KONTROLLUTVALGET I ÅS KOMMUNE

Kommunestyret i Ås
Ås kommune
HER

Ås, den 17. desember 2012
Jnr 212 /12 A 417

SAK FRA KONTROLLUTVALGET TIL KOMMUNESTYRET

Vedlagt oversendes særutskrift av følgende sak fra kontrollutvalget:

KU-sak 45/12
Forvaltningsrevisjonsrapport om info.sikkerhet og IT-drift

Med vennlig hilsen

Jan T. Løkken
sekretær

Kopi: Rådmannen

Sekretariat: Follo interkommunale kontrollutvalgssekretariat

Postadresse	**Postboks 195, 1431 Ås**
Besøksadresse	**Rådhusplassen 29**
Telefon (m)	**959 39 656**
E-post	**FIKS@as.kommune.no**
Internett:	**www.follofiks.no**

FIKS

KONTROLLUTVALGET I ÅS KOMMUNE

SÆRUTSKRIFT

fra kontrollutvalgets møte den 11. desember 2012:

KU-sak 45/12
FORVALTNINGSREVISJONSRAPPORT OM INFO.SIKKERHET OG IT-DRIFT

Sekretariatets innstilling:

1. Kontrollutvalget tar rapporten om Informasjonssikkerhet og IT-drift til orientering.
2. Saken oversendes kommunestyret med innstilling:

   Kommunestyret tar rapporten om Informasjonssikkerhet og IT-drift til orientering.

   Rådmannen bes følge opp rapportens anbefalinger og melde tilbake til kontrollutvalget om oppfølgingen innen seks måneder.

Kontrollutvalgets behandling 11.12.2012:

Revisjonen presenterte hovedtrekkene i rapporten. Revisjonen understreket behovet for at de vedtatte sikkerhetstiltakene årlig blir etterprøvd for om de virker i praksis. Det nåværende avvikssystemet i kommunen er ganske nytt og revisjonen har ikke sjekket bruken av dette, men har fått opplyst at det ikke er meldt vesentlige avvik vedr. IT-sikkerhet.
Fra utvalgets side ble det pekt på at rapporten gir viktig informasjon som vil være nyttig lesing for de folkevalgte i kommunen.

Votering:

Innstillingen ble enstemmig vedtatt.

Kontrollutvalgets vedtak 11.12.2012:

1. Kontrollutvalget tar rapporten om Informasjonssikkerhet og IT-drift til orientering.
2. Saken oversendes kommunestyret med innstilling:

   Kommunestyret tar rapporten om Informasjonssikkerhet og IT-drift til orientering.

   Rådmannen bes følge opp rapportens anbefalinger og melde tilbake til kontrollutvalget om oppfølgingen innen seks måneder.

Sekretariat: Follo interkommunale kontrollutvalgssekretariat
Postadresse **Postboks 195, 1431 Ås**
Besøksadresse **Rådhusplassen 29**
Telefon **64 96 20 58 (m)959 39 656**
E-post **FIKS@as.kommune.no**
Internett: **www.follofiks.no**

Ås, den 17. desember 2012

Jan T. Løkken
Sekretær

Vedlegg: Forvaltningsrevisjonsrapport om informasjonssikkerhet og IT-drift fra Follo distriktsrevisjon datert 30.11.2012.
Utv.sak 45/12

Sekretariat: Follo interkommunale kontrollutvalgssekretariat
Postadresse Postboks 195, 1431 Ås
Besøksadresse Rådhusplassen 29
Telefon 64 96 20 58 (m)959 39 656
E-post FIKS@as.kommune.no
Internett: www.follofiks.no

KU-sak 45/12
FORVALTNINGSREVISJONSRAPPORT OM INFO.SIKKERHET OG IT-DRIFT

Saksbehandler: Jan T. Løkken	Arkivnr: 219	Saksnr.: 12/2883
Utvalg	**Utv.nr.**	**Møtedato**
Kontrollutvalget	45/12	11.12.2012

først.

Sekretariatets innstilling:

1. Kontrollutvalget tar rapporten om Informasjonssikkerhet og IT-drift til orientering.
2. Saken oversendes kommunestyret med innstilling:

   Kommunestyret tar rapporten om Informasjonssikkerhet og IT-drift til orientering.

   Rådmannen bes følge opp rapportens anbefalinger og melde tilbake til kontrollutvalget om oppfølgingen innen seks måneder.

Tidligere politisk behandling:

Kontrollutvalget sak 14/12

Avgjørelsesmyndighet:

Kommunestyret

Behandlingsrekkefølge:

Kontrollutvalget
Kommunestyret

Vedlegg som følger saken trykt:

Forvaltningsrevisjonsrapport om Informasjonssikkerhet og IT-drift i Ås kommune fra FDR datert 30.11.2012.

SAKSUTREDNING:

Kontrollutvalget vedtok prosjektplanen for den foreliggende rapporten i sitt møte den 8. mai d.å., jf. sak 14/12.
Sekretariatet konstaterer at rapporten drøfter de problemstillinger som ble vedtatt i prosjektplanen. I henhold til planen skulle rapporten vært ferdig ved utgangen av august d.å.

Rapporten opplyser at undersøkelsen er basert på en kombinasjon av analyser av innhentede dokumenter og intervjuer med personer i ulike roller knyttet til IKT- og informasjonssikkerhet i kommunen.

Viktige funn i rapporten:

- Sikkerhetsmål og sikkerhetsstrategi er utarbeidet
- Kommunen har oversikt over personregistrene
- Avvikssystem finnes
- IKT–plan er utarbeidet

Rapporten forteller at det er et godt samarbeid mellom IT-avdelingen og andre enheter.

Rapporten avdekker også noen svakheter som foreslås rettet opp gjennom revisjonens anbefalinger:

- *Oppgavene som sikkerhetsansvarlig og IT- sjef bør ikke innehas av samme person.*
- *Fullverdig sikkerhetsrevisjon bør gjennomføres årlig.*
- *Beredskapsplan for IT- avdelingen bør utarbeides.*
- *Innføre rutine om å kontrollere tilganger i kommunens fagsystemer jevnlig der dette ikke gjøres i dag.*
- *Utarbeide skriftlige rutinebeskrivelser for bruk av manuelle systemer ved en ITdriftsstans.*
- *Vurdere å innføre vaktordning utenom ordinær arbeidstid.*
- *Vurdere loggføring av oppe-/nedetid på IT-systemene.*

Sekretariatet merker seg at avvik i forbindelse med IT-sikkerhet skal meldes via det elektroniske avviks- og forbedringssystemet til kommunen. Rapporten skriver at «*det er ikke framkommet informasjon på at det er meldt vesentlige avvik innen IKT de siste årene*» (s. 15). De ville vært interessant å få vite hvordan revisjonen har undersøkt dette og i hvilken grad dette systemet benyttes.

Sekretariatet merker seg at rapporten beskriver hvordan personalopplysnings-reglene ivaretas ved bruken av de elektroniske systemene i kommunen. I rapportens beskrivelse av sykehjemmenes bruk av Gerica går det fram at det bl.a. skrives ut brukerkort fra systemet hvor personopplysninger samt diagnose framgår s. 26 -27). Noe av dette blir arkivert i egen perm. Tilsvarende skrives det ut lister med personopplysninger etc. i hjemmetjenesten og ved helsestasjonene. Det ville vært nyttig med en vurdering av rutinene her i forhold til overnevnte regler.

Rådmannens høringsuttalelse er tatt inn mot slutten av rapporten. Uttalelsen har ingen innvendinger mot rapportens konklusjoner og anbefalinger. Spørsmål 5 lyder: *"Vil rådmannen vurdere iverksetting av tiltak på bakgrunn av rapportens konklusjoner og anbefalinger?"* Vi minner her om at kontrollutvalget sender rapporten til kommunestyret som vanligvis gjør vedtak om rådmannens oppfølging.

Follo distriktsrevisjon

Forvaltningsrevisjonsrapport

Informasjonssikkerhet og IT-drift

ÅS kommune

Dato 30.11.2012

RAPPORT 3/12

Forord

Forvaltningsrevisjon er en lovpålagt oppgave for Ås 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 Ås kommune.

Prosjektet er gjennomført i perioden mai – september 2012. Follo distriktsrevisjon vil benytte anledningen til å takke kommunens kontaktperson og øvrige ansatte i Ås kommune som har bistått revisjonen i forbindelse med gjennomføringen av undersøkelsen.

Steinar Neby
Revisjonssjef

Even Tveter
Prosjektleder

Innholdsfortegnelse

1 Sammendrag

Forvaltningsrevisjonsprosjektet om informasjonssikkerhet og IT-drift i Ås kommune er gjennomført iht. vedtak i kontrollutvalget i Ås kommune. Formålet med prosjektet er å kartlegge og vurdere kommunens sentrale IKT-funksjoner med fokus på sikkerhet, drift, overordnede målsettinger og rutiner.

Revisjonen har vurdert at følgende forhold i Ås kommune er tilfredsstillende:

- Sikkerhetsmål og sikkerhetsstrategier er utarbeidet. Sikkerhetsorganisasjon, ansvar og rollefordelinger er tydelig beskrevet.
- En oversikt over personregistrene i kommunen.
- Ås kommune har et avvikssystem for å håndtere avvik, og det er utarbeidet rutinebeskrivelse for håndtering av avvik.
- IKT- strategiplan som inneholder mål, delmål og satsningsområder er utarbeidet.

Gjennom prosjektet er det identifisert forhold hvor endringer bør vurderes:

- Det bør foretas en arbeidsdeling av oppgavene som sikkerhetsansvarlig og IT- sjef. Disse oppgavene innehas i dag av samme person.
- Sikkerhetsrevisjon i forhold til å etterprøve de sikkerhetstiltakene som er vedtatt bør gjennomføres årlig.
- Beredskapsplan for IT- avdelingen bør utarbeides.
- Rutine for jevnlig kontroll av gitte tilganger i kommunens fagsystemer bør innføres der dette ikke gjøres i dag.
- Skriftlige rutinebeskrivelser for bruk av manuelle systemer ved en IT driftsstans bør utarbeides.
- Vaktordning utenom ordinær arbeidstid for IT- avdelingen bør vurderes.
- Loggføring av oppe-/nedetid på kommunens servere for å måle om man når kravene satt i strategiplanen.

Follo distriktsrevisjon har med bakgrunn i de funn som er gjort, avslutningsvis gitt en del anbefalinger som vi mener kan bidra til forbedringer innen informasjonssikkerhet og IT-drift.

2 Formål og problemstillinger

2.1 Bakgrunn

Kontrollutvalget fattet i møte 22. mars 2012 vedtak om at det skulle gjennomføres en forvaltningsrevisjon av informasjonssikkerhet og IT-drift i Ås kommune. Prosjektet ble godkjent som sak 14/12.

2.2 Formål og problemstillinger

Formålet med prosjektet er å kartlegge og vurdere kommunens sentrale IKT-funksjoner med fokus på sikkerhet, drift, overordnede målsettinger og rutiner.

Følgende problemstillinger er belyst:

Informasjonssikkerhet
- Har kommunen tilfredsstillende rutiner og retningslinjer for å sikre personopplysningsforskriftens krav til konfidensialitet, integritet og tilgjengelighet?

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

2.3 Avgrensninger

Prosjektet omfatter ikke en kartlegging av Ås 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 er avgrenset til et overordnet nivå i kommunen og inkluderer av den grunn ikke de enkelte virksomheters/ansattes aktiviteter.

3 Metoder og gjennomføring

Undersøkelsen er basert på en kombinasjon av analyser av innhentede dokumenter og intervjuer med personer i ulike roller knyttet til IKT- og informasjonssikkerhet i kommunen. Hensikten med dokumentanalysen er å vurdere om styringsdokumentene innen IKT er tilstrekkelige i forhold til aktuelle anbefalinger (beste praksis) knyttet til IKT-drift og krav i forskrift knyttet til informasjonssikkerhet. Intervjuene av ansatte og ledere innen IKT- og informasjonssikkerhet er rettet mot å få en forståelse av praksis og etterlevelsen av regelverket og rutiner i kommunen.

3.1 Gjennomføring

Kontaktperson i kommunen har vært kommunens service- og kommunikasjonssjef.

Ut fra en vurdering av avhengighet, størrelse og bruk av sensitive opplysninger ble ovennevnte funksjoner valgt ut for intervju:

- Service- og kommunikasjonssjef
- Helse- og sosialsjef
- Systemansvarlig Gerica
- Systemansvarlig Hspro
- Systemansvarlig OPPAD
- Enhetsleder hjemmetjenesten
- Superbrukere Gerica

3.2 Dataenes pålitelighet og gyldighet

Kvalitetssikring av datagrunnlaget omfatter en vurdering av reliabilitet og validitet.

Begrepet **reliabilitet** beskriver analysens pålitelighet. I dette ligger at pålitelighet setter krav til nøyaktig datainnsamling og at det ikke er skjedd systematiske feil underveis i innsamlingen. Begrepet **validitet** beskriver analysens gyldighet, det vil si hvor godt det gitte materialet belyser problemstillingen i en undersøkelse.

Intervjusituasjonen gjør det også mulig å kunne oppklare misforståelser og stille oppfølgingsspørsmål, hvilket også bidrar til styrket reliabilitet. Det styrker også reliabiliteten at intervjuobjektene selv har verifisert de opplysningene de har gitt i intervjuene. Rapportens faktadel har også vært på høring hos kommunens kontaktperson før rapporten er ferdigstilt.

4 Informasjonssikkerhet

Har kommunen tilfredsstillende rutiner og retningslinjer for å sikre personopplysningsforskriftens krav til konfidensialitet, integritet og tilgjengelighet?

4.1 Revisjonskriterier

Av Personopplysningsloven (POL) § 13 framgår det at *" den behandlingsansvarlige[1] databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet men hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger".*

Av veileder til sikkerhetsbestemmelsen utgitt av Datatilsynet[2] framgår det at 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.

Tilfredsstillende informasjonssikkerhet skal oppnås ved hjelp av planlagte og systematiske tiltak. Begrepet innebærer at kjente teknikker og anerkjente standarder for kvalitetsstyring, internkontroll og informasjonssikkerhet skal legges til grunn ved sikkerhetsarbeidet.

Personopplysningsforskriften (POF) definerer nærmere hvilke krav som hviler på kommunen for at tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger finner sted:

§ 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. Ledelsen skal jevnlig gjennomgå sikkerhetsmål og strategi.

§ 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.

[1] For Ås kommune vil dette være rådmannen.
[2] Desember 2000

§ 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.

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

§ 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.

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. Arbeidsoppgaver for sikkerhetsleder vil normalt omfatte forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner samt kontroll med risikovurdering og avviksbehandling.

§ 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[3], 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.

§ 2-11 sier at det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er viktig.

§ 2-12 sier at det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgang er nødvendig. Av veileder fra Datatilsynet framgår det at det skal tas backup av personopplysninger.

§ 2-13 sier at det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig. Av veileder fra Datatilsynet framgår det at dette innebærer bl.a. tilstrekkelig beskyttelse mot datavirus og annen ødeleggende programvare.

Kriterier

På bakgrunn av det ovennevnte legges følgende kriterier til grunn for undersøkelsen:

- Kommunen skal ha etablert en sikkerhetsledelse som jevnlig gjennomgår sikkerhetsmål og strategi.
- Kommunen skal ha en klar organisering med etablerte ansvars- og myndighetsforhold.
- Kommunen skal ha tilstrekkelig oversikt over de personregistre som finnes og gjennomføre risikovurdering av disse.
- Kommunen skal jevnlig gjennomføre sikkerhetsrevisjon.

[3] TV-202:2005

- Kommunen skal ha et avvikssystem for å håndtere sikkerhetsbrudd.
- Kommunen skal ha gjennomført tiltak som:
  - Ivaretar fysisk sikring av IKT-utstyr.
  - Hindrer uautorisert innsyn i personopplysninger.
  - Sikrer tilgang til personopplysninger.
  - Hindrer uautorisert endring av personopplysninger.

4.2 Faktabeskrivelse

4.2.1 Sikkerhetsledelse, sikkerhetsmål og strategi

Den utarbeidede *Plan for informasjonssikring,* inngår som en del av Ås kommunes kvalitetssystem. Planen er revidert i 2011 og er forankret i prosess for informasjonssikkerhet og personopplysningsforskriften § 2-3. Planens mål er:

> *Ås kommunes informasjonssikkerhetsplan bidrar til å sikre en effektiv og rasjonell organisasjon med store krav til sikring av informasjon på alle nivåer, og at ansatte er seg bevisst det ansvaret man har for å sikre at informasjon blir behandlet slik lov og forskrifter krever.*

I planen framgår det ansvar og oppgaver for de enkelte roller:

Rådmannen (behandlingsansvarlig):

Ansvar:

- Sørge for at det er etablert et styringssystem for IKT-sikkerhet og at dette vedlikeholdes.
- Sørge for at informasjonssikkerheten er tilfredsstillende.
- Beslutter formålet med behandlingen av personopplysninger.
- Beslutter hvilke hjelpemidler som skal brukes.

Oppgaver:

- Melde og eventuelt å søke konsesjon for behandling til Datatilsynet.
- Vedta, implementere, vedlikeholde og følge opp bruken av styringssystem for IKT-sikkerhet.

Service- og kommunikasjonssjef (sikringsansvarlig):

Ansvar:

- Overvåke at informasjonssystemet benyttes i samsvar med bestemmelser og prosedyrer og rapporterer til databehandlingsansvarlig.

Oppgaver:

- Utarbeide og vedlikeholde prosedyrer rundt egen funksjon.

- Utforming av styrende, utførende og kontrollerende dokument i kommunen sitt kvalitetssystem.
- Forberede ledergruppens årlige gjennomgang.
- Følge opp iverksetting av tiltak som er besluttet etter gjennomganger.
- Samordne og gjennomføre sikkerhetsrevisjoner.
- Vurdere rapporterte avvik.
- Forestå risikovurderinger.
- Godkjenne dokument til kommunens kvalitetssystem.
- Erverve og vedlikeholde kunnskap om trusler, sårbarhet, sikkerhetstiltak og teknikker, sikkerhetskrav.
- Overordnede ansvaret for at det jevnlig blir holdt opplæring av de ansatte for å gi alle kunnskap om kommunens sikringspolitikk, slik at alle kjenner til hvilke regler som gjelder for behandling av personsensitive opplysninger.
- Opplæring.
- Rådgiving.

Systemeiere

Systemeiere er de som har ansvar for de ulike fagsystemene.

Ansvar:

- Sørge for at sitt informasjonssystem er tilgjengelig.
- Sørge for at sitt informasjonssystem oppfyller lovbestemte og andre krav.
- Sørge for at sitt informasjonssystem fungerer som besluttet.
- Definere tilgangsroller.
- Rapporterer til IKT-ansvarlig.
- Delegering av daglige ansvar for oppfølging av systemet til en systemansvarlig.

Systemansvarlige

Ansvar:

- Systemansvarlig er de som systemeier delegerer ansvaret til for oppfølging av daglig drift.

Når det gjelder oppgaver for systemansvarlig framgår dette av den utarbeidede retningslinje for systemansvarlig og superbruker. Her framgår det:

- Systemansvarlig skal definere roller og lage filter til disse slik at de ansatte får tilgang til nødvendig opplysninger.
- Systemansvarlig skal passe på at roller og filter hindrer innsyn i opplysninger de ansatte ikke trenger.
- Systemansvarlige må kontrollere at tildelte tilganger (roller og filtre) fungerer etter forutsetningene.
- Systemansvarlig gir opplæring til superbrukere og sørger for at de har nødvendig kompetanse.
- Systemansvarlig skal være kontaktperson mellom IT-team og de ansatte og mellom leverandør og IT-team.

Enhetsledere/ledere

Ansvar:

- Sørge for opplæring av de ansatte
- Beredskap
- Tildeling, vedlikeholde og inndragning av roller / tilgang
- Rapportere avvik i kommunens avvikssystem

Oppgaver:

- Sørge for at det gis opplæring i nødvendige systemer og i sikkerhet
- Lage og teste beredskapsprosedyrer for systemsvikt
- Tildele den enkelte medarbeider korrekt rolle og bestille tilgang til nettverk, system og fagapplikasjon.
- Vedlikeholde medarbeiderens tilgangsnivå
- Sørge for stenging av tilganger når arbeidsforhold opphører
- Håndtere sikkerhetsavvik
- Kontroll av tilgang på tvers

Ledelsens gjennomgang

Ledergruppen skal årlig gjennomgå og revidere sikring av informasjon i kommunen. Dette gjøres gjennom årlig gjennomgang og rullering av plan for informasjonssikring.

Revisjonen innebærer at ledergruppa vurderer:

- Målet for sikringsarbeidet
- Informasjonssikkerhetspolicy
- Internkontrollsystemet
- Avviksbehandlingen
- Organiseringen av sikringsarbeidet

Ås kommunes sikkerhetsorganisasjon er utarbeidet i henhold til Personopplysningsforskriften § 2-7 Organisering.

Rådmannen har delegert det overordnede kontrollerende ansvaret for informasjonssikkerhet til sikringsansvarlig (Service- og kommunikasjonssjef) i Ås kommune.

Ansvaret for de enkelte fagsystemene i Ås kommune er videredelegert til systemeierne.

4.2.2 Sikkerhetsrevisjon

Sikringsansvarlig skal i henhold til Plan for informasjonssikring minst en gang i året iverksette revisjon av informasjonssystemet og informasjonstryggheten. Revisjonen skal benyttes som grunnlag for mulige endringer i mål og strategi.

Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres en gang pr år. Denne skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Det er henvist til en mal som skal brukes til dette.

Ås kommunes gjennomgang av informasjonssikkerhet er forankret i sikkerhetsbestemmelser i personopplysningsforskriften § 2-5. Sikkerhetsrevisjon gjennomføres i henhold til prosedyre for kvalitetssystemets krav, og prosedyrer for ledelsens gjennomgang. Ledergruppen skal årlig gjennomgå og revidere sikringen av informasjon i kommunen.

Revisjonen innebærer at ledelsen vurderer:

- Målet for sikringsarbeidet
- Informasjonssikkerhetspolicy
- Internkontrollsystemet
- Avviksbehandlingen
- Organiseringen av sikringsarbeidet.

I planen inngår en risikovurdering av de enkelte systemene. Det er utarbeidet risiko- og tiltaksskjema hvor det er vurdert 30 risiki. Det er vurdert både sannsynlighet og konsekvens opp mot akseptabel risiko. Det er videre utarbeidet en handlingsplan med risikoreduserende tiltak hvor ansvar og oppfølging er fastsatt.

Prosessbeskrivelse

Det er laget en prosessbeskrivelse for informasjonssikkerhet. Denne skal sikre at alle krav blir ivaretatt i forbindelse med daglig bruk og innkjøp/etablering av informasjonssystemer i Ås kommune.

Prosessbeskrivelsen skal benyttes i forbindelse med:

- Administrative og organisatoriske forhold som omfatter informasjonssystemer.
- Risiko- og sårbarhetsanalyser.
- Avbruddsplanlegging (katastrofeplanlegging).
- Program- og maskinvaresikkerhet.
- Tilgangskontroller.
- Kommunikasjonssikkerhet.
- Drift og vedlikehold av informasjonssystemer.
- Fysisk sikkerhet.

De forskjellige ansvarsforhold er videre beskrevet:

- Rådmannen har ansvar for at det utarbeides overordnet policy og retningslinjer for informasjonssikkerhet i Ås kommune.
- Ansvaret for det praktiske sikkerhetsarbeidet ligger hos de respektive enheter i kommunen, og koordineres av sikkerhetsansvarlig som er Service- og kommunikasjonssjefen.
- Etatssjefer har et selvstendig tilsyns-, sikkerhets- og kontrollansvar for etatens bruk av informasjonssystemer.
- Alle ledere i Ås kommune har ansvar for gjennomføring og opprettholdelse av informasjonssikkerhet. Dette innebærer:

- At det i eget ansvarsområde vedtas og iverksettes tiltak i samsvar med gjeldende policy og retningslinjer for informasjonssikkerhet.
- Å legge forholdene slik til rette at berørte ansatte i ansvarsområdet får tilført nødvendig kompetanse, forståelse og innsikt i sikkerhetsarbeidet.
- Påse at vedtatte sikringstiltak følges og overholdes.
- Alle ansatte og innleide medarbeidere i kommunen skal overholde instrukser og bestemmelser om sikring av informasjon og verdier.
- Det er de respektive ledere som har ansvaret for at medarbeidere får den nødvendige kunnskap om og forståelse for sikkerhet.
- Service og kommunikasjonssjefen har ansvar for at prosessbeskrivelsen og referanser etableres og ajourføres.

Gjennomføringsprosessen er videre beskrevet:

- Informasjonssikkerhet i Ås kommune innebærer iverksettelse av nødvendige sikkerhetstiltak for å redusere sårbarheten knyttet til Ås kommunes informasjonsbehandling og for å være best mulig forberedt på å håndtere evt. feil og uhell, dvs. sikre at:
- Informasjon ikke blir kjent for uvedkommende.
- Informasjonen er fullstendig, korrekt og à jour.
- Informasjon er tilgjengelig når det er behov for den.
- Det gjennomføres risikoanalyse minst en gang i året.
- På bakgrunn av gjennomført risikoanalyse skal det etableres tiltaksliste som skal godkjennes av ledergruppen.
- Tiltakene gjennomføres av de systemansvarlige innenfor det området tiltaket gjelder.
- Det utarbeides rapport som inneholder dokumentert risikoanalyse og tilhørende tiltaksplan.

4.2.3 Personregistre

Behandlingsansvarlig er ansvarlig for at personopplysninger behandles i samsvar med personopplysningsforskriften. Det er laget en oversikt over alle personregistre som kommunen har. Oversikten beskriver hvordan konfidensialitet, tilgjengelighet og integritet skal sikres. Oversikten er en del av grunnlaget for risikovurderingen. Rådmannen skal fastlegge kriterium for den risiko som kan aksepteres, eller som eventuelt må reduseres med hjelp av sikkerhetstiltak.

Som vedlegg til planen for informasjonssikring foreligger skjema for meldepliktige registre. Her fremgår hvilke personopplysninger som Ås kommune behandler. Det framgår av skjemaet hva formålet med opplysningene er, hjemmel for opplysninger, type opplysninger, sikringstiltak, hvor informasjonen er lagret og backuprutiner, registerets omfang, om opplysningene er meldepliktige eller konsesjonspliktige, hvilken avdeling som har ansvar, samt hvem som er systemeier av systemet som behandler personopplysninger. Ås kommune behandler i følge dette skjemaet opplysninger innen:

- Lønn og personal
- Skole og barnehage
- Barnevern
- Helsetjenester barn/ unge
- Sosialstøtte

- Pleie og omsorg
- Verge

Meldinger er sendt Datatilsynet for disse personopplysningene, og meldingene er arkivert i Ås kommunes arkiver.

4.2.4 Avviksbehandling

Av Plan for informasjonssikring framgår det at avvik i forbindelse med IT- sikkerhet skal meldes gjennom det elektroniske avviks- og forbedringssystemet Kvalitetslosen. Eksempler på avvik er gitt i planene. Det er også henvist til prosedyre for denne håndteringen, *Prosess for forbedring*. Av denne framgår det at formålet er *«sikre at kvalitetssystemet kontinuerlig bidrar til forbedring og utvikling av kvalitet i tjenesteproduksjon og forvaltning, samt ivaretagelse av lovkrav»*. Videre i prosedyren er det beskrevet ansvarsforhold både når det gjelder melding av avvik men også oppfølging og lukking av avvik.

Det er ikke framkommet informasjon på at det er meldt vesentlige avvik innen IKT de siste årene.

4.2.5 Sikring av informasjon og tilgangskontroll

Ås kommunes IT- systemer driftes lokalt med egen serverpark lokalisert i rådhuset. Serverrommet er sikret med låst dør. Det er bare ansatte i IT- avdelingen som har tilgang til dette rommet. Det er bare en inngang og ikke mulig å få tilgang til serverrommet fra utsiden av rådhuset. Det ble i 2010 foretatt en risikoanalyse, samt full gjennomgang av kommunens serverrom. Det ble konstatert at det var en stor risiko i forbindelse med kjøling av serverrommet. De foreslåtte forbedringene er gjennomført, og det er opplyst at det ikke har vært stopp på kjøleaggregatet siste året.

I Plan for informasjonssikring framgår det at det skal tas sikkerhetskopi av databasen på elektronisk lagringsmedium. Det er utarbeidet *«retningslinjer for sikkerhetskopi av data i Ås kommune»*. Retningslinjene skal *«sikre at Ås kommune tar sikkerhetskopi av alle tilgjengelige data. Skal sikre at Ås kommune ikke taper data»*

Backup over dagens endringer kjøres hver kveld. «Full» backup tas hver fredag og lørdag. Backup skrives til taper, og ukentlige taper blir lagret i brannsikre skap på rådhuset. Måneds- og årstaper blir lagret på fjernarkivet.

I plan for informasjonssikring er det utarbeidet et eget avsnitt for sikringstiltak. Det fremgår her at bevisstgjøring av de ansatte er en kontinuerlig prosess og at det er fokus på dette gjennom opplæring og informasjon. Det er i denne forbindelse utarbeidet 10 sikringsregler for god bruk av IKT. De personene vi har intervjuet har opplyst at disse er slått opp på strategiske steder bl.a. ved kopimaskiner og skrivere.

Planen har også fokus på hvilke kunnskapsmål både ansatte og ledere skal ha i forbindelse med informasjonssikkerhet.

Planen inneholder videre retningslinjer for hvordan opplysninger skal sikres mot uautorisert tilgang for uvedkommende. Det skal bl.a. bare gis tilgang til områder eller soner i den grad det er nødvendig for å utøve pålagte oppgaver og nødvendig tjenestebehov.

Det fremgår videre at det bare skal brukes kommunalt utstyr og i forbindelse med håndtering av sensitive opplysninger skal man bruke «tynne klienter»[4] uten muligheter for lokal lagring. IT- sjef har opplyst at alle som har tilgang til sensitive opplysninger som ligger på sikker sone, bruker tynne klienter. Det er ikke mulig å kopiere data ut fra disse.

Alle fagsystemene er lagret sentralt på Ås kommune sin server. Sensitive opplysninger ligger på «sikker sone». Alle fagsystemene har utnevnt systemeiere, systemansvarlige og superbrukere. Det er utarbeidet egen retningslinje for systemansvarlige og superbrukere. Av denne framgår det: Systemansvarlig skal definere roller og lage filter til disse slik at ansatte får tilgang til nødvendige opplysninger i forhold til hvilke tjenester de yter. Superbruker oppretter passord til nyansatte, superbrukerne skal også følge opp brukerne og sørge for at tilgangene avsluttes i de tilfeller hvor den ansatte slutter eller ikke lenger har behov for tilgangen.

Vi har gjennomført samtaler med systemeiere/systembrukere for systemene:

- Gerica – Elektronisk pleie- og omsorgssystem
- Hspro – Modulbasert system for helsestasjoner og skolehelsetjenesten
- OPPAD – System for tildeling av barnehageplasser.

Gjennom intervjuer med overnevnte blir det bekreftet at Ås kommunes retningslinjer følges. Systemansvarlig for Gerica har oppgitt at det er utnevnt superbrukere på de forskjellige avdelingene og at disse har ansvar for å gjennomgå ansattelister slik at de som ikke lenger er ansatt i kommunen blir slettet. Det er anbefalt at dette gjøres en gang pr. mnd. Superbrukerne har bekreftet at de gjennomgår ansattelister og sørger for å vedlikeholde tilganger. IT- sjef har opplyst at det er den enkelte leder som har ansvaret for å melde ansatte ut og inn av IT-systemene. Dette gjøres via eget skjema til IT-avd. Som en ekstra service sender IT- avd. ut lister til enheter som tradisjonelt har store endringer i arbeidsstokken. I systemet er det definert roller og tilganger slik at man har tilgang på ulik informasjon. Det er også tjenestebasert tilgang slik at man bare har tilgang til de pasientene som man yter tjenester til. I de tilfeller ansatte arbeider på flere avdelinger må de aktivt bytte tilgang i systemet til rett avdeling. Det er flere muligheter i systemet til å skjerme eller dele informasjon på tvers av avdelingene. Det er oppgitt at det har vært fokus på håndtering av sensitive opplysninger og at det oppleves at det er en bevisst holdning til dette.

I hjemmetjenesten benytter man seg av PDAer for tilgang til systemet når man er ute hos pasienter. Det er utarbeidet egne retningslinjer for bruk av disse for å sikre konfidensialitet og tilgjengelighet for helse- og personopplysninger.

Når det gjelder Hspro skal man ta i bruk en ny versjon av dette systemet høsten 2012. I den nye versjonen vil man i langt større grad kunne «styre» de brukertilganger som blir gitt. Den nye versjonen er også tilpasset de nye kravene fra Helsenettet og vil også kunne utveksle informasjon med sykehusene. Det er utarbeidet retningslinje for bruk av elektronisk journal

[4] Arbeidsstasjon uten engen lagringsmulighet og programvare, må kobles opp mot en server.

for forebyggende helse. Her er det beskrevet rutiner for oppretting, endring og avslutning av brukere. De aktuelle roller er definert her og da med hvilke tilganger de skal ha.

OPPAD brukes til å tildele både kommunale og private barnehageplasser, og det ligger ikke sensitive opplysninger i dette systemet. Det er systemansvarlig som har ansvar for å gi tilganger til brukerne. Dette er hovedsystem for alle elever og lærere som skal ha tilganger i IT- systemene. Skolene registrerer elever og lærere og informasjon tilflyter alle IT- systemene den enkelte skal ha tilgang til. Når en lærer slutter vil tilgangene stenges. De private barnehagene har bare tilgang til sine «områder». Det er opplyst at det har vært lite endringer på tilganger og skifte av brukere.

Ansatte i sentraladministrasjonen og i «Erik Johansen-bygget» har printere med koder. Det er planlagt at det skal innføres koder på alle andre printere også. En systemansvarlig har oppgitt at det har forekommet at det er skrevet ut på feil printer. På sykehjemmene står printerne inne på vaktrommene.

I de tilfeller hvor bærbar pc skal brukes i Ås kommune sitt datanett er det utarbeidet sikringstiltak for denne bruken. Dette framgår av Plan for informasjonssikring. Her er det også redegjort for hvilket sikkerhetsnivå som skal ligge til grunn ved fjernaksess til kommunens nettverk.

Planen omtaler også hvordan man håndterer informasjon i e-post. Det framgår her at sensitive opplysninger ikke skal sendes. Det er opplyst at alle ansatte ved ansettelse rutinene får informasjonssikkerhet og bruk av elektronisk kommunikasjon. De må skrive under at de har lest og forstått dette. Dette er den enkelte leders ansvar.

4.3 Vurderinger

4.3.1 Sikkerhetsledelse, sikkerhetsmål og - strategi

I henhold til Ås kommunes *«Plan for informasjonssikring»* har rådmannen det overordnede ansvaret (behandlingsansvarlig). Service- og kommunikasjonssjef har ansvaret for å overvåke at informasjonssystemet benyttes i samsvar med bestemmelser og prosedyrer i tillegg å rapportere til databehandlingsansvarlig. Service- og kommunikasjonssjef innehar også rollen som IT- sjef i Ås kommune. Rollen som ansvarlig for å utføre IT- oppgaver, samt å ha ansvaret for å gjennomføre kontroll innen informasjonssystemet, er altså lagt til samme person. I Datatilsynets kommentarer til sikkerhetsbestemmelsene i personopplysningsforskriften, påpekes det at det er viktig at ansvar og myndighet relatert til drift av informasjonssystemet og for oppfølging av sikringsarbeidet er tillagt forskjellige medarbeidere. Ås kommune bør således skille disse oppgavene slik at samme person ikke innehar begge oppgavene.

Plan for informasjonssikring er oppe til gjennomgang i kommunens ledergruppe årlig. Her blir det bl.a. foretatt en årlig vurdering av målet for sikringsarbeidet, samt kommunens informasjonssikkerhetspolicy. Revisjonen anser således at Ås kommune jevnlig har gjennomgått kommunens sikkerhetsmål og sikkerhetsstrategi slik anbefalingene sier. Den resterende organiseringen og ansvarsforholdene er beskrevet i plan for informasjonssikring

både for systemeiere, systemansvarlige og enhetsledere. Det er også utarbeidet egen retningslinje for systemansvarlig og superbruker som beskriver ansvar og oppgaver for disse.

Revisjonen anser at Ås kommune har en klar organisering og fordeling av oppgaver og ansvar innenfor arbeidet med informasjonssikkerhet. I intervjuer med både systemeiere, systemansvarlig og superbrukere bekrefter de at denne organiseringen samsvarer med det faktiske arbeidet.

4.3.2 Personregistre

Ås kommune har utarbeidet en oversikt over alle personopplysninger som kommunen innehar. Denne er en del av plan for informasjonssikring. Gjennom Plan for informasjonssikring blir det årlig foretatt en risikovurdering av de personregistre som kommunen har. Risikoene er vurdert opp mot akseptabel risiko og det er utarbeidet en handlingsplan for de risikoene som er over akseptabelt nivå. I oversikten over personregistrene framgår også tilstrekkelig informasjon om hjemmel for å inneha personopplysningene, sikringstiltak, lagring, og ansvar for personregisteret. Det er sendt melding til Datatilsynet for alle de registrene som Ås kommune har. All kommunikasjon mot Datatilsynet er arkivert i Ås kommunes arkiver.

Revisjonen anser at Ås kommune har oversikt over de personregistre som kommunen har og formålet med disse. Det synes også som det er foretatt tilstrekkelig risikovurdering av disse.

4.3.3 Sikkerhetsrevisjon

Foretatte undersøkelser viser at det er fokus på sikkerhetsrevisjon gjennom kommunens plan for informasjonssikring. Det framgår her hvilke tiltak som skal gjennomføres. Det er også utarbeidet en handlingsplan som skal dekke opp de risikoene som er avdekket i forbindelse med utarbeidelse av den årlige planen.

§ 2-5 i Personopplysningsforskriften stiller krav til at det jevnlig skal gjennomføres sikkerhetsrevisjon. Denne skal omfatte vurdering av organisering sikkerhetstiltak og bruk av kommunikasjonspartnere og leverandører. I kommentarer til Sikkerhetsbestemmelsene i personopplysningsforskriften[5] framgår det at *bestemmelsen pålegger den behandlingsansvarlige jevnlig, eksempelvis årlig, å etterprøve sikkerhetsarbeidet for å verifisere at de sikkerhetstiltak som er besluttet, faktisk er iverksatt og fungerer etter sin hensikt. Ved sikkerhetsrevisjon sammenlignes faktisk bruk av informasjonssystemet med de retningslinjer for slik bruk som er besluttet. Slik revisjon må ikke blandes sammen med ledelsens gjennomgang av sikkerhetsmål og strategi .....*

Etter vårt skjønn dekker ikke kommunens arbeid på området fullt ut sikkerhetsbestemmelsenes krav om at det skal etterprøves at de sikkerhetstiltakene som er besluttet, faktisk brukes. Sikringsansvarlig burde således gjennomført årlige undersøkelser for å avdekke dette.

[5] Datatilsynet desember 2000

4.3.4 Avviksbehandling

Ås kommune benytter seg av kvalitetslosen som avvikssystem innenfor informasjonssikkerhet. Plan for informasjonssikkerhet inneholder eksempler på hva som kan regnes som avvik. Det er også utarbeidet prosedyre for håndtering av avvikshåndtering gjennom *Prosess for forbedring.* Det er opplyst at det ikke er meldt avvik i forbindelse med informasjonssystemet de siste årene. Revisjonen ser det som positivt at Ås kommune har et avvikssystem samt prosedyrer for ansvarsforhold og bruk av systemet. Revisjonen har ikke foretatt en kontroll av at avvikssystemet brukes på rett måte. Det er opplyst at det ikke er meldt om avvik innen IT de siste årene. For at et slikt system skal ha en verdi er det viktig at alle reelle avvik blir meldt slik at forbedringer kan oppnås. Det er viktig at det er tilstrekkelig kunnskap og vilje blant kommunens ansatte til å bruke avvikssystemet.

4.3.5 Sikring av informasjon og tilgangskontroll

Det synes som om Ås kommune har truffet tiltak som sikrer serverparken på en tilfredsstillende måte. Alle kommunens IT- systemer driftes lokalt og ligger på kommunens servere. Det gjennomføres også jevnlig backup på kommunens systemer slik at den informasjonen som ligger på kommunens servere er tilstrekkelig sikret.

Revisjonen ser det også som positivt at kommunen har fokus på sikring av personopplysningene gjennom plan for informasjonssikring. Det er også utarbeidet en «plansje» med 10 sikringsregler som er slått opp på strategiske steder. Disse skal hjelp de ansatte til å ha tilstrekkelig fokus på sikring av informasjon i det daglige arbeidet. Det er også i planen satt fokus på hvilke kunnskap både de ansatte og lederne skal ha når det gjelder informasjonssikkerhet. Alle ansatte har tilganger som er styrt gjennom passord. Det er systemansvarlig som har ansvaret for å gi tilganger, samt å definere roller og tilganger. For Gerica er det oppgitt at superbrukere foretar en jevnlig kontroll av at ansatte som har sluttet eller på annen måte ikke lenger skal ha tilgang til systemene. Dette er ikke fastsatt i en nedfelt rutine. Kommunes rutiner på dette området er etter vårt skjønn med på å ivareta kravet til å hindre uautorisert innsyn, samt å sikre personopplysningene. Vi mener likevel at kommunen bør innføre en fast rutine for en slik gjennomgang for alle kommunens systemer selv om dette for enkelte systemer gjøres jevnlig i dag. Etter vårt skjønn er det viktig at dette blir formalisert og at denne gjennomgangen blir gjennomført etter en bestemt hyppighet og uavhengig av endring av nøkkelpersoner i organisasjonen.

I forbindelse med bruk av PDA i hjemmetjenesten er det også utarbeidet egne retningslinjer som skal sikre tilgjengelighet og konfidensialitet for bruk av disse.

Ås kommune har vært bevisste på bruk av sikker sone og tynne klienter slik at ikke sensitive opplysninger kan kopieres over på andre maskiner og lagringsmedium. Dette er også et tiltak som i stor grad er med på å sikre uautoriserte innsyn i personopplysningene.

Ås kommune har også utarbeidet sikringstiltak i forbindelse med bruk av bærbare pcer. Det er også fastsatt sikkerhetsnivå for fjernaksess til kommunens servere.

4.4 Konklusjon

Sikkerhetsledelse, sikkerhetsmål og- strategi

Sikkerhetsmål og sikkerhetsstrategier er utarbeidet og blir jevnlig gjennomgått slik regelverket anbefaler. Sikkerhetsorganisasjonen og ansvars- og rollefordelingene er tydelig beskrevet i Plan for informasjonssikring som utarbeides årlig. Oppgaven som sikringsansvarlig og IT- sjef bør imidlertid fordeles på to personer og ikke innehas av samme person som i dag slik at det blir et skille mellom utøvende og kontrollerende funksjoner slik regelverket sier.

Personregistre

Det er utarbeidet oversikt over alle personregistrene i kommunen. Det er også foretatt en risikovurdering av disse slik regelverket tilsier. Meldinger er også sendt Datatilsynet.

Sikkerhetsrevisjon

Gjennom Plan for informasjonssikring er det gjennomført sikkerhetstiltak ut fra en risikovurdering. Etter vårt skjønn er det ikke gjennomført tilstrekkelig sikkerhetsrevisjon i forhold til å etterprøve at disse sikkerhetstiltakene faktisk er gjennomført.

Avviksbehandling

Kvalitetslosen brukes som avvikssystem i Ås kommune. I plan for informasjonssikkerhet er det gitt eksempler på hva som kan anses som avvik på dette området. Det er også utarbeidet prosedyre for avvikshåndtering. Det anses at Ås kommune har et avvikssystem som kan brukes til å melde avvik innen IT.

Sikring av informasjon og tilgangskontroll

Ås kommune har tiltak som sikrer kommunens serverpark på en tilfredsstillende måte. Rutiner vedrørende backup er også på plass. Det gjennomføres flere tiltak for å sikre uautorisert innsyn i personopplysninger, samt endring av disse. Alle kommunens fagsystemer har systemansvarlige og superbrukere som har ansvar for å gi tilganger og å vedlikeholde disse. Noen av disse foretar jevnlig kontroll av de tilganger som er gitt. Det bør imidlertid innføres en fast rutine for slik gjennomgang for alle kommunens systemer. Alle sensitive personopplysninger ligger på sikker sone. Kommunen bruker også tynne klienter slik at sensitive opplysninger ikke kan kopieres over på annet lagringsmedium. Dette er med på å hindre at sensitive opplysninger kan komme på avveie.

5 IT-drift

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

5.1 Revisjonskriterier

Overordnede mål, retningslinjer og rutiner

ISACA[6] har publisert anbefalinger for God IT-skikk. I denne undersøkelsen har vi lagt til grunn publiseringer og anbefalinger fra denne foreningen.

God IT-skikk og COBIT[7] *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: [8]

- **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[9] og KS[10] *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:

[6] Information Systems Audit and Control Association (ISACA) er en verdensomspennende forening for IT-styring og kontroll, sikkerhet, kontroll og revisjon av informasjonsteknologi
[7] Control Objectives for Information and Related Technology (COBIT) er utviklet av ISACA og IT Governance Institute (ITGI) og gir anbefalinger for god IT-skikk.
[8] Anbefaling til God IT-skikk (nr. 1) Dokumentasjon av IT-systemer 2001
[9] IKT i det offentlige 2002

- **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.

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.

Kriterier

På bakgrunn av det ovennevnte legges følgende kriterier til grunn for undersøkelsen:

- Det skal være utarbeidet IT-strategi/-planer og mål for IT-drift i kommunen.
- Det skal være et klart skille mellom roller innen organisasjonen.
- Det skal være planer som ivaretar driftskontinuiteten.
- Det skal være retningslinjer og prosedyrer for endringshåndtering, samt dokumentasjon fra kommunens IT-systemer.

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

5.2 Faktabeskrivelse

5.2.1 Overordnede mål og strategier

Kommunestyret vedtok 27. april 2005 at Plan for drift og investering for IT skulle utarbeides hvert år og rulleres ved neste års handlingsplan. Administrasjonsutvalget skulle ha ansvaret for oppfølging av planen. Fra 2010 er planen endret til en IKT- strategiplan. Del 1 tar for seg dagens situasjon i forhold til IKT- området, hva som fungerer bra og hva som ikke fungerer så bra. Del 2 beskriver satsningsområder mål, og delmål.

Ås kommune har ca. 850 brukere i administrasjonssonen fordelt på ca. 400 arbeidsstasjoner. I tillegg kommer ca. 2500 brukere i skolesonen. IT- avdelingen drifter om lag 50 datasystemer.

IKT- strategiplan henviser til at kommunens mål og satsningsområde for IKT bygger på føringer fra KS og er i tråd med IKT- strategi for Follo.

Et viktig poeng for Ås kommunes IKT-strategi er at den skal bidra til å nå mål i kommuneplan og handlingsprogram.

Kommunens satsningsområder er hentet fra KS, som har anbefalt følgende satsingsfelt:

- Lokaldemokrati og deltagelse i informasjonssamfunnet.
- Tjenester på nett.
- Elektronisk samhandling i helse og omsorgssektoren.
- Geografisk informasjon.
- Digital forvaltning.
- Informasjonssikkerhet.
- Grønn IKT.
- Infrastruktur, utstyr og programvare.
- IKT- funksjonen.
- Kompetanseutvikling.
- IKT i grunnopplæringen.

I planen er det det egne avsnitt for alle satsningsområdene ovenfor. Det er først beskrevet generelle forhold rundt satsningsområdet samt kommunens praksis pr i dag. Til slutt er det satt opp mål innenfor de satsningsområdene som er nevnt ovenfor. Totalt er det listet opp nærmere 60 mål for Ås kommune.

Service- og kommunikasjonssjef har opplyst at mye at kommunens strategi er påvirket av utenforliggende forhold, som for eksempel statlige pålegg og endringer, samt at planene samkjøres av felles planer innenfor Follo.

5.2.2 Organisering og ansvarsdeling

IT- avdelingen har 6,7 årsverk og er organisert under Service- og organisasjonsavdelingen. Ås kommune har ikke egen IT- sjef. Service- og kommunikasjonssjef har ansvaret for området i tillegg til servicetorg, arkivtjenester og politisk sekretariat. Dette med bakgrunn i

kommunestyret sitt vedtak om organiseringen i kommunen fra 2002. Bakgrunnen for denne organiseringen er at man ønsker å se ressurser og behov i sammenheng og utnytte dette ved denne organiseringen.

Styringsrollen

Rådmannen har det overordnede ansvaret og er ansvarlig for at det utarbeides en overordnet IKT-strategi og at kommunen har en forsvarlig sikkerhetspolitikk.

Leverandørrollen

Det er IT- avdelingen som skal fungere som det utførende leddet, og innehar dermed leverandørrollen. Det er ikke utarbeidet noe «avtale» mellom IT og de respektive enheter. Det er heller ikke beskrevet noen overordnede målsetninger for IT- avd. Det er imidlertid laget avtale mellom IT- avd. og de eksterne (interkommunale selskaper) som Ås kommune forestår IT- driften av.

Service- og kommunikasjonssjefen opplyser at han er tilfreds med den kompetansen som finnes i IT- avd. i dag. Det er imidlertid en utfordring å levere de tjenester som avdelingene ønsker. Det blir større og større press på IT- avd. og kravet til systemintegrasjon øker. Antallet brukere øker også samt at det innføres en utstrakt bruk av PDA, lesebrett osv. Det er opplyst at man i IT- avd. jobber i team slik at flere skal ha kunnskap på forskjellige områder. Man har også sterkt fokus på å effektivisere driften og kunne gjenbruke data på tvers av de ulike systemene. Derfor har systemintegrasjon høyt fokus. Dette vil være med på effektivisere administrasjonen av ansatte og tilbudet til innbyggerne blir bedre. Skolesektoren har bl.a. overtatt ansvaret for å legge inn ansatte og lærere som nye brukere i kommunens systemer.

Service- og kommunikasjonssjefen oppgir at kommunen har vært i forkant når det gjelder servere og drift og har hatt en god utskiftingstakt slik at man er tilfreds med kommunens utstyr. Kommunen har bevisst satset på standardiserte og like systemer. Man har også bevisst satset på «tynne» klienter. Service- og kommunikasjonssjef har uttalt at utfordringen for IT-avd. framover blir å rekruttere personer med rett kompetanse.

Systemeier

Det er utpekt systemeiere for alle kommunens systemer. I følge Plan for informasjonssikring har systemeiere ansvaret for:

- Sørge for at sitt informasjonssystem er tilgjengelig
- Sørge for at informasjonssystemet oppfølger lovbestemte og andre krav
- Sørge for at informasjonssystemet fungerer som besluttet
- Definere rolletilganger
- Rapportere til IKT-ansvarlig
- Delegering av daglig ansvar for systemet til en systemansvarlig.

Systemansvarlige/superbrukere

Det er utpekt systemansvarlige for alle fagsystemer i Ås kommune. Det er systemansvarlig som har ansvaret for å bestille de endringer og oppgraderinger som skal gjøres på systemene. Det er opplyst at det er dialog mellom systemeier/systemansvarlig og IT avd. i denne prosessen. Man har hatt en bevisst holdning til ikke å være først ute med oppgraderinger på systemene slik at eventuelle «små feil» er blitt rettet opp. Dersom oppgraderinger får budsjettmessige konsekvenser blir systemeier også involvert.

Det er utarbeidet retningslinjer for systemansvarlige og superbrukere. Her framgår ansvar og oppgaver for de enkelte funksjonene.

Alle de intervjuede oppgir at den rollefordeling og ansvarsdeling som fremgår av plan for informasjonssikring er dekkende for de faktiske forhold og fremstår som fornuftig.

Opplæring

Systemansvarlige og superbrukere er ansvarlige for at tilstrekkelig opplæring i fagsystemene blir gjennomført. Når det gjelder opplæring i Gerica er det oppgitt at det gjennomføres tre vakter hvor man også har fokus på opplæring innen bruk av systemet.

Alle de intervjuede systemansvarlige og superbrukere har oppgitt at de anser at de har tilstrekkelig kompetanse på sine fagsystemer, de mener også at kompetansen blant brukerne er god.

Når det gjelder opplæring på Office- programvare og filbehandling er det IT avd. som har ansvaret for dette. Det gjennomføres kurs ved behov i eget kursrom. Det er også blitt avholdt kurs ute i enkelte avdelinger. Det er også utarbeidet en egen opplæringsportal på intranettet hvor det ligger mange oppskrifter og veiledninger på hvordan oppgaver kan løses. Tanken er også at dette skal avhjelpe helpdesk slik at den enkelte kan løse mindre «problemer» selv.

5.2.3 Driftskontinuitet/ driftssikkerhet

Måling og evaluering av kontinuitet

IT- avdelingen har ikke systemer for å måle oppetid på kommunens IT- systemer. Brukerne av systemene oppgir at det ikke foretas noen registrering av oppe-/nedetid fra deres side. Alle har imidlertid opplyst at det har vært svært lite nedetid på kommunens systemer. I de tilfeller hvor det er planlagt vedlikehold på kommunens systemer er det oppgitt at det er informert omkring dette.

I den utarbeidede IKT-strategiplan er det satt som mål at det skal være god tilgjengelighet til datasystemene dvs. oppetid på minimum 98 %.

Driftssikkerhet/ Helpdesk

Det skal kun gis autorisasjon for de programmer som den enkelte ansatte er avhengig av i sitt daglige arbeid. Når det det gjelder backup er det utarbeidet rutiner for sikkerhetskopiering. Denne skal sørge for at det blir foretatt tilstrekkelig backup av kommunens datasystemer.

Det er ikke utarbeidet noen beredskapsplan for å håndtere uforutsette hendelser innen IT-området. Det er imidlertid utarbeidet prosedyrer for driftsstans, både når det gjelder å «ta» serveren kontrollert ned og å få den i gang igjen etter en driftsstans. Det er pr i dag ikke nødstrømsaggregat på serverparken. En batteripakke gjør at serverne er i drift i 30 min. før de tas kontrollert ned ved strømstans. Det er opplyst at det er planer om å få på plass et nødstrømsaggregat i nær framtid. Det jobbes også med avtaler innen IKT Follo om å kunne ha beredskap i annen kommune slik at man kan benytte deres servere hvis man skulle få en langvarig driftsstans. Kommunen anser at det er pleie- og omsorgsavdelingen som er mest sårbar dersom det skulle oppstå en driftsstans. Det er opplyst at det er satt i gang arbeid for å kunne ha servere på sykehjemmet som kan benyttes dersom det blir en driftsstans på rådhuset. Det er også opplyst at det er «speiling» av alle servere og disker slik at disse er like og dermed lett kan byttes dersom det skulle være behov for dette. Man har også en terminalserver ekstra som kan settes inn dersom en av serverne skulle ryke.

IT- avdelingen har overvåkningssystem for serverrommet. Videre er det overvåking av alle servere og nettverkskomponenter både på trafikkmengde, belastning på servere, diskfylling og bruk av minne. Overvåking gjøres på egen skjerm i tillegg får teknikere mail/SMS hvis feil oppstår. Dette gjør at en tidlig kan gå inn å gjøre endringer for å bedre ytelsen og sikre stabil drift.

Helpdesk er bemannet i normal arbeidstid. En person i 70 % stilling betjener normalt denne funksjonen, men også andre ansatte i IT- avdelingen svarer også på henvendelser ved stor pågang. Alle henvendelser får et saksnr.

Alle de vi har intervjuet har oppgitt at de har et godt samarbeid med IT- avd. De oppgir at IT-avd. strekker seg langt for å hjelpe og tilfredsstille de behov som de enkelte avdelingene har. Det er imidlertid ingen beredskap utenfor ordinær arbeidstid, i helger og helligdager. Flere av de vi har hatt samtaler med har etterlyst en slik beredskap. I IKT- strategiplan er det henvist til at det er kommet sterke ønsker fra døgninstitusjoner om en vaktordning for IT- avd. Det framgår videre at det er foreslått en slik ordning i forbindelse med budsjettbehandlingen.

Det er ikke utarbeidet beredskapsplaner for de avdelinger hvor vi har gjennomført intervjuer. Det er heller ikke utarbeidet manuelle systemer eller rutiner i forbindelse med uforutsette hendelser. Det varierer mellom avdelingene hvor kritisk en driftsstans vil være. Selv om det ikke er utarbeidet manuelle rutiner eller systemer oppgir de intervjuede i ulik grad at det ved driftsstans er muligheter for å opprettholde ordinær drift ved bruk av manuelle systemer.

Gerica – Elektronisk pleie- og omsorgssystem:

På sykehjemmene har de enkelte avdelinger skrevet ut brukerkort fra systemet hvor personopplysninger samt diagnose og fastlege framgår. Det er også skrevet ut medisinlister hvor det framgår hvilke medisiner den enkelte skal ha. Det kjøres ut daglige arbeidslister som grunnlag for det som skal gjøres med den enkelte beboer. Denne arkiveres i egen perm, og

fagkoordinator har ansvaret for dette. Det er opplyst at det ofte gjøres daglige endringer for beboere på korttidsavdelingen. Nedetid vil skape større problemer for denne avdelingen sammenlignet med beboere på langtidsavdelingen, hvor det sjelden er endringer. Siste utskrevne arbeidslister vil så langt det er mulig benyttes dersom det er nedetid på systemet over lang tid. Det må da fortløpende noteres på papir det som skal dokumenteres for den enkelte beboer for så å legge dette inn i Gerica når systemet er oppe og går igjen. Det er oppgitt at dersom det skjer noe «akutt» med beboeren kan det være kritisk selv ved kortere nedetid. Nedetid rundt vaktskifte kan også skape problemer for overføring av informasjon.

Når det gjelder hjemmetjenesten skrives det ut daglige arbeidslister hvor det framgår hva som skal gjøres hos den enkelte beboer. Det skrives også ut brukerkort med medisinoversikt når disse endres, samt arbeidslister for hver dag. Disse listene arkiveres i en uke. Dersom det er nedetid på systemet og man ikke får skrevet ut arbeidslister, kan foregående ukes lister brukes som grunnlag for hva som skal gjøres hos den enkelte. I tillegg er det opplyst at man har en egen bok hvor alle endringer eller beskjeder blir skrevet i. Denne gjennomgås hver morgen slik at alle får med seg eventuelle endringer. Enhetsleder for hjemmetjenesten har opplyst at man anser at man kan klare seg godt opp mot en uke selv om Gerica ville være nede.

HsPro – Modulbasert system for helsestasjoner og skolehelsetjenesten:
Det er opplyst at helsestasjonen har papirjournaler av barnejournalen fra sykehuset og eventuelt andre journaler fra spesialister. For barn som har flyttet til kommunen foreligger det som regel hele papirjournalen. De foreliggende journalene er ikke oppdatert i forhold til hva som er lagt inn i HsPro.

OPPAD – System for tildeling av barnehageplasser:
Systemet inneholder ikke opplysninger som er kritisk i forhold til liv og helse, slik at det ikke vil være kritisk om systemet er nede i noe tid. Mest kritisk vil det være dersom systemet var nede på det tidspunktet hvor fordeling av barnehageplasser skal gjøres.

5.2.4 Endringshåndtering, dokumentasjon

Ås kommune har bevisst satset på standardiserte og like systemer som snakker godt sammen. Systemeierne bestiller de endringer som skal gjøres på systemene, og det er opplyst at det er en dialog mellom systemeier og IT- avd. i prosessen. Er det store oppgraderinger eller endringer kjøres dette av systemleverandørene.

Systemer kan testes i eget miljø dersom det er behov. Systemene og oppgraderingene blir testet av systemleverandørene før de implementeres i kommunen. Ås kommune har ønske om ikke å være den første som får oppgraderinger, men heller ikke den siste. Årsaken til dette er å unngå oppdateringer og rettinger av feil i systemene. Systemansvarlige tester ut ved større oppgraderinger. Erfaringsmessig har det vært lite feil ved de etablerte systemene.

Det dokumenteres hva som gjøres av endringer på systemene, endringsloggen arkiveres i egen perm. Daglige endringer dokumenteres i en egen logg både på systemene og på de tekniske løsningene. Ved oppgraderinger tas det backup av både programmene og av databasen slik at alt kan rulles tilbake til før oppgraderingen dersom det skulle være behov for det. All brukerdokumentasjon er tilgjengelig i de enkelte fagsystemene. Alle IT- systemene er dokumentert i IT- avdelingen.

5.3 Vurdering

5.3.1 Overordnede mål og strategier

Ås kommune har utarbeidet en IKT- strategiplan som rulleres hvert år. Etter vårt skjønn synes det som om kommunens IKT- strategi tilfredsstiller de anbefalinger som bl.a. er gitt gjennom god IT-skikk. Strategiplanen bygger opp under kommunens mål og planer og inneholder som anbefalt satsningsområder, mål og delmål.

5.3.2 Organisering og ansvarsdeling

Ås kommune har etablert en organisering av IKT- arbeidet hvor rådmannen har det overordnede ansvaret. For alle fagsystemene er det utpekt systemeiere og systemansvarlige. Systemeierne er ansvarlig for fagsystemet og at disse fungerer slik det er besluttet. Systemansvarlige har ansvaret for å bestille og følge opp endringer og oppgraderinger. IT-avdelingen er den som har ansvaret for å utføre kommunens IKT- oppgaver. Denne rollefordelingen samsvarer med de anbefalinger som er gitt, hvor det er et tydelig skille mellom øverste ansvar og bestiller og utføreroppgaven. Service- og kommunikasjonssjef, som også er IT- sjef, er tillagt en del kontrolloppgaver bl.a. av sikkerhetsrevisjoner. Ansvaret for kommunens kontrolloppgaver bør etter vår oppfatning skilles fra den som har oppgaven med å utføre disse.

5.3.3 Driftskontinuitet/ driftssikkerhet

Driftsforstyrrelser og nedetid på kommunens IT- systemer logges ikke av IT- avdelingen. Det oppleves som at det er lite nedetid på kommunens systemer. I strategiplanen er det satt som mål at oppetiden skal være minimum 98 %. Revisjonen er av den oppfatning at det bør vurderes å loggføre driftsforstyrrelser, da mindre driftsforstyrrelser over tid også kan gå ut over effektiviteten ved avdelingene. Loggingen gir også informasjon og tilbakemelding både til IT- avdelingen og til systemeiere og brukere. Man kan dermed også måle om man oppfyller det kravet om er satt til oppetid i strategiplanen.

Det synes som om Ås kommune har tilfredsstillende rutiner når det gjelder backup av IT-systemene. Det er bl.a. utarbeidet en egen rutine for sikkerhetskopiering av data. Denne sikrer at det blir tatt backup av kommunens systemer.

Det er ikke utarbeidet egne beredskapsplaner for hvordan alvorlige hendelser skal håndteres. Det er viktig med slike planer for å sikre at kommunen er tilstrekkelig forberedt og kan redusere konsekvensene av disse. God IT-skikk anbefaler at det etableres beredskapsplaner for ivaretakelse av driften ved alvorlige hendelser. Revisjonen ser det som positivt at det jobbes for å få på plass nødstrømsaggregat som kan sikre drift ved eventuelle strømbrudd. Det jobbes også internt i IKT Follo om felles beredskap. Server i beredskap på sykehjemmet vil også være ett tiltak som vil bedre beredskapen i forbindelse med uforutsette hendelser. Det

synes som om Ås kommune kan foreta mindre utskiftninger av egne servere i løpet av kort tid dersom det skulle være behov for dette.

Revisjonen ser det som positivt at det er overvåkning av alle servere og nettverkskomponenter, dette gjør at man kan ta tidlige «grep» dersom noe uforutsett oppstår.

Det er gjennom intervju bekreftet at det er et godt samarbeid mellom IT- avdelingen og andre enheter. Helpdesk/ brukerstøtte oppgis også å fungere godt. Det er imidlertid kommet ønske om en vaktordning utenom ordinær arbeidstid. Dette vil etter vårt skjønn være med på å redusere risikoen for at driftsstans utenom arbeidstid får konsekvenser for de som har døgnkontinuerlig drift.

Våre undersøkelser viser at selv om det ikke er utarbeidet beredskapsplaner/ eller rutinebeskrivelser ved de avdelinger vi har undersøkt har de i noe grad manuelle «systemer» som gjør at normal drift kan opprettholdes ved en driftstans. Etter vår oppfatning bør man foreta en gjennomgang av mulighetene for slike manuelle systemer og sørge for å skriftliggjøre disse i nedfelte rutinebeskrivelser.

5.3.4 Endringshåndtering, dokumentasjon

Våre undersøkelser viser at kommunen følger god IT-skikk i forbindelse med endringer som gjøres på kommunens IT- systemer. Det er systemeier som er ansvarlig for å bestille de endringer som skal gjøres samtidig som det er en god dialog med IT- avd. Revisjonen registrerer også at Ås kommune har en bevisst holdning til de oppgraderinger som skal gjøres av systemene for å unngå feil og mangler i nye systemer. Det foretas også ekstra bacup ved større endringer slik man raskt kan stille tilbake til opprinnelig versjon ved eventuelle feil. Det foretas loggføring av de endringer som gjøres slik at kommunen har tilstrekkelig dokumentasjon over de endringer som er gjort. Brukerdokumentasjon er tilgjengelig i de enkelte systemene.

5.4 Konklusjon

Overordnede mål og strategier

Ås kommune sin IKT- strategiplan rulleres jevnlig og inneholder mål, delmål og satsningsområder.

Organisering og ansvarsdeling

Det er klare rolle- og ansvarsfordelinger innen IKT- området i Ås kommune. Imidlertid er det lagt en del kontrolloppgaver til Service og kommunikasjonssjef. Denne innehar også rollen som IT- sjef som da har ansvaret for den utførende delen. En slik blanding av roller samsvarer ikke med de anbefalinger som god IT- skikk gir.

Driftskontinuitet/driftssikkerhet

IT- avdelingen har ikke utarbeidet egne beredskapsplaner for alvorlige hendelser. Revisjonen mener at dette bør utarbeides. Det arbeides imidlertid med løsninger for å bedre beredskapen både internt og i samarbeid med IKT Follo. Mindre reparasjoner og utskiftninger kan også gjøres i løpet av kort tid med interne krefter. Ås kommune har tilfredsstillende overvåkning av kommunens servere, men nedetid logges imidlertid ikke. Dette bør vurderes slik at man kan måle om man når det målet om oppetid som er satt i strategiplanen. Det er også et ønske fra enkelte avdelinger om en vaktordning utenom ordinær arbeidstid, noe som vil styrke beredskapen på området.

Det finnes flere manuelle muligheter for å opprettholde og sikre tilfredsstillende drift ved en driftsstans på kommunens IT- systemer. Disse bør gjennomgås slik at man sørger for å skriftliggjøre disse i nedfelte rutinebeskrivelser.

Endringshåndtering, dokumentasjon

Alle endringer på kommunens systemer gjøres på bakgrunn av meldinger fra systemeierne, mens IT- avdelingen utfører endringene. Alle endringer logges, og det foretas også ekstra backup ved større endringer. Brukerdokumentasjon er også tilgjengelig i kommunens systemer.

6 Anbefalinger

På bakgrunn av de forhold som fremkommer i rapporten foreslår Follo distriktsrevisjon følgende tiltak som kan bidra til forbedringer innen informasjonssikkerhet og IT-drift:

- Oppgavene som sikkerhetsansvarlig og IT- sjef bør ikke innehas av samme person.
- Fullverdig sikkerhetsrevisjon bør gjennomføres årlig.
- Beredskapsplan for IT- avdelingen bør utarbeides.
- Innføre rutine om å kontrollere tilganger i kommunens fagsystemer jevnlig der dette ikke gjøres i dag.
- Utarbeide skriftlige rutinebeskrivelser for bruk av manuelle systemer ved en IT-driftsstans.
- Vurdere å innføre vaktordning utenom ordinær arbeidstid.
- Vurdere loggføring av oppe-/nedetid på IT-systemene.

7 Rådmannens uttalelse

Ås kommune

RÅDMANN
Service- og kommunikasjonsavdelingen

Follo Distriktsrevisjon

Pb 3010
1402 SKI

Deres ref.	Vår ref.	Saksbehandler	Dato
	Saknr. 12/1429-3/219 Løpenr. 25406/12	Andreas Brodahl dir. tlf.: 64 96 20 11	29.11.2012

SVAR - FORVALTNINGSREVISJONSRAPPORT - INFORMASJONSSIKKERHET OG IT-DRIFT

Høringsuttalelse fra Rådmannen i Ås kommune.

1. Har informasjon om prosjektets hensikt vært tilstrekkelig klar?
   - Ja, forvaltningsrevisjonen er en lovpålagt oppgave for Ås kommune etter kommuneloven. Informasjonen fra prosjekt ansvarlig i Follo distriktsrevisjon har vært god.

2. Har rådmannen kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?
   - Rapporten er basert på intervju og dokumenter som kommunen har funnet frem. En har ikke gått inn i de tekniske løsningene for å se hvilke sikkerhetsbarrierer som er etablert for sikring av data. Dette er omfattende og komplekse løsninger som ivaretar sikkerhet på mange nivåer. Ved å ha sett på disse løsningene ville en kunne fått et klarere bilde av kommunens fokus på informasjonssikkerhet og utfordringene som ligger i krysningspunktet mellom sikkerhet og tilgjengelighet.

3. Har rådmannen kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?
   - Nei.

4. Hva er rådmannens samlede vurdering av rapportens konklusjoner og anbefalinger?
   - Rådmannen mener rapporten viser at kommunen har et høyt fokus på informasjonssikkerhet og en bra bevissthet blant de ansatte. Rapporten viser at sikkerhetsrutinen er kjent ute i organisasjonen ut over leder nivået. Arbeidet med bevisstgjøring i forhold til sikkerhet er et kontinuerlig oppgave. Dette må få et sterkere fokus fremover, tiltak er gjort allerede i løpet av høsten 2012. Rådmannen

Postadresse: Postboks 195 1431 Ås
Besøksadresse: Skolevelen 1 1430 Ås
Telefon: 64 96 20 00 Telefaks: 64 96 20 29 E-post: post@as.kommune.no
Bankgiro: 1654.07.99605
Org.nr: 964948798

ser at vektleggingen av å dokumentere utførte tiltak ikke har vært grundig nok. Fokus er ofte på å være operativ og i iverksette de ulike tiltakene.

5. Vil rådmannen vurdere iverksetting av tiltak på bakgrunn av rapportens konklusjoner og anbefalinger?
   a) Oppgavene som sikringsansvarlig og IT-sjef bør ikke innehas av samme person. En riktig vurdering, som også ble trukket frem av administrasjonen under revisjonen. Informasjonssikkerhets ansvarlige bør tilhøre en annen del av organisasjonen. Da fortrinnsvis innenfor organisasjon og personal, som allerede har et ansvar i forhold til kvalitetssystemet og avvikssystemet. Dette vil bli gjennomført i 2013
   b) Fullverdig sikkerhetsrevisjon bør gjennomføres årlig.
   Det gjøres en revisjon av kommunens informasjonssikkerhetsplan hvert år. Det som mangler er en god historikk på alle de tiltak som er gjennomført.
   Rådmannen vil sørge for at sikkerhetsrevisjonene kommer inn i sak og arkiv systemet, slik at en kan etter prøve de tiltakene som er gjennomført.
   Gjennomføres i 2013
   c) Beredskapsplan for IT-avdelingen bør utarbeides.
   Det vil bli utarbeidet en skriftlig beredskapsplan for IT-avd, som skal være en del av kommunens informasjonssikkerhetsplan. Gjennomføres i 2013
   d) Rutine for jevnlig kontroll av gitte tilganger i kommunens fagsystemer bør innføres der dette ikke gjøres i dag.
   Alle tilganger styres ved at ledere melder ansatt inn og ut av systemene. Det er en utfordring for ledere å huske dette, da mange som slutter skal jobbe som ekstra vakter etc. Det bør derfor legges inn i rutinene for systemansvarlig for fagsystemer tar en sjekk en gang i kvartalet. Det samme bør da gjøres på IT avd. for alle avdelinger som har stor utskifting av ansatte. Dette innarbeides i retningslinjene for bruker håndtering på IT avd. Dette gjennomføres i 2013.
   Det jobbes med prosjekt for tilgangsstyring, der det skal bli en forenkling av tilgangsstyring.

   e) Skriftlige rutinebeskrivelser for bruk av manuelle systemer ved en IT driftsstans bør utarbeides.
   Aktuelle avdelinger vil utarbeide dette og det vil legges inn som vedlegg til informasjonssikkerhetsplanen i kvalitetssystemet. Gjennomføres i 2013.
   f) Vaktordning utenom ordinær arbeidstid for IT-avdelingen bør vurderes.
   Det er gjort flere forsøk på å finne penger til dette, men under budsjettarbeidet er dette kuttet pga. i forhold til andre tiltak i kommunen. Kostnad etter standard som AHUS krever er ca. 500.000,- pr.år. Det er ikke funnet plass til dette i budsjettet for 2013. En ser på mulighetene for en felles løsning for en eller flere Follo kommuner. Men dette er noe lengre frem i tid. Må vurderes som egen sak, der en får inn dette tiltaket som en del av budsjett.
   g) Loggføring av opp-/ nedetid på kommunes servere for å måle om man når kravene satt i strategiplanen.

Rådmannen vil under revideringen av IKT planen vurdere om målet om opptid på servere er et relevant mål. Før en eventuelt starter arbeide med måling av opptid for servere. Gjennomføres i 2013.

6. Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av aktuelle tiltak?
   - Dette beskrevet under de aktuelle tiltak. Men det som går på oppdatering og utarbeidelse av dokumentasjon vil gjennomføres i 2013.

7. Oppfattes rapporten som nyttig av rådmannen?
   Rådmannen mener det er nyttig at andre kommer inn og ser på eksisterende praksis på dette området. Det gir nyttig informasjon og gode tilbakemeldinger på hva som fungerer og hvilke områder som må forbedres.

8. Hvordan vurderes rapportens oppbygning og språkbruk?
   - Rapporten oppleves om oversiktlig og lett forståelig. Helt greit i forhold til en slik type revisjon.

9. Sluttmerknad?
   Arbeide med informasjonssikkerhet er et krevende arbeide, da den totale sikkerheten avhenger av mange nivåer. Både menneskelige og tekniske nivåer. Hoved arbeidet må ligge på kompetanse og bevisstgjøring av alle ansatte i kommunen. Det vil alltid være et motsetningsforhold mellom tilgjengelighet og sikkerhet. Det er vanskelig å balansere dette i en hektisk hverdag. I forbindelse med samhandlingsreformen vil det komme flere forskrifter som vil utfordre dagens løsninger og som vil kreve større ressurser i både i IT avdelingen og ute hos de som er systemansvarlige for de ulike fagsystemene.
   Rapporten viser at det er en utfordring å ha tilstrekkelig med ressurser for å skulle tilfredsstille alle kravene til dokumentasjon innenfor området. Det vil være nødvending med en styrking av dette området i fremtiden, etter hvert som kommunen vokser.
   Når det gjelder IT drift, er de økende kravene til bruken av IKT i alle ledd av forvaltingen med på å øke behovet for ressurser innenfor IKT område. Kravene til drift innenfor normal arbeidstid holder ikke lenger. Kommunen har klart seg med dette og god proaktiv drift i mange år. Nå vil aktører (Ahus) stille krav om døgn vaktordninger innenfor IKT. I tillegg vil økte krav til samordning av ulike systemer kreve at en ser på løsninger flere kommuner sammen. Ås jobber godt sammen med flere av Follo kommunene for å løse driftsoppgaver sammen. Men det er likevel nødvending å styrke lokal IT avd. i budsjett for 2013.

En presisering i forhold til faktadelen, det er 5,7 årsverk som har arbeidsoppgaver knyttet til IKT.

Med hilsen

Trine Christensen
Rådmann

Andreas Brodahl
Service og kommunikasjonssjef

Kopi til:

8 Revisjonens kommentarer til rådmannens uttalelse

Revisjonen har ingen særskilte kommentarer til Rådmannens uttalelse.

9 Litteraturliste

Lov:

- Lov om behandling av personopplysninger (personopplysningsloven) 1.1.2001

Forskrift:

- Forskrift om behandling av personopplysninger (personopplysningsforskriften) 1.1.2001
- Datatilsynet (2000) Sikkerhetsbestemmelsene i personopplysningsforskriften - med kommentarer

Dokumenter fra Ås kommune:

- IKT-strategiplan 2011 og 2010
- Plan for informasjonssikring
- Plan for Ås kommunes kriseledelse (2008-2011)
- Helhetlig kommunikasjonsstrategi 2010
- IKT- plan skole
- Retningslinjer for bruk av håndholdte enheter PDA i hjemmetjenesten i Ås kommune
- IKT- reglement for skolene i Ås
- Prosess for informasjonssikkerhet
- Retningslinje for elektronisk kommunikasjon
- Retningslinjer for brukeradministrasjon i Ås kommune
- Retningslinjer for systemansvarlig og superbruker
- Ås kommune sikkerhetsregler
- Prosjektplan Retningslinjer for sikkerhetskopi av data i Ås kommune (Backup)
- Retningslinje for registrering av personopplysninger i skolen
- Register for meldepliktige registre (sensitive opplysninger)
- Retningslinjer for brukeradministrasjon i Ås kommune
- Systemdokumentasjon Feide – Ås kommune
- Rapport på ansatte tilknyttet en avdeling, for superbrukere.
- Retningslinje for bruk av elektronisk journal i Enhet for forebyggende helse.
- Informasjon/ rutiner i hjemmetjenesten distrikt sør
- Prosedyre prosess for forbedring.
- Utskrift av journal og kopi av kommunikasjon mot Datatilsynet

Annet:

- 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