvar og oppgåver dei har med omsyn til informasjonstryggleik. Revisjonen meiner at det er særleg alvorleg at nesten ein av fire av respondentane svarar at dei har delt passordet sitt, enten med IT-avdelinga eller andre. Dette bryt med heilt grunnleggjande prinsipp for informasjonstryggleik. Det er revisjonen si vurdering at dei tilsette i Lindås kommune ikkje har tilstrekkeleg kjennskap til eksisterande 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 som gjeld for handsaming av personopplysningar, og for informasjonstryggleika i kommunen generelt.

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

1. oppdatere og ferdigstille styringssystemet for informasjonstryggleik slik at dette 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 vert handsama

b) sikre at det vert gjennomført risikovurderingar av IT-system og behandlingar av personopplysningar opp mot fastsette akseptkriterium for informasjonstryggleik

c) gjennomføre tilstrekkeleg konktroll 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. formalisere og ev. etablere beredskapsrutinar for både den generelle brukarstøtta og for brukarstøtte til dei ulike fagsystema som er i bruk i kommunen
4. Sikre at samarbeidsavtalene med IKTNH vert overhaldt og klargjort, særleg med omsyn til:

   a) rolle- og ansvarsdeling mellom kommunen og IKTNH med omsyn informasjonstryggleik

   b) opningstid for og organisering av brukarstøtta

   c) rapportering frå IKTNH til kommunen, særleg knytt til nedetid i IKT-systema

Vedlegg 1: Høyringsuttale

LINDÅS KOMMUNE
Utviklingsavdelinga

Deloitte AS

Referanser:	Saksbehandlar:	Dato:
Dykkar: Løvlie, Frode (NO - Bergen)	Nils-Erik Buck	14.11.2017
Vår: 17/538 - 17/32339	nils-erik.buck@lindas.kommune.no	

Forvaltningsrevisjon til høyring - informasjonstryggleik i Lindås kommune

Lindås kommune v/Rådmannen er i all hovudsak einig i konklusjonar og tilrådingar som fremgår i forvaltningsrevisjonen.

Et par faktafeil vil me likevel påpeike:

- Rapporten seier at kommunen ikkje gjennomførar risiko- og sårbarhetsanalysar av sine fagsystem. Det er ikkje heilt riktig. IKT-leiar har nyleg gjennomført ROS analyser i samarbeid med omsorgsteknologitenesta for dei fagsystema som inngår i tenesta. Likevel gjenstår systematisk gjennomføring og revisjon av ROS-analyser for dei fleste fagsystem.
- Kommunen har ikkje manglande oppfylgjing av avvik meldt på informasjonstrygleik. Statistikk frå avviksystemet viser at avvik vert behandla.

Rådmannen ser på **manglande kapasitet** hos dei trygleiksansvarlege som ei hovudårsak til at kommunen ikkje har:

- eit tilfredsstillande styringssystem for informasjonstrygleik
- tilfredsstillande opplæring av dei tilsette i informasjonstrygleik
- tilfredsstillande internkontroll
- gjennomført ROS-analyser for alle fagsystem
- Ei komplett og oppdatert oversikt over alle personopplysningar me handsamar

I tillegg gjer fråver av prosessstøtte i styringssystemet den kontrollerande delen av internkontrollen vilkårleg og lite effektiv.

Når det gjeld arbeid med tiltak som Deloitte tilrår, meiner Rådmannen at disse bør gjerast i regi av Alver kommune.

Post
postmottak@lindas.kommune.no
Dokumentsenteret
Kvernhusmyrane 20, 5914 Isdalstø

Kontakt
www.lindas.kommune.no
Telefon +47 56 37 50 00
Telefaks +47 56 37 50 01

Konto 3201.05.89311
Org.nr. 935 084 733

Med helsing

Nils-Erik Buck
Rådgiver

Dette dokumentet er elektronisk godkjent og har difor ingen signatur.

Mottakarar:
Deloitte AS

Vedlegg 2: Revisjonskriterium

Innleiing

Revisjonskriteria er henta frå og utleia av autoritative kjelder, rettsreglar, politiske vedtak og fastsette retningsliner. I dette prosjektet har personopplysningslova med forskrift, eForvaltningsforskrifta, helseregisterlova, norm for informasjonstryggleik i helse-, omsorgs- og sosialsektoren og sikkerheitslova vore nytta for utleiing av revisjonskriterier.

Krav i lov og forskrift

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

Å sørgje for konfidensialitet inneberer å hindre ikkje-autorisert innsyn i informasjon som ikkje skal vere tilgjengeleg for alle; å sørgje for integritet inneberer å hindre ikkje-autorisert endring og sletting av informasjon; å sørgje for tilegjengelegheit inneberer 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[75] og databehandlaren[76] «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.[77] 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 vert 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 internkontroll.

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

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

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.

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.»

Vidare stiller ISO27001:2013 kapittel 9 krav om overvaking av informasjonstryggleik for å kunne måle og evaluere og utbetre informasjonstryggleiksystemet.

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 innarbeida 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: Lister og tabellar

IKTNH

Liste over fagapplikasjonar som IKTNH driftar for kommunane i samarbeidet:

- Acos Barnevern
- Acos CosDoc
- Acos Sosial
- Acos Websak
- Agrando
- Conexus –Vokal
- DSB Sim
- E-tid
- Fakturabehandling
- Feide
- GisLine
- HK Data
- Info EDI
- Visma Link
- Infodoc
- It's Learning
- KF Kvalitetsstyring
- Kirkedata
- Komtek
- Konsensus
- Labora
- Landlord/Weblord
- Lindorff Hurtiglink
- Micromarc
- Min Skule/Min Barnehage
- Mitt Nordhordland
- NAV-Citrix
- Powel Gemini
- Procasso
- Sofus
- Speed Admin
- Uni Micro
- Visma barnehage
- Visma Flyktning
- Visma Flyt
- Visma HRM Enterprise
- Visma IOP
- Visma IP
- Visma Min Side
- Visma Mobil Omsorg
- Visma PPI
- Visma Profil
- Welch Allyn

Kommunane har ikkje laga ei oversikt over sine kritiske applikasjonar, men IKTNH har ei liste som går fram av tabell 7.

Tabell 7: IKTNH si liste over kritiske fagsystem og tenester

Fagsystemer og Tjenester i SLA-klasse[78] "Prioritet 1"			
Fagsystem/tjeneste	**RTO[79]**	**RPO[80]**	**Kommentar**
Epost	48 timer	24 timer	Informasjon og støtte for DSB Sim
Tilgang Internett	48 timer	24 timer	Fagapplikasjoner er avhengige av internett. Informasjon til publikum. Beredskapsverktøy
Kommunens hjemmesider	48 timer	24 timer	Informasjon til publikum
Gis-Line / Powel Gemini	48 timer	24 timer	Beslutningsstøtte
DSB Sim	48 timer	24 timer	Beredskapsverktøy
TDC Bedriftsnett	48 timer	24 timer	Kontakt med kommunene
SD-Anlegg	48 timer	24 timer	Fjernstyring av bygg
CosDoc	48 timer	24 timer	Pasientsikkerhet. Kritisk fra dag 2 for hjemmeboende.

[78] Difi definerer ein tenestenivåavtale eller Service Level Agreement (SLA) slik: «Tenestenivåavtalen beskriv og regulerer ytingsnivået på den jamlege tenesta». https://www.anskaffelser.no/it/it-drift/sla-tjenesteavtale [Henta 04.10.2017]
[79] Recovery Time Objective (RTO) eller mål for gjenopprettingstid er: «Den maksimale tiden som tillattes brukt etter et avbrudd for å gjenopprette en IT-tjeneste». Side 89. ITIL-ordliste og forkortelser på norsk. 01.10.2012.
[80] Recovery Point Objective (RPO) eller mål for gjenoppretting er: «Gjenopprettingsmål kan beskrive en maksimal mengde data som kan gå tapt når tjenesten gjeninnføres etter et avbrudd. Mål for gjenoppretting uttrykkes som et tidsrom før svikt». Side 88. ITIL-ordliste og forkortelser på norsk. 01.10.2012.

Visma Profil	48 timer	24 timer	Pasientsikkerhet. Kritisk fra dag 2 for hjemmeboende.
Infodoc	48 timer	24 timer	Knyttes direkte til CosDoc og Profil
Visma mobilomsorg	48 timer	24 timer	Pasientsikkerhet. Kritisk fra dag 2 for hjemmeboende.
Info Edi	48 timer	24 timer	Elektroniske pasientmeldinger
Visma Link	48 timer	24 timer	Elektroniske pasientmeldinger

Fagsystemer og Tjenester i SLA-klasse "Prioritet 2"

Fagsystem/tjeneste	**RTO**	**RPO**
Acos Barnevern	7 dager	24 timer
Acos Sosial	7 dager	24 timer
Acos Websak	7 dager	24 timer
Agrando	7 dager	24 timer
HK Data	7 dager	24 timer
It's Learning	7 dager	24 timer
KF Kvalitetsstyring	7 dager	24 timer
Kirkedata	7 dager	24 timer
Komtek	7 dager	24 timer
Labora	7 dager	24 timer
Landlord/Weblord	7 dager	24 timer
Micromarc	7 dager	24 timer
NAV-Citrix	7 dager	24 timer
Procasso	7 dager	24 timer
Sofus	7 dager	24 timer
Uni Micro	7 dager	24 timer
Visma barnehage	7 dager	24 timer
Visma Flyktning	7 dager	24 timer
Visma Flyt	7 dager	24 timer
Visma HRM Enterprise	7 dager	24 timer
Visma Min Side	7 dager	24 timer
Visma Mobil Omsorg	7 dager	24 timer
Visma PPI	7 dager	24 timer
Welch Allyn	7 dager	24 timer

Generelle tenester	7 dager	24 timer
Antivirus	7 dager	24 timer
Arbeidsstasjon	7 dager	24 timer
Brukaradministrasjon	7 dager	24 timer

Brukarstøtte	7 dager	24 timer
Brukerstøtteverktøy: TMS	7 dager	24 timer
Distribusjonssenter: SCCM	7 dager	24 timer
Feide	7 dager	24 timer
Fil- og heimeområder	7 dager	24 timer
Fjernstyringsverktøy: Bomgar	7 dager	24 timer
Fjerntilgang	7 dager	24 timer
Innkjøp	7 dager	24 timer
Intranett	7 dager	24 timer
Kontorstøtteverktøy	7 dager	24 timer
Kopi/utskrift/scanning	7 dager	24 timer
Lisensadministrasjon	7 dager	24 timer
Reservekopiering/tilbakekopiering	7 dager	24 timer

Fagsystemer og Tjenester i SLA-klasse "Prioritet 3"

Fagsystem/tjeneste	**RTO**	**RPO**
Conexus –Vokal	14 dager	48 timer
Fakturabehandling	14 dager	48 timer
Feide	14 dager	48 timer
Konsensus	14 dager	48 timer
Lindorff Hurtiglink	14 dager	48 timer
Min Skule/Min Barnehage	14 dager	48 timer
Mitt Nordhordland	14 dager	48 timer
Speed Admin	14 dager	48 timer
Visma Min Side	14 dager	48 timer
Generelle tenester	14 dager	48 timer
Avhending av utstyr	14 dager	48 timer
E-læring	14 dager	48 timer
E-læring: IKTNH.knowledgeportal.no	14 dager	48 timer
Lisensadministrasjon	14 dager	48 timer
Overvåkningsverkøty: WhatsUpGold	14 dager	48 timer
Programvaresenter	14 dager	48 timer
Infrastruktur	14 dager	48 timer
Betalingsterminal	14 dager	48 timer
Elektroniske tavler	14 dager	48 timer
Infoskjerm	14 dager	48 timer

Vedlegg 4: Sentrale dokument og litteratur

Regelverk

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

Rettleiarar og standardar

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

Kommunale dokument og avtaler

- Lindås kommune: Samarbeidsavtale interkommunale IKT-tenester. 2011.
- Lindås kommune: Tenesteleveringsavtale med Osterøy som vertskommune for IKTNH. 2013.
- Lindås kommune: Behandlingsoversikt Lindås kommune.
- Lindås kommune: Rapport Avvik Informasjonstryggleik. Mars 2016 - April 2017.
- Lindås kommune: Sjekkliste Introduksjon. Dok.ref.: 14/3566 – 2.
- Lindås kommune: Datahandsamaravtale med Kommuneforlaget. 2008.
- Lindås kommune: Datahandsamaravtale med Ergo Group. 2010
- Lindås kommune: Datahandsamaravtale med NAV Hordaland. 2012.
- Lindås kommune: Datahandsamaravtale med NETS Norway AS. 2012.
- Lindås kommune: Datahandsamaravtale med Osterøy kommune (IKTNH) og Lindås kommune. 2015.
- Lindås kommune: Datahandsamaravtale med Vakt og alarm AS. 2016.
- Lindås kommune: Datahandsamaravtale med Alarm24. 2017.

Interkommunale dokument

- IKTNH: Overordnet sikkerhetspolicy for kommuner tilknyttet Felles IKT Nordhordland. 2014.
- IKTNH: Rutine for hendelseshåndtering for kommuner tilknyttet Felles IKT Nordhordland. 2014.
- IKTNH: Tilgangskontrollpolicy for kommuner tilknyttet IKTNH. 2014
- IKTNH: Rutine for brukerregistrering for kommuner tilknyttet IKTNH. 2015.
- IKTNH: Rutine for beredskap for kommuner tilknyttet IKTNH. 2017.
- IKTNH: Felles IKT-strategi 2015-2018.
- IKTNH: Organisering av IKT-verksemda i regionen v4.
- IKTNH: IKT-reglement for kommunane i SING.
- IKTNH: Risiko og sårbarhetsanalyse for IKT i kommunene.
- IKTNH: Vurdering og bedømming av risiko ved uønskte hendingar / ROS-analyse
- IKTNH: Tiltak og gjennomføringsplan.

Deloitte.