2009

REVISJONSRAPPORT 69 / F - 08 Dato: 05.11.2009

Forvaltningsrevisjonsprosjektet

Informasjonssikkerhet og behandling av personopplysninger i Bergen kommune

BERGEN KOMMUNE
KOMMUNEREVISJONEN

Forord

Deloitte har på oppdrag fra Bergen kommunerevisjon gjennomført en forvaltningsrevisjon av kommunens rutiner og praksis knyttet til informasjonssikkerhet og elektronisk behandling av personopplysninger. Prosjektet ble vedtatt i kontrollutvalget i møte 09.12.2008, sak 88-08 og 02.02.2009, sak 12-09.

Rapporten fra undersøkelsen belyser følgende problemstillinger:

1. I hvilken grad har kommunen sikret en helhetlig tilnærming til informasjonssikkerhet?
2. I hvilken grad har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?
3. I hvilken grad er det etablert tiltak for å tilfredsstille krav i lovverket på områdene:
    - Informasjonssikkerhet knyttet til behandling av personopplysninger
    - Bruk av fødselsnummer og lignende identifikasjonsmiddel

Rapportens sammendrag oppsummerer resultatet av forvaltningsrevisjonen, og viser at det er avdekket mangler på flere områder, herunder avvik fra krav i personopplysningsforskriften om risikovurderinger i § 2-4, sikkerhetsrevisjon i § 2-5, avviksbehandling i § 2-6, klare og dokumenterte ansvars- og myndighetsforhold i § 2-7, medarbeidernes kunnskap i § 2-8 og krav om dokumentasjon i § 2-16.

Et sentralt funn i forvaltningsrevisjonen er at Bergen kommunes styringsdokumenter innen området informasjonssikkerhet ikke er tilstrekkelig systematisert og forankret i organisasjonen. Videre kommer det frem at kommunens rutiner og retningslinjer knyttet til informasjonssikkerhet ikke er oppdaterte. De reviderte byrådsavdelingene slutter seg i all hovedsak bak vurderingene og anbefalingene som fremkommer i rapporten.

Bergen kommunerevisjon støtter Deloittes vurderinger og anbefalinger knyttet til informasjonssikkerhet og behandling av personopplysninger i Bergen kommune. Kommunerevisjonen merker seg videre at det er igangsatt et arbeid for å systematisere og utbedre kommunens rutiner knyttet til informasjonssikkerhet. Kommunerevisjonen vil understreke viktigheten i dette arbeidet.

Rapporten fra Deloitte presenteres i det etterfølgende i sin helhet.

Til slutt vil vi takke administrasjon og ansatte i Bergen kommune for nødvendig bistand og velvilje underveis i prosjektet.

Bergen, 05.11.09
Bergen Kommunerevisjon

Monika Amundsen

Monika Amundsen
kommunerevisor

Innholdsfortegnelse

Sammendrag

I samsvar med bestilling fra kontrollutvalget i Bergen kommune datert 09.12.08 og vedtak i sak 88-08 og sak 12-09, er det gjennomført forvaltningsrevisjon av Bergen kommunes rutiner og praksis knyttet til informasjonssikkerhet og elektronisk behandling av personopplysninger.

Formålet med forvaltningsrevisjonen har vært å undersøke om Bergen kommune har tilfredsstillende system og rutiner for informasjonssikkerhet i forbindelse med behandling av personopplysninger, og om gjeldende regelverk blir fulgt.

Forvaltningsrevisjonen viser at Bergen kommune ikke oppfyller krav i personopplysningsforskriften på flere områder. Det dreier seg blant annet om krav om risikovurderinger i § 2-4, sikkerhetsrevisjon i § 2-5, avviksbehandling i § 2-6, klare og dokumenterte ansvars- og myndighetsforhold i § 2-7, medarbeidernes kunnskap i § 2-8 og krav om dokumentasjon i § 2-16.

Et sentral funn i forvaltningsrevisjonen er at Bergen kommune sine styringsdokumenter innen området informasjonssikkerhet ikke er tilstrekkelig systematisert og forankret i organisasjonen. Videre kommer det frem at kommunens rutiner og retningslinjer knyttet til informasjonssikkerhet ikke er oppdatert.

Bergen kommune har ikke tilstrekkelig oversikt over hvilke personopplysninger som behandles i kommunen. Bergen kommune sitt informasjonssikkerhetssystem inneholder heller ikke rutiner for gjennomføring av risikovurderinger. Videre er det ikke fastlagt kriterier for akseptabel risiko forbundet med behandling av personopplysninger.

Det er ikke tilfredsstillende at kommunen ikke har et system for gjennomføring av sikkerhetsrevisjoner som omfatter hele virksomheten. Det er stor risiko forbundet blant annet med det at man ikke gjennomfører jevnlige kontroller av hvorvidt rutiner og sikkerhetstiltak blir fulgt opp som forutsatt.

Bergen kommune har ut fra den dokumentasjonen revisjonen har mottatt, ikke spesifisert og dokumentert godt nok det ansvar som tilligger ulike roller når det gjelder informasjonssikkerhet og behandling av personopplysninger.

Kommunens retningslinjer og rutiner for informasjonssikkerhet er ikke tilstrekkelig implementert på alle nivå i kommunen. Dette fremgår blant annet i en spørreundersøkelse innen skole, barneverntjenesten og PPT, der ansatte rapporterer om mangel på kjennskap til retningslinjer og rutiner, og lite fokus på temaet fra nærmeste ledelse. Det kommer også frem at et klart flertall av de spurte ikke er kjent med kommunens rutiner for å melde avvik i forbindelse med informasjonssikkerhet. Manglende implementering av rutiner og retningslinjer kan utgjøre en risiko for informasjonssikkerheten.

I Bergen kommune er det igangsatt et arbeid for å systematisere og utbedre kommunens system og dokumentasjon knyttet til informasjonssikkerhet. Dette arbeidet omfatter i hovedsak de mangler som er nevnt over. For at et nytt system skal fungere hensiktsmessig, og forbedre informasjonssikkerheten og regeletterlevelsen, vil revisjonen bemerke at det er viktig at arbeidet med å utvikle og implementere dette systemet følges opp.

1. Innledning

I samsvar med bestilling fra kontrollutvalget i Bergen kommune datert 09.12.08 og vedtak i sak 88-08 og sak 12-09, er det gjennomført forvaltningsrevisjon av Bergen kommunes rutiner og praksis knyttet til informasjonssikkerhet og elektronisk behandling av personopplysninger.

Prosjektet er gjennomført i samsvar med RSK 001, standard for forvaltningsrevisjon.

1.1 Formål og problemstillinger

Formålet med forvaltningsrevisjonen har vært å undersøke om Bergen kommune har tilfredsstillende system og rutiner for informasjonssikkerhet i forbindelse med behandling av personopplysninger, og om gjeldende regelverk blir fulgt.

Følgende problemstillinger er undersøkt:

1. I hvilken grad har kommunen sikret en helhetlig tilnærming til informasjonssikkerhet?
2. I hvilken grad har de ansatte kjennskap til retningslinjer og rutiner for informasjonssikkerhet?
3. I hvilken grad er det etablert tiltak for å tilfredsstille krav i lovverket på områdene
    - Informasjonssikkerhet knyttet til behandling av personopplysninger
    - Bruk av fødselsnummer og lignende identifikasjonsmiddel

1.2 Avgrensning og metode

I den delen av prosjektet som går inn på den praktiske gjennomføringen av tiltak i forbindelse med informasjonssikkerhet, er prosjektet avgrenset til å gjelde tre utvalgte kommunale enheter. Skole, PPT[1] og barnevern er valgt ut på bakgrunn av at dette er enheter som behandler og lagrer personopplysninger om et stort antall tjenestemottakere, som et stort antall ansatte har tilgang til.

Revisjonen har gjennomgått skriftlig dokumentasjon knyttet til informasjonssikkerhet i Bergen kommune. Dette omfatter blant annet rutiner, retningslinjer, styrende dokumenter og korrespondanse.

Revisjonen har videre gjennomført møter med personer som har et overordnet ansvar for informasjonssikkerhet og IT-drift i kommunen (leder for IKT Drift og IKT Sikkerhetsansvarlig). I tillegg har det blitt gjennomført møte/intervju innen seksjon skole/byrådsavdeling for barnehage og skole (BBS), og revisjonen har hatt kontakt med barnevernstjenesten/ byrådsavdeling for helse og omsorg (BHOS) på e-post for å få mer detaljert informasjon vedrørende system og rutiner. I tillegg har en del spørsmål og problemstillinger fortløpende blitt avklart gjennom telefonsamtaler og e-post. Intervjudata som har blitt benyttet i denne rapporten er verifisert av intervjuobjektene.

Et utvalg ansatte innen områdene skole, PPT og barnevern har mottatt en elektronisk spørreundersøkelse som blant annet omhandler kjennskap til og praktisering av kommunens rutiner for informasjonssikkerhet og behandling av personopplysninger. Utvalget omfatter alle ansatte ved barnevernskontorene og PPT-kontorene i Bergen kommune[2]. Når det gjelder Seksjon skole, er det valgt ut fire tilfeldige skoler i hver bydel, og spørreundersøkelsen er sendt til tre-fire ansatte i

[1] Pedagogisk-psykologisk tjeneste.
[2] I barnevernstjenesten ble undersøkelsen sendt til ansatte i seks av åtte bydeler, innen PPT ble undersøkelsen sendt til ansatte i alle åtte bydeler.

administrasjonen og tre-fire kontaktlærere ved hver av disse skolene[3]. Til sammen har 367 personer svart på undersøkelsen, hvilket utgjør en svarprosent på 75,2 %.

2. Revisjonskriterier

Innsamlet data er vurdert opp mot revisjonskriterier i form av lover og regelverk. Kriteriene er utledet fra autoritative kilder i samsvar med kravene i gjeldende standard for forvaltningsrevisjon[4].

2.1 Informasjonssikkerhet

I de innledende kommentarene til personopplysningsforskriftens kapittel 2 fremgår det at begrepet informasjonssikkerhet omfatter følgende:

- 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. sørge for at tilstrekkelige og relevante opplysninger er til stede.

God informasjonssikkerhet skal således sikre både at selve systemene fungerer hensiktsmessig og ikke er utsatt for manipulasjon, og at informasjonen i systemene er pålitelig og ikke blir misbrukt eller blir tilgjengelig for uvedkommende.

Revisjonskriterier for informasjonssikkerhet er i første rekke knyttet til kommunens plikt, etter personopplysningsloven § 13 og personopplysningsforskriftens kapittel 2, til å ha tilfredsstillende sikring av informasjonssystemet. Bestemmelsene i personopplysningsforskriftens kapittel 2 gjelder kun for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler.

Av personopplysningsloven § 13 fremgår det at *"Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger."* Videre går det frem at den behandlingsansvarlige og databehandleren for å oppnå tilfredsstillende informasjonssikkerhet skal dokumentere informasjonssystemet og sikkerhetstiltakene.

Kapittel 2 i personopplysningsforskriften lister opp en rekke krav til sikringen av informasjonssystemet. Disse er knyttet til organisering, dokumentasjon og kontroll og tiltak.[5]

2.2 Ledelsens ansvar

§ 2-3 i personopplysningsforskriften slår fast at det er den som har den daglige ledelsen av virksomheten som har ansvar for at bestemmelsene i forskriftens kapittel 2 blir fulgt. I Datatilsynets veileder i informasjonssikkerhet for kommuner og fylker går det fram at *"Behandlingsansvarlig, normalt representert ved den administrative ledelse, er ansvarlig for at sikkerhetsbestemmelsene i personopplysningslovens § 13 og personopplysningsforskriftens kapittel 2 følges"*[6].

---

[3] Revisjonen har ikke mottatt e-postadresser til ansatte ved alle de utvalgte skolene, og har dermed ikke fått sendt ut undersøkelsen til hele utvalget. Ansatte ved 28 skoler har mottatt undersøkelsen, og revisjonen anser dette for å være tilstrekkelig.

[4] RSK 001, Standard for forvaltningsrevisjon

[5] Presentasjonen av kravene i personopplysningsforskriften i dette kapittelet bygger delvis på Datatilsynets veiledere SV-100:2000 «Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer» og TV-202:2005 «Veiledning i informasjonssikkerhet for kommuner og fylker».

[6] Side 8.

Behandlingsansvarlig har ansvar for å beskrive mål for sikkerhetsarbeidet og en strategi som beskriver valg og prioriteringer i sikkerhetsarbeidet. Ledelsen skal jevnlig gå gjennom strategi og mål for å vurdere arbeidet med informasjonssikkerheten og hvilke behov virksomheten har.

2.3 Risikovurderinger og etterprøving

Virksomheten er, etter § 2-4 i personopplysningsforskriften, pliktig til å gjennomføre risikovurderinger som en del av arbeidet med informasjonssikkerhet. I risikovurderingene skal sannsynligheten for og konsekvensene av sikkerhetsbrudd vurderes. Resultatet av risikovurderingen skal sammenlignes med fastlagte kriterier for akseptabel risiko som virksomheten selv har fastsatt. Beslutning om akseptabelt risikonivå skal blant annet uttrykkes i virksomhetens sikkerhetsmål[7]. Som en del av grunnlaget for dette arbeidet skal virksomheten føre oversikt over hva slags personopplysninger som blir behandlet med elektroniske hjelpemidler, og hvilke opplysninger det er nødvendig å sikre konfidensialitet, integritet og tilgjengelighet for.

Risikovurdering skal gjennomføres før behandling av personopplysninger med elektroniske hjelpemidler blir satt i gang, og etter dette ved endringer som har innvirkning på informasjonssikkerheten.

I tillegg skal også virksomheten gjennomføre sikkerhetsrevisjoner (forskriftens § 2-5). I sikkerhets-revisjonen skal sikkerhetsarbeidet jevnlig etterprøves for å verifisere at tiltak er iverksatt og fungerer. Dette er ikke den samme gjennomgangen som ledelsens gjennomgang (§ 2-3), men kan være en del av grunnlaget for denne gjennomgangen.

Sikkerhetsbrudd og bruk av informasjonssystem som er i strid med fastlagte rutiner skal registreres som avvik (forskriftens § 2-6). Resultatet fra håndteringen av avvik skal dokumenteres, og dersom avviket har medført uautorisert utlevering av personopplysninger der konfidensialitet er nødvendig, skal virksomheten varsle Datatilsynet.

2.4 Organisering og administrative rutiner

Arbeidet med informasjonssystemet skal organiseres slik at tilfredsstillende informasjonssikkerhet blir oppnådd. Dette omfatter tiltak knyttet til blant annet ansvarsforhold, opplæring, autorisasjon, konfigurasjon av systemer og fysisk sikring.

Personopplysningsforskriften § 2-7 stiller krav til at det skal være etablert klare ansvars- og myndighetsforhold for bruk av informasjonssystemet. Det er videre et krav at konfigurasjonen av informasjonssystemet, altså hvordan program, utstyr og koblinger er satt opp, er slik at virksomheten oppnår tilfredsstillende informasjonssikkerhet.

Virksomheten skal redusere risikoen knyttet til informasjonssikkerhet ved å sette grenser for de ansatte sin bruk av informasjonssystemet og sikre at de ansatte har nok kunnskap til å benytte informasjonssystemet i samsvar med fastlagte rutiner (forskriftens § 2-8). Virksomheten skal også sørge for at det er tilstrekkelig fysisk sikring for utstyr som er viktig for informasjonssikkerheten (§ 2-10).

§§ 2-11 – 2-13 i forskriften dreier seg om tiltak knyttet til å hindre uautorisert innsyn i (konfidensialitet), å sikre tilgang til (tilgjengelighet) og å hindre uautorisert endring av informasjonen i systemene (integritet). Slike tiltak omfatter kryptering eller annen sikring av informasjon, backup og vern mot virus og annen skadelig programvare. Sikkerhetstiltak skal omfatte tiltak som fungerer uavhengig av medarbeidernes handlinger (§ 2-14). Formålet med sikkerhetstiltakene er både å hindre

[7] Jf Datatilsynets veileder for internkontroll og informasjonssikkerhet, veileder 07/01.

sikkerhetsbrudd og å avdekke hendelser som kan føre til sikkerhetsbrudd, og forsøk på uautorisert bruk av informasjonssystemet skal registreres.

Dokumentasjon som er relevant for informasjonssikkerheten, for eksempel beskrivelser av tekniske sikkerhetstiltak og rutiner for arbeid med informasjonssystemet skal etter forskriftens § 2-16 arkiveres. Slik informasjon skal lagres i fem år. Også hendelsesregister, dvs. registrering av uautorisert bruk av informasjonssystemet og forsøk på uautorisert bruk av informasjonssystemet, skal lagres. For slik informasjon skal lagringstiden være minst tre måneder.

Dersom virksomheten overfører personopplysninger elektronisk til andre, for eksempel databehandlere, skal disse tilfredsstille kravene i bestemmelsene (forskriftens § 2-15). Virksomheten plikter å ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører og jevnlig forsikre seg om at disse har tilfredsstillende informasjonssikkerhet.

2.5 Bruk av fødselsnummer som identifikasjonsmiddel

Av Personopplysningsloven § 12 første ledd fremgår følgende: *"fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering."*

Videre stiller Personopplysningsforskriften § 10-2 følgende krav ved sending av fødselsnummer: *"Postsendinger som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten. Tilsvarende gjelder sendinger som formidles ved hjelp av telekommunikasjon."*

Datatilsynet stiller krav om at fødselsnummer krypteres eller på annen måte sikres når man legger til rette for elektronisk kommunikasjon av fødselsnummer over usikret nettverk[8].

3. Data

3.1 Overordnet organisering og ledelse

IKT-funksjonen i Bergen kommune er organisert etter en bestiller – leverandør modell. En egen resultatenhet i kommunen, IKT Drift, har rollen som teknisk leverandør av løsninger, mens oppgaver knyttet til konsernovergripende løsninger og overordnet ansvar for å forvalte IKT området i Bergen kommune er lagt til IKT Forretningsutvikling. Sistnevnte er en avdeling under Seksjon for konkurranse og utvikling[9].

Per april 2009 består Bergen kommunes informasjonssikkerhetsorganisasjon av

- Behandlingsansvarlig
- IT-Sikkerhetsråd (kommunaldirektører + leder for etat for samfunnssikkerhet og beredskap)
- IKT Sikkerhetsansvarlig
- IT-Sikkerhetsforum (IKT-koordinatorer for byrådsavdelinger).

Rollen som IKT Sikkerhetsansvarlig innebærer blant annet å være informasjonssikkerhetsrådgiver for kommunen, og å ivareta informasjonssikkerhet og personvern innen IKT i kommunen. IKT Sikkerhetsansvarlig skal også delta i møter i Sikkerhetsrådet og Sikkerhetsforumet. Stillingen som IKT

[8] www.datatilsynet.no
[9] Seksjonen tilhører Byrådsavdeling for finans, konkurranse og eierskap.

Sikkerhetsansvarlig hører inn under IKT Forretningsutvikling. Stillingen er nyopprettet[10], og har et utvidet ansvar i forhold til det som tidligere var lagt til en IKT Sikkerhetskoordinator. IKT Sikkerhetsansvarlig gir selv uttrykk for at hans rolle bør gjøres tydeligere i organisasjonen, noe som vil bli gjort i forbindelse med etablering av nytt system for administrasjon av informasjonssikkerhet.

Det formelle behandlingsansvaret ligger ifølge Bergen kommunes retningslinjer for informasjonssikkerhet hos byrådsleder, men er delegert til kommunaldirektørene[11].

Revisjonen får opplyst at IT-sikkerhetsråd og sikkerhetsforum ikke har fungert optimalt, blant annet fordi det har vært få møter og lite oppslutning om disse gruppene[12].

3.2 Styrende dokumenter

Bergen kommunes system for informasjonssikkerhet består av blant annet følgende styrende dokumenter:

- Retningslinjer for informasjonssikkerhet
- Overordnet retningslinje for behandling av personopplysninger
- Standarder på IKT-området
- IT-sikkerhetserklæring
- Diverse rutiner/retningslinjer for bruk av IKT-utstyr i kommunen

Informasjonssikkerhet er inkludert i den siste versjonen av IT-strategien til Bergen kommune, men per august 2009 var denne strategien ennå ikke formelt vedtatt[13].

Kommunens retningslinjer for informasjonssikkerhet inneholder mål for informasjonssikkerhet. I tillegg inneholder retningslinjene overordnede føringer for sikkerhetsorganisasjon, klassifisering og kontroll, personellsikkerhet, fysisk og miljømessig sikkerhet, kommunikasjon og administrasjon, tilgangskontroll, systemutvikling og vedlikehold, beredskapsplanlegging og roller og ansvarsområder. IKT Sikkerhetsansvarlig opplyser at man har et mål om i løpet av 2009 å revidere disse retningslinjene og å sørge både for at de blir "bredere" og forankret i strategien, og for at de forankres i ledelsen. Revisjonen registrerer at retningslinjene for informasjonssikkerhet flere steder både i selve retningslinjene og i andre dokumenter omtales som *Policy for informasjonssikkerhet*.

I retningslinjene, avsnitt 3.1.3 står følgende: *"Retningslinjer for informasjonssikkerhet skal – som et minimum – revideres årlig."* Retningslinjene som revisjonen har mottatt er datert 14. juni 2006.

Retningslinjene viser også til supplerende retningslinjer og rutiner som *skal* utarbeides, deriblant rutiner for klassifisering og rutiner for autorisasjon og tilgangskontroll. Revisjonen har ikke mottatt dokumentasjon som viser at disse rutinene er utarbeidet.

Det er satt i gang en prosess for å forbedre kommunens system for informasjonssikkerhet på flere områder. Herunder etablering av et styrings- og kvalitetssystem for informasjonssikkerhet. En sentral del av den pågående prosessen er en gjennomgang av oversikter, rutiner og retningslinjer. I dette

---

[10] Stillingen ble første gang besatt høsten 2008.
[11] Andre dokumenter, for eksempel *Overordnet retningslinje for behandling av personopplysninger i Bergen kommune*, oppgir at byrådet er behandlingsansvarlig for Bergen kommune.
[12] Dette kommer frem i møte med IKT Sikkerhetsansvarlig 17.04.2009. I høringssvar til forvaltningsrevisjonsrapporten utdyper Byrådsavdeling for finans, konkurranse og eierskap utfordringer knyttet til IT-sikkerhetsforum og den generelle sikkerhetsorganisasjonen (se vedlagt høringssvar).
[13] Byrådsavdeling for finans, konkurranse og eierskap forklarer i høringssvar til forvaltningsrevisjonsrapporten at utkastet til ny strategi for Bergen kommune på IKT-området, eBergen 2013, innehar en beskrivelse av en strategisk retning for sikkerhetsarbeidet frem mot 2013. Her beskrives også mål og tiltaksområder som gir et overordnet bilde av hvordan kommunen skal jobbe med satsingsområdet "systematisering og effektivisering av sikkerhetsområdet". Denne strategien skal opp til politisk behandling.

arbeidet inngår også *"produksjon av manglende og oppdatering av utdaterte dokumenter"*[14]. I beskrivelsen av prosjektet blir det vist til *at "det er et mål å få samlet all relevant informasjon, satt dette i system og få knyttet det sammen på en mer hensiktsmessig og effektiv måte"*[15]. Videre går det frem at systemet skal ivareta ISO/IEC 27001[16] sine krav til dokumentasjon og rapportering. Av fremdriftsplanen går det frem at dette arbeidet ved utløpet av august 2009 er godt i gang.

3.3 Risikovurderinger og etterprøving

3.3.1 Oversikt over personopplysninger

I intervju kommer det frem at det ikke finnes noen oversikt over hvilke personopplysninger som blir behandlet i Bergen kommune.

Av kommunenes retningslinjer for informasjonssikkerhet går det fram at *"all informasjon, inkludert informasjon som mottas skal klassifiseres"*[17]. Videre går det fram at klassifisering kan realiseres i forhold til konfidensialitet, tilgjengelighet og fysisk tilgang, og at det vil bli utarbeidet rutiner for klassifisering. Slike rutiner foreligger ikke i dokumentasjonen revisjonen har mottatt.

Av retningslinjene fremgår det at informasjon skal behandles som intern dersom den ikke er spesifikt klassifisert i ovenfor nevnte kategorier. Videre vises det til at det er systemeierne som skal klassifisere informasjonen, og som skal bestemme hvem som skal ha tilgang til informasjonen. Når det gjelder systemer som behandler informasjon som omfattes av personopplysningsloven, er det daglig behandlingsansvarlig som har det øverste ansvaret, ifølge retningslinjene. I avsnitt 3.4.1 blir det gjort nærmere rede for rolle- og ansvarsfordeling knyttet til arbeidet med informasjonssikkerhet.

Av intervju går det frem at det i praksis er noe usikkerhet knyttet til klassifisering. Slik revisjonen oppfatter det, er ikke prosedyrene som beskrives i retningslinjene i aktiv bruk.

I intervju med seksjonsleder for skole, går det fram at det er saksbehandlere som har ansvar for å unnta informasjon fra offentlighet, i tråd med lovkrav. Seksjonsleder er imidlertid ikke kjent med om informasjon klassifiseres i henhold til kommunens retningslinjer for informasjonssikkerhet.

Fra barneverntjenesten får revisjonen opplyst at all informasjon blir klassifisert, men kun i kategoriene sensitive eller ikke sensitive persondata.

3.3.2 Risikoanalyser

Av kommunens retningslinjer for informasjonssikkerhet går det frem at det skal gjennomføres en risikovurdering før ny programvare, eller større endringer, settes i produksjon. Det eksisterer imidlertid ingen systematisk tilnærming til risikoanalyser i forhold til informasjonssikkerhet i Bergen kommune. Dette er noe man nå jobber med å få etablert. IKT Sikkerhetsansvarlig viser til at målet er å få gjennomført risikovurderinger av alle endrings- og utviklingsprosjekt, og at dette blir rapportert til IKT styringsgruppen[18].

Akseptabelt risikonivå fremgår ikke eksplisitt av Bergen kommunes retningslinjer for informasjonssikkerhet. I rapport fra en risiko og sårbarhetsanalyse som ble gjennomført i 2008, er det vist til at prosjektgruppen har utarbeidet kriterier for akseptabel risiko, da de ikke har hatt fullverdige

---

[14] Bergen kommune: *Forespørsel om konsulentbistand/avrop på rammeavtale. Konsulentbistand for innføring av system for administrasjon av informasjonssikkerhet (ISMS) i Bergen kommune.* Side 2.
[15] Bergen kommune: *Forespørsel om konsulentbistand/avrop på rammeavtale. Konsulentbistand for innføring av system for administrasjon av informasjonssikkerhet (ISMS) i Bergen kommune.* Side 1.
[16] ISO-standard for informasjonsstyringssystemer.
[17] Retningslinjer for informasjonssikkerhet, side 6.
[18] Jf møte med IKT Sikkerhetsansvarlig 17.04.2009.

kriterier å gå ut ifra. Videre vises det til at deres vurdering av akseptabel risiko er prosjektgruppens forslag, og *"ikke i følge en offisiell politikk i Bergen kommune"*[19].

Til tross for at det ikke finnes et overordnet system for gjennomføring av risikoanalyser, blir det gjennomført noen slike analyser. Første halvår 2008 gjennomførte Bergen kommune en større risiko- og sårbarhetsanalyse (ROS-analyse). Denne analysen var begrenset til IT-systemer som behandler eller inneholder sensitive personopplysninger i Bergen kommune[20]. Videre går det fram at det er *"(…) avdekket til dels stor risiko knyttet til behandling av personopplysninger innenfor Bergen kommunes ansvarsområder. Risikoen knytter seg spesielt til faren for skadet tillit til kommunen som følge av konfidensialitetsbrudd grunnet menneskelig feil eller mangelfulle rutiner"*[21]. Det blir i rapporten vist til at de tekniske sikkerhetstiltakene de siste årene har blitt så gode, at det nå er brukerne i organisasjonen som vanligvis utgjør den største trusselen mot informasjonssikkerheten. Det blir også vist til at prosjektgruppen i forbindelse med ROS-analysen har blitt gjort oppmerksom på lite tilfredsstillende forhold knyttet til hendelseshåndtering i kommunen, og det anbefales at det blir satt i gang et prosjekt for utarbeidelse av rutiner for hendelseshåndtering.

Seksjonsleder for skole bekrefter i intervju at det er gjennomført en ROS-analyse i kommunen som også omfattet IT-systemene som benyttes i Byrådsavdeling for barnehage og skole. Hun kjenner ikke til at det er gjennomført andre risikovurderinger knyttet til informasjonssikkerhet i seksjonen. Også i Byrådsavdeling for helse og omsorg (BHOS)/barneverntjenesten blir det vist til at det ble gjennomført en ROS analyse i 2008. Videre blir det opplyst det at det nå arbeides med en ny analyse for alle systemene som benyttes av Bergen kommune.

3.3.3 Risikovurderinger og etterprøving innen IKT Drift

Direktør for IKT Drift opplyser i brev til revisjonen, datert 27. mars 2009, at IKT Drift har utarbeidet enkelte retningslinjer til bruk i enheten, for eksempel prosedyrer for risikovurderinger.

I *Retningslinjer for risikovurdering i forhold til personvern*, står det at det til enhver tid skal *"(…) foreligge en risikovurdering av alle IKT Drifts systemer (applikasjoner), tjenester og teknisk infrastruktur (…)".* Videre går det frem at vurderinger skal gjennomføres og dokumenteres i forbindelse med nyutvikling/nyetablering, endringer som kan antas å få betydning for risiko samt når det oppstår endringer i omgivelsene som kan antas å få betydning for risiko. Revisjonen har ikke undersøkt om det foreligger risikovurderinger for alle applikasjoner og endringer i informasjonssystemet.

IKT Drift har også som en del av arbeidet med å bedre informasjonssikkerheten blant annet fått gjennomført en årlig ekstern IT-revisjon siden 2005. I rapporten fra IT revisjonen i 2008 går det frem at blant annet dokumentasjon, sikkerhetsretningslinjer, rutiner, endringshåndtering, etablerte standarder og beredskapsplaner er vurdert. Det vises også til at *"(…) der en kommer inn på premissgivers områder ifht IT styring og Informasjonssikkerhet, er også dette validert (…)"*[2223]. I rapporten fremgår en del forslag til forbedringer innen områder som ligger utenfor IKT Drifts mandat, og som må håndteres av andre instanser innen Bergen kommune. Fra IKT Drift får revisjonen opplyst at rapporten rutinemessig har blitt oversendt relevant ledelse og de som har sentrale roller innenfor IKT i Bergen kommune.

---

[19] Rapport fra ROS-analyse, side 15.
[20] Ifølge rapport fra ROS analysen ble 16 IT-systemer gjennomgått, deriblant systemer brukt av barneverntjenesten, PPT og skoler.
[21] Side 4.
[22] Side 6.
[23] Med premissgiver menes Bergen kommune.

3.3.4 Beredskapsplaner

I kommunens retningslinjer for informasjonssikkerhet står det at *"det skal være utarbeidet beredskapsplan(er) som dekker alle viktige og kritiske informasjonssystemer og infrastruktur"*[24]. Ifølge IKT Sikkerhetsansvarlig finnes det per april 2009 ingen beredskapsplaner for informasjonssikkerhet i kommunen, men dette er planlagt utarbeidet. Det er også planlagt å ha en beredskapsøvelse innen IKT-området i 2009[25].

3.3.5 Sikkerhetsrevisjon

Revisjonen har ikke mottatt dokumentasjon som viser at Bergen kommune har et system for å gjennomføre jevnlige sikkerhetsrevisjoner, utover den årlige IT revisjonen initiert av IKT Drift.

3.3.6 Avviksmeldinger

Avviksmeldinger blir registrert på skjema. Ifølge IKT sikkerhetsansvarlig har man imidlertid eksempler på situasjoner der det burde blitt meldt om avvik, men der dette ikke har blitt gjort[26].

IKT sikkerhetsansvarlig opplyser at det er opprettet en e-postliste, hvor det fremgår hvem man kan sende e-post til dersom det dukker opp avvik i tilknytning til informasjonssikkerhet[27]. Denne listen er tenkt benyttet som en del av avvikshåndteringen. IKT Sikkerhetsansvarlig viser til at rutinene knyttet til avvikshåndtering skal gjøres bedre kjent, og blant annet inngå i en ny intranettside for informasjonssikkerhet som skal opprettes.

I spørreundersøkelsen som er gjennomført i forbindelse med forvaltningsrevisjonen, svarer 83,1% av respondentene at de *ikke* kjenner til rutinene for å melde avvik knyttet til informasjonssikkerhet (tabell 1 i vedlegg 1).

3.4 Organisering og administrative rutiner

3.4.1 Rolle- og ansvarsfordeling

I ROS-analysen som ble gjennomført i Bergen kommune i 2008, kom det frem at ansvaret for systemforvaltning var organisert ulikt fra byrådsavdeling til byrådsavdeling, og at roller og ansvar ikke var entydige og dokumenterte. Det blir vist til at *"systemforvaltningens oppgaver bør fordeles på de ulike aktørene, og dokumenteres gjennom rollebeskrivelser"*[28].

En oversikt over daglig behandlingsansvarlig, daglig behandlingsansvarliges representant og navn på IT-system innen de ulike byrådsavdelingene i kommunen, inngår som en del av kommunens overordnede retningslinjer for behandling av personopplysninger. I intervju med seksjonsleder for skole, kommer det frem at oversikten ikke er oppdatert.

I kommunens retningslinjer for informasjonssikkerhet går det frem at det er systemeierne som har ansvar for å klassifisere informasjon, og som er ansvarlige for den informasjonen de eier. Systemeiere skal også bestemme *"(…) hvem som skal ha tilgang til informasjonen (autorisering), og på hvilken måte denne informasjonen skal kunne benyttes"*[29]. Videre fremgår det at *"IT Sikkerhetskoordinator skal skriftlig spesifisere systemeiers ansvar for databaser, filer, dokumenter og eventuelt andre former*

[24] Side 10.
[25] Jf møte med IKT Sikkerhetsansvarlig 17.04.2009.
[26] Jf møte med IKT Sikkerhetsansvarlig 17.04.2009.
[27] Telefonsamtale 19. august 2009.
[28] Side 27.
[29] Side 7.

for delt informasjon"[30]. Det kommer frem i intervju at systemeier vil være seksjon eller avdeling, ikke en fysisk person. Hvert system skal ha en systemkoordinator som har ansvar for å følge opp systemet/applikasjonen. Skriftlig angivelse av dette ansvaret fremgår ikke av den dokumentasjonen revisjonen har mottatt.

Verken BBS eller BHOS har utarbeidet egne dokumenter som spesifiserer roller og ansvar knyttet til informasjonssikkerhet. Det blir vist til de sentrale retningslinjene som er gitt av Bergen kommune.

I spørreundersøkelsen som er gjennomført i forbindelse med forvaltningsrevisjonen, svarer 65,7% av respondentene at de *ikke* kjenner til hvem i kommunen de skal kontakte dersom de har spørsmål knyttet til informasjonssikkerhet og behandling av personopplysninger[31]. 25% av resultatenhetslederne svarer at de *ikke* kjenner til hvem de skal kontakte dersom de har spørsmål om disse temaene (tabell 2 i vedlegg 1). Videre svarer 25,7% av resultatenhetslederne at de ikke vet hvem som er systemeiere av systemene som benyttes i hans eller hennes resultatenhet (tabell 3 i vedlegg 1), og 31,8% vet ikke hvem som er systemkoordinator /-ansvarlig for de systemene han eller hun bruker mest (tabell 4 i vedlegg 1).

IKT Sikkerhetsansvarlig viser til at formalisering og dokumentasjon av roller og ansvar knyttet til informasjonssikkerhet vil være en sentral del av systemet som er under utarbeidelse[32].

3.4.2 Soneinndeling

Nettverket i Bergen kommune er delt inn i intern og sikker sone: *"Systemer som er definert å inneholde personsensitive opplysninger iht. Personopplysningsloven"* ligger på sikker sone[33]. Kun ansatte som er autorisert for ett eller flere personsensitive systemer har tilgang til sikker sone. De to sonene holdes ifølge retningslinjene adskilt, også for ansatte med tilgang til begge soner, og det er ikke mulig å flytte dokumenter som er produsert i sikker sone over til intern sone eller omvendt. På den annen side går det fram av IKT Drifts IT-revisjon fra 2008 at det finnes åpninger mellom intern og sikker sone. Dette blir kommentert ytterligere under punkt 3.6 under.

I rapport fra ROS-analysen som ble gjennomført i 2008 går det frem at det ligger flere systemer som inneholder sensitive personopplysninger på intern sone[34]. IKT Sikkerhetsansvarlig bekrefter overfor revisjonen at dette er en prinsipielt viktig sak. Han viser til at det i utgangspunktet var slik at informasjon som er avhengig av konsesjon eller melding skal ligge på sikker sone, mens andre applikasjoner/opplysninger skal ligge på intern sone. Imidlertid er det i dag informasjon på intern sone som etter disse retningslinjene burde vært på sikker sone, og informasjon på sikker sone som burde vært på intern sone[35].

3.4.3 Autorisasjon

I intervju med seksjonsleder for skole går det fram at søknader om tilgang til systemer innen BBS går via seksjonsleder. Det er IKT-koordinator som tildeler tilgang til systemer. Kontorpersonalet i seksjonen holder oversikt over hvilke brukertilganger de ansatte har.

---

[30] Side 7.
[31] I høringsuttalelse til forvaltningsrevisjonsrapporten fra Seksjon skole, blir det vist til at sikkerhet og personvern er et særlig ansvar for systemeiere, og at dette ivaretas aktivt i BBS. Videre blir det vist til at brukerne erfaringsmessig henvender seg til systemkoordinatorene som forvalter systemeierskapet, vedrørende problemstillinger og utfordringer innen personvern og sikkerhet.
[32] Telefonsamtale 31. august 2009.
[33] Bergen kommune: *Retningslinjer vedrørende brukertilgang, e-post og datalagring i kommunens datanett.* 16. januar 2004.
[34] Side 16.
[35] Jf telefonsamtale med IKT Sikkerhetsansvarlig 31. august 2009.

I ROS-analysen fra 2008 vises det til at det i kommunen i varierende grad er etablert rutiner for å deaktivere brukertilganger det ikke lenger er behov for. På det grunnlag anbefalte prosjektgruppen som gjennomførte analysen at brukerlistene til alle de undersøkte systemene burde revideres og oppdateres så snart som mulig, samt at det burde innføres rutiner for dette.

IKT Forretningsutvikling er kjent med svakhetene som kom frem i ROS-analysen, og IKT Sikkerhetsansvarlig bemerker at disse har sammenheng med at det overordnede systemet for informasjonssikkerhet i Bergen kommune ikke har vært godt nok. De har derfor prioritert arbeidet med å få på plass et overordnet system, i stedet for å fokusere på detaljer som har vært mangelfulle. Et bedre system skal i sin tur bidra til å rette opp mangler som er avdekket.

I spørreundersøkelsen som er gjennomført i forbindelse med forvaltningsrevisjonen, svarer til sammen 8,7% av respondentene at det har hendt at de har lånt ut brukernavn og passord til andre enn IT-avdelingen eller tilsvarende. Andelen er høyest innen barneverntjenesten, med 13,7% (tabell 5 i vedlegg 1).

3.4.4 Rutiner og standarder på IKT-området

Bergen kommune har rutiner for anskaffelse og oppkobling av IKT-utstyr, utarbeidet av Seksjon for konkurranse og utvikling/IKT Strategi. Disse er beskrevet i dokumentene *Standarder på IKT området*, *Prinsipper for oppkobling av enheter og utstyr i Bergen kommunes nettverk*, *Retningslinjer for bærbare PC-er*, *Retningslinjer for stasjonære PC-er* og *Retningslinjer for kabling (data og telefoni) av bygg for Bergen kommune.* Av dateringen av flere av disse dokumentene går det frem at de ikke er oppdatert de siste årene.

Det er også utarbeidet en teststrategi for Bergen kommune, som gjelder for de av kommunens virksomheter som jobber med utvikling og/eller innføring av IT-løsninger/programvare. Denne beskriver krav til testing av systemer og rutiner knyttet til dette.

I retningslinjer for bærbare PC-er, datert i 2005, fremgår det at kommunen holder på med å legge til rette for bruk av trådløs teknologi. Det fremgår ikke om dette er gjennomført, og hvordan dette eventuelt påvirker krav og retningslinjer i forbindelse med bruk av IKT-utstyr.

Også når det gjelder programvare fremkommer det at flere av retningslinjene er utdaterte og blant annet viser til programvare som ikke lengre er i bruk. For eksempel viser dokumentet *Standarder på IKT området* til endringer som skal gjennomføres i 2007, uten at det er angitt om endringene er gjennomført. Under krav til systemsikkerhet listes det i nevnte dokument opp antispywareløsninger som per i dag ikke lenger er i bruk.

Retningslinjene fra Seksjon for konkurranse og utvikling/IKT Strategi har varierende detaljeringsgrad. På enkelte områder er de svært detaljerte, mens de på andre områder, for eksempel kryptering, legger lite føringer for arbeidet IKT Drift skal utføre. Revisjonen har blitt informert om at IKT Drift også har egne utfyllende og til dels overlappende retningslinjer og rutiner innenfor disse områdene.

Ifølge IKT Sikkerhetsansvarlig i Bergen kommune har brukerne av kommunens system per i dag for vide fullmakter til nedlasting og installasjon av programvare på PC-ene. Han mener at det faktum at alle ansatte har lokale administratorrettigheter på sin PC, utsetter kommunen for unødvendig høy grad av risiko[36].

3.4.5 Utskrift av dokumenter som inneholder personopplysninger

I ROS-analysen fra 2008 går det frem at det er et gjennomgående problem at utskrifter sendes til feil nettverksprinter og skrives ut på andre lokasjoner enn det som var ment. På dette grunnlag ble det i

[36] Jf møte med IKT Sikkerhetsansvarlig 17.04.2009.

rapporten fra ROS analysen anbefalt at kommunen snarest burde videreføre arbeidet med å innføre systemet "Follow Me Printing" for å sikre konfidensialiteten i forbindelse med utskrifter.

Bergen kommune har et prosjekt som har som mål å innføre en utskriftsløsning der brukeren må benytte et digitalt ansattkort for å hente ut en utskrift. Ansvar for prosjektet ligger hos IKT Forretningsutvikling, og er ikke sluttført per august 2009. Det blir opplyst at en rekke av multifunksjonsskriverne som blir benyttet i dag har støtte for sikker utskrift i ulike varianter, eksempelvis ved hjelp av kode eller passord på maskinen. Dette er imidlertid opp til den enkelte bruker å benytte.

I spørreundersøkelsen som er gjennomført i forbindelse med revisjonen, er respondentene bedt om å opplyse om sine rutiner for å hente utskriften når de skriver ut informasjon som inneholder personopplysninger. Til sammen 5,4% av respondentene svarer at det hender at de lar utskriften ligge på printeren for å hente den senere. Andelen er størst innen barneverntjenesten, der 11,1% svarer at det hender at de lar utskriften ligge på printeren for å hente den senere (tabell 6 i vedlegg 1).

3.4.6 Dokumentasjon

Kommunen har ikke etablert en samlet oversikt over all dokumentasjon som omhandler informasjonssikkerhet. Det finnes heller ikke rutiner for å sikre at dokumentasjon lagres i henhold til krav i personopplysningslov og personopplysningsforskrift.

IKT Sikkerhetsansvarlig gir uttrykk for at all dokumentasjon som er relevant for informasjonssikkerheten sannsynligvis ikke blir lagret på en forskriftsmessig måte. Han opplyser videre at systemet som er under utarbeidelse skal sørge for at krav til dokumentasjon blir ivaretatt[37].

3.5 Kjennskap til retningslinjer og rutiner

3.5.1 System for opplæring og informasjon

I kommunens retningslinjer for informasjonssikkerhet fremgår det at *"brukere av kommunens IT-systemer skal få tilstrekkelig opplæring og oppdatering i Policy for informasjonssikkerhet og relevante retningslinjer og prosedyrer. Det vil være varierende grad av krav til opplæring"*[38]. Det er utarbeidet to brosjyrer om informasjonssikkerhet: *Nettvett i bergensskolen* og *Informasjon om datasikkerhet.*

Bergen kommune sin IT-sikkerhetserklæring skal være lest og godkjent av alle som har tilgang til kommunens nettverk. Alle brukere av kommunens IKT-system får årlig opp en elektronisk beskjed, og må bekrefte at de kjenner til retningslinjene for informasjonssikkerhet i Bergen kommune.

Formålet med IT-sikkerhetserklæringen er å sikre at alle brukere av kommunens IT-systemer kjenner til gjeldende regler for bruk av kommunens nettverk[39]. Videre går det frem av rutinebeskrivelsen for sikkerhetserklæringen at den ansatte skal sette seg inn i kommunens brosjyre om IT-sikkerhet og i *Retningslinjer for IT-sikkerhet i Bergen kommune* før tilgang blir gitt. Sikkerhetserklæringen inneholder ikke retningslinjer vedrørende for eksempel bruk av bærbar PC eller ulike lagringsmedier.

I sikkerhetserklæringen er det en elektronisk lenke til *"Retningslinjer for IT-sikkerhet i Bergen kommune"*. Ved forvaltningsrevisjonen kom det frem at lenken er til et utdatert dokument, ikke til gjeldende retningslinjer for informasjonssikkerhet.

---

[37] Jf telefonsamtale med IKT Sikkerhetsansvarlig 31. august 2009.
[38] Side 7.
[39] Rutinebeskrivelse IT-sikkerhetserklæring, BKDOK-2002-00018.

IKT Sikkerhetsansvarlig opplyser at kommunen har et mål om å utarbeide en IKT sikkerhetshåndbok på intranettet, som skal være basert på reviderte retningslinjer for informasjonssikkerhet. Han viser også til at det er et mål at retningslinjene skal være skrevet for ikke-teknisk personell.

3.5.2 Avdelingsspesifikke retningslinjer for informasjonssikkerhet

Innen BBS foreligger det ikke styrende dokumenter eller rutiner for informasjonssikkerhet utover det som finnes sentralt[40]. BHOS/barneverntjenesten viser til at det er utarbeidet skriftlige manualer og rutiner knyttet til saksbehandlingen i barneverntjenesten. Det fremgår ikke at det er utarbeidet særskilte rutiner knyttet til informasjonssikkerhet.

I spørreundersøkelsen som er gjennomført i forbindelse med forvaltningsrevisjonen, har resultatenhetslederne fått spørsmål om det er utarbeidet utdypende retningslinjer knyttet til informasjonssikkerhet og/eller personvern i den enheten han eller hun er resultatenhetsleder for. Til sammen har 30,6% svart at slike retningslinjer er utarbeidet. Forskjellen mellom de ulike fagområdene er stor, andelen som har svart at slike retningslinjer er utarbeidet er 75% innen barneverntjenesten, 83,3% innen PPT og 8% innen skole (tabell 7 i vedlegg 1). Flere av respondentene spesifiserer at det ikke er utarbeidet særskilte retningslinjer for informasjonssikkerhet i deres enhet, men at disse er innarbeidet i for eksempel saksbehandlingsrutinene.

3.5.3 Egenrapportering om opplæring og kjennskap til retningslinjer og rutiner

I spørreundersøkelsen svarer til sammen 7,4% av respondentene at de *ikke* har lest IT-sikkerhetserklæringen for Bergen kommune, mens 10,2% svarer at de *ikke vet* om de har lest denne. Andelen som *ikke* har lest eller som *ikke vet* om de har lest erklæringen er størst innen PPT, med henholdsvis 10,8 og 18,9% (tabell 8 i vedlegg 1).

Av de som har svart at de har lest IT sikkerhetserklæringen, svarer 20,3% at de i liten eller svært liten grad husker innholdet i erklæringen. Andelen er størst innen barneverntjenesten, med 25,7% (tabell 9 i vedlegg 1). Innen barneverntjenesten svarer videre 31,6% av respondentene at de bare i *noen grad* opplever innholdet i IT-sikkerhetserklæringen som forståelig (tabell 10 i vedlegg 1).

Til sammen svarer 42,5% av respondentene at de *ikke* har satt seg inn i dokumentet *Retningslinjer for IT-sikkerhet i Bergen kommune*. Det er relativt små forskjeller mellom skole, PPT og barneverntjenesten (tabell 11 i vedlegg 1) . Av resultatenhetslederne innen de tre enhetene svarer til sammen 19,4% at de *ikke* har satt seg inn i disse retningslinjene (tabell 12 i vedlegg 1).

Videre er respondentene bedt om å svare på om de har fått tilstrekkelig opplæring i hvordan IT-systemene de benytter skal brukes. Til sammen 29,6% svarer *"nei, opplæringen kunne vært bedre"*. Andelen er relativt lik innen barneverntjenesten, skole og PPT (tabell 13 i vedlegg 1).

Det er stor variasjon når det gjelder i hvilken grad respondentene rapporterer at deres nærmeste ledelse har fremhevet viktigheten av informasjonssikkerhet. Innen barnevernet svarer 20,6% av respondentene at deres nærmeste ledelse i liten eller svært liten grad har fremhevet viktigheten av informasjonssikkerhet. Andelen er 18,4% innen skole og 10,8% innen PPT (tabell 14 i vedlegg 1). Til sammen 25% av resultatenhetslederne svarer at deres nærmeste ledelse i liten eller svært liten grad har fremhevet viktigheten av informasjonssikkerhet (tabell 15 i vedlegg 1).

En del respondenter kommenterer at det er behov for mer informasjon om regler for å ivareta personvernet når man bruker informasjonsteknologi. Det blir også vist til at det er behov for jevnlige repetisjoner.

[40] Intervju i Seksjon skole 8. mai 2009.

I spørreundersøkelsen kommenterer flere ansatte i barneverntjenesten at det hender de mottar henvendelser på e-post fra barnehager og skoler der hele barnets/elevens navn fremgår. De viser til at det generelt i Bergen kommune burde informeres bedre om hva slags informasjon man ikke skal sende per e-post.

3.6 Systemteknisk sikkerhet

Som del av det systemtekniske sikkerhetsarbeidet, gjennomfører IKT Drift penetrasjons- og sikkerhetstester både internt og eksternt, ifølge direktør for IKT Drift[41].

I IT revisjonen som ble gjennomført innen IKT Drift i 2008 ble det blant annet vist til at det ikke var etablert rutiner for rapportering av sikkerhetshendelser, som for eksempel antall virus, antall uautoriserte påloggingsforsøk og driftsproblematikk som har forårsaket tapt tilgjengelighet. I samme revisjon vises det til at IKT-drift har en avtale med EDB ASA for backup av data. Backuprutinene ble ikke testet i IT-revisjonen.

I rapport fra IT revisjonen går det frem at det er relativt god dokumentasjon på tekniske løsninger, men at denne i liten grad er gjenstand for oppgraderinger. Det går videre frem at regelverk knyttet til registrering av uautorisert bruk av informasjonssystemet, og forsøk på uautorisert bruk, ikke etterleves i tilstrekkelig grad. I rapporten anbefales det at IKT Drift, sammen med premissgiver, bør gjennomgå retningslinjer for og logging av bruken av informasjonssystemene.

Fra IKT Drift får revisjonen opplyst at de totalt sett har bedret sikkerheten på en del identifiserte områder i etterkant av IT revisjonen i 2008. Blant annet har IKT Drift hatt en ny gjennomgang av brannmurreglene mellom intern sone og sikker sone. Ny IT-revisjon konkluderer med at dette må forbedres ytterligere. Konklusjonen i revisjonsrapporten for 2009 er, ifølge direktøren for IKT Drift, at det har skjedd en viss forbedring av sikkerheten totalt sett.

3.7 Samarbeidspartnere

I kommunenes retningslinjer for informasjonssikkerhet går det fram at *"alle eksterne tjenesteleverandører må akseptere og følge kommunens Policy for informasjonssikkerhet og relevante retningslinjer. Et relevant sammendrag av Policy for informasjonssikkerhet og retningslinjer skal presenteres alle tjenesteleverandører før disse leverer tjenester"*[42].

Det er utarbeidet et vedlegg til taushetserklæring for partnere og leverandører, som omhandler tilkobling av bærbare PC-er i Bergen kommune sitt interne nettverk.

I henhold til personopplysningsforskriften § 2-15 femte ledd, skal den behandlingsansvarlige ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.

Bergen kommunes retningslinjer for informasjonssikkerhet sier ikke noe om hva kommunen skal gjøre for å etterleve dette kravet.

3.8 Bruk av fødselsnummer som identifikasjonsmiddel

Bruk av foresattes fødselsnummer i det skoleadministrative systemet i Bergen kommune (Extens) har vært omdiskutert, og FAU ved en skole i kommunen har blant annet stilt spørsmål ved denne bruken. Kommunen har i den forbindelse vært i dialog med Datatilsynet. I et brev til Datatilsynet blir det vist

[41] Brev til revisjonen datert 27. mars 2009.
[42] Side 7.

til at Bergen kommune aksepterer Datatilsynets vurdering i saken, og vil tilpasse sine interne administrative systemer i henhold til pålagte endringer, blant annet gjennom å be systemleverandøren om å foreta nødvendige endringer og tilpasninger i systemet[43]. Etter dette var det imidlertid kontakt mellom Datatilsynet og systemleverandøren International Software Technology AS, og Datatilsynet konkluderte da med at lagring og behandling av fødselsnummer i Extens for administrativ bruk (som skissert av systemleverandøren) ikke er i strid med personopplysningslovens § 12.

Flere viser til at det har vært en hendelse der fødselsnummer fra Extens har blitt publisert på It's Learning[44] i forbindelse med en importrutine knyttet til nye elever i skolen. Fødselsnumrene ble synlige for alle brukere av It´s Learning. Dette skyldtes at skolen ikke hadde gått inn og registrert brukernavn i stedet for fødselsnummer før importen ble igangsatt. Hendelsen ble ikke meldt som avvik, men ble behandlet som det når den ble kjent gjennom media.

Revisjonen får opplyst at Bergen kommune vil strekke seg mot å forsøke å bruke fødselsnummer minst mulig, og lagre dem i færrest mulig registre[45]. Det er dette Datatilsynet har ytret ønske om. Mer spesifikke retningslinjer for bruk av fødselsnummer og rutiner for melding av dette skal utarbeides i kommunen[46].

Det opplyses videre at MinID bruker fødselsnummer som identitetsbærer for innlogging, og at dette vil binde opp de systemene i Bergen kommune som er avhengig av denne innloggingen. Arbeidet DIFI[47] er i gang med, med utvikling av et oppgradert samtrafikknav (eID), vil muligens kunne gjøre kommunen mindre avhengig av fødselsnummer som ID-bærer.

4. Vurderinger og anbefalinger

4.1 Overordnet organisering

Bergen kommune sine styringsdokumenter innen området informasjonssikkerhet er ikke tilstrekkelig systematisert og forankret. Revisjonen vurderer at en systematisering av alle styringsdokumenter innen dette området er en forutsetning for at arbeidet med informasjonssikkerhet skal kunne implementeres i tilstrekkelig grad innen alle nivå i organisasjonen.

I kommunens retningslinjer for informasjonssikkerhet er det vist til ulike rutiner og retningslinjer som skal utarbeides. Retningslinjene er datert 14. juni 2006, og revisor stiller spørsmål ved hvorfor disse rutinene og retningslinjene fremdeles ikke foreligger. Generelt er det viktig at alle rutiner, retningslinjer og lignende oppdateres jevnlig. Dette for å sikre at henvisninger til blant annet andre dokumenter, til ansvarlige instanser eller personer er korrekt. Revisjonens undersøkelser viser at Bergen kommune ikke har tilfredsstillende rutiner på dette området.

Revisjonen ser positivt på at det er igangsatt et arbeid for å systematisere og utbedre kommunens system og dokumentasjon knyttet til informasjonssikkerhet.

For at informasjonssikkerhetsarbeidet skal fungere effektivt og hensiktmessig, må Bergen kommune tilrettelegge for et godt samarbeid mellom de ulike aktørene på IKT området i kommunen (ansvarlige i de ulike byrådsavdelingene, IKT Forretningsutvikling og IKT Drift). Det er videre viktig at alle aktører

[43] Brev fra Bergen kommune til Datatilsynet datert 29. februar 2008.
[44] En digital læringsplattform som elever og lærere har tilgang til.
[45] Telefonsamtale med IKT Sikkerhetsansvarlig 19. august 2009.
[46] I høringsuttalelse fra Seksjon skole går det frem at Extens fremdeles kommer til å bruke fødselsnummer, fordi dette er eneste entydige identifikator og fordi systemet krever dette.
[47] Direktoratet for forvaltning og IKT.

har en klar forståelse av hvordan ansvar og oppgaver er fordelt. Dette vil slik revisjonen vurderer det være spesielt viktig i en situasjon der IKT Drift blir etablert som et selvstendig aksjeselskap. Kommunen har videre en jobb å gjøre når det gjelder å sikre at det administrative arbeidet med informasjonssikkerhet og vern av personopplysninger blir godt integrert med IKT Drifts arbeid med systemtekniske og fysiske sikkerhetstiltak.

4.2 Risikovurderinger og etterprøving

Bergen kommune har slik revisjonen ser det ikke god nok oversikt over hvilke personopplysninger som behandles i kommunen. Ifølge kommunens retningslinjer for informasjonssikkerhet skal klassifisering av all informasjon benyttes som et hjelpemiddel for å sikre konfidensialitet, integritet og tilgjengelighet for personopplysninger. Imidlertid viser undersøkelsene at disse retningslinjene ikke følges opp som forutsatt.

Bergen kommune har heller ikke et tilfredsstillende system for gjennomføring av risikovurderinger knyttet til informasjonssikkerhet og personopplysninger.

Slik revisjonen vurderer det, er det nødvendig at kommunen gjennomgår rutinene på området og sikrer at det foreligger en oppdatert oversikt over personopplysninger, at det fastsettes kriterier for akseptert risiko og at risikovurderinger blir gjennomført i tråd med kravene i personopplysningsforskriften § 2-4.

Revisjonen registrerer at IKT Drift har utarbeidet egne rutiner for gjennomføring av risikovurderinger knyttet til sine ansvarsområder, noe som er positivt. Revisjonen mener at man ved utarbeiding av et overordnet system for gjennomføring av risikovurderinger, bør se på i hvilken grad IKT Drifts rutiner på dette området kan integreres bedre i det overordnede systemet.

Revisjonen merker seg at IT revisjonene som utføres på bestilling fra IKT Drift også omhandler problemstillinger som ligger utenfor IKT Drift sitt mandat, og at enkelte av anbefalingene er rettet mot "premissgiver". På dette grunnlag anbefaler revisjonen at Bergen kommune vurderer hvorvidt IT revisjonene er tilstrekkelig forankret når de gjennomføres på initiativ og bestilling fra IKT Drift, eller om de bør forankres på et høyere nivå i kommunen og dermed omfatte en bredere del av organisasjonen.

Det er ikke tilfredsstillende at kommunen ikke har et system for gjennomføring av sikkerhetsrevisjoner som omfatter hele virksomheten (jf personopplysningsforskriften § 2-5). Det er risiko forbundet blant annet med det at man ikke gjennomfører jevnlige kontroller av hvorvidt rutiner og sikkerhetstiltak blir fulgt opp som forutsatt.

Det er heller ikke tilfredsstillende at Bergen kommune ikke har utarbeidet beredskapsplaner for informasjonssikkerhet, men revisjonen registrerer at det er satt i gang et arbeid på dette området.

4.3 Implementering av rutiner

Av revisjonens undersøkelser kommer det frem at kommunens retningslinjer og rutiner for informasjonssikkerhet ikke er tilstrekkelig implementert på alle nivå i kommunen, og medarbeidere har ikke nødvendig kunnskap i henhold til personopplysningsforskriften § 2-8. Dette fremgår blant annet av spørreundersøkelsen, som viser at ansatte har manglende kjennskap til retningslinjer og rutiner, og at ansatte rapporterer om lite fokus på temaet fra ledelsen.

Revisjonen ser på det som positivt at det er satt i gang et arbeid med å samle og forbedre rutiner og retningslinjer knyttet til informasjonssikkerhet, blant annet med en egen intranettside. For at dette skal fungere hensiktsmessig, vil revisjonen påpeke at det også er en forutsetning at kommunen får på

plass rutiner for jevnlig å oppdatere alle relevante dokumenter og lagre disse i henhold til bestemmelsene i personopplysningsforskriften § 2-16.

Bergen kommune bør ha rutiner for å sikre etterlevelse av IT sikkerhetserklæringen. Videre bør kommunen vurdere om flere rutiner/ytterligere informasjon bør inngå i sikkerhetserklæringen, for å samle denne typen rutiner og informasjon i ett sentralt dokument.

Det er etter revisjonens vurdering ikke tilfredsstillende at et klart flertall av respondentene i spørreundersøkelsen som er utført i forbindelse med forvaltningsrevisjonen, ikke kjenner til kommunens rutiner for å melde avvik i forbindelse med informasjonssikkerhet. Samtlige respondenter er brukere av informasjonssystemer som behandler personopplysninger, og skal kjenne til denne typen rutiner. Revisjonen anbefaler at Bergen kommune snarest setter i gang tiltak for å bevisstgjøre og informere sine ansatte om rutiner på dette området, slik at man sikrer at avvikshåndteringen er i tråd med personopplysningsforskriften § 2-6.

4.4 Organisering og administrative rutiner

Bergen kommune har ut fra den dokumentasjonen revisjonen har mottatt, ikke spesifisert og dokumentert godt nok det ansvar som tilligger ulike roller når det gjelder informasjonssikkerhet og behandling av personopplysninger, for eksempel systemeier og systemkoordinators oppgaver og ansvar. Dette er ikke i samsvar med personopplysningsforskriftens krav om klare ansvars- og myndighetsforhold. Kommunen bør utarbeide skriftlige rollebeskrivelser som tydeliggjør ansvar og oppgaver. Kommunen bør også innføre bedre rutiner for å oppdatere oversikter over hvem som innehar ulike roller og oppgaver i de ulike byrådsavdelingene. Revisor registrerer at systemet som er under utarbeidelse i Bergen kommune skal dekke også disse punktene.

Bergen kommune bør i forbindelse med etablering av oversikter over hvilke personopplysninger som blir behandlet i kommunen, også se nærmere på hvilken informasjon som ligger på sikker sone og hvilken informasjon som ligger på intern sone. Dette for å sikre at soneinndelingen fungerer som forutsatt med hensyn til vern av personopplysninger.

Det at ansatte med tilgang til sikker sone låner ut brukernavn og passord til andre, skal ikke forekomme. Bergen kommune bør iverksette tiltak for å bevisstgjøre ansatte når det gjelder denne problemstillingen.

Kommunen bør vurdere om ansatte har for vide fullmakter når det gjelder for eksempel nedlasting og installasjon av programvare, da dette kan utgjøre en risiko for informasjonssikkerheten.

Når det gjelder retningslinjer for bruk av IKT, går det frem av dokumentasjonen at flere av disse ikke er oppdaterte. Videre er retningslinjene på enkelte områder så detaljerte at det synes lite hensiktsmessig.

Revisjonen merker seg at det kan være betydelig risiko knyttet til utskrifter som inneholder personopplysninger, og som enten blir sendt til feil printer eller blir liggende på printeren. Revisjonen støtter derfor anbefalingen fra prosjektgruppen i Bergen kommune som gjennomførte ROS-analysen i 2008, om å legge til rette for bruk av ”Follow Me Printing”, eller andre systemer for sikker utskrift, i alle enheter som behandler personopplysninger. Revisjonen merker seg at Bergen kommune har et prosjekt som har som mål å innføre en slik utskriftsløsning, noe som er positivt.

Ut fra de opplysninger revisjonen har mottatt, vurderer revisjonen at Bergen kommune ikke tilfredsstiller kravene til dokumentasjon som går frem av personopplysningsloven og personopplysningsforskriften. Bergen kommune må snarest få på plass rutiner som sikrer at all dokumentasjon som er relevant for informasjonssikkerheten blir lagret. Revisjonen registrerer at dette skal inngå som en del av det nye systemet for informasjonssikkerhet som er under utarbeidelse.

4.5 Teknisk sikkerhet

Revisjonen merker seg at det i regi av IKT Drift er innført ulike tiltak som bidrar til en høyere grad av informasjonssikkerhet, derunder rutiner for risikoanalyser og årlige IT-revisjoner. Det er viktig at dette arbeidet fortsetter og at man kontinuerlig sørger for å utbedre svakheter som avdekkes. Som det fremgår av avsnitt 4.2, anbefaler revisjonen at Bergen kommune vurderer hvorvidt IT revisjonene som gjennomføres er tilstrekkelig forankret i kommunen.

4.6 Samarbeidspartnere

Bergen kommune bør jf krav i personopplysningsforskriften § 2-15 få på plass rutiner som beskriver behandlingsansvarliges plikt til å skaffe seg kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og hvordan dette skal gjennomføres i praksis.

4.7 Bruk av fødselsnummer som identifikasjonsmiddel

Revisor registrerer at det har vært og er dialog mellom Bergen kommune og Datatilsynet i forbindelse med bruk av fødselsnummer som identifikasjonsmiddel. Det er viktig at kommunen får på plass rutiner som sørger for at hendelser der fødselsnummer blir offentliggjort ikke forekommer.

Når det gjelder bruk av fødselsnummer generelt, er det viktig at det kommer på plass rutiner for dette, og at disse gjøres kjent. Dette er slik revisor vurderer det meget viktig for at en stor organisasjon som Bergen kommune skal forholde seg korrekt til bruk av fødselsnummer. Revisor ser derfor positivt på at det i Bergen kommune foreligger planer om å utarbeide mer spesifikke retningslinjer for bruk av fødselsnummer og rutiner for melding av dette.

4.8 Oppsummering

Av de foregående avsnittene i dette kapittelet fremgår en rekke vurderinger og anbefalinger vedrørende informasjonssikkerhet og behandling av personopplysninger i Bergen kommune. Noen av de mest sentrale anbefalingene er gjengitt under.

Det er revisjonens vurdering at Bergen kommune bør:

- Opprettholde fokus på arbeidet med det nye systemet for informasjonssikkerhet, og sikre at dette ivaretar kravene i personopplysningsforskriften, bl.a. når det gjelder
    - Risikovurderinger
    - Sikkerhetsrevisjon
    - Avvikshåndtering
    - Dokumentasjon
    - Sikkerhet hos kommunikasjonspartnere og leverandører

- Sørge for at rutiner og retningslinjer knyttet til informasjonssikkerhet holdes oppdatert og blir tilstrekkelig implementert på alle nivå i kommunen, samt at medarbeiderne har nødvendig kunnskap for å bruke informasjonssystemet i samsvar med fastlagte rutiner.

- Tilrettelegge for et godt samarbeid mellom de ulike aktørene som er involvert i kommunens IKT arbeid, og utarbeide skriftlige rollebeskrivelser som tydeliggjør ansvar og oppgaver.

Referanser

Regelverk

- Fornyings- og administrasjonsdepartementet: *Forskrift om behandling av personopplysninger (personopplysningsforskriften).* FOR-2000-12-15-1265.
- Justis- og politidepartementet: *Lov om behandling av personopplysninger (personopplysningsloven)*. LOV-2000-04-14-31.

Øvrige referanser

- Datatilsynet: *Veiledning i informasjonssikkerhet for kommuner og fylker*. TV-202:2005.
- Datatilsynet: *Internkontroll og informasjonssikkerhet.* Veileder 07/01.
- Datatilsynet: *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer*. Desember 2000. SV-100:2000.
- Datatilsynet: *Kommentarer til International Software Technology AS sine spørsmål*. Brev til International Software Technology AS, 23. April 2008.

Internettreferanser

- http://www.datatilsynet.no/templates/article____1594.aspx

Dokumenter fra Bergen kommune

- *Bruk av fødselsnummer i det skoleadministrative systemet i Bergen kommune.* Brev til Datatilsynet, 29. Februar 2008. Vår ref.: 200800038-7 STFO.
- *Forespørsel om konsulentbistand/avrop på rammeavtale. Konsulentbistand for innføring av system for administrasjon av informasjonssikkerhet (ISMS) i Bergen kommune*. Mars 2009.
- *Gjennomgang av informasjonssikkerhet hos IKT Drift*. IT Revisjon – internkontroll. 2. Juli 2008.
- *Informasjon om datasikkerhet*. Brosjyre. Vedtatt i IT sikkerhetsråd 04.12.2001.
- *IT-sikkerhetserklæring.* BKDOK-2002-00018. Dato: 4.12.2001.
- *Nettvett i bergensskolen*. Brosjyre. Uten dato.
- *Overordnet retningslinje for behandling av personopplysninger i Bergen kommune.* Dok.nr.: BKDOK-2004-00655.06. Rev. Dato: 080108.
- *Prinsipper for oppkobling av enheter og utstyr i Bergen kommunes nettverk*. Doknr.: BKDOK-2003-00301.03. Rev.dato: 280403.
- *Regler for avhending av utrangert IT-utstyr*. Notat, 28. Januar 2008. Saksnr.: 200514545-18.
- *Retningslinjer for bærbare PC-er*. Doknr.: BKDOK-2006-00034.01. Rev. Dato: 170106.
- *Retningslinjer for informasjonssikkerhet i Bergen kommune*. Saksnr.: 200411089/65. Dato: 14/6-2006.
- *Retningslinjer for risikovurdering i forhold til personvern*. IKT Drift. Uten dato.
- *Retningslinjer vedrørende brukertilgang, e-post og datalagring i kommunens datanett*. 16. Januar 2004. Saksnr.: 200400496-2.
- *Retningslinjer for stasjonære PC-er*. Doknr.: BKDOK-2006-00033.01. Rev. Dato: 170106.
- *Retningslinjer for kabling (data og telefoni) av bygg for Bergen kommune*. Doknr.: BKDOK-2004-00531.05. Rev. Dato: 101007.

- *Risiko og sårbarhet: behandling av sensitive personopplysninger i Bergen kommune*. ROS-analyse. 2008.
- *Standarder på IKT-området*. Saksnr.: 200514545-4. Oppdatert 01.03.2007.
- *Teststrategi for Bergen kommune*. Doknr.: BKDOK-2002-00302. Februar 2003.
- *Vedlegg til taushetserklæring for partnere og leverandører. Tilkobling av bærbare PC-er i Bergen kommune sitt interne nettverk*. Doknr.: BKDOK-2003-00554.
- *Vedrørende forvaltningsrevisjon 2009 – oppstart og dokumentasjon*. Brev til kommunerevisjonen fra IKT Drift v/direktør. 27. Mars 2009.08.28

Vedlegg 1: Tabeller

Tabell 1: Kjenner du rutinene for å melde avvik knyttet til informasjonssikkerhet?

	PPT	Skole	Barnevern	Annet	Total
Ja	12,2 %	22,4 %	13,7 %	10,0 %	16,9 %
Nei	87,8 %	77,6 %	86,3 %	90,0 %	83,1 %
Antall	74	152	131	10	367

Tabell 2: Vet du hvem i kommunen du skal kontakte dersom du har spørsmål knyttet til informasjonssikkerhet og behandling av personopplysninger?

	Resultat-enhetsledere	Andre	Total
Ja	75,0 %	29,9 %	34,3 %
Nei	25,0 %	70,1 %	65,7 %
Antall	36	331	367

Tabell 3: Vet du hvem som er systemeiere av systemene som benyttes i din resultatenhet?

Ja	74,3 %
Nei	25,7 %
Antall	35

Tabell 4: Vet du hvem som er systemkoordinator/-ansvarlig for de systemene du bruker mest?

Ja	68,2 %
Nei	31,8 %
Antall	22

Tabell 5: Har du noen gang lånt ut brukernavn og passord til andre?

	PPT	Skole	Barnevern	Annet	Total
Ja	6,8 %	5,3 %	13,7 %	10,0 %	8,7 %
Ja, men kun til IT-avdeling eller tilsvarende	10,8 %	8,6 %	10,7 %	0,0 %	9,5 %
Nei	81,1 %	84,9 %	74,0 %	80,0 %	80,1 %
Ikke aktuelt	1,4 %	1,3 %	1,5 %	10,0 %	1,6 %
Antall	74	152	131	10	367

Tabell 6: Hvis jeg skriver ut informasjon som innholder personopplysninger…

	PPT	Skole	Barnevern	Annet	Total
Henter jeg alltid utskriften med en gang (evt. bruker sikker utskrift)	94,4 %	86,0 %	87,3 %	100,0 %	88,6 %
Hender det at jeg lar utskriften ligge for å hente den når jeg skal forbi	5,6 %	0,7 %	11,1 %	0 %	5,4 %
Ikke relevant, jeg har egen skriver på mitt kontor	0 %	11,9 %	1,6 %	0 %	5,4 %
Ikke aktuelt	0 %	1,4 %	0 %	0 %	0,6 %
Antall	72	143	126	10	351

Tabell 7: Er det utarbeidet utdypende retningslinjer knyttet til informasjonssikkerhet og/eller personvern i den enheten du er resultatenhetsleder for?

	PPT	Skole	Barnevern	Annet	Total
Ja	83,3 %	8,0 %	75,0 %	100,0 %	30,6 %
Nei	16,7 %	88,0 %	25,0 %	0,0 %	66,7 %
Vet ikke	0,0 %	4,0 %	0,0 %	0,0 %	2,8 %
Antall	6	25	4	1	36

Tabell 8: Har du lest IT-sikkerhetserklæring for Bergen kommune?

	PPT	Skole	Barnevern	Annet	Total
Ja	70,3 %	88,0 %	83,8 %	70,0 %	82,4 %
Nei	10,8 %	8,0 %	4,6 %	10,0 %	7,4 %
Vet ikke	18,9 %	4,0 %	11,5 %	20,0 %	10,2 %
Antall	74	150	130	10	364

Tabell 9: I hvilken grad husker du innholdet i IT-sikkerhetserklæringen?

	PPT	Skole	Barnevern	Annet	Total
I svært stor grad	3,8 %	2,3 %	4,6 %	0,0 %	3,3 %
I stor grad	32,7 %	37,1 %	23,9 %	14,3 %	31,0 %
I noen grad	46,2 %	43,9 %	44,0 %	57,1 %	44,7 %
I liten grad	15,4 %	11,4 %	19,3 %	28,6 %	15,3 %
I svært liten grad	1,9 %	5,3 %	6,4 %	0,0 %	5,0 %
Vet ikke	0,0 %	0,0 %	1,8 %	0,0 %	0,7 %
Antall	52	132	109	7	300

Tabell 10: I hvilken grad er innholdet i IT-sikkerhetserklæringen forståelig for deg?

	PPT	Skole	Barnevern	Annet	Total
I svært stor grad	20,9 %	13,6 %	13,9 %	20,0 %	15,2 %
I stor grad	62,8 %	65,5 %	53,2 %	60,0 %	60,8 %
I noen grad	16,3 %	20,0 %	31,6 %	20,0 %	23,2 %
I liten grad	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %
I svært liten grad	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %
Vet ikke	0,0 %	0,9 %	1,3 %	0,0 %	0,8 %
Antall	43	110	79	5	237

Tabell 11: Har du satt deg inn i dokumentet «Retningslinjer for IT-sikkerhet i Bergen kommune»? Tjenesteområde.

	PPT	Skole	Barnevern	Annet	Total
Ja	37,8 %	38,2 %	31,3 %	10,0 %	34,9 %
Nei	39,2 %	40,8 %	44,3 %	70,0 %	42,5 %
Vet ikke	23,0 %	21,1 %	24,4 %	20,0 %	22,6 %
Antall	74	152	131	10	367

Tabell 12: Har du satt deg inn i dokumentet «Retningslinjer for IT-sikkerhet i Bergen kommune»? Resultatenhetsledere.

	Resultat-enhetsledere	Andre	Total
Ja	69,4 %	31,1 %	34,9 %
Nei	19,4 %	45,0 %	42,5 %
Vet ikke	11,1 %	23,9 %	22,6 %
Antall	36	331	367

Tabell 13: Har du fått tilstrekkelig opplæring i hvordan IT-systemene du benytter skal brukes?

	PPT	Skole	Barnevern	Annet	Total
Ja, opplæringen har vært tilstrekkelig	39,2 %	40,4 %	44,6 %	30,0 %	41,4 %
Ja, men ikke i alle IT-systemene jeg bruker	28,4 %	32,5 %	21,5 %	0,0 %	28,4 %
Nei, opplæringen kunne vært bedre	29,7 %	25,2 %	31,5 %	70,0 %	29,6 %
Ikke aktuelt	2,7 %	2,0 %	2,3 %	0,0 %	2,3 %
Antall	74	151	130	10	365

Tabell 14: I hvilken grad har din nærmeste ledelse fremhevet viktigheten av informasjonssikkerhet?

	PPT	Skole	Barnevern	Annet	Total
I svært stor grad	18,9 %	10,5 %	11,5 %	50,0 %	13,6 %
I stor grad	35,1 %	34,2 %	33,6 %	20,0 %	33,8 %
I noen grad	35,1 %	32,9 %	31,3 %	20,0 %	32,4 %
I liten grad	5,4 %	15,8 %	13,0 %	10,0 %	12,5 %
I svært liten grad	5,4 %	2,6 %	7,6 %	0,0 %	4,9 %
Vet ikke	0,0 %	3,9 %	3,1 %	0,0 %	2,7 %
Antall	74	152	131	10	367

Tabell 15: I hvilken grad har din nærmeste ledelse fremhevet viktigheten av informasjonssikkerhet? Resultatenhetsledere

Navn	Prosent
I svært stor grad	2,8 %
I stor grad	27,8 %
I noen grad	39 %
I liten grad	22,2 %
I svært liten grad	2,8 %
Vet ikke	5,6 %
Antall	36

Vedlegg 2: Høringssvar fra Byrådsavdeling for finans, konkurranse og eierskap

BERGEN KOMMUNE

Byrådsavdeling for finans, konkurranse og eierskap

Intern korrespondanse

Saksnr.: 200819682-18
Saksbehandler: ANDH
Emnekode: SARK-1729

Til: Finans - Stab v/ Rune Haugsdal

Fra: IKT Forretningsutvikling

Dato: 16. oktober 2009

Tilsvar til høringsutkast til revisjonsrapport om "Informasjonssikkerhet og behandling av personopplysninger i Bergen kommune"

INNLEDNING

Utkastet til revisjonsrapport om "Informasjonssikkerhet og behandling av personopplysninger i Bergen kommune" (heretter: rapporten), bekrefter nødvendigheten av den strategiske retningen Seksjon for konkurranse og utvikling (SKU) og IKT-forretningsutvikling (IKT-FU) har foreslått i utkastet til ny IKT-strategi for Bergen kommune i perioden 2010-2013 - eBergen 2013.

Derfor slutter vi oss i all hovedsak til de vurderinger og anbefalinger som fremkommer i rapporten. På samme tid vil vi understreke at dette området, informasjonssikkerhet og personvern, det siste året har fått et vesentlig fokus og er i ferd med å bli et viktig satsingsområde for Bergen kommune.

Dagens utgangspunkt

I 2008 ble stillingen IKT-sikkerhetsansvarlig opprettet da den tidligere IT-sikkerhetskoordinator gikk av med pensjon. Formålet med opprettelsen var å starte arbeidet for økt fokus og mer systematisert arbeid med informasjonssikkerhet og personvern i Bergen kommune.

Ny IKT-sikkerhetsansvarlig ble ansatt i november 2008, og har siden arbeidet målrettet med analyse og klargjøring for innføringen av et styringssystem for informasjonssikkerhet. For øvrig har IKT-sikkerhetsansvarlig også oppfølgingen av og koordinering mellom de ulike IKT-koordinatorene og IKT-prosjektene i kommunen.

IKT-sikkerhetsansvarlig startet tidlig jobben med å systematisere informasjonssikkerhetsarbeidet i kommunen, og jobber mot et styringssystem for informasjonssikkerhet. Allerede første kvartal 2010 starter implementering av styringssystemet for informasjonssikkerhet i Byrådsavdeling for helse og inkludering (BHI). Valget av BHI er gjort både fordi det der er gjort noe arbeid på området knyttet til Helsedirektoratets "Norm for informasjonssikkerhet i helsesektoren" og tilknytningen til Norsk helsenett.

KOMMENTARER TIL "3. DATA"

I kapittel 3 gjør rapporten rede for datagrunnlaget revisjonen er gjennomført på grunnlag av og vil for det meste forbli uten kommentar fra IKT-FU i denne omgang. Det er likevel noen punkter som krever en kommentar, presisering eller utdyping.

På side 9 i rapporten står det å lese at "IT-sikkerhetsråd og sikkerhetsforum ikke har fungert optimalt", og kilden oppgis til å være et intervju med IKT-sikkerhetsansvarlig. Selv bekrefter IKT-sikkerhetsansvarlig samtalen, men presiserer at fremstillingen gir et forenklet bilde basert på faktum som at IKT-sikkerhetsansvarlig i slutten av januar 2008 kalte inn til ett møte i IT-sikkerhetsforum. Resultatet var at kun to av medlemmene møtte hvorav den ene kun for å be om å bli fritatt. På grunnlag av dette og gjennom samtaler med blant andre avdelingssjef IKT-FU, trakk IKT-sikkerhetsansvarlig den slutningen at arbeidet med systematisering av sikkerhetsarbeidet også måtte omfatte en reorganisering, eller i det minste en formalisering av det eventuelle ansvaret som ad-hoc anses å påligge den enkelte leder i organisasjonen. Det vil være avgjørende i det videre arbeidet med systematisering av informasjonssikkerhet og personvern, at IKT-FU og IKT-sikkerhetsansvarlig får en formalisert sikkerhetsorganisasjon å forholde seg til. En sikkerhetsorganisasjon som naturlig involverer både IKT-koordinatorer og systemeierne på et overordnet nivå, og systemkoordinatorene på et mer operasjonelt nivå.

Videre anser også IKT-sikkerhetsansvarlig det som nødvendig å presisere et utsagn på side 10, hvor det hevdes at "Systemet skal etter planen godkjennes på politisk nivå før utgangen av 2009". IKT-sikkerhetsansvarlig bekrefter samtalen, men vil påpeke en misforståelse. IKT-sikkerhetsansvarlig har fortalt om IKT-strategien - eBergen 2013 -, og dermed strategien som går ut på å etablere et styringssystem basert på ISO 27001, og at denne skal opp til politisk behandling. Det er altså ikke styringssystemet i seg selv, men strategien som legger til rette for å implementere et slikt system som skal opp til politisk behandling.

Utkastet til ny strategi Bergen kommune på IKT-området, eBergen 2013, innehar en beskrivelse av en strategisk retning for sikkerhetsarbeidet frem mot 2013. I tillegg beskrives det mål og tiltaksområder som gir et overordnet bilde av hvordan dette skal oppnås i og med strategiens satsingsområde "Systematisering og effektivisering av sikkerhetsområdet". Det er ikke et styringssystem som skal opp til politisk behandling og godkjenning, men godkjenningen av en strategi som legger til rette for arbeidet mot et styringssystem basert på ISO27001.

KOMMENTARER TIL VURDERING, ANBEFALINGER OG FORESLÅTTE TILTAK

I rapporten vises det ofte til den ROS-analysen som ble gjennomført medio 2008 hvor det ble levert en rapport. Denne rapporten kommer med noen forslag til tiltak for å redusere risiko i kommunen.

Foreslåtte tiltak i ROS 2008 og utkastet til revisjonsrapport sammenfaller på en del områder, selv om ROS-analysen går mer systemspesifikt og detaljert til verks har den også forslag til tiltak på et mer overordnet nivå.

Begge rapportene tar opp tiltak som omhandler bevisstgjøring og/eller kompetanseheving av de ansatte. Dette tiltaket vil bli godt ivaretatt gjennom den langsiktige satsingen på innføringen av styringssystem for informasjonssikkerhet, og som det står i utkastet til ny IKT-strategi så er det et mål at "*arbeidet med informasjonssikkerhet og personvern skal synliggjøres og være forankret organisatorisk både i ledelsen og i resten av organisasjonen som et satsingsområde*".

Revisjonsrapporten påpeker en grunnleggende mangel på rutiner og prosedyrer knyttet til informasjonssikkerhet. ROS-analysen på sin side foreslår eksempelvis nye rutiner for besøkende. Dette er ett av mange av mange rutiner som er vurdert av IKT-FU til å ha en god effekt på sikkerhetskulturen i Bergen kommune, og er en viktig del av "Ansattekort" prosjektet, som allerede har levert en behovsanalyse og starter opp i 2. fase i oktober d.å.. Prosjektet har analysert og vurdert innføring av et flerbrukskort for alle ansatte og andre som opererer på vegne av Bergen kommune, både for å kunne etablere strengere "rutiner for besøkende" og krav om legitimering i utvalgte miljøer.

Et styringssystem for informasjonssikkerhet vil også naturlig utbedre problemet med manglende rutiner ved at det fører til et mer gjennomført og helhetlig sikkerhetsarbeid, hvor for eksempel jevnlig revidering av sikkerhetspolicy, kontinuerlige risikovurderinger og fortløpende sikkerhetsrevisjoner ute i organisasjonen vil være naturlige deler av systemet. Arbeidet med systematisering vil føre til revidering av både retningslinjer for informasjonssikkerhet, IT-sikkerhetserklæringen og "Overordnet retningslinje for informasjonssikkerhet", bare for å nevne noen.

Det er planlagt et møte mellom kommuneadvokaten, HR-avdelingen og IKT-FU i nær fremtid.

Noen rutiner er også allerede foreslått slik som "Forslag til e-postinstruks" og "Forslag til vedtak om innsyn i e-post". Disse er utarbeidet i tett dialog med Datatilsynet i forbindelse med "Forskrift om endring i forskrift om behandling av personopplysninger" som trådte i kraft 1. mars inneværende år. Disse benyttes på ad-hoc basis, men vil naturlig gå inn som en del av revidert policy og vil bli å finne i planlagt prosedyrehåndbok på intranettet når det prosjektet blir en realitet.

Et konkret forslag som kun er nevnt i ROS-analysen er "Follow me print", og også på dette området er IKT-FU godt i gang med forberedelsene til å gjennomføre dette tiltaket i praksis. Av andre konkrete forslag ROS-analysen tar opp som "clean desk", "formalisering av systemforvaltningen" og "dokumentasjon av rutiner" er tatt hånd om i ulike prosjekter. "Clean desk" inngår som et av sikkerhetselementene i prosjektet "Papirløs forvaltning". "Dokumentasjon av rutiner" og "rutiner for deaktivering av brukere" blir tatt hånd om i og med etablering av et ISO 27001-basert styringssystem.

Revisjonsrapporten tar opp risikovurderinger og legger vekt på at Bergen kommune heller ikke har "...et tilfredsstillende system for gjennomføring av risikovurderinger..." Dette er et vesentlig poeng både med hensyn til nevnte krav i personopplysningsforskriften, men også for å kunne gjennomføre et systematisk, repeterbart og rapporterbart arbeid med informasjonssikkerhet. Derfor har IKT-FU utarbeidet et rammeverk for risikovurderinger for Bergen kommune. Det er planlagt å integrere dette med Avdeling for prosjekt og rådgivning sin "Prosjekthåndbok".

Enda et element både revisjonsrapporten og ROS-analysen påpeker, og som anses for et grunnleggende element ved et ISO 27001-basert styringssystem, er behovet for en tydelig og forankret sikkerhetsorganisasjon. Per i dag er det dokumentert et ansvar fra Byrådet som behandlingsansvarlig og ned til IT-sikkerhetsforum, via IT-sikkerhetsrådet og IT-sikkerhetskoordinator i mellom[1]. IKT-FU foreslår følgende:

Dagens sikkerhetsorganisasjon:	Foreslått utvidelse av sikkerhetsorganisasjonen:
1. Behandlingsansvarlig	
2. IKT-sikkerhetsrådet	
3. IKT-sikkerhetsansvarlig	
4. IKT-sikkerhetsforum	
	5. IKT-koordinator
	6. Systemansvarlig
	7. Systemkoordinator
	8. Daglig databehandler

Videre mener IKT-FU at hver rolle bør få en beskrivelse i den planlagte sikkerhetshåndboken, at rollene bør få beskrevet konkrete aksjonspunkter knyttet til styringssystemet, og at noen roller også bør være en obligatorisk del av planarbeidet knyttet til jevnlig oppfølging av systemet. Han påpeker også at et alternativ kan være at Bergen kommune utvider antallet ansatte som arbeider med informasjonssikkerhet og personvern, eksempelvis ved å ansatte et personverneombud. Et personverneombud kan blant annet være med på å "styrke dialogen" både med Datatilsynet og kommunens innbyggere, slik det står i den foreslåtte IKT-strategien, eBergen 2013.

KONKLUSJON

Revisjonen bekrefter langt på vei at det arbeidet som er påbegynt i og med utkastet til ny IKT-strategi for Bergen kommune - eBergen 2013 -, og pågår gjennom IKT-Forretningsutvikling sitt arbeid med etablering av et ISO27001-basert styringssystem for informasjonssikkerhet, er både nødvendige og riktige for Bergen kommune.

For at det planlagte arbeidet foreslått forankret i eBergen 2013, "systematisering og effektivisering av sikkerhetsområdet", skal gjennomføres på en god og effektiv måte er det viktig at Bergen kommune setter av tilstrekkelig med ressurser og tar dagens bemanningssituasjon med i betraktning.

Andreas Høistad

[1] "Overordnet retningslinje for behandling av personopplysninger i Bergen kommune" (BKDOK-2004-00655.06)

Vedlegg 3: Høringssvar fra Seksjon skole

Fra: Instebø Brita
Sendt: 12. oktober 2009 15:33
Til: Mydland, Rune; Alme, Aud Merethe
Emne: VS: Høringsbrev

Fra Seksjon skole er vårt innspill/kommentar fra vår IKT-koordinator Jarle Kandal som følger:

Kommentarer til høringsbrev av 24. sept 2009 vedrørende
Informasjonssikkerhet og behandling av personopplysninger i Bergen kommune.

1. Generelt
Brevet er generelt sett dekkende for den faktiske situasjonen i forhold til informasjonssikkerhet i BK, herunder BBS. Så jeg har derfor kun noen få kommentarer.

2. Spesielt

vedr 3.4.1 Rolle- og ansvarsfordeling
Sikkerhet og personvern er et særlig ansvar for systemeiere. Dette ivaretas aktivt av det personellet som forvalter systemeierskapet i BBS. Derfor henvender brukerne seg også dit vedrørende problemstillinger og utfordringer inne personvern og sikkerhet. Så at rapporten påstår at 67% ikke vet hvor de skal henvende seg blir merkelig, da de erfaringsmessig henvender seg til systemkoordinatorene som forvalter systemeierskapet.

vedr 3.8. Bruk av fødselsnummer som identifikasjonsmiddel
BBS vil ikke gå bort fra bruk av fødselsnummer i sitt fagsystem Extens, men må i stedet ha kontroll på at ikke fødselsnumre distribueres eller havner på avveie. Fødselsnummer er eneste entydige identifikator og må brukes i vårt fagsystem Extens for å sikre at opplysninger er knyttet til riktig person. Leverandør IST vil heller ikke foreta endringer i sitt system i forhold til dette. For øvrig vil BBS de nærmeste årene tilby sikker innlogging via Portalen som gir foresatte direkte innsyn i opplysninger lagret om dem og deres barn.

mvh

Brita R. Instebø

Fagavdeling barnehage og skole
seksjonsleder skole
mailto:brita.instebo@bergen.kommune.no
tlf 55 56 23 48

BERGEN KOMMUNE

GRAFISK SENTER
BERGEN KOMMUNE