TELEMARK
KOMMUNEREVISJON IKS

Informasjonssikkerhet

- Lardal kommune -

Forvaltningsrevisjonsrapport nr: 701004

2010

Innholdsfortegnelse

Sammendrag ..... **iii**

1 Innledning **1**

1.1 Bakgrunn 1
1.2 Problemstillinger 1
1.3 Avgrensing 1

2 Metode og kvalitetsikring **2**

2.1 Den praktiske gjennomføringen 2
2.2 Høring 2

3 Risikovurdering og sikkerhetsstrategi **2**

3.1 Revisjonskriterier 2
3.2 Fakta og funn 2
3.3 Revisors vurderinger 3

4 Dokumentasjon om informasjonssystemene **3**

4.1 Revisjonskriterier 3
4.2 Fakta og funn 3
4.3 Revisors vurderinger 5

5 Virksomhetens organisering og etablerte sikkerhetstiltak **5**

5.1 Revisjonskriterier 5
5.2 Fakta og funn 5
5.2.1 Organisering 5
5.2.2 Tilgangskontroll 6
5.2.3 Fysisk sikring 7
5.2.4 Arbeidsdeling og kompetanse 8
5.2.5 Sikkerhetskopiering 9
5.2.6 Installering og oppgradering av programvare 9
5.2.7 Virus 10
5.2.8 Rutiner 10
5.3 Revisors vurderinger 10

6 Revisors konklusjoner og anbefalinger **11**

Litteratur og kildereferanser **12**

Vedlegg 1: Kommunens høringssvar **13**

Vedlegg 2: Begreper som benyttes i rapporten **14**

Vedlegg 3: Risikovurdering og sikkerhetsstrategi - revisjonskriterier **15**

Vedlegg 4: Dokumentasjon om informasjonssystemene - revisjonskriterier **17**

Vedlegg 5: Virksomhetens organisering - revisjonskriterier **18**

Vedlegg 6: Liste over servere og applikasjoner **21**

Vedlegg 7: Eksempel på oppbygging av skjema for risikovurdering **22**

Sammendrag

Bakgrunn

Rapporten er utarbeidet på oppdrag fra kontrollutvalget i Lardal.

Informasjonssikkerhet kan deles inn i tiltak som sikrer tilgjengelighet, integritet og konfidensialiteten til informasjonen. Å sikre tilgjengelighet er å sikre at den som trenger informasjonen har den tilgjengelig ved behov. Integritet betyr at informasjonen skal være riktig og pålitelig. Konfidensialitet innebærer at ingen andre enn de som trenger informasjonen skal få tilgang på den. Informasjonssikkerhet er ikke et mål i seg selv, men et middel for å oppnå tilfredsstillende kvalitet på kommunens tjenester. Prosjektet skal bidra til bedre informasjonssikkerhet i kommunen og avdekke eventuelle mangler.

Problemstillinger

1) Er sikkerhetsrisikoen vurdert ved en systematisk gjennomgang for å identifisere trusler og er det etablert en sikkerhetsstrategi?
2) Er alle relevante lover og kontraktmessige krav tydelig definert og dokumentert for hvert enkelt informasjonssystem?
3) Sikrer virksomhetens organisering og etablerte sikkerhetstiltak en god IT-sikkerhet?
   a) Er det klare ansvars- og myndighetsforhold?
   b) Er det etablert sikkerhetstiltak?
   c) Har kommunen personvernombud?

Resultater

Vår gjennomgang viser at Lardal kommune har hatt en praktisk tilnærming til IT- og informasjonssikkerhet de siste årene. Kommunen har fått nye servere og innført sikre og usikre soner for behandling av ulik type informasjon. Lardal kommune hadde en systematisk gjennomgang av risiko og utarbeidet alle dokumentene som personvernlovgivningen krever i 2002. Disse dokumentene er hverken oppdatert eller i bruk.

Vi har ikke sett at kommunen har faste rutiner for å oppfylle meldeplikten og konsesjonsplikt til Datatilsynet. Det ble sendt to meldinger i november 2009 angående registrering av sensitive personopplysninger om ansatte i lønnssystemet. Ellers er det ikke sendt melding siden 2002. Lardal kommune har ikke personvernombud.

Det foreligger ikke en skriftlig avtale angående samarbeidet med Andebu kommune om drift av hjemmesiden og intranett. Lardal kommune har heller ikke skriftlig avtale med et lokalt firma som hjelper kommunen med problemer med egne servere. Med andre leverandører har kommunen skriftlige avtaler basert på standardavtaler.

Få av de vi intervjuet kjente til dokumentene om informasjonssikkerhet. De fleste hadde likevel en oppfatning av hva som var risikoene ved IT-systemene, og hva som burde gjøres hvis det oppstår en uheldig situasjon. Alle vi har snakket med i kommunen har et bevisst forhold til behandling av sensitiv informasjon.

Personalet på sykehjemmet og i hjemmetjenesten har gruppevis felles brukernavn og passord for å logge seg inn på usikker sone. Derfra logger de seg inn i fagapplikasjonen Prosys med personlig brukernavn og passord. Fra usikker sone har personalet direkte tilgang til dokumenter i kommunens mapper i sikker sone via Word. Sykehjemmet har rutine for at dokumenter med personopplysninger som lages utenfor Prosys, skal lagres slik at sykepleierne må ha passord for å åpne dokumentet igjen. I forbindelse med datainnsamlingen

oppdaget revisjonen at dokumenter med personopplysninger ikke ble lagret i tråd med enhetens rutiner. Sykehjemmet har en brukerperm for Prosys, men den er ikke oppdatert og i bruk. Prosys blir stadig oppdatert, men personalet på sykehjemmet har ikke fått opplæring i å bruke de nye mulighetene som Prosys byr på.

Generelle konklusjoner
Det bør gjennomføres en risikovurdering, og dokumentene om informasjonssikkerhet bør oppdateres til dagens organisasjon, tekniske situasjon og risikovurderinger. Oversikten over hva slags opplysninger kommunen behandler bør oppdateres. Kommunen bør lage rutiner for å overholde melde- og konsesjonsplikten. Dokumentene og rutinene bør gjøres levende i administrasjonen. Kommunen bør vurdere å ha et personvernombud.

Det bør være skriftlige avtaler med alle leverandører. Standardavtaler sikrer ofte klare ansvarsforhold og rettigheter.

Kommunen bør vurdere å innføre generelle rutiner for låsing av kontorer når personalet ikke er tilstede.

Det bør innføres et system for utskrifter fra sikker sone, slik at utskriften ikke skrives ut før rette person står ved skriveren.

Konklusjoner angående Lardal sykehjem
Alle bør ha individuelle brukernavn og passord.

Dørene inn til kontorer der det oppbevares dokumenter eller pc-er med sensitiv informasjon bør låses.

Brukerpermen for Prosys bør oppdateres og være et levende dokument for sykehjemmet.

Kommunen bør vurdere behovet for å øke personalets kompetanse på bruk av IT.

Skien 24.9.2010
Telemark kommunerevisjon IKS

Kirsti Torbjørnson
oppdragsansvarlig forvaltningsrevisor

Gerd Smedsrud Mikelborg
prosjektleder

1 Innledning

Rapporten er utarbeidet på oppdrag fra kontrollutvalget i Lardal. I møte 16.12.2009, sak 19/09 bestilte kontrollutvalget forvaltningsrevisjon av informasjonssikkerhet. Hjemmel for forvaltningsrevisjon er gitt i kommunelovens § 77 nr. 4, jamfør forskrift om kontrollutvalg kapittel 5 og forskrift om revisjon kapitel 3.

Ifølge forskrift om revisjon § 7 skal forvaltningsrevisjon gjennomføres og rapporteres i henhold til god kommunal revisjonsskikk og etablerte og anerkjente standarder på området. Denne rapporten er utarbeidet med grunnlag i RSK 001 Standard for forvaltningsrevisjon[1].

1.1 Bakgrunn

Informasjonssikkerhet kan deles inn i tiltak som sikrer tilgjengelighet, integritet og konfidensialiteten til informasjonen. Å sikre tilgjengelighet er å sikre at den som trenger informasjonen har den tilgjengelig ved behov, i praksis betyr det ofte at IT-systemene må fungere som de skal. Integritet betyr at informasjonen skal være riktig og pålitelig. Informasjonen bør være oppdatert og bare autorisert personell skal ha tilgang til å endre informasjonen. Konfidensialitet innebærer at ingen andre enn de som trenger informasjonen skal få tilgang på den.

Informasjonssikkerhet er ikke et mål i seg selv, men et middel for å oppnå tilfredsstillende kvalitet på kommunens tjenester, og skal ikke minst være med å gi innbyggerne tillit til kommunen. Prosjektet skal bidra til bedre informasjonssikkerhet i kommunen og avdekke eventuelle mangler.

1.2 Problemstillinger

1) Er sikkerhetsrisikoen vurdert ved en systematisk gjennomgang for å identifisere trusler og er det etablert en sikkerhetsstrategi?
2) Er alle relevante lover og kontraktmessige krav tydelig definert og dokumentert for hvert enkelt informasjonssystem?
3) Sikrer virksomhetens organisering og etablerte sikkerhetstiltak en god IT-sikkerhet?
   a) Er det klare ansvars- og myndighetsforhold?
   b) Er det etablert sikkerhetstiltak?
   c) Har kommunen personvernombud?

1.3 Avgrensing

Denne revisjonen omhandler IT-systemene til Lardal kommune. Vi har valgt å se nærmere på arkivprogrammet Websak, regnskapsprogrammet Agresso, fakturabehandlingsprogrammet Basware og fagsystemet Prosys, som hjemmetjenestene, psykiatri og sykehjemmet bruker. Vi har ikke gjennomført en teknisk IT-revisjon, og vi har heller ikke vurdert kvaliteten på internettilkoblingen for de ulike enhetene.

[1] RSK 001 er fastsatt av Norges Kommunerevisorforbunds styre 23. mai 2005 og gjort gjeldende som god kommunal revisjonsskikk. Standarden bygger på norsk regelverk og internasjonale prinsipper og standarder som er fastsatt av International Organization of Supreme Audit Institutions (INTOSAI) og Institute of Internal Auditors (IIA).

Ved Ringveien helsesenter har vi ikke sett på IT-sikkerhet i barnevern, siden barnevern i Lardal gjennomføres som vertskommunesamarbeid der Larvik er vertskommune. Vi har også avgrenset mot NAV og legekontoret.

2 Metode og kvalitetsikring

Metodebruken har bestått av dokumentanalyse, møter og intervjuer med administrasjonen i Lardal kommune.

2.1 Den praktiske gjennomføringen

Vi har gjennomgått kommunens dokumenter angående informasjonssikkerhet, både de som er utarbeidet internt og kontrakter med eksterne leverandører. Vi har intervjuet rådmannen, stabsleder, enhetsledere og andre med praktisk kjennskap til bruken av kommunens IT-systemer. Den tidligere IKT-konsulenten har bistått med informasjon underveis i prosjektet.

2.2 Høring

Rapporten ble sendt til rådmannen for uttalelse. Høringssvaret har ført til mindre endringer i kapittel 5.2.2. Det har ikke ført til endringer i våre vurderinger og konklusjoner. Høringssvaret ligger i vedlegg 1.

3 Risikovurdering og sikkerhetsstrategi

3.1 Revisjonskriterier

Med bakgrunn i utredningen i vedlegg 4 blir revisjonskriteriene slik:

- Kommunen skal dokumentere at det er utført en systematisk risikovurdering av informasjonssikkerheten.
- Risikovurderingen bør beskrive risiko som er avdekket og sammenlikne dette med det som er definert som akseptabelt risikonivå.
- Kommunen skal ha utarbeidet et overordnet dokument for sin sikkerhetsstrategi, med bakgrunn i disse vurderingene.

3.2 Fakta og funn

I 2002 utarbeidet Lardal kommune dokumenter angående informasjonssikkerhet. De har et overordnet dokument som dokumenterer gjennomført risikoanalyse, med retningslinjer for informasjonssikkerhet og oversikt over personopplysninger. Kommunen har også skriftlige rutiner for blant annet sikkerhetskopiering, avviksregistrering, fysisk sikkerhet, systemteknisk sikkerhet og ledelsens gjennomgang. Disse dokumentene er ikke oppdatert og brukes ikke lenger aktivt av kommunen.

Få av de vi intervjuet hadde kjennskap til dokumentene om informasjonssikkerhet. De fleste enhetslederne hadde likevel klart for seg hva som var risikoene ved deres IT-systemer, hvilke konsekvenser dette kunne få, og hva som burde gjøres hvis ulike uheldige situasjoner skulle inntreffe.

Kommunen har det siste året hatt en praktisk tilnærming til IT-sikkerhet. Serverne er fornyet, sammen med katalogstrukturen, som har fått sikre soner for oppbevaring av sensitiv

informasjon. Lardal kommune har i 2009 utarbeidet en plan for hva som videre bør forbedres ved IT-sikkerheten.

Fagsystemet Prosys brukes av sykehjemmet, hjemmetjenestene og psykiatri. Hjemmetjenestene og psykiatri ligger organisert under Ringveien helsesenter. Helsesenteret har utarbeidet en kvalitetshåndbok for Prosys med en enkel risikoanalyse. Det er rutiner for hvilke opplysninger som skal være tilgjengelig og hvordan personopplysninger skal behandles hvis Prosys ligger nede. Særlig om sommeren er kommunen utsatt for strømbrudd etter tordenvær, slik at disse rutinene brukes aktivt. Da skal rapportene skrives på papir og oppbevares innelåst. Rapportene føres inn i Prosys når strømmen kommer tilbake. Ved Ringveien helsesenter er kvalitetshåndboka oppdatert og i bruk. Sykehjemmet har en brukerperm for Prosys med skriftlige rutiner. Den oppbevares på kontoret på en av avdelingene. Den er ikke oppdatert og i aktiv bruk.

3.3 Revisors vurderinger

Lardal kommunes dokumenter om informasjonssikkerhet bør oppdateres og tilpasses dagens organisasjon og tekniske systemer. Administrasjonen har et godt grunnlag å bygge videre på.

Rutinene for tilgjengelighet og sikkerhet knyttet til Prosys er klare på Ringveien helsesenter. Helsesenter gir inntrykk av å jevnlig oppdatere kvalitetshåndboka, mens Lardal sykehjem ikke har prioritert denne oppgaven. Sykehjemmet bør oppdatere brukerpermen.

4 Dokumentasjon om informasjonssystemene

4.1 Revisjonskriterier

Med bakgrunn i utredning i vedlegg 4 blir revisjonskriteriene slik:

- Kommunen skal ha dokumentasjon som viser en oversikt over hva slags opplysninger som blir behandlet i de forskjellige datasystemene, og hvilke lover som er knyttet til opplysningene.
- Kommunen skal ha dokumenterte rutiner som sikrer at det søkes konsesjon eller sendes melding til Datatilsynet for behandling av de opplysningene som kan finnes i datasystemet.
- Det skal være skriftlige avtaler med underleverandører, med klart definerte ansvars- og rettighetsforhold.

4.2 Fakta og funn

Blant dokumentene om informasjonssikkerhet fra 2002 ligger en oversikt som viser hvilke opplysninger som kommunen behandler, formålet med det, hjemmelen for å behandle opplysningen, sikringstiltak, hvordan opplysningene skal lagres og hvor mange personer registeret omhandler. Vi har ikke sett dokumentasjon på at kommunen har oppdatert oversikten.

I intervju har enhetsledere som behandler personopplysninger gitt utrykk for at de er klar over hvilke opplysninger de behandler. De fleste enhetene hadde rutiner for trygg lagring av opplysningene. En enhet lagret sensitiv informasjon i et manuelt arkiv som ikke var innelåst. Her var de i gang med å endre rutinene.

Kommunen har flere applikasjoner[2] som de benytter i sin saksbehandling som inneholder opplysninger som ikke kan gjøres offentlig. I noen applikasjoner ligger det også sensitive personopplysninger.[3] Kommunen har laget en oversikt over hvilke servere og applikasjoner kommunen benytter[4]. Oversikten er sortert etter hvem som drifter dem og hvor serverne er plassert.

Lardal kommune bruker sakarkivet Websak og følger 12K's rutiner for arkiv.12K er et interkommunalt samarbeid mellom 12 kommuner i Vestfold, som blant annet har til målsetning å utvikle, forbedre og effektivisere kommunenes tjenestetilbud. Websak driftes av Nøtterøy kommune. Rådmannen, stabsleder, administrator, arkivansvarlig og sekretær i postmottaket har tilgang til alt i Websak. Ellers gis det tilgang til de mappene den enkelte har behov for i sitt arbeid. Skole og barnehager har ikke eget fagsystem, men oppretter henholdsvis elevmapper og barnemapper i Websak. Disse mappene har høyeste gradering. I tillegg til de nevnte, har rektor, sekretær og rådgiver for skole tilgang til elev- og barnemappene.

Vi har ikke sett at kommunen har faste rutiner for å oppfylle meldeplikt og konsesjonsplikt til Datatilsynet. Det ble sendt melding i november 2009 angående registrering av sensitive personopplysninger om ansatte i lønnssystemet. For behandlinger i Websak er det ikke sendt melding. For behandling av personopplysninger i forhold til helseregisterloven er det ikke sendt melding siden 2002. Skolen har vurdert at de ikke har meldeplikt for den type opplysninger de registrerer.

Det foreligger skriftlige avtaler med Itum Drift as basert på standardavtale fra IKT Norge og Nøtterøy kommune basert på standardavtale fra Statskonsult (som nå heter Difi). Itum Drift as drifter Agresso (lønns- og regnskapsprogrammet), hele nettverket med sikre og usikre soner og brannmurene. Nøtterøy kommune som drifter Exchange (e-post) og Websak (arkivsystemet). Vi har gjennomgått avtalene om Agresso og Exchange. Avtalen om Agresso er fra 2004. Avtalen om Exchange er fra 2008. Avtalene er tilpasset ved at deler av kontraktene som ikke passer er utelatt eller deler er lagt til. I avtalen om Exchange er det lagt til at kravene i personopplysningsloven § 13 og § 15 skal følges av leverandøren. Avtalene inneholder punkter om fordeling av ansvar. I avtalen om Exchange er dette spesifisert i vedlegg med leverandørens kravspesifikasjon. I avtalen om Agresso er dette spesifisert i veldegg om organisasjon. Avtalene inneholder krav om at ansatte hos leverandørene skal undertegne taushetserklæringer. Avtalen om Agresso inneholder en vid definisjon av hva som skal holdes konfidensielt.

Ved problemer med egne servere har kommunen muntlig avtale med et lokalt firma. Kommunen har innhentet skriftlige taushetserklæringer fra det lokale firmaet.

Det foreligger ikke en skriftlig avtale angående samarbeidet med Andebu kommune om drift av Webserver (hjemmeside, intranett).

Nøtterøy kommunes og Lardal kommunes nettverk er koblet sammen. Nøtterøy har tilgang inn i den usikre sonen i Lardal kommune, men ikke til sikker sone. Itum Drift as drifter både det sikre og usikre nettverket og brannmurene. De har derfor full tilgang til Lardal kommunes

[2] Applikasjon er en programvare.
[3] Se vedlegg 3 for definisjon på sensitive opplysninger.
[4] Se vedlegg 2.

systemer. Prosys har ikke tilgang til Lardal kommunes systemer. Ved behov vil de få midlertidig tilgang som IKT-konsulenten overvåker.

4.3 Revisors vurderinger

Oversikten over personopplysninger bør oppdateres, og det bør utarbeides skriftlige rutiner for å overholde melde- og konsesjonsplikten. Den bør også inkludere manuelle arkiver.

Bruk av standardavtaler er som regel et godt grunnlag for en god kontrakt. Her er det meste innarbeidet, slik at det er mulig å inngå avtaler som ivaretar de fleste hensyn, og som kan tilpasses avtalepartenes behov. At avtalene faktisk er tilpasset, viser at administrasjonen bevisst jobbet med avtalen, og vurderte hva som burde legges vekt på. Vi vil peke på at løpende avtaler bør utlyses jevnlig i samsvar med reglene om offentlige anskaffelser.

Alle driftsavtaler bør være skriftlige. Å bare ha skriftlige taushetserklæringer er et absolutt minimum. Løpende avtaler uten tidsbegrensning eller avtaler som løper for lenge uten konkurranse kan være ulovlige direkteanskaffelser etter regelverket om offentlige anskaffelser.

5 Virksomhetens organisering og etablerte sikkerhetstiltak

5.1 Revisjonskriterier

Med bakgrunn i utredningen i vedlegg 5 blir revisjonskriteriene slik:

- Det bør være klare ansvars- og myndighetsforhold i kommunen.
- Det bør være arbeidsdeling som ledd i internkontrollen og for å redusere sårbarhet ved sykdom eller annet fravær.
- Kommunen bør sikre at personalet har tilstrekkelig kompetanse.
- Det skal være skriftlige sikkerhetstiltak som sikrer en god IT-sikkerhet.

5.2 Fakta og funn

5.2.1 Organisering

I Lardal kommune er det IKT-konsulenten som er ansvarlig for å utføre oppgavene knyttet til IT-systemene. IKT-konsulenten rapporterer til stabssjefen, som igjen rapporterer til rådmann. Det er rådmannen som har det overordnede ansvaret. Kommunen har en periode vært uten IKT-konsulent, ny IKT-konsulent startet i stillingen fra 1.juli 2010.

Lardal kommune har ikke personvernombud.

Delegering av ansvar følger ansvarshierarkiet i kommunen og er naturlig fordelt etter hvilke oppgaver de ansatte har i hverdagen. Med unntak for melde- og konsesjonsplikt, har alle vi intervjuet vært klar over sitt ansvar og hvilken myndighet de har blitt delegert i følge delegasjonsreglementet. Det var klart for alle vi intervjuet hvem som i praksis skulle gjennomføre ulike oppgaver med systemene, også i perioden kommunen ikke hadde IKT-konsulent.

5.2.2 Tilgangskontroll

Vanlige brukere har PC og logger seg inn på kommunens server med personlig brukernavn og passord, men da bare til usikker sone.

Kommunen har installert en Citrix terminalserver som står i sikker sone. Det er bare denne maskinen som kan kjøre applikasjoner som er definert som sikre. De maskinene som kobler seg til en Citrix terminalserver må ha en ICA klient installert på maskinen for å komme inn på en Citrix terminalserver. En ICA er et program som brukes for å koble opp mot en terminalserver slik at man kan bruke de programmene som ligger på serveren som om de var installert lokalt på maskinen. Brukerne som skal inn i sikker sone logger seg også inn med brukernavn og passord, og merker i det daglige ikke at deres oppkobling er annerledes.

IKT konsulenten vurderer hvilken autorisasjonstilgang den enkelte medarbeider skal ha og har ansvar for at tilgangen tilpasses stillingen. Det er normalt faste tilganger som følger med en stilling. Ved endring av arbeidsoppgaver er det rutine å endre tilgangen etter behov. Kommunen har det ikke gode nok rutiner for melding til IKT-konsulenten når noen slutter. Kommunen opplyser at dette sjelden har vært et praktisk problem i Lardal kommune, siden Lardal er en liten kommune og IKT-konsulenten raskt fanger opp slike endringer. Det er ikke vanlig å gjøre noe med tilgang ved permisjoner. Dette regnes som lite aktuell problemstilling, siden personalet i skolene og barnehagene ikke har tilgang til kommunens felles system, og ved staben, sykehjemmet og Ringveien helsesenter må personalet være fysisk tilstede for å logge seg på.

Det normale er at hver medarbeider har hver sin tilgang, med eget brukernavn og passord. Ved Ringveien helsesenter og Lardal sykehjem er det flere brukere som har samme brukernavn med faste passord for å logge seg inn i usikker sone. Fra denne usikre sonen har brukerne tilgang til Word og kommunens mapper med dokumenter som ligger i sikker sone. Tilgangen til fagapplikasjonen Prosys i sikker sone er beskrevet under.

Websak
Websak er kommunens arkivsystem. All inngående og utgående korrespondanse og alle kommunens dokumenter skal arkiveres i Websak. IKT-konsulenten gir nye brukere tilgang til Websak etter bestilling fra systemansvarlig. Systemansvarlig angir brukertilgangene inne i Websak og tildeler brukernavn og passord. Alle som mottar post skal i utgangspunktet ha tilgang til Websak. Det blir gitt tilganger i Websak etter hvilket nivå den enkelte ansatte skal kunne arbeide i. Rådmann, stabsleder, administrator, arkivansvarlig og sekretær i postmottak har tilgang til alt i Websak. Stabsleder har denne tilgangen fordi hun er rådmannens stedfortreder. Arkivsansvarlig og sekretær har behov for denne tilgangen for å lage/avslutte mapper i systemet når de registrerer/journalfører post. I Websak ligger en oversikt over hvem som her tilgang og med hvilket nivå. Når en person slutter, blir brukertilgangen gjort inaktiv.

Agresso og Basware
Agresso er kommunens lønns- og regnskapssystem og Basware er et program for å behandle fakturaer. IKT-konsulenten gir nye brukere tilgang til programmene etter bestilling fra systemansvarlig. Systemansvarlig og medarbeidere på økonomiavdelingen har myndighet til å tildele brukernavn og passord i Agresso og Basware. Økonomiavdelingen definerer behovet for hva den nyansatte trenger tilgang til. I Agresso ligger en oversikt over hvem som til enhver tid har tilgang. Oversikten viser også brukernavn og hvor lenge tilgangen varer.

Økonomiavdelingen har nylig utarbeidet en oversikt for å klassifisere brukertilgangene. Dette skal brukes til å vurdere i hvilken grad en ansatt skal ha direkte tilgang der man kommuniserer direkte med applikasjonene eller et web-basert system som gjør at en ansatt får tilgang til mer forhåndsdefinerte områder i Agresso. Dette er økonomisk motivert, fordi web-basert tjeneste er vesentlig billigere enn den vanlige direkte tilgangen. Kommunen ønsker derfor at flest mulig skal være web-basert. Da får de ansatte bare se den delen de skal bruke, for eksempel lønn eller rapporter, dermed får de heller ikke gått inn og gjort endringer på områder som ikke er relevante for deres arbeid.

Når brukere slutter i jobben blir de slettet /gjort inaktive i systemet. Det er ingen god rutine for å gi beskjed når arbeidsforholdet avsluttes, men økonomiavdelingen ser det i lønnssystemet, og mener at det fanges raskt opp i en liten kommune.

Prosys
Lardal sykehjem, hjemmetjenestene og psykiatri bruker fagsystemet Prosys. IKT-konsulenten legger Prosys inn hos de brukerne som har behov for det. Systemansvarlig for Prosys tildeler individuelle brukernavn og passord for ansatte ved sykehjemmet og helsesenteret til systemet i samsvar med kvalitetshåndboka. En medarbeider med tilgang på nivå 1 får bare tilgang til de avdelingene de jobber ved. Medarbeidere med tilgang på nivå 5 får tilgang til alle avdelingene. I Prosys ligger en oversikt over hvem som har tilgang med hvilket nivå.

Skolene
Rektor gir tilganger til lærernes og elevenes nettverk og Fronter[5]. Rektor vurderer hvilket sikkerhetsnivå elever og ansatte trenger, og hvilke passord som må endres jevnlig. I systemene ligger det oversikter over hvem som til enhver tid har tilgang. Rektor har en årlig gjennomgang av hvem som har tilgang til systemene. Ved permisjoner gjøres det ikke endringer.

5.2.3 Fysisk sikring

Herredshuset
Servicetorget er plassert slik at alle besøkende på herredshuset i Lardal ser skranken med skiltet over. Servicetorget er alltid bemannet og det er naturlig å henvende seg der først. De som jobber på servicetorget tar aktivt kontakt med besøkende som eventuelt ikke kommer direkte til skranken. De øvrige i teamet som har kontorer i tilknytning til skranken og som fra tid til annen har ansvar for å betjene servicetorget, møter besøkende så fort de kommer inn. Ytterdøra er låst utenom åpningstidene til kommunen.

Kommunen har ingen rutiner på å låse dørene til kontorene når de ikke er tilstede. Enhetsledere, rådmann og IKT-konsulenten har bærbare pc-er. Tre i staben har bærbare pc-er, resten i staben har faste pc-er inne på sine kontorer.

Serverne til kommunen er plassert i et eget avlåst rom.

Økonomiavdelingen har to bærbare pc-er. Den ene bærbare pc-en brukes mest når noe skal vises felles på projektor på kontoret, og til Excell og Word. Den ene rådgiveren har bærbar pc i stedet for en stasjonær pc. Alle opplysninger ligger normalt lagret i Agresso eller Basware, men han har anledning til å hente ut opplysninger og lagre dem på pc-en. Hva som lagres på

[5] Et nettbasert plattform for skoler, som tilbyr ulike verktøy slik at lærere og elever kan kommunisere digitalt, lagre arbeid og levere oppgaver.

pc-en har ikke vært diskutert i økonomiavdelingen, utover det som ligger i det etiske regelverket og taushetsplikten.

På herredshuset i Lardal er det to skrivere som begge er tilgjengelige for alle i administrasjonen. Det er forhåndsbestemt at utskriften kommer til den nærmeste skriveren, men man kan velge den andre skriveren ved behov. Utskriften ligger på skriveren til den som har skrevet den ut henter den.

Ringveien helsesenter
På Ringveien har enhetsleder, saksbehandler, psykiatrisk sykepleier og vernepleier egne kontorer med egne stasjonære pc-er. Disse kontorene blir låst når personene ikke er til stede. Hjemmetjenestene har et felles kontor, med to pc-er. Dette blir låst hvis ingen er til stede. Etter arbeidstid blir hovedinngangen låst, og døra inn til kontorene blir låst. Da bruker hjemmetjenesten bakdøra, for å komme inn på sine kontorer.

Saksbehandler har egen skriver på sitt kontor. Ellers er det felles skriver inne på et rom nederst i gangen, rett over gangen for hjemmetjenesten.

Sykehjemmet
Dementavdelingene har et felles kontor med en pc. Somatisk- og rehabiliteringsavdelingene har et felles kontor med en pc, og i tillegg har de en pc på det ene kontoret, som ikke er koblet mot kommunens server. Pleierne forsøker å lukke døra inn til kontorene når de ikke er der. Den blir ikke låst. Det er alltid pleiere i nærheten.

Kjøkkenet har egen pc på kontor ved siden av kjøkkenet. Kjøkkenet er alltid åpent, og døra mellom kjøkkenet og kontoret har vrideren på låsen mot kjøkkenet, så selv om døra fra kontoret og ut på gangen låses, vil kontoret aldri kunne låses av.

Enhetsleder har eget kontor med pc. Dette låses når det ikke er i bruk.

Skriveren står inne på et eget rom i gangen mellom avdelingene. Døra pleier å være lukket igjen, men ikke låst.

Skole og barnehage
Skolen har skrivere plassert mange steder på skolen. Alle kan fritt velge hvilken skriver de vil skrive ut på. Det er en fast skriver som skal brukes når det tas utskrifter med sensitiv informasjon, men det er fritt valg av skriver.

I barnehagene er pc-er og printere plassert inne på styrers kontor.

5.2.4 Arbeidsdeling og kompetanse

I Lardal kommune er det vanlig at ansatte har flere ansvarsområder, de har sjelden mulighet til å gi flere samme arbeidsoppgave for å øke kompetansen i organisasjonen. Det er ofte bare en person som sitter med en gitt kompetanse. Da IKT-konsulenten sluttet, måtte de klare seg uten denne kompetanse noen måneder inntil de ansatte en ny IKT-konsulent. Den avgåtte IKT-konsulenten stilte seg til rådighet for kommunen i denne perioden, slik at administrasjonen kunne bruke ham i spesielle situasjoner. Administrasjonen utnevnte en kontaktperson som alle medarbeidere kunne kontakte ved IT-problemer. Hun løste det hun klarte selv, og vurderte når de måtte tilkalle ekstern hjelp.

De systemansvarlige er ansvarlige for sine systemer, og at IKT-konsulenten utfører oppgaver i systemet på deres initiativ. Tildeling av tilgang til systemene er fordelt ved at IKT-konsulenten oppretter brukere og gir dem tilgang til de ulike fagsystemene. Systemansvarlig tildeler brukernavn og passord i fagsystemene. Dermed er risikoen mindre for at feil person får feil tilganger.

Enhetsledere og systemansvarlige vi intervjuet vurderte oftest egen kompetanse som tilfredsstillende i forhold til sitt behov. De vet hvor de skal spørre hvis de trenger hjelp, og er fornøyd med den støtten de får.

IKT-konsulenten har ansvar for opplæring av nytilsatte innen IT-sikkerhet. Systemansvarlige har ansvar for opplæring av nytilsatte og ved behov i bruk av deres system. Staben får kontor- og datasikkerhetsopplæring etter behov.

Lærerne får kurs på skolen i nødvendige applikasjoner. Alle nyansatte ved skolen får en mentor som hjelper dem. Alminnelige prosedyrer blir gjennomgått på første planleggingsdag hver høst. Da blir det også vist til skolens retningslinjer for bruk av skolen datasystemer, selv om de ikke har tid til å gå grundig gjennom disse. To ganger i året skriver lærerne halvårsrapporter om arbeidet med elever med spesialpedagogiske behov. I forbindelse med dette arbeidet blir det minnet om hvordan sensitive personopplysninger skal behandles, særlig før jul. Elevene får opplæring i samsvar med en fagplan for IKT.

Ved Ringveien helsesenter og Lardal sykehjem får nyansatte opplæring i bruk av Prosys av kolleger. En sykepleier på hjemmesykepleien, som tidligere jobbet på sykehjemmet, er Prosys-kontakt og ansvarlig for at Prosys er oppdatert. Hvis sykepleierne lurer på noe, kontakter de enten Prosys-kontakten eller merkantil. Prosys blir stadig oppdatert, men personalet på sykehjemmet har ikke fått opplæring i å bruke de nye mulighetene som Prosys byr på. Dette gjelder også løsninger som er utviklet for å hjelpe sykehjemmet å følge nye krav i lover, forskrifter og retningslinjer, for eksempel krav om oppfølging av beboernes ernæring.

5.2.5 Sikkerhetskopiering

IKT-konsulenten er ansvarlig for sikkerhetskopieringen. IKT-konsulenten bytter tape daglig i samsvar med skjema på servere rom og kontrollerer at sikkerhetskopien er i orden. Tapene oppbevares i brannsikker safe. Hver 10 dag har IKT-konsulenten rutine på teste at sikkerhetskopiene er i orden ved å gjenopprette tilfeldig valgte filer. En fast saksbehandler bytter tape de dagene IKT-konsulenten ikke har anledning.

5.2.6 Installering og oppgradering av programvare

Alle kan installere programvare på de datamaskinene de bruker i usikker sone, men ikke i sikker sone.

IKT-konsulenten gjør generelle oppgraderinger av Lardal kommunes systemer og utstyr, ofte i samarbeid med eksterne leverandører. Rutinene for oppgraderinger av programmer er todelt. Agresso og Websak oppgraderes av de eksterne leverandørene som drifter programmene. For Prosys gjør IKT-konsulenten oppgraderinger på initiativ fra systemansvarlig.

5.2.7 Virus

Alle pc-ene har installert antivirusprogram som oppdateres via internett. Lardal kommune har ikke et sentralt overvåkningsverktøy som rapporterer om antivirus programmet feiler på en eller flere pc-er.

5.2.8 Rutiner

Selv om kommunen ikke har skriftlige rutiner på området er alle vi har intervjuet bevisst på hvordan personopplysninger bør behandles, både internt mellom ansatte og ut av kommunen. Dette gjelder spesielt de som behandler sensitiv informasjon.

Sensitiv informasjon om pasienter/klienter som skal formidles mellom enhetene skjer via post eller muntlig beskjed. Sensitiv informasjon blir ikke sendt ut via e-post, men ansatte har opplevd at pårørende/foresatte har sendt sensitiv informasjon via e-post til dem.

Man unngår å låne passord av hverandre. I spesiell situasjoner er det likevel behov for å låne passord. Da skal den som låner ut passordet sitt bytte passord så snart det ikke er behov for å låne det ut lenger.

På skolen jobber lærerne på bærbare pc-er. Der skal dokumenter med personopplysninger lagres på server og ikke på maskinens harddisk. Skolen vil innføre bruk av tynne klienter[6] for lærerne, slik at de ikke ved en misforståelse lagrer personopplysninger på den bærbare pc-ens harddisk.

Minnepinner brukes i liten grad. De brukes mest til å lagre presentasjoner, og aldri til sensitive opplysninger.

Sykehjemmet har rutine for at dokumenter med personopplysninger som lages utenfor Prosys, skal lagres slik at sykepleierne må ha passord for å åpne dokumentet igjen. I forbindelse med datainnsamlingen oppdaget revisjonen at dokumenter med personopplysninger ikke ble lagret i tråd med enhetens rutiner. Vi vet ikke noe om hvor vanlig denne rutinesvikten er, fordi vi oppdaget den tilfeldig på én maskin.

5.3 Revisors vurderinger

Administrasjonen i Lardal blir sårbar fordi de er så få personer, slik at det ofte er bare en person som sitter med en gitt kompetanse. Da IKT-konsulenten sluttet, måtte de klare seg uten denne kompetansen noen måneder.

Fordelen med en så liten organisasjon er den klare fordelingen av ansvar og roller. Kommunen bør etterstrebe at minst to bytter på å gjøre en arbeidsoppgave, slik at kommunen ikke blir avhengig av én persons kompetanse. Vi har inntrykk av at Lardal kommune har fleksible medarbeidere, som kan ta på seg koordineringen av oppgaver utenfor deres daglige ansvars- og kompetanseområde.

Lardal kommune bør vurdere om det er aktuelt å ha et personvernombud.

For å gi nye medarbeidere tilgang til programvare har Lardal en god arbeidsdeling der IKT-konsulenten legger programmene inn hos den aktuelle brukeren, og systemansvarlig gir

[6] Ved bruk av tynne klienter kjøres all programvare fra en sentral server, dokumentene som lages på en tynn klient vil bli lagret på serveren og ikke på lærerens pc.

brukernavn og passord. Dermed reduseres risikoen for at feil personer får tilgang. Alle som har tilgang til kommunens systemer bør ha individuelle brukernavn og passord.

Lardal kommune bør forbedre kontrollen med utskrifter fra sikker sone. Det bør ikke ligge utskrifter på skriveren med sensitiv informasjon slik at andre kan rekke å se den før utskriften blir hentet.

Det er ulik praksis for fysisk sikring av rom med tilgang på personopplysninger. Kommunen bør vurdere å innføre generelle rutiner for låsing av rom når personalet ikke er tilstede, og det bør legges fysisk til rette for at rom der det oppbevares personopplysninger kan låses. Sykehjemmet bør ha en egen vurdering av behovet for å låse dører.

Sykehjemmet gir inntrykk av liten satsing på IT-kompetanse. Når personalet ikke bruker rutiner for lagring av dokumenter, tyder det på liten forståelse for verdien av rutinen som igjen kan bunne i for liten kompetanse. Kommunen bør vurdere personalets behov for økt kompetanse både på generell bruk av pc og på fagsystemet. Personalet vil kunne utnytte mulighetene som ligger i verktøyet på en bedre måte. Økt kunnskap kan motivere til å bruke og videreutvikle de gode rutinene.

6 Revisors konklusjoner og anbefalinger

Generelle konklusjoner
Det bør gjennomføres en risikovurdering, og dokumentene om informasjonssikkerhet bør oppdateres til dagens organisasjon, tekniske situasjon og risikovurderinger. Oversikten over hva slags opplysninger kommunen behandler bør oppdateres. Kommunen bør lage rutiner for å overholde melde- og konsesjonsplikten. Dokumentene og rutinene bør gjøres levende i administrasjonen. Kommunen bør vurdere å ha et personvernombud.

Det bør være skriftlige avtaler med alle leverandører. Standardavtaler sikrer ofte klare ansvarsforhold og rettigheter.

Kommunen bør vurdere å ha et personvernombud.

Kommunen bør vurdere å innføre generelle rutiner for låsing av kontorer når personalet ikke er tilstede.

Det bør innføres et system for utskrifter fra sikker sone, slik at utskriften ikke skrives ut før rette person står ved skriveren.

Konklusjoner angående Lardal sykehjem
Alle bør ha individuelle brukernavn og passord.

Dørene inn til kontorer der det oppbevares dokumenter eller pc-er med sensitiv informasjon bør låses. Rommet med skriver bør låses, eller det bør være et system som nevnt i avsnittet før.

Brukerpermen for Prosys bør oppdateres og være et levende dokument for sykehjemmet.

Kommunen bør vurdere behovet for å øke personalets kompetanse på bruk av IT.

Litteratur og kildereferanser

Lover og forskrifter:
Lov 25. september 1992 nr. 107 om kommuner og fylkeskommuner (kommuneloven).
Forskrift 15. juni 1994 nr. 905 om revisjon i kommuner og fylkeskommuner mv.
Lov 14. april 2000 nr. 31 om behandling av personopplysninger
Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger
Lov 18. mai 2001 nr 24 om helseregistre og behandling av helseopplysninger

Bøker:
Moen, Tove-Gunn og Bjørgunn Havstein. 2005. *Regnskapsorganisasjon, bokføring og internkontroll.* Oslo: Cappelens Akademisk Forlag

Veiledere:
Datatilsynet. 2009. *En veiledning om internkontroll og informasjonssikkerhet*
Datatilsynet. 2005. *Veiledning i informasjonssikkerhet for kommuner og fylkeskommuner*
Sosial- og helsedirektoratet. 28.06.2006. *Norm for informasjonssikkerhet i helsesektoren*

Artikler
Schartum, D. W. 2000. Lov om behandling av personopplysninger, Lov og rett

Offentlige dokument:
Ot.prp. nr. 92 (1998-99): *Om lov om behandling av personopplysninger (personopplysningsloven)*

Vedlegg 1: Kommunens høringssvar

Lardal kommune
Stab- og støttefunksjon

Saksbehandler: Eivind Yttervik
Direkte telefon: 33 15 52 12
Vår ref.: 10/5255
Arkiv: FE-
Deres ref.:
Dato: 22.09.2010

Telemark kommunerevisjon IKS
Gerd Smedsrud Mikelborg

Ad. FR-rapport nr: 701004 2010 Informasjonssikkerhet Lardal kommune

Punkt 5.2.2 Tilgangskontroll. Andre linje
"På de maskinene som skal inn på sikker sone har kommunen sikret oppkoblingen ved å installere en ICA."
Kommunen har installert en Citrix terminalserver som står i sikker sone. Det er bare denne maskinen som kan kjøre applikasjoner som er definert som sikre. De maskinene som kobler seg til en Citrix terminalserver må ha en ICA klient installert på maskinen for å komme inn på en Citrix terminalserver.

Punkt 5.2.2 Tilgangskontroll. Tredje avsnitt.
Det er riktig at flere brukere logger seg inn på usikker sone med samme brukernavn og passord. Men samtlige sikre applikasjoner har individuelle brukernavn og passord. Disse brukernavnene og passordene brukes ikke om hverandre. Det er "bare" tilgangen til usikker sone som deles.

Punkt 5.2.2 Websak. Andre linje.
"IKT konsulenten gir nye brukere tilgang".
Alle brukere i Lardal kommune har tilgang til Websak applikasjonen. Men Websak applikasjonen er avhengig av eget brukernavn og passord. Det er systemansvarlig for applikasjonen som tildeler dette etter behov.

Generelt sett gir rapporten et godt bilde av dagens situasjon vedr. informasjonssikkerhet. Det er viktig å merke seg at en del av tiltakene som Telemark Kommunerevisjon synliggjør også er forbundet med kostnader. Mens andre handler om endring av rutiner og dokumentasjon.

Med hilsen

Eivind Yttervik
IKT-konsulent

Postadresse: Svarstadtunet 15, 3275 Svarstad
Besøksadresse: Lardal herredshus
E-post: post@lardal.kommune.no
Telefon: 33 16 52 00
Telefaks: 33 16 52 01
Internett: www.lardal.kommune.no
Bank: 2442.05.22815
Org.nr.: 964962434

Vedlegg 2: Begreper som benyttes i rapporten

Definisjon av personopplysninger jf. personopplysningsloven:

§ 2. *Definisjoner*

I denne loven forstås med:

1) personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson,
2) behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter,
3) personregister: registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen,
4) behandlingsansvarlig: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes,
5) databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige,
6) registrert: den som en personopplysning kan knyttes til,
7) samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv,
8) sensitive personopplysninger: opplysninger om
a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
c) helseforhold,
d) seksuelle forhold,
e) medlemskap i fagforeninger.

Vedlegg 3: Risikovurdering og sikkerhetsstrategi - revisjonskriterier[7]

Risikovurdering

Risiko kan måles på to måter: hvor sannsynlig det er at noe skjer og hva slags konsekvenser denne hendelsen kan få.

En risikovurdering skal resultere i[8]:

- oversikt over identifiserte trusler
- vurdering av hvor sannsynlig det er at en uønsket hendelse skal skje
- vurdering av konsekvenser av en uønsket hendelse
- vurdering av hva slags effekt sikkerhetstiltakene vil ha opp mot risiko

En risikovurdering skal være et styringsredskap for den som har ansvaret for informasjonssikkerheten. Gjennom arbeidet med risikovurdering bør kommunen dokumentere hva slags sikkerhetstiltak som er gjennomført og hva slags sikkerhetstiltak som bør gjennomføres. Det er virksomhetens ledelse som har ansvaret for utarbeidelse av en risikovurdering.

Risikovurdering er utgangspunktet for ethvert arbeid med å sikre sikkerheten. Det er en forutsetning for å avdekke sårbare punkt og sette i verk sikringstiltak. *Formålet med risikovurdering er å sikre at den risiko som avdekkes ved behandling av personopplysninger er innenfor de akseptkriterier virksomheten har fastlagt. Risikovurderingen danner grunnlag for iverksetting av nødvendige sikkerhetstiltak, og inngår i underlaget for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten.*[9]

Noen opplysninger i datasystemet krever særskilte sikringstiltak, som for eksempel personopplysninger. I personopplysningsloven[10] § 13, 1.ledd står det: *Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.* I personopplysningsforskriften[11] § 2-4, 2. og 5. ledd: *Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten. Resultatet av risikovurderingen skal dokumenteres.*

Personopplysingsloven inneholder regler om informasjonssikring og internkontroll. Ledelsen er ansvarlig for å etterkomme sikkerhetskravene. *Internkontrollbestemmelsen i § 14 innebærer en plikt for den behandlingsansvarlige til å vurdere om det er behov for iverksette tiltak for å oppfylle de krav til behandlingen av personopplysninger som er fastsatt i eller i medhold av lov. Tiltakene skal være* ***planlagte****, dvs. de må foreligge på forhånd, primært før behandlingen starter. Tiltakene skal videre være* ***systematiske****, noe som innebærer at de skal være resultat av en helhetlig tilnærming og ikke ha karakter av å være tilfeldige. Tiltakene skal ikke minst være* ***dokumenterte****, dvs. de må foreligge i en form som gjør det mulig å*

[7] Revisjonskriterier er en samlebetegnelse på de regler og normer som gjelder innenfor det området som undersøkes. Revisjonskriteriene er basis for de analyser og vurderinger som foretas, konklusjonene som trekkes, og de er et viktig grunnlag for å kunne dokumentere avvik eller svakheter.

[8] Datatilsynet, 2009, s. 22

[9] Datatilsynet, 2009, s 26

[10] Lov 14.04.2000 nr. 31 om behandling av personopplysninger

[11] Forskrift: 15.12.2000 nr. 1265 om behandling av personopplysninger

tilegne seg kunnskap om dem (skrift, tegning, bilder m.v.).[12] Det samme gjelder i henhold til helseregisterloven.[13] Personopplysningsforskriftens kapittel 3 beskriver nærmere hva internkontrollen skal omfatte.

I faktaark 7[14] heter det; *Virksomhetens ledelse er ansvarlig for å gjennomføre risikovurdering av behandling av helse- og personopplysninger. Risikovurdering skal gjennomføres før behandling av helse- og personopplysninger startes, og ved endringer av behandlinger som kan påvirke sikkerheten.* I dette faktaarket finner vi blant annet anbefalinger om hvordan risikovurdering av personopplysninger bør gjennomføres. Se vedlegg 4 for eksempel på skjema for risikovurdering.

Sikkerhetsrevisjon og strategidokument
I personopplysningsforskriften § 2-5, 1. og 2.ledd står det:
Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Og i 5.ledd: *Resultatet av sikkerhetsrevisjon skal dokumenteres.* Ledelsen har ansvaret for at det gjennomføres sikkerhetsrevisjon hvert år.

Formålet med sikkerhetsrevisjon er å sikre at vedtatte sikkerhetsmål, -strategier og organisering blir fulgt. Resultatet av revisjonen danner grunnlaget for eventuelle endringer. Valg og prioriteringer i sikkerhetsarbeidet skal komme fram i et strategidokument.

Kravet til kommunen om utarbeidelse av skriftlige strategidokument finner vi i personopplysningsforskriften § 2-3, 2. og 3.ledd:
Formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål. Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi. Sikkerhetsmålene skal blant annet vise overordnede krav til konfidensialitet, integritet og tilgjengelighet for personopplysninger. Sikkerhetsmålene skal ta utgangspunkt i lovpålagte krav til informasjonssikkerhet.

Med bakgrunn i denne utredningen blir revisjonskriteriene slik:

- Kommunen skal dokumentere at det er utført en systematisk risikovurdering.
- Risikovurderingen bør beskrive risiko som er avdekket og sammenlikne dette med det som er definert som akseptabelt risikonivå.
- Kommunen skal ha utarbeidet et overordnet dokument for sin sikkerhetsstrategi, med bakgrunn i disse vurderingene.

[12] Schartum, D.W. 2000. Lov om behandling av personopplysninger, *Lov og* rett, s 554
[13] Lov 18.05.2001 nr 24 om helseregistre og behandling av helseopplysninger, kapittel 3.
[14] Sosial- og helsedirektoratet, 28.06.2006. *Norm for informasjonssikkerhet i helsesektoren*

Vedlegg 4: Dokumentasjon om informasjonssystemene - revisjonskriterier

Hvilke lover som er relevante er avhengig av hva slags informasjon som skal behandles av det aktuelle informasjonssystemet. Personopplysninger skal behandles i samsvar med personopplysningsloven og eventuelt helseregisterloven. I forskrift om behandling av personopplysninger § 2-4, 1. ledd, 1.setning står det: *Det skal føres oversikt over hva slags personopplysninger som behandles.*

Om kommunen trenger konsesjon på forskjellige elektroniske personopplysningsregister må vurderes i hvert enkelt tilfelle. Noen elektroniske register kan opprettes med hjemmel i lov, for eksempel sosialtjenesteloven og kommunehelsetjenesteloven. Kommunen har meldeplikt til Datatilsynet når kommunen oppretter et elektronisk register med hjemmel i lov, hvis det ikke eksplisitt er gitt fritak for dette. Etter forskrift om behandling av personopplysninger § 3-1, 3.ledd bokstav f, skal kommunen ha rutiner for oppfyllelse av sine plikter i forbindelse med personopplysningslovens regler om melde- og konsesjonsplikt. Etter § 3-1 andre ledd plikter kommunen å ha tilstrekkelig og oppdatert dokumentasjon for gjennomføring av slike rutiner, samt ha denne dokumentasjonen tilgjengelig for de den måtte angå.

Når kommunen benytter hjelp fra en tredjepart, for eksempel en konsulent eller underleverandør, bør det være en skriftlig avtale som klart definerer ansvar/rettigheter. Det bør også være en tilgangskontroll som gjør at tredjepart bare får de tilgangene som trengs i en avgrenset periode og krav om at leverandøren personell undertegner taushetserklæring.[15]

Med bakgrunn i denne utredningen blir revisjonskriteriene slik:

- Kommunen skal ha dokumentasjon som viser en oversikt over hva slags opplysninger som blir behandlet i de forskjellige datasystemene, og hvilke lover som er knyttet til opplysningene.
- Kommunen skal ha dokumenterte rutiner som sikrer at det søkes konsesjon eller sendes melding til Datatilsynet for behandling av de opplysningene som kan finnes i datasystemet.
- Det skal være skriftlige avtaler med underleverandører, med klart definerte ansvars- og rettighetsforhold

[15] Datatilsynet, 2009, s. 41.

Vedlegg 5: Virksomhetens organisering - revisjonskriterier

Hva som er kommunens politikk for informasjonssikkerhet bør være kjent for alle ansatte i kommunen. Kommunen bør utarbeide klare retningslinjer for informasjonssikkerhet. Behandling av personopplysninger er for kommuner regulert i personopplysningsloven og helseregisterlova. Personopplysningsloven § 13 og helseregisterlova § 16 stiller krav til sikring av personopplysninger og krav til dokumentert internkontroll. Den som har ansvaret for behandling av opplysningene er normalt representert ved administrativ ledelse. Ansvaret innebærer og at det settes av tilstrekkelige ressurser, både med tanke på personell og økonomi, slik at tilfredsstillende informasjonssikkerhet blir opprettholdt. Samarbeid mellom parter og leie av personell som utfører oppgaver kommunen ikke kan utføre selv, bør være regulert i en avtale.

Informasjonssystemet skal[16] benyttes i samsvar med faste rutiner. I den grad det er nødvendig for å oppnå tilfredsstillende informasjonssikkerhet, skal det være skriftlige rutiner for bruk, drift og vedlikehold av utstyr eller program. Dette for å sikre at alle aktiviteter som er viktige for sikkerheten gjennomføres og at arbeidsoppgavene blir utført likt hver gang. Rutinene skal ha en detaljeringsgrad som er tilpasset kommunens behov og skal vise:

- ansvar for at arbeidsoppgaven blir utført
- ansvar for utarbeidelse og vedlikehold av rutinen
- tidspunkt for utføring av arbeidsoppgaven
- hva slags aktivitet som skal gjennomføres
- hva slags resultat en skal oppnå og hvordan dette blir rapportert i organisasjonen

Organisering

Kommunen må etablere klare ansvars- og myndighetsforhold slik at det kommer klart fram hvem som har fått delegert oppgavene.[17] Dette bør være dokumentert slik at de ansatte kjenner og følger faste rutiner for bruk av informasjonssystemet, og gjennomføring av de sikkerhetstiltakene ansatte selv er ansvarlig for. Samme gjelder også for ansatte og personell som er leid inn for å utføre drift og vedlikehold, dvs. at de utfører arbeidet i samsvar med faste rutiner. Ansvaret for utarbeidelse av rutiner kan delegeres til den som er best kjent med arbeidsoppgavene.

I følge datatilsynet[18], kan eksempler på organisatoriske tiltak være å etablere klare ansvars- og myndighetsforhold i organisasjonen, sørge for tilfredsstillende kompetanse blant de ansatte, og bare gi tilgang til personopplysninger i den grad det er nødvendig for å utføre pålagte oppgaver. *Brukerne bør få opplæring i sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle sikkerhetsrisikoer.*[19]

Arbeidsdeling er et av de viktigste tiltakene en kan gjøre for å motvirke mislighold.[20] Det er og viktig å ha klare ansvarslinjer, slik at alle ledere og medarbeidere vet hvem som har ansvaret for de forskjellige funksjonene.

[16] Avsnittet er basert på: Datatilsynet, 2005, s. 37-39
[17] Personopplysningsforskriften § 2-7
[18] Ot.prp.nr. 92 (1998-1999) om behandling av personopplysninger kapittel 2 – Til § 13 Informasjonssikkerhet
[19] Datatilsynet, 2009, s. 39
[20] Moen og Havstein, s. 85

Sikkerhetstiltak
Det bør være etablerte rutiner for tilgangskontroll, sikkerhetskopiering og avviksbehandling. Det bør være krav til kompetanse hos de som arbeider med IT i kommunen. Det bør videre være rutiner for vedlikehold og for oppdatering av programvare.

I personopplysningsforskriften § 2-14 og § 2-16 står det:
Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Forsøk på uautorisert bruk av informasjonssystemet skal registreres. Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være avgrenset til handlinger som den enkelte forutsettes å utføre. Sikkerhetstiltak skal dokumenteres. Rutiner for bruk av informasjonssystemet og annen informasjon av betydning for informasjonssikkerheten, skal dokumenteres.

Datatilsynets anbefaler at det konfigureres soner og sikkerhetsbarrierer. Følgende avsnitt er hentet fra rettledningen[21]:
Soner benyttes som et grunnleggende prinsipp i sikkerhetsarkitekturen. En sone er de deler av et informasjonssystem som tillates å kommunisere ved datakommunikasjon. Soner opprettes etter analyse av behovet for tilgang og datakommunikasjon. For å begrense tilgangen til personopplysninger benyttes følgende soner internt i en virksomhet:

- *Sikret sone hvor sensitive personopplysninger behandles (ved behov opprettes flere sikrede soner i virksomheten). Den enkelte sikrede sone er sikkerhetsmessig avskilt fra resten av det interne nettverk og eventuelle andre sikrede soner, foruten mot eksterne nettverk.*
- *Intern sone hvor ikke sensitive personopplysninger behandles, denne kan også omfatte andre opplysninger i virksomheten som ikke skal eksponeres eksternt.*

Det skal ikke være mulig for medarbeidere å endre konfigurasjonen uten autorisasjon. Dette skal være dokumentert. Det bør være en hensiktsmessig delegering av ansvaret for sikkerheten, inkludert tilgangskontroll, overvåking, opplæring mm. Brukerne bør tildeles tilgang etter behov.

Personvernombud
Personvernombud er en frivillig ordning etter personvernloven § 7-12. Personvernombudet skal *sikre at den behandlingsansvarlige følger personopplysningsloven med forskrift.*[22] Personvernombudet får tilbud om opplæring fra Datatilsynet om behandling av personopplysninger. Han eller hun blir en rådgiver for kommunen på området, en publikum kan kontakte ved behov og en kontaktperson for Datatilsynet. Et personvernombud skal føre en oversikt over hvilke behandlinger kommunen gjør med personopplysninger. Kommunen får fritak fra meldeplikten til Datatilsynet. Hvis kommunen ønsker å ha et personvernombud, må de finne en person som er motivert for oppgaven og søke Datatilsynet. Siden dette er en frivillig ordning, kommer dette ikke som et punkt under oppsummeringen av revisjonskriteriene.

[21] Datatilsynet, 2005, s. 25

[22] Personvernloven § 7-12

Med bakgrunn i denne utredningen blir revisjonskriteriene slik:

- Det bør være klare ansvars- og myndighetsforhold i kommunen.
- Det bør være en arbeidsdeling som sikrer tilfredsstillende kompetanse hos de ansatte og mindre sårbarhet ved sykdom eller annet fravær.
- Det skal være skriftlige sikkerhetstiltak som sikrer en god IT-sikkerhet.

Vedlegg 6: Liste over servere og applikasjoner

(utdrag fra større dokument ang IKT i Lardal kommune):

Applikasjoner som driftes utenfor huset

BVPro = Barnevern applikasjon (Itum)
Agresso = Faktura/lønn (Itum)
Websak = Sakarkiv (Nøtterøy kommune)
Exchange server = E-post (Nøtterøy kommune)
Webserver = Hjemmeside/Intranett (Andebu kommune)

Applikasjoner som driftes i huset

Prosys - Pasient register
Shiftmanager - Time registrering
Office 2003 - Tekstbehandling, regneark osv.
Socio - Sosial applikasjon
Matrikel - Kart
Well communicator - Blodprøver
Winmed - Sykemeldinger og henvisninger
Backup - Sikkerhetskopi
Aspire - Telefonsystem

Servere som driftes i huset

5dcs01 – Fil og print server
5sql01 – Shiftmanager / Oracel database
5app01 – Kart applikasjon / SQL server
6dcs01 – Domenekontroller
Sos02 – Prosys og Socio, fil og print sikker sone
Sosi022 – Terminal server pålogging sikker sone

Servere som står utenfor men som vi har ansvar for

5dcs02 – Står hos Nøtterøy Kommune (Kopi av domenekontroller)
Legeserver – Legekontor

Nettverk som driftes av Lardal kommune

Admin/intern sone
Lukket/sikker sone
Telefon Voip
Trådløst
Skolenett (driftes stort sett av skolene)
Helsenett (legekontor)
Bibliotek

Vedlegg 7: Eksempel på oppbygging av skjema for risikovurdering

Eksempel på oppbygging av skjema for risikovurdering

Forklaring til koder i skjema for risikovurdering

Brudd på nivå for akseptabel risiko:		K = Konfidensialitet		I = Integritet		T = Tilgjengelighet		
Sannsynlighet: (Angitt som antall pr. år)	1	Usannsynlig <=1/5 (En gang hvert 5. år eller sjeldnere)	2	Mindre sannsynlig 1/1 (En gang hvert år)	3	Mulig 12/1 (En gang hver måned)	4	Sannsynlig >= 365/1 (Daglig eller oftere)
Konsekvens: (Angitt for tilgjengelighet, konfidensialitet og integritet)	1	Ubetydelig - Stans i <system> <= 10 minutter - Ingen uautorisert innsyn i personopplysninger - Journal er komplett	2	Moderat - Stans i <system> i 30 minutter - Uautorisert innsyn i enkelte personopplysninger og lovbrudd - Noen mangler i journal	3	Alvorlig - Stans i <system> 4 timer - Uautorisert innsyn i enkelte personopplysninger, mulighet for endring og brudd på lov - Viktig informasjon mangler i journal og brudd på lov	4	Kritisk - Stans i <system> 8 timer eller mere - Fullt uautorisert innsyn i eller mulighet for endring av alle personopplysninger og brudd på lov - Kritisk informasjon mangler i journal og brudd på lov

Tabell 2

Risiko = S x Ko
Risiko > 4 krever vurdering av tiltak

Skjema for risikovurdering

Nr	Brudd på	Årsak / trussel	Uønsket hendelse	S	Ko	R (S x Ko)	Mulige konsekvenser	Eksisterende tiltak / forslag til nye tiltak	Ansvarlig / tidsfrist
1	K[1], T	Bærbar PC oppbevares usikret i bil eller på reise. Barbar PC inneholder helse- og personopplysninger.	Tyveri av bærbar PC inneholdende helse- og personopplysninger.	2	4	8	a) Fullt uautorisert innsyn i helse- og personopplysninger b) Stans i behandling av helse- og personopplysninger på bærbart utstyr	Eksisterende tiltak a) Ingen Forslag til tiltak a) Kryptering av lagringsmedium på barbart utstyr b) Sikkerhetskopi av data lagret på bærbart utstyr c) Eventuelt forbud mot å behandle helse- og personopplysninger på bærbart utstyr	

Tabell 3

[1] Brudd på nivå for akseptabel risiko: "Det aksepteres ikke at uvedkommende får innsyn i helse- og personopplysninger" fra faktaark 5 - Fastsettelse av aksept kriterier for tilgjengelighet, integritet og konfidensialitet.

Faktaark 7 - Risikovurderinger.doc

Side 3 av 3