Follo distriktsrevisjon

Forvaltningsrevisjonsrapport

Informasjonssikkerhet og IT-drift

Enebakk kommune

29. MAI 2007 RAPPORT 6/2007

Forord

Forvaltningsrevisjon er en lovpålagt oppgave for Enebakk kommune etter Kommuneloven av 25. september 1992 med endringer av 12. desember 2003. Formålet med forvaltningsrevisjon er nedfelt i lovens § 77 nr. 4 som har følgende ordlyd:

> Kontrollutvalget skal påse at kommunens eller fylkeskommunens regnskaper blir revidert på en betryggende måte. Kontrollutvalget skal videre påse at det føres kontroll med at den økonomiske forvaltning foregår i samsvar med gjeldende bestemmelser og vedtak, og at det blir gjennomført systematiske vurderinger av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak og forutsetninger (forvaltningsrevisjon).

I denne undersøkelsen har Follo distriktsrevisjon vurdert informasjonssikkerhet og IT-drift i Enebakk kommune. I rapporten drøftes vesentlige funn i tilknytning til problemstillingene og det gis anbefalinger som kan bidra til at Enebakk kommune kan ivareta oppgavene tilknyttet informasjonssikkerhet og IT på bedre måter.

Prosjektet er gjennomført i perioden februar 2007 til april 2007. Follo distriktsrevisjon vil benytte anledningen til å takke kommunens kontaktperson IT-sjef Jon Digranes og øvrige ansatte i Enebakk kommune som har bistått revisjonen i forbindelse med gjennomføringen av undersøkelsen.

Prosjektet er gjennomført av rådgiver Ole Anders Sandtrøen.

Steinar Neby
Revisjonssjef

Ole Anders Sandtrøen
Prosjektleder

29.05.2007

Innholdsfortegnelse

1 Sammendrag

Forvaltningsrevisjonsprosjektet om informasjonssikkerhet og IT-drift er gjennomført i henhold til vedtak i kontrollutvalget i Enebakk kommune 24. august 2006.

Formålet med prosjektet er å kartlegge og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard. Konklusjonene i rapporten er delt opp i områdene informasjonssikkerhet og IT-drift.

Undersøkelsen har avdekket mangler i forhold til kravene i lov og forskrift når det gjelder informasjonssikkerhet. Revisjonen har funnet at Enebakk kommune ikke har etablert retningslinjer og rutiner som tilfredsstiller sikkerhetsbestemmelsene i personopplysnings-forskriften. Dette medfører en høyere risiko for at personopplysninger ikke behandles i tråd med lov og forskrift i Enebakk kommune. Det viser seg også at kommunens serverrom er ikke tilstrekkelig sikret med hensyn til mulig oversvømmelse eller uautorisert tilgang til lokalene. Videre viser det seg at backup av kommunens data oppbevares i samme rom som originalene. Dette innebærer at backup er utsatt for noen av de samme risikoene som originalene.

Undersøkelsen har avdekket svakheter i forhold til anbefalinger i God IT-skikk når det gjelder IT-drift. Revisjonen har funnet at IT-avdelingen er sårbar for uforutsett fravær av personell og at det er lite ressurser til å ivareta IT-oppgaver som planlegging, rådgivning og dokumentering. Videre fant revisjonen at IT-planen er forlenget inntil videre selv om den gikk ut året 2006. Beredskapsplaner for sikring av IT-driftskontinuitet ved alvorlige hendelser er ikke etablert. Det viste seg også at dokumentering av IT-systemene etter endringer ikke oppdateres jevnlig, samt at IT-avdelingen i liten grad dokumenterer driftsdokumentasjon. Gjennomgangen av arbeidsdelingen innen IT i kommunen viste at denne oppfattes å være tilfredsstillende ved at en skilte mellom styringsrollen, bestillerrollen og leverandørrollen i kommunen.

2 Innledning

2.1 Bakgrunn for prosjekt

I kontrollutvalgsmøte 12. desember 2005, saksnummer 26/05, ble det vedtatt prioritering mellom forvaltningsrevisjonsprosjekter basert på plan for forvaltningsrevisjon for perioden 2006-2008. *IKT* ble vurdert å være et prioritert område for forvaltningsrevisjon for 2006. Bakgrunnen for valg av prosjekt var overordnet analyse for forvaltningsrevisjon som vurderte risikoen innen IT – standard til å være høy. I kontrollutvalgsmøte 24.8.2006 ble det vedtatt gjennomført forvaltningsrevisjonsprosjekt *Informasjonssikkerhet og IT-drift* i Enebakk kommune.

3 Formål og problemstillinger

3.1 Formål

Formålet med prosjektet er å kartlegge og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard.

3.2 Problemstillinger

Basert på den overordnede analysen og formål for prosjektet har revisjonen definert følgende problemstillinger:

- **Informasjonssikkerhet**
  - Har kommunen tilfredsstillende rutiner og retningslinjer for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet?

- **IT-drift**
  - Er det etablert overordnede mål, retningslinjer og rutiner for IT i kommunen?
  - Er det tilfredsstillende arbeidsdeling vedrørende IT?
  - Har kommunen tilfredsstillende rutiner for å gjenoppta normal drift etter en driftsstans?
  - Har kommunen rutiner for endringshåndtering innen IT som sikrer autorisering, testing og dokumentasjon?

3.3 Avgrensninger

Prosjektet omfatter ikke en kartlegging av Enebakk kommunes IT-systemer, således heller ikke revisjon av de enkelte systemer. Det er ikke vurdert om informasjonssystemene er hensiktsmessige for virksomhetens behov. Kartlegging av informasjonssikkerhetsarbeidet avgrenses til et overordnet nivå i kommunen, og inkluderer av den grunn ikke de enkelte virksomheters/ansattes aktiviteter.

4 Metoder og gjennomføring

Undersøkelsesopplegget er basert på en kombinasjon av analyser av utlevert dokumenter og intervjuer med personer i ulike roller knyttet til IKT og informasjonssikkerhet i kommunen. Dokumentene analyseres for å vurdere om de er tilstrekkelige i forhold til aktuelle anbefalinger (beste praksis) knyttet til IT-drift og krav i forskrift knyttet til informasjons-sikkerhet. Intervjuene av ansatte og ledere innen IKT og informasjonssikkerhet skal gi en forståelse av praksis og etterlevelsen av regelverket og rutiner i kommunen.

4.1 Gjennomføring

Prosjektet er gjennomført av rådgiver Ole Anders Sandtrøen. Revisjonens kontaktperson i Enebakk kommune var kommunens IT-sjef.

Revisjonen valgte ut følgende roller for intervju:

- Kommunens IT-sjef
- Personalsjef
- 1 systemansvarlig for system som behandler sensitive personopplysninger
- IT-veileder for skolene

For dokumentgjennomgangen ble kontaktpersonen i Enebakk kommune forespurt om de dokumentene de hadde innen informasjonssikkerhet og IT-drift, samt kommunens IT-strategi. Tabell 1 viser oversikt over hvilken dokumentasjon som er gjennomgått av revisjonen.

Tabell 1 Liste over revisjonens dokumentunderlag fra Enebakk kommune

Tittel	Dato
Avtale om drift av EDB-systemer – Rammeavtale på stormaskin	02.11.1998
IKT-samarbeidsavtale mellom Rælingen og Enebakk kommuner inkl 3 vedlegg.	01.04.2003
Kopi av referat fra evalueringsmøte mellom Rælingen og Enebakk kommune	09.06.2006
Kopi av serviceavtale med Umoe IKT (ny revidert avtale er inngått våren 2006 ikke oversendt)	Mangler dato
Prosjektnotat - bytte av budsjett og regnskapssystem – forslag til prosess og organisering	22.08.2002
Prosjektnotat – Nytt sak/arkivsystem og webportal	Mangler dato
Oversikt over kommunens viktigste IT-systemer/applikasjoner (tabell)	2006
Powerpoint presentasjon i utvidet lederforum	18.10.2005
Kravspesifikasjon Helpdesksystem	2007
IKT budsjett 2007	2007

4.2 Dataenes pålitelighet og gyldighet

Undersøkelsen bygger i første rekke på opplysninger fra gjennomgang av dokumenter og intervjuer med ulike personer som har sentrale roller i forhold til informasjonssikkerhet og IT-drift. Informasjon som er fremkommet er referert og bekreftet av de som er intervjuet.

Kvalitetssikring av datagrunnlaget omfatter en vurdering av pålitelighet (reliabilitet) og gyldighet (validitet). Pålitelighet er et uttrykk for hvor nøyaktig innsamling av data har vært, og at det ikke er skjedd systematiske feil underveis i innsamlingen. Revisjonen har sett på dokumenter knyttet til informasjonssikkerhet og IT-drift. Alle dokumenter som er gjennomgått er mottatt fra kommunen og i tillegg bekreftet å være gjeldende dokumentasjon. Intervjuene med ansatte har også båret preg av refleksjon og åpenhet.

Gyldighet brukes gjerne som et uttrykk for om vi har målt det vi ønsker å måle. Gyldigheten ble sikret ved at revisjonen innhentet sentrale dokumenter som er spesifisert i revisjons-kriteriene og intervjuet ansatte om praktiseringen av rutiner definert i revisjonskriteriene og i kommunens egne dokumenter.

5 Informasjonssikkerhet

5.1 Revisjonskriterier

I personopplysningsloven (POL) § 13 pålegges den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Dette omfatter å sørge for at tilstrekkelig sikkerhetsfaglig kompetanse er tilgjengelig hos den behandlingsansvarlige. Virksomhetens behandlingsansvarlige er normalt representert ved den administrative ledelse. For en kommune vil dette normalt være ved rådmann.

I tillegg til ansvar for sikkerheten i egen organisasjon, må den behandlingsansvarlige også forsikre seg om at informasjonssikkerheten er tilfredsstillende hos kommunikasjonspartnere og leverandører. Begrepet informasjonssikkerhet omfatter:

- Sikring av **konfidensialitet**, dvs. beskyttelse mot at uvedkommende får innsyn i opplysningene.
- Sikring av **integritet**, dvs. beskyttelse mot utilsiktet endring av opplysningene.
- Sikring av **tilgjengelighet**, dvs. å sørge for at tilstrekkelige og relevante opplysninger er til stede.

Personopplysningsforskriften (POF) definerer nærmere hvilke krav som hviler på kommunen for at tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger finner sted. Revisjonen har valgt å vektlegge følgende krav i denne undersøkelsen:

Personopplysningsforskriften § 2-3 stiller krav om at det skal etableres en sikkerhetsledelse. Ansvaret for at bestemmelsene for informasjonssikkerhet følges påhviler virksomhetens daglige ledelse. Videre skal virksomheten etablere sikkerhetsmål og sikkerhetsstrategi hvor formålet, overordnede føringer, valg og prioriteringer framkommer.

Personopplysningsforskriften § 2-4 stiller krav om at det skal føres en oversikt over hvilke personopplysninger som behandles. Videre kreves det at den behandlingsansvarlige gjennomfører en risikovurdering for å kartlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ved endringer av betydning for informasjonssikkerheten skal ny risikovurdering gjennomføres.

Personopplysningsforskriften § 2-5 stiller krav om at det jevnlig gjennomføres sikkerhetsrevisjon. Denne skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Resultatet av sikkerhetsrevisjonen skal dokumenteres.

Personopplysningsforskriften § 2-6 stiller krav om at bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd skal behandles som avvik.

Personopplysningsforskriften § 2-7 stiller krav om at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet. Ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarlige daglige leder (rådmann). I Datatilsynets kommentarer til sikkerhetsbestemmelsene i personopplysningsforskriften påpekes det at det er viktig at ansvar og myndighet relatert til drift av

informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeidet (sikkerhetsledelse) er klarlagt. Disse funksjonene er henholdsvis "utøvende" og "kontrollerende" og bør ideelt sett tillegges forskjellige medarbeidere i virksomheten. For mindre virksomheter kan det likevel være nødvendig å legge begge funksjoner til en og samme person. Arbeidsoppgaver for sikkerhetsleder vil normalt omfatte forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner samt kontroll med risikovurdering og avviksbehandling.

Personopplysningsforskriften § 2-10 stiller krav om fysisk sikring mot uautorisert tilgang til utstyr som brukes for å behandle personopplysninger definert i forskriften eller annet utstyr av betydning for informasjonssikkerheten. I veileder for informasjonssikkerhet for kommuner og fylker, utgitt av Datatilsynet, framkommer det vedrørende fysisk sikkerhet at virksomheten skal sørge for at lokaler og utstyr den benytter er forsvarlig sikret. Det skal spesielt legges vekt på de rom hvor det er plassert utstyr benyttet for behandling av sensitive personopplysninger, eller for sikring av slike.

5.2 Faktabeskrivelse

5.2.1 Sikkerhetsmål, strategi og oversikt over personopplysninger kommunen behandler

Enebakk kommune har ikke etablert noen sikkerhetsmål eller strategi. I en oversikt over hvilke programmer kommunen benytter er de programmene som behandler sensitive personopplysninger markert. Det eksisterer derfor en oversikt over hvilke programmer som anvendes av kommunen til behandling av sensitive personopplysninger.

5.2.2 Sikkerhetsorganisasjon

Enebakk kommune har ikke etablert en dokumentert sikkerhetsorganisasjon.

5.2.3 Sikkerhetsrevisjon, risikoanalyse, avvikshåndtering og oppdateringer

Enebakk kommune har ikke gjennomfører jevnlige sikkerhetsrevisjoner. Det viser seg også at det ikke er gjennomført risikoanalyse for informasjonssikkerhet i kommunen. Det er ikke etablert noen dokumentert rutine for avvikshåndtering i kommunen. Oppdatering av sikkerhetsmål, sikkerhetsstrategi, sikkerhetsorganisasjon mv. synes ikke å foregå siden disse dokumentene ikke er etablert.

5.2.4 Fysisk sikring

All elektronisk informasjon i kommunens datasystemer som behandler sensitiv personopplysninger og helseregisteropplysninger, behandles i et lukket system og lagres i kommunens serverpark.

Den fysiske sikringen av sensitiv personopplysninger i elektronisk form begrenser seg hovedsakelig til serverrommet i kommunen. Revisjonen befarte serverlokalet til kommunen sammen med IT-sjef. Serverrommet er sikret på følgende måte:

- Bygningsmessig plassert i kjeller i et bygg som er døgnbemannet
- Brannalarm
- Vanlig dør med systemlås
- Aircondition/kjøling med reserveløsning

- UPS (batteristrøm) for å sikre strømtilførsel inntill aggregatet overtar eller systemet er tatt ned på betryggende måte (slått av)

Ved befaring ble revisjonen gjort kjent med følgende risikoområder knyttet til kommunens serverpark.

- Gulvet er ikke hevet for å beskytte mot oversvømmelse
- Vannledninger ligger i åpne rør i taket over serverne
- Renholdspersonell og vaktmester har direkte adgang til serverlokale uten tilsyn av IT-personell
- Det er ikke innbruddsalarm tilknyttet vaktsentral

Revisjonen ble også gjort kjent med at det tidligere har vært vannlekkasje på serverommet grunnet vannlekkasje i vaskerommet som ligger rett over gangen for serverrommet. Dette medførte ingen skade ved det tilfellet siden serverstativene stod på hjul og var litt over bakkenivå.

I tillegg til fysisk sikring av serverrom er backup av informasjonen som lagres der viktig. I Enebakk kommune har man følgende backuprutine:

- Hver natt tas det komplett backup. Backupen tas på tape som står i rack i samme rom som serverparken står. Backuptaper som er ferdig tas ut og legges i egen brannsikker safe som er plassert i samme rom som serverparken.

IT-sjef opplyser at backuprutinene er under vurdering for ytterligere sikring av kommunens data. Det vurderes å sette en egen backupserver i et annet bygg som løpende tar backup av serverparken.

5.2.5 Annet

Enebakk kommune har anskaffet et system for avvikshåndtering fra firmaet Kvalitetslosen AS. Dette er et nettbasert verktøy for internkontroll og avviksrapportering som dekker hele kommunens virksomhet. Inkludert i dette er også retningslinjer for internkontroll iht. sikkerhetsbestemmelsene i personopplysningsforskriften. Enebakk kommune er i ferd med å etablere egne mål og strategier som skal inngå i dette systemet. Det nye internkontroll systemet er planlagt iverksatt i Enebakk kommune innen sommeren 2007.

5.3 Vurdering

Revisjonen har undersøkt Enebakk kommunes etterlevelse av kravene til sikkerhetsmål, sikkerhetsstrategi og hvilken oversikt som foreligger for personopplysninger som behandles i kommunens informasjonssystemer. Undersøkelsen viser at Enebakk kommune ikke har etablert sikkerhetsmål og sikkerhetsstrategi, videre er det heller ikke etablert en dokumentert sikkerhetsorganisasjon eller gjennomført noen risikoanalyse i Enebakk kommune. Enebakk kommune har en oversikt over personopplysninger som kommunen behandler ved at disse systemene er markert i den samlede oversikten over applikasjoner i kommunen.

Sikkerhetsrevisjon er en aktivitet som skal gjennomføres i alle deler av virksomheten innen en 12 måneders periode. Resultatene fra dette skal også dokumenteres. I Enebakk kommune viser det seg at dette ikke gjennomføres. Revisjonen har heller ingen informasjon som tyder

på at det er gjennomført sikkerhetsrevisjon siden forskriften trådde i kraft 1.1.2001. Sikkerhetsrevisjon er en viktig kontrollaktivitet for å sørge for at nødvendig informasjonssikkerhet ivaretas i kommunen. Uten denne kontrollaktiviteten vil det være vesentlig risiko for at manglende informasjonssikkerhet oppstår og ikke blir fanget opp og korrigert.

Revisjonen har befart den fysiske sikringen av serverlokalet til Enebakk kommune. Den fysiske sikringen har noen svakheter. Serverlokalet står utsatt til for mulig vannlekkasje fra både vannledninger i tak og fra vaskerom vis a vis serverrommet. Videre er det ikke egen sikkerhetslås eller innbruddsalarm som begrenser adgangen til lokalet til andre enn IT-avdelingen eller autorisert personell. I tilegg utfører annet personell i kommunen arbeid i rommet uten tilsyn fra IT-avdelingen. Lokaler som lagrer sensitiv personopplysninger og som er kritiske for den daglige driften av kommunen bør ha en streng adgangsbegrensning av hensyn til dataenes konfidensialitet, integritet og tilgjengelighet.

IT-avdelingen har faste backuprutiner og tapene fra backup oppbevares innlåst i brannsafe i samme rom som serverne. Oppbevaring av backup i samme rom som originalene medfører at backup er utsatt for noen av de samme risikoene som originalene. Oppbevaring et annet sted enn originalene vil kunne redusere denne risikoen. Revisjonen har fått opplyst at IT-avdelingen vurderer å endre på backuprutinene slik at det også foretas backup til et annet bygg enn det serverne står i. Revisjonen oppfatter dette som et positivt tiltak i forhold til å trygge dataene til kommunen.

Sikkerhetsbestemmelsene i personopplysningsforskriften har som formål å påse at virksomheter som behandler sensitive personopplysninger har tilstrekkelige sikkerhetsrutiner som sikrer at denne typen informasjons konfidensialitet, integritet og tilgjengelighet ikke trues. Manglende etterlevelse av personopplysningsforskriftens sikkerhetsbestemmelser er alvorlig[1]. Revisjonen registrerer dog at Enebakk kommune er i ferd med å etablere et internkontroll system som også inkluderer informasjonssikkerhet. Dette systemet er derimot ikke i drift i kommunen før sommeren 2007 og er således ikke vurdert av revisjonen. Revisjonen vil imidlertid påpeke at denne forskriften har vært gjeldende siden 01.01.2001.

[1] Jf. personopplysningsloven §48e kan det ved behandling av personopplysninger i strid med § 13 (se kap 5.1 revisjonskriterier) i tilfeller av forsett eller grov uaktsomhet straffes med bøter og/eller fengsel inntil 1 år .

6 IT-drift

6.1 Revisjonskriterier

Overordnede mål, retningslinjer og rutiner
COBIT[2] og God IT-skikk *anbefaler* at en etablerer IT strategi/planer og at disse er forankret i og bygger opp under kommunens mål og planer. I tillegg bør en ha konkrete handlingsplaner og investeringsplaner for hvordan de overordnede strategiene skal nås.

God IT-skikk anbefaler at det foreligger dokumentasjon som viser samtlige IT-systemer og sammenhengen mellom disse. Dokumentasjonen bør inneholde en overordnet informasjon om systemene. En samlet dokumentasjon av et system skal for øvrig bestå av: [3]

- **Systemdokumentasjon**: IT-systemet skal beskrives tilstrekkelig detaljert til at forsvarlig systemforvaltning (vedlikehold og videreutvikling) muliggjøres.

- **Brukerdokumentasjon**: Dokumentasjonen skal på en oversiktlig og lettfattelig måte beskrive systemet med tilhørende manuelle rutiner slik det arter seg for brukeren.

- **Driftsdokumentasjon**: Dokumentasjonen er en beskrivelse av systemets oppbygging og driftsmønster for å sikre korrekt drift av IT-systemet, driftsmessig vedlikehold og stabilitet.

Arbeidsdeling
Statskonsult[4] og KS[5] *anbefaler* at IT-organisasjonen klart skiller mellom rollene: styring av IT-området, bestiller av IT-løsninger og leverandør av IT-løsninger. Innholdet i disse rollene er:

- **Styringsrollen:** Styringsrollen omfatter den overordnede strategiske planleggingen, koordineringen og styringen som er nødvendig for å følge opp IT-virksomheten.

- **Bestillerrollen:** Systemeier er en bestiller av funksjonalitet og IT-løsninger. (Det største brukermiljøet på bestillersiden er normalt systemeier.) Bestillerrollen omfatter ansvaret for brukerkrav/funksjonelle krav.

- **Leverandørrollen:** Leverandøren skal, på oppdrag fra kunden, levere spesifiserte IT-løsninger og IT-tjenester. Leverandørrollen skal ha ansvar for å fremskaffe den funksjonalitet som er ønsket. Dette omfatter leveranse av maskiner, basis programvare, standardsystemer, utviklingsprosjekter, system- og programmeringstjenester og tjenester til drift og forvaltning samt brukerstøtte. En IT-avdeling er ofte tildelt en vesentlig del av ansvaret for leverandørrollen, selv om det kjøpes inn ressurser fra eksterne leverandører på en del av oppgavene. COBIT anbefaler at det bør være etablert en IT-organisasjon med klare roller og nødvendig myndighet til å utøve ansvaret for IT i kommunen. Klare roller med beskrivelse av oppgaver og ansvar bør også foreligge.

[2] Control Objectives for Information and Related Technology (COBIT) er utviklet av Information Systems Audit and Control Association (ISACA) og IT Governance Institute (ITGI) og gir anbefalinger for god IT-skikk.
[3] Anbefaling til God IT-skikk (nr. 1) Dokumentasjon av IT-systemer 2001
[4] IKT i det offentlige 2002
[5] Verktøykasse for IKT-planlegging 2004 Analyse av IKT organiseringen, Kommunenes Sentralforbund TN 7

Driftskontinuitet
God IT-skikk anbefaler at det etableres beredskapsplaner som ivaretar kontinuiteten i driften ved alvorlige/katastrofale hendelser.

God IT-skikk anbefaler at driftsforstyrrelser logges og at det informeres til systemeiere og brukere ved driftsbrudd. Det bør også settes et nivå for når en forstyrrelse er så alvorlig at katastrofe/beredskapsplanen settes i verk.

Endringshåndtering
God IT-skikk definerer en rekke aktiviteter en virksomhet må iverksette for å sikre en forsvarlig gjennomføring av endringer som påvirker drift av IT-systemene, herunder tiltak for å sikre at alle endringer blir gjennomført på en effektiv og kontrollert måte, til rett tid og med forventet resultat. Dette forutsetter at alle endringer er autorisert, planlagt, prioritert, risikovurdert, dokumentert, testet og godkjent. God IT-skikk anbefaler at en etablerer retningslinjer, prosedyrer og instrukser for endringshåndtering.

6.2 Faktabeskrivelse

6.2.1 Overordnede mål og strategier

Enebakk kommune har en IKT-plan for perioden 2003-2006. Denne gjelder inntil ev. ny IKT-plan vedtas. Planen er inndelt i hovedmål, delmål, tidsramme med investeringsplan for perioden 2003-2006. Rammen for planen er oppgitt å være blant annet kommunens politiske og administrative målsetninger, jf. Kommuneplan, økonomiplan osv. IT-sjef oppgir at gjeldende plan er videreført i 2007 på grunn av at de målsetningene som var satt i nåværende plan ikke er nådd innen planperioden.

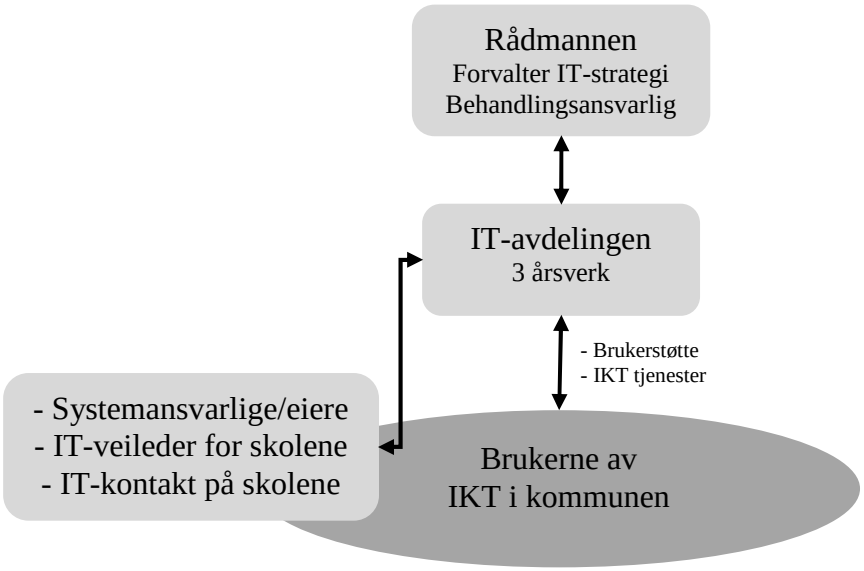
6.2.2 Arbeidsdeling og organisering av IT i kommunen

Enebakk kommune er organisert med tre tjenesteytende enheter (Kultur og oppvekst, helse og sosial og teknisk) og en sentraladministrasjon. IT-avdelingen er organisert i sentraladministrasjonen og er direkte underlagt rådmannen. Organisasjonskartet viser en oversikt over de ulike funksjonene knyttet til IT i kommunen.

Rådmannen har det overordnede ansvaret for IKT i kommunen. Rådmannen som øverste administrative leder er også behandlingsansvarlig for informasjonssikkerheten i kommunen iht. personopplysningsloven §13.

Systemansvarlige har ansvaret for sine respektive fagsystemer og skal fungere som bindeledd mellom virksomhetene og IT-avdelingen. De administrerer tilganger, tilrettelegger/tilpasser fagsystemene, ivaretar opplæring og brukerstøtte, melder inn behov for oppdateringer til IT-avdelingen og ivaretar sikkerheten i sine systemer.

IT-veileder og IT-kontakter for skolene har ansvaret for drift av maskinparken for elever og lærere. Den enkelte skole har i tillegg egne IT-kontaktpersoner som har ansvar for driften av IT på den enkelte skole samt administrerer tilganger til brukerkonto/e-post for elever og lærere. Skolene deltar i et interkommunalt skolenett som driftes av Rælingen kommune.



Figur 1 Organisasjonskart over ulike IT-relaterte funksjoner i Enebakk kommune (revisjonens utgave)

IT-avdelingen er organisert under sentraladministrasjon og er delegert overordnet operativt ansvar for drift av IKT i kommunen og IT-sjef rapporterer direkte til rådmann. Arbeidsfeltet er å tilby IT-tjenester til kommunen hvor det er ca 200 brukere i administrativt nett og ca 1500 brukere på skolene. Den økonomiske rammen for IT i kommunen er på ca 1,5 millioner kr i driftsbudsjett og ca 500 tusen kr i investeringsbudsjett (2007).

IT-avdelingen er en enhet med tre ansatte inkludert IT-sjef. Alle ved avdelingen overlapper hverandre på de ulike oppgavene for å unngå problemer i forbindelse med ferieavvikling/sykdom. Det er likevel en viss grad av spesialisering i og med at noen oppgaver som telefoni/kopimaskin og AV-utstyr er fordelt på de to IT-konsulentene. For brukerstøtte ringer brukerne en av de som er tilgjengelige eller kontakter avdelingen via e-post. IT-sjefen oppgir i tillegg at han også tar seg av driftsoppgaver og support. IT-sjef oppgir videre at driftsoppgaver og support tar vesentlig tid og at det er lite tid igjen til å jobbe med planlegging, rådgivning og øvrige lederoppgaver.

Gjennomgang av den formelle kompetansen i IT-avdelingen viser at to har høyere utdannelse innen teknisk/IT fag og en har lang arbeidserfaring innen IT-drift.

6.2.3 Driftskontinuitet

Beredskapsplanlegging

IT-avdelingen har ingen beredskapsplan. IT-avdelingen gjennomfører sårbarhetsvurderinger som blant annet ligger til grunn for en omfattende avtale med Umoe IKT om beredskap ved alvorlige hendelser og bistand ved større endringer. Disse er derimot ikke systematisert og dokumentert.

Måling og evaluering av kontinuitet

Hendelser logges ikke av IT-avdelingen. Supporthenvendelser mottas i dag via telefon eller e-post og behandles og logges i Outlook[6]. IT-avdelingen har anskaffet et nytt dedikert helpdesk (brukerstøtte) system i fellesskap med Rælingen og Fet kommune.

6.2.4 Endringshåndtering og dokumentering

Endringshåndtering

Rutine for endringshåndtering i Enebakk kommunes IT-avdeling er at endringer foretas etter at leverandørene melder om oppdateringer/endringer. Hvis disse vurderes som viktige avklares et passende tidspunkt som belaster kommunen minst mulig for endringsarbeidet. Nedetid varsles via e-post/intranett. Endringer skjer som oftest direkte på de aktuelle systemene og ikke i testsystemer. Dette er begrunnet i at de fleste oppdateringer/endringer som kommer fra leverandørene er testet ut på tilsvarende plattformer der, før de sendes ut.

Endringer/oppdateringer av fagsystemer meldes inn til IT-avdelingen av leverandør eller systemansvarlige, både systemansvarlige og IT-avdelingen får melding fra leverandør om oppdateringer/endringer. IT-avdelingen og systemansvarlige vurderer i fellesskap om det er hensiktsmessig å foreta endringene med en gang eller om det kan samle opp flere endringer/oppdateringer. Systemansvarlig autoriserer endringene/tidspunkt, mens IT-avdelingen står for den tekniske tilretteleggingen. Endringer/oppdateringer av betydning for fellessystemer/IT-utstyr ligger inn under IT-avdelingen ansvar og autoriseres av IT-sjef.

Dokumentering skjer i etterkant av endringer hvor det legges inn informasjon om endringer som er foretatt. Det brukes en felles perm for endringer som brukes som dokumentasjon. Dette skjer vanligvis ved at endringslogg, spesifikasjon som gis fra leverandør vedrørende den aktuelle endringen skrives ut og legges i felles perm. Øvrige endringer skal også resultere i at endringene dokumenteres i permen. I følge IT-sjef blir ikke dette oppdatert jevnlig.

Dokumentasjon

Dokumentasjonen knyttet til IT er fordelt i tre hovedtyper som beskrevet i revisjonskriteriene.

- **Systemdokumentasjon** beskrives i Enebakk kommune gjennom den dokumentasjonen som leverandørene leverer sammen med løsningene. Siden Enebakk kommune kjøper standard programvare utvikler de i liten grad systemdokumentasjon.

- **Driftsdokumentasjon** IT-sjef oppgir at IT-avdelingen i liten grad dokumenterer rutiner og aktiviteter. Det oppgis at det innen de tidsressursene som avdelingen har i liten grad gir IT-sjef tid til å jobbe med dokumentering.

- **Brukerdokumentasjon** er også en type dokumentasjon som i hovedsak leverandørene for IT-utstyr/applikasjonene leverer sammen med løsningene.

[6] Microsoft Office Outlook er et program for behandling av avtaler, e-post mv. som kan deles over nettverk

6.2.5 Standard

Enebakk kommune forutsetter i IT-planen at kommunen skal være bruker av markedsledende standard systemløsninger innefor sine tjenesteområder. I samtale med IT-sjef oppgir han at det alltid er fokus på å kjøpe IT-utstyr og spesielt programvare som er standard innen sine områder.

6.3 Vurdering

Revisjonen har undersøkt om Enebakk kommune har etablert IT-strategi og at denne er forankret i kommunens mål og planer. Enebakk kommune har etablert en IT-plan som gjaldt for perioden 2003-2006. IT-planen var forankret i kommunens mål og planer slik God IT-skikk anbefaler. IT-planen gjaldt kun fram til 2006, men er videreført i 2007 siden alle målsetninger ikke er nådd innen planperioden 2003-2006. En IT-strategi bør likevel oppdateres slik at mål nådd for perioden kan gjennomgås og nye/videreførte mål/tiltak kan planlegges.

Revisjonen har undersøkt organisering og arbeidsdeling av IT i Enebakk kommune. Faktabeskrivelsen viser at IT-avdelingen er sentralt plassert i organisasjonen med kort vei til rådmann. Videre har systemansvarlige en selvstendig rolle som ansvarlige for sine fagapplikasjoner. Fagapplikasjonene og øvrig IKT realtert utstyr driftes av IT-avdelingen (Rælingen kommune drifter kommunens regnskapssystem, sak/arkivsystem og skolenettet). Arbeidsdelingen følger i hovedsak skillet mellom styringsrollen (rådmannen), bestillerrollen (systemansvarlige/eiere) og leverandørrollen (IT-avdelingen). Denne rollefordelingen synes å være i tråd med anbefalt arbeidsdeling for IT.

IT-avdelingen er organisert slik at alle skal kunne utføre de fleste oppgavene. Dette kan bidra til redusert sårbarhet ved uforutsett fravær hvor en ikke er avhengig av at enkeltpersoner er tilgjengelig. IT-avdelingen består av tre ansatte. Dette innebærer at IT-avdelingen er sårbar ved plutselig reduksjon i bemanningen som for eksempel ved sykefravær. Kompetansemessig har IT-avdelingen ansatte med utdannelse innen IT/teknologiske fag og lang erfaring med IT-drift.

IT-sjef oppgir at han har liten tid til å drive med dokumentering, rådgivning og ledelse. Dokumentering er viktige oppgaver for en IT-virksomhet for å sikre at nødvendig dokumentasjon av de aktivitetene en gjør i driften oppdateres. Rådgivning er også en viktig oppgave ovenfor brukerorganisasjonen (virksomhetene i kommunen) ved at de får hjelp/bistand ved spørsmålstillinger som for eksempel ved anskaffelser. Disse oppgavene sammen med ledelse av IT-avdelingen bør derfor prioriteres.

Kontinuitet i driften er sentralt for en effektiv utnyttelse av IT som verktøy i oppgaveutførelsen i kommunen. God IT-skikk anbefaler at en etablerer beredskapsplaner for hvordan en ivaretar driftskontinuiteten ved alvorlige hendelser. IT-avdelingen har ikke etablert en beredskapsplan hvor rutiner for håndtering av alvorlige hendelser tas opp. Dette er et viktig verktøy for å sikre at en er forberedt for alvorlige hendelser og kan redusere konsekvensene ved disse.

Logging av driftsforstyrrelser er viktig. Ofte kan mindre forstyrrelser over tid belaste virksomheten mest. Revisjonens undersøkelse viser at driftsforstyrrelser ikke logges i Enebakk kommune. IT-avdelingen er derimot i gang med å etablere et nytt helpdesksystem i

samarbeid med Rælingen og Fet kommune som skal lette arbeidet med å registrere og behandle feil i IT-systemene. Det opplyses også at brukere og systemeiere varsles ved planlagte driftsbrudd. Revisjonen ser positivt på at IT-avdelingen jobber for å få på plass et helpdesksystem. Dette vil kunne bidra til at en får raskt oversikt over hvilke problemer som oppstår og hva som ble gjort for å løse disse.

IT-avdelingen har ingen fastlagt rutine for endringshåndtering. Endringer foretas vanligvis direkte mot systemene iht. leverandørenes veiledning. Dette er en praksis som kan innebære en risiko for driftskontinuiteten i tilfeller hvor brukerne tar i bruk systemer etter endringer som ikke i tilstrekkelig grad er testet og risikovurdert på forhånd. I tilfeller hvor leverandørene påser at testing mot tilsvarende konfigurasjon er gjort, vil denne risikoen være lavere. Planlagte endringer foretas som oftest ved at de som har ansvaret for systemet godkjenner at endringen foretas hvorpå IT-avdelingen foretar endringene. Dette er en praksis som er i tråd med god IT-skikk ved at den sikrer at de som har ansvaret for systemene også autoriserer endringene. Dokumentasjonen skjer i etterkant av endringene i en felles perm for IT-avdelingen. Denne loggingen av endringer foretas ikke jevnlig. Dokumentasjon er en viktig aktivitet for å kunne spore mulige feilkilder og sikre at en har oversikt over hvilke versjoner og endringer som er gjort.

Revisjonen har gjennomgått dokumentasjonsrutinene i kommunen med sikte på å få en oversikt over hvordan systemdokumentasjon, driftsdokumentasjon og brukerdokumentasjon håndteres i kommunen. Siden kommunen kjøper IT-programmer fra leverandører i stedet for å utvikle dette selv, er systemdokumentasjon og brukerdokumentasjon i hovedsak dokumentert av leverandørene. Revisjonene oppfatter dette som en tilfredsstillende praksis i lys av at kommunen kjøper systemene framfor å utvikle løsningene selv.

IT-avdelingen dokumenterer i liten grad driftsdokumentasjon. Manglende kapasitet oppgis som hovedgrunn for dette. Driftsdokumentasjon er viktig for å sikre korrekt håndtering av systemene ved for eksempel hendelser hvor en trenger rutiner for sikker nedstegning av serverpark ved strømbrudd. Denne typen dokumentasjon og oppdatering av denne er viktig og bør prioriteres.

7 Konklusjon

Formålet med prosjektet er å kartlegge og vurdere kommunens sentrale IT-funksjoner med fokus på sikkerhet, ytelse og standard. Konklusjonene i rapporten er delt opp i områdene informasjonssikkerhet og IT-drift.

7.1 Informasjonssikkerhet

- Enebakk kommune har ikke etablert retningslinjer og rutiner som tilfredsstiller sikkerhetsbestemmelsene i personopplysningsforskriften. Dette medfører en høyere risiko for at personopplysninger ikke behandles i tråd med lov og forskrift i Enebakk kommune.

- Kommunens serverrom er ikke tilstrekkelig sikret med hensyn til mulig oversvømmelse eller uautorisert tilgang til lokalene.

- Backup oppbevares i samme rom som originalene. Dette innebærer at backup er utsatt for noen av de samme risikoene som originalene.

7.2 IT-drift

- IT-avdelingen er sårbar for uforutsett fravær av personell

- Det er lite ressurser til å ivareta IT-oppgaver som planlegging, rådgivning og dokumentering

- IT-planen er forlenget inntil videre selv om den gikk ut året 2006.

- Beredskapsplaner for sikring av IT-driftskontinuitet ved alvorlige hendelser er ikke etablert

- Dokumentering av IT-systemene etter endringer oppdateres ikke jevnlig

- IT-avdelingen dokumenterer i liten grad driftsdokumentasjon

- Arbeidsdelingen innen IT i kommunen oppfattes å være tilfredsstillende.

8 Anbefalinger

8.1 Informasjonssikkerhet

Revisjonen mener Enebakk kommune må gjennomføre tiltak som sikrer at informasjonssikkerhetsarbeidet gjennomføres i tråd med regelverket, herunder:

- At det etablere sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisasjon
- At kommunen igangsetter jevnlig sikkerhetsrevisjon hvor resultatet av sikkerhetsrevisjonen dokumenteres
- At det gjennomføres en risikovurdering som kartlegger risikoen for sikkerhetsbrudd

Videre vil revisjonen anbefale Enebakk kommune å:

- Forbedre den fysiske sikringen av serverlokalene med hensyn til vannlekkasjer, adgangsbegrensning og innbruddsalarm
- Oppbevare backup på enn annen lokasjon enn originalene

8.2 IT-drift

Revisjonen mener Enebakk kommune kan gjennomføre tiltak som forbedrer IT-drift, herunder:

- Oppdatere IT-planen slik at den gir en strategisk forankring for de valgene som gjøres også etter 2006
- Prioritere ressurser til dokumentering, rådgivning og ledelse innen IT
- Etablere beredskapsplaner for håndtering av alvorlige hendelser

ENEBAKK KOMMUNE
Rådmannskontoret

Follo distriksrevisjon
Postboks 3010
1402 Ski

Att. Ole Anders Sandtrøen

Deres dato:	Deres ref.:	Vår ref.:	Arkivkode:	Dato:
27.04.2007		2006/834/KJOI	216	07.05.2007

Rådmannens uttalelse - Informasjonssikkerhet og IT-drift

Rådmannen ble i brev datert 22.08.2006 gjort oppmerksom på at Kontrollutvalget i Enebakk kommune i sak 23/06 hadde gitt Follo distriktsrevisjon i oppdrag å gjennomføre et forvaltningsrevisjonsprosjekt om IT-sikkerhet og drift. Det vises i den forbindelse til forvaltningsrevisjonsrapport – informasjonssikkerhet og IT-drift datert 27.04.2007, der det bes om en uttalelse fra rådmannen til rapporten.

Rådmannens uttalelser vil bli gitt i samsvar med guide til høringsuttalelse:

Rådmannen er av den oppfatning at det i god tid ble gitt tilstrekkelig informasjon om prosjektets hensikt gjennom brev datert 22.08.06. Rådmannen har videre ingen kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner. Rådmannen ønsker imidlertid å påpeke at arbeidet som er lagt til grunn for rapporten oppleves i mindre grad som en vurdering av IT-sikkerheten i kommunen, men i større grad en vurdering av dokumentasjonen knyttet til denne.

Revisjonskriteriene som er lagt til grunn for gjennomgangen av kommunens informasjonssikkerhet er knyttet opp til personopplysningsloven § 13 der det pålegges den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Når det gjelder kriteriene knyttet til IT-drift er det henvist til COBIT og God IT-skikk. Rådmannen har ingen kommentarer til disse kriteriene, men ønsker å presisere at rådmannen ser nytteverdien av å etablere systemer slik at Enebakk kommune etterlever de ulike kravene som stilles i lovverket.

Rådmannen har vært klar over de mangler som er påpekt i rapporten og har på denne bakgrunn iverksatt følgende tiltak:

1. Informasjonssikkerhet

Det er inngått en avtale med Kvalitetslosen AS, som valgt leverandør av IT løsning for å ivareta informasjonssikkerhet, HMS, avvik og tiltak i Enebakk kommune. Det er i den forbindelse utarbeidet en overordnet sikkerhetsstrategi, mål for IT-sikkerhet, det er etablert en sikkerhetsorganisasjon med en beskrivelse av sikkerhetsrevisjoner, avviksbehandling og en

oversikt over de forskjellige avdelingers dataløsninger med hjemler. Det vil bli en gjennomgang med leverandøren, der vi etablerer flytkart. Disse flytkartene vil gi oss en oversikt over informasjonsflyten i de datasystemene som behandler sensitive opplysninger. Det vil bli gjennomført en trusselvurdering av alle fagsystemene, samt gjennomført en ROS analyse. ROS analysen vil deretter bli presentert for kommunens ledelse. Dette arbeidet ferdigstilles medio mai 2007, og vil bli revidert årlig framover.

2. IT-drift

Etter rådmannens oppfatning er kommunens IT-sikkerhet god i den forstand at den designes og implementeres i henhold til Datatilsynets forskrifter og retningslinjer. Rådmannen deler imidlertid rapportens oppfatning av at dokumentasjonen er mangelfull.

I rapporten konkluderes det med at IT-avdelingen er sårbar for uforutsett fravær av personell. Dette har rådmannen iverksatt tiltak for å endre ved at avdelingen får tilført en ny stilling, en IKT – driftsansvarlig. Dette vil medføre at det kan settes av ressurser til det videre arbeidet med planlegging, rådgivning og dokumentering. IKT – driftsansvarlig vil kunne være på plass tidlig høst 2007. Som beskrevet i rapporten, er det igangsatt et arbeid for å etablere et helpdesk system i samarbeid med Rælingen og Fet kommune for å sikre logging av hendelser knyttet til de ulike systemene.

Rådmannen har ingen merknader til rapportens oppbygning og språkbruk. Innholdet og funnene i rapporten ses på av rådmannen som et nyttig verktøy i arbeidet med å bedre rutinene knyttet til informasjonssikkerhet og IT-drift i Enebakk kommune.

Med vennlig hilsen

Nils Schaug
rådmann

10 Revisjonens kommentarer til rådmannens uttalelse

Revisjonen ser positivt på at rådmannen i sin uttalelse har sluttet seg til de konklusjoner og anbefalinger som revisjonen har fremmet i rapporten. Revisjonen ser det også som positivt at rådmannen har iverksatt ulike tiltak for å utbedre forhold som er kommentert i rapporten, herunder etablering av tiltak for å sikre tilfredsstillende internkontroll innen informasjonssikkerhet i løpet av mai 2007 og økning i bemanning for å øke kapasiteten og redusere sårbarheten i IT-avdelingen. Revisjonen har for øvrig merket seg at rådmannen ser rapporten som et nyttig verktøy i arbeidet med å bedre rutinene knyttet til informasjonssikkerhet og IT-drift i kommunen.

Revisjonen registrerer at rådmannen påpeker at arbeidet som er lagt til grunn for rapporten i mindre grad oppleves som en vurdering av IT-sikkerheten i kommunen, men i større grad en vurdering av dokumentasjonen knyttet til denne. I redegjørelsen for revisjonskriteriene klargjør revisjonen hvilke kriterier personopplysningsforskriften legger til grunn for en tilfredsstillende informasjonssikkerhet. Revisjonen har undersøkt etterlevelsen av disse kriteriene, hvor det også stilles krav om dokumentering av de aktivitetens som skal gjennomføres.

11 Litteraturliste

Anbefalinger til God IT-skikk (GITS) (nr. 0, 1 og 3)

COBIT – Control Objectives for Information and Related Technology

Datatilsynet (2000) Sikkerhetsbestemmelsene i personopplysningsforskriften - med kommentarer

Datatilsynet (2005) Veileder i informasjonssikkerhet for kommuner og fylkeskommuner

Forskrift om behandling av personopplysninger (personopplysningsforskriften) 1.1.2001.

Lov om behandling av personopplysninger (personopplysningsloven) 1.1.2001

Statskonsult: IKT i det offentlige 2002

Verktøykasse for IKT-planlegging 2004 Analyse av IKT organiseringen, Kommunenes Sentralforbund TN 7