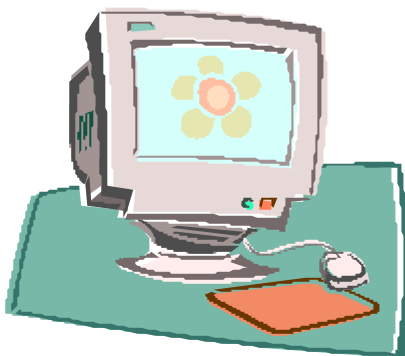


IT-REVISJON

LEVANGER KOMMUNE

RAPPORT NR. 1.1/2003

FORVALTNINGSREVISJON



1 INNLEDNING

Søndre Innherred revisjonsdistrikt startet arbeidet med It-revisjon i Levanger kommune ved informasjonsbrev 03.01.01. Imidlertid har dette arbeidet blitt utsatt. Arbeidet med it-revisjonen ble tatt opp igjen høsten 2002. Vi har benyttet e-post og personlige møter med representanter fra Levanger kommune. Følgende personer har vært i dialog med oss: Torbjørn Olsen, Monica Valde Sørland og Ingjar Eggen.

Vi vil presisere at IT-revisjon er en fortløpende revisjon og vil ikke ha typiske prosjektkjennetegn som start og sluttdatoer. IT-revisjon er en prioritert oppgave for revisjonsdistriktet og vi vil fortsatt ha fokus på IT i Levanger kommune. Vi vil forsette arbeidet med IT-revisjon ved å gå nærmere inn på utvalgte områder. Pr i dag er det ikke besluttet hvilke områder vi skal undersøke nærmere.

Revisjonen er basert på "Anbefaling til God IT-skikk" som er basert på internasjonale standarder og utarbeidet av Information Systems Audit and Control Association (ISACA) i samarbeid med Den Norske Dataforening. Datatilsynets "**Veiledning i informasjonssikkerhet** for kommuner og fylker" er også benyttet. Revisjonen har benyttet skjema for IT-revisjon som er utarbeidet av Norges Kommunerevisorforbund.

Vi gjør oppmerksom på at vi er kjent med at Levanger kommune skal inngå i samkommune og vil få felles IT-løsning med Frosta og Verdal kommune.

Søndre Innherred Revisjonsdistrikt samarbeider med Innherred Revisjonsdistrikt om IT-revisjon. Rapporten er skrevet i samarbeid med Svein-Arne Myrvold, Innherred Revisjonsdistrikt.

Rapporten er sendt på høring til Levanger kommune. Revisjonen har aldri mottatt skriftlig besvarelse på tross av flere purringer. Vi har fått muntlig beskjed om at de ikke har noen merknader.

2 RESULTATER

I vår undersøkelse har vi konsentrert oss om generelle forhold rundt IT, som drift av systemene, backup og dokumentasjon, økonomisystemet og lønnsystemet Unique. Vi beskriver sentrale deler av rutineene. Våre kommentarer gis fortløpende.

Grupperingen nedenfor viser til skjemaet *IT-kontroller Vurdering av intern-kontroll-IT*. Skjemaet er tidligere sendt til Monica Valde Sørland og Ingjar Eggen til kontroll. Nedenfor har vi gjennomgått innholdet i skjemaet og konkludert.

2.1 ENDRINGER I EKSISTERENDE PROGRAMVARE

2.1.1 Endringsforespørsel (Unique)

Rutineene er ikke skriftlig, som god IT-skikk anbefaler. Antall brukere er forholdsvis stort, men miljøet er oversiktlig. Imidlertid anbefaler vi Levanger kommune å lage skriftlige rutiner på hvordan endringsforespørsler skal håndteres. Men som beskrevet nedenfor bør Levanger kommune utarbeide flere skriftlige dokumentasjoner. Endringsforespørsler er da en naturlig del av dokumentasjonen.

2.1.2 Testing av endringer i programmer (Unique)

Endringer i Unique blir ikke testet før innleggelse i produksjonsbasen. Ved eventuelle problemer blir Unique kontaktet. Avhengig av typen problem vil enten Levanger kommunes egne folk rette feil ut i fra anvisning fra Unique eller Unique kobler seg inn på Levanger kommunes server og retter feilen.

Revisjonen vil presisere at når eksterne personer (som Unique) er inne i Levanger kommunes systemer, er det viktig at Unique dokumenterer utført oppdrag. Vi anbefaler at Levanger kommune standardiserer testing hvor brukerne blir involvert. En standardisering av test vil også komme til nytte i andre datasystemer.

2.1.3 Dokumentasjon og opplæring (Unique)

Brukerne synes fornøyde med dokumentasjonen av standard programvare. Alle endringer blir lagt inn i Unique, og alle brukerne har tilgang til logg som viser de siste endringer. Det er ikke laget egne rutinebeskrivelser for Levanger kommune.

Det er ikke oppdatert skriftlig systemdokumentasjon for Levanger kommune. Dette bør prioriteres med tanke på sårbarheten for IT-avdelingen. Levanger kommune leier inn konsulenter ved behov og ved ferieavvikling.

I anbefaling til god IT-skikk dokument ”Dokumentasjon av IT-systemer” avsnitt 3.1 står følgende:

”Det skal foreligge en dokumentasjon som viser samtlige IT-systemer og sammenhengen mellom disse. Denne dokumentasjonen bør inneholde en overordnet informasjon om systemene. En samlet dokumentasjon av et system skal for øvrig bestå av:

- ✓ *Systemdokumentasjon*

✓ Brukerdokumentasjon

✓ Driftsdokumentasjon

Dokumentasjonen skal omfatte både automatiske og manuelle rutiner i forbindelse med IT-systemer. ”

2.2 IT-SIKKERHET

2.2.1 Ledelsens tilsyn

Det er ikke utarbeidet skriftlige krav til IT-sikkerhet. Kontrollen for lønns- og økonomisystemet er tillagt IT-avdelingen. Alle brukere har ulike brukernavn og passord. I ”Anbefaling til god IT-skikk – tilgangskontroll IT-systemer” kan vi sitere følgende:

”Virksomhetens styre og daglig ledelse må ta bevisst stilling til de påfølgende områder vedrørende tilgangskontroller. Prinsippene for tilgangskontroll må kommuniseres til de ansatte på en klar måte f.eks i en sikkerheshåndbok. Holdningsskapende arbeid må prioriteres for å sikre at de prinsipper ledelsen fastsetter, etterleves av organisasjonen”

I tråd med retningslinjene over, bør kommunens ledelse ta et bevisst valg om hvilke rettigheter de forskjellige brukerroller skal ha. Ledelsen behøver ikke å detaljbestemme innholdet, men gi retningslinjer for overordnede målsettinger for tilgangsrettighetene. I tillegg vil vi anbefale at alle brukerne underskriver ”etiske retningslinjer” for brukere av Levanger kommunes nettverk. Det er viktig at både interne og eksterne brukere er kjent med disse. Retningslinjene bør periodevis gjennomgås og oppdateres.

2.2.2 Tilgangskontroller på systemnivå

Tilgangskontroller er etablert. Men det foretas ingen rutinemessige kontroller med at systemet blir fulgt opp når folk får endrede arbeidsoppgaver eller slutter. Sikkerhetsprogramvare benyttes ikke. IT-avdelingen består av tre faste personer og alle har samme rettigheter til alle systemer. Revisjonen har ikke selv sjekket hvem som har tilgang til Unique Security fordi det eksisterer ikke rapport over tilganger. Men vi har fått muntlig beskjed om at det kun er de tre personene på IT-avdelingen som har tilgang (T. Olsen, M.V.Sørland, G.Strøm) med personlig brukerident. Det finnes ingen dummybruker av typen ”Unique”.

2.2.3 Tilgangskontroller på programvarenivå (Unique)

Tilgangskontroller er etablert, men det foretas ingen rutinemessig kontroll med at systemet blir fulgt opp når folk får endrede arbeidsoppgaver eller slutter. Vi har fått informasjon om at en egen arbeidsgruppe skal gjennomgå rutinene for tilgangskontroller. Det er en viktig jobb som bør prioriteres. I ”Anbefaling til god IT-skikk – tilgangskontroll IT-systemer” kan vi sitere følgende:

”Sikkerhetsreglene må være skriftlige og være uttrykt på en slik måte at de gir mening for brukerne.”

2.2.4 Fysisk sikring

Alle backuper er lagret i brannsikkert skap og månedsbackup blir lagret i banken. Maskinrommet er sikret med lås, og IT-ansatte er de eneste som har tilgang til dette rommet. Det finnes ikke servere på utsiden av maskinrommet. Sikkerheten vurderes til å være god.

2.2.5 Beskyttelse mot datavirus

Mot Internett er nettverket er beskyttet med ytre og indre brannmur. I tillegg er det installert programvare for virussekk på hver enkelt pc. Levanger kommune har aldri hatt alvorlige problemer med datavirus verken på arbeidsstasjoner eller i kommunes datanettverk.

2.3 IT-DRIFT

2.3.1 Driftsansvar

IT-ansatte har ingen sertifisering og kan selv beslutte hvilken faglig oppdatering som trengs. Formell opplæring av IT-personell er dyrt. Faglig kompetanse blir tilført IT-avdelingen under arbeid. Det er derfor en litt "tilfeldig" opplæring, men IT-avdelingen er fornøyd med ordningen.

Sett fra vårt synspunkt bør opplæringen formaliseres med en opplæringsplan. Det er viktig å presisere IT-leders ansvar for at avdelingen får den opplæring som kreves for å holde driften i gang. Det er viktig at oppdatering på nye områder er en kontinuerlig prosess.

I Datatilsynets "**Veiledning i informasjonssikkerhet** for kommuner og fylker" står det om kompetansekrav i del V:

Alle medarbeidere som bruker, administrerer, vedlikeholder eller utvikler informasjonssystemene, eller på annen måte påvirker informasjonssikkerheten, skal ha nødvendig kompetanse til å utføre sine oppgaver. Medarbeidere med overordnet operativt ansvar for drift av informasjonssystemet eller med informasjonssikkerheten, skal kunne dokumentere nødvendig kompetanse relevant for den teknologi virksomheten benytter i informasjonssystemet.

Virksomheten skal utarbeiderutiner som sørger for at kompetanse vedlikeholdes og utvikles. Sentrale elementer i slike rutiner består av:

- oversikt over den enkelte medarbeiders kompetanse
- oversikt over kompetansekrav for de ulike oppgaver og funksjoner
- årlige planer for kompetanseutvikling

2.3.2 Batchkjøringer

Det er ingen overordnet batchkjøringsplan. IT-avdelingen mener at planlegging av batchkjøringer er ikke nødvendig da dette er av meget lite omfang. Driftsrutiner for batchkjøringer bør utarbeides.

2.3.3 Sikkerhetskopiering

Det tas sikkerhetskopi hver natt av alle data og programmer. I tillegg tas kopi hver uke, 14.dag, måned, kvartal og en årsbackup. Tilbakelegging av sikkerhetskopier er også utført i

praksis. Her er det gode rutiner som fungerer. Det bør utarbeides en skriftlig rutine for hvordan tilbakeføring av backup skal utføres.

2.3.4 Oppstartsrutiner etter driftsfeil

I arbeidstiden er det opprettet et eget telefonnummer for varsling av driftsfeil. Utenfor arbeidstiden er det mulig å ringe til IT-sjefens mobiltelefon. Det er opprettet et eget register for driftsfeil og oppfølging. Driftsrutinene fungerer godt. Enhetslederne er selv ansvarlig for å varsle sine medarbeidere om driftsproblemer.

2.3.5 Sikring av nettverk

Det er ikke installert noen ekstra ekstern linje. Ved behov kan eksterne leverandører levere oppringt samband på kort varsel.

2.3.6 Katastrofeplaner

Levanger kommune har ikke katastrofeplan for IT-området.

Vi vil henvise til ”Grunnleggende retningslinjer for god IT-skikk”.

Følgende er bla beskrevet om katastrofeplaner i ”Grunnleggende retningslinjer for god IT-skikk”:

” God IT-skikk forutsetter at informasjonsbehandlingen er sikret på en slik måte at kontinuitet i drift opprettholdes selv om en katastrofe skulle inntreffe. Virksomheten må i denne forbindelse etablere en katastrofeplan og denne må minst inneholde:

- ✓ *Virksomhetens definisjon av en katastrofesituasjon*
- ✓ *Virksomhetens krav til kontinuitet i informasjonsbehandlingen definert for det enkelte system.*
- ✓ *Rutiner for varsling dersom en katastrofe inntreffer”*

Vi vil anbefale Levanger kommune å gjennomgå IT-systemene med tanke på katastrofeplanlegging ut i fra punktene i God IT-skikk. Planen må jevnlig oppdateres.

2.3.7 Sikring av support fra leverandør

Ved normale forhold er ikke support problematisk. Ved en eventuell konkurs hos leverandør, kan Levanger kommune fortsatt benytte egne data.

2.4 REVISORS KONKLUSJON

Etter vår mening kan intern-kontrollen på IT-området bli enda bedre.

- Det bør utarbeides mer skriftlig dokumentasjon i henhold til God IT-skikk.
- Ledelsen må utarbeide overordnede retningslinjer for brukertilgang og tilgangskontroll.
- Opplæringsplan bør utarbeides for å sikre at IT-kompetanse vedlikeholdes og utvikles.

- Katastrofeplan må utarbeides for IT-området. Informasjonsbehandlingen må være sikret på en slik måte at kontinuitet i drift opprettholdes selv om en katastrofe skulle inntreffe.
- Ledelsen må utarbeide overordnede retningslinjer for brukertilgang og tilgangskontroll.