Hofors kommun

Informationssäkerhet
Revisionsrapport

KPMG AB
19 mars 2014
Antal sidor: 11
Bilagor: 3

Innehåll

1. Sammanfattning

KPMG har av Hofors kommuns revisorer haft i uppdrag att granska kommunens rutiner för hur den styr, utreder, inför, upprätthåller och kontrollerar informationssäkerheten i sin verksamhet.

Revisionen utesluter inte att det finns risk för att det finns brister i de rutiner som skall säkerställa en god informationssäkerhet, och bedömer därför att det är väsentligt att klarlägga på vilket sätt och i vilken form kommunstyrelse och -ledning samt operativt ansvariga styr informationssäkerhetsarbetet. Det är även väsentligt att veta vilka riskbedömningar säkerhetsarbetet vilar på, hur regler, anvisningar etc. rörande säkerhetsarbetet kommuniceras, införs, underhålls samt hur efterlevnaden av beslutad informationssäkerhet kontrolleras.

Syftet med granskningen har varit att med underlag av Myndigheten för samhällsskydd och beredskaps (MSB) skrift, ”Kommunens informationssäkerhet – en vägledning” (Bilaga 1), innehåll och struktur säkerställa att kommunen har infört och lever efter de externa och interna regler som styr ett modernt och uppdaterat informationssäkerhetsarbete. MSB: s vägledning är en tillgänglig och initierad sammanfattning av informationssäkerhetsarbetet i en kommun. MSB utlovar en kontinuerlig uppdatering av vägledningen och redovisar på www.informationssakerhet.se även en stor mängd praktiska råd.

Från granskningen vill vi särskilt framhålla följande:

Generellt sett finns det en medvetenhet i kommunen om vad informationssäkerhet är. Insikt finns att det är väsentligt att säkerställa ändamålsenlig informationssäkerhet i kommunen. Historiskt sett har i princip *inget* formellt beslutat informationssäkerhetsarbete bedrivits. De äldre inte formellt beslutade styrdokumenten som inte är vare sig kända eller efterlevda i nämnvärd grad bör inte användas om de inte genomgår en omfattande revidering och komplettering.

Det pågår ett ännu inte planlagt, kommunicerat och väl dokumenterat arbete för att åtgärda informationssäkerhetsbristerna. Man engagerar sig och tar del av det arbete som bedrivs på länsnivån. Formalisera snarast arbetet och berätta för kommunens medarbetare vad som är på gång och varför. Operativt ansvariga anser vi skall arbeta väl planlagt och det som görs bör rapporteras till och stämmas av med en styrgrupp. Svaren på våra allmänna frågor om informationssäkerhet vid gruppintervjun redovisade i avsnitt 9 nedan indikerar ett behov av stöd redan idag. Bortsett från det framåtriktade arbetet bör gruppen därför även få ett övergripande ansvar för att det dagliga informationssäkerhetsarbetet bedrivs under former som innebär att risker är analyserade och relevanta åtgärder är vidtagna.

Aktivera de anställda med de kurser via webben som MSB tillhandahåller. De är en bra grund för medarbetaren att stå på när policyn är beslutad samt kommunicerad och tillämpningsföreskrifterna successivt framställs och introduceras.

Vi rekommenderar informationssäkerhetsansvariga (ytterst kommunstyrelsen) att snarast säkerställa att kommunen inte hanterar personinformation på ett lagstridigt sätt oavsett var drift av system sker och data lagras. Mest aktuellt för detta är system vars data hanteras i moln utanför kommuns driftansvar.

Informationssäkerhetsmål har en given plats i internkontrollplanen. Kontrollmål och -åtgärder förutsätter vi finns dokumenterade redan i planen för 2014. Ett lämpligt mål torde vara att kontrollera att det finns kunskap bland kommunens medarbetare att det pågår ett arbete med att införa informationssäkerhet i kommunen och vad målsättningen är med detta arbete.

2. Bakgrund

2.1 Allmänt

KPMG har av Hofors kommuns revisorer haft i uppdrag att granska kommunens rutiner för hur den styr, utreder, inför, upprätthåller och kontrollerar informationssäkerheten i sin verksamhet.

2.2 Risk och väsentlighet

Revisionen utesluter inte att det finns risk för att det finns brister i de rutiner som skall säkerställa en god informationssäkerhet, och bedömer därför att det är väsentligt att klarlägga på vilket sätt och i vilken form kommunstyrelse och -ledning samt operativt ansvariga styr informationssäkerhetsarbetet. Det är även väsentligt att veta vilka riskbedömningar säkerhetsarbetet vilar på, hur regler, anvisningar etc. rörande säkerhetsarbetet kommuniceras, införs, underhålls samt hur efterlevnaden av beslutad informationssäkerhet kontrolleras.

2.3 Informationssäkerhet

Myndigheten för samhällsskydd och beredskap (MSB) har ***inte*** någon föreskriftsrätt mot kommuner, men driver ett kraftfullt program för ökad informationssäkerhet mot verksamheter där även kommuner ingår. De publicerade i december 2012 på sina internetsidor dokumentet ”Kommunens informationssäkerhet – en vägledning” (Bilaga 1). Av förordet framgår: *”Sveriges kommuner hanterar en betydande del av samhällets tjänster och kommunernas informationsförsörjning är därför en kritisk del i samhällets informationssäkerhet. För att kunna säkerställa en tillräcklig nivå av informationssäkerhet i en kommuns olika förvaltningar och bolag är det av stor betydelse att informationssäkerhetsarbetet bedrivs metodiskt och långsiktigt.”*

Tidigt i vägledningen påminns vi om att: *”Informationssäkerhet handlar om att ge kommunens information rätt skydd och omfattar:*

- *Tillgänglighet: Att information är tillgänglig i förväntad utsträckning och inom önskad tid*
- *Riktighet: Att den skyddas mot oönskad och obehörig förändring eller förstörelse*
- *Konfidentialitet: Att den inte i strid med lagkrav eller lokala överenskommelser/riktlinjer tillgängliggörs eller delges obehörig*
- *Spårbarhet: Att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare (vem, vad, när)*

Informationssäkerhet omfattar hela kommunens verksamhet och all information oavsett om den finns i datorer, i ett telefonsamtal eller på ett papper. Då stora delar av informationen hanteras med hjälp av IT-system så handlar informationssäkerhet även om teknik.”

3. Syfte och avgränsning

3.1 Syfte

MSB: s vägledning är en modern och initierad sammanfattning av informationssäkerhetsarbetet i en kommun. MSB utlovar en kontinuerlig uppdatering av vägledningen och redovisar på www.informationssakerhet.se även en stor mängd praktiska råd. Syftet med granskningen har varit, med underlag av vägleddnings innehåll och struktur, att säkerställa att kommunen har infört och lever efter de externa och interna regler som styr ett modernt och uppdaterat informations-säkerhetsarbete.

3.2 Avgränsning

Granskningen har omfattat kommunen exklusive bolag i kommunkoncernen.

4. Revisionskriterier

De kriterier som legat till grund för analys, bedömning och rekommendationer är hämtade från kommunallagens 6 kapitel samt reglemente för intern kontroll och tillämpningsanvisningar.

Den interna kontrollen är viktig att utgå från då den är ett medel för ledningens kontroll av att verksamheten efterlever lagar, förordningar och riktlinjer. Intern kontroll är en process vilken styrelsen, ledningen och annan personal skaffar sig rimlig säkerhet för att målen uppnås och som påverkas av hur man agerar i vad man säger och utför.

5. Ansvarig styrelse

Granskningen avser kommunstyrelsen och nämnder.

6. Metod och genomförande

Som metod har intervjuer och dokumentstudier (de dokument som finns redovisas alla i avsnittet 8.1 nedan) använts. En gruppintervju genomfördes 2014-03-03 och där deltog:

- Kommunens fem förtroendevalda revisorer och heltidsarvoderat kommunalråd.
- IT-chef tillika IT-samordnare på socialförvaltningen samt kommunens IT-strateg.
- Kommunchef och förvaltningschefer
- Verksamhetsutvecklare för skolan
- Skolans IT-samordnare och tillika skolhälsoansvarig
- Kommunchef och förvaltningschefer

Följande dokument hade gjorts tillgängliga för deltagarna innan gruppintervjun:

- Granskningens projektplan.
- MSB: s dokument ”Kommunens informationssäkerhet – en vägledning” (Bilaga 1).
- Frågekomplex att besvara (Bilaga 2).

Rapporten är saklighetsgranskad av IT-chef tillika IT-samordnare på socialförvaltningen samt IT-starteg och kommunchef.

7. Projektorganisation

Granskningen har genomförts av Lars Anteskog. Camilla Karlsson har deltagit i granskningen genom sin roll som kundansvarig.

8. Granskningsnoteringar

Gransknoteringarna följer samma upplägg som redovisades i det frågekomplex som besvarats. Rapporten är kompletterad med avsnitt som redovisar:

- Sammanfattning av svar på konkreta frågor om informationssäkerhetsåtgärder i kommunen. Frågorna redovisas i bilaga 3.
- Sammanfattning av svar på frågor ställda om det åtgärdsarbete avseende informationssäkerhet som uppges pågå i kommunen.

8.1 Finns det kommungemensamma styrdokument?

Följande dokument har identifierats av kommunens IT-strateg. De återfinns enligt uppgift på kommunens intranät och bedöms av deltagarna vid gruppintervjun som inte kända:

- **IT-strategi**. Daterat 2003-03-24 med uppgift som kan tyda på en revidering i januari 2009. Det framgår inte vem som vare sig upprättat eller reviderat dokumentet. Inte heller vad som reviderats framgår. Av dokumentet framgår att ”Kommunfullmäktige fastställer och ansvarar för kommunens IT-strategi”. Av dokumentet framgår det *inte* att det är antaget av KF eller någon annan beslutande instans. Dokumentet innehåller inget som modernt och fullständigt styr eller informerar om informationssäkerhet i kommunen. Däremot står det bland annat att läsa att systemförvaltaren har arbetsuppgiften att ”hantera eventuella behörigheter” till systemen. Dokumentet redovisar krav på tillgänglighet till IT-resurser och system som inte motsvarar den utrustning som används 2014. Kommunstyrelse uppges ansvara för IT-säkerheten. Sekretess nämns och vikten av att följa gällande lagar nämns. Kortfattat sägs under den rubriken att ”alla allmänna handlingar, även elektroniskt lagrade, ska vara tillgängliga för allmänheten”. Dokumentets sista mening lyder: ”För att garantera den dagliga driften av systemen och hanteringen av säkerhetsfrågor skall tillräcklig kompetens finnas inom kommunkoncernen.”

- **IT-säkerhetshandledning**. Dokumentet förefaller vara upprättat av före detta ekonomichefen 2009-06-18. Vilken beslutande instans som antagit dokumentet framgår inte. Dokumentet innehåller inget som styr eller informerar om informationssäkerhet i kommunen. Däremot innehåller dokumentet en målformulering som lyder: ”Målet med instruktionen är ge alla medarbetare kunskap och kännedom om hur kommunikationsnät, datasystem och arbetsplatser skall hanteras för att felaktigheter och störningar skall undvikas.” Dokumentet innehåller en hel del goda råd men här finns också uppmaningar och påståenden som kan ifrågasättas vara riktiga och/eller inte har bäring på den IT-miljö som idag finns i kommunen.

- **IT-standard**. Förfaller vara en del av ett strategidokument från 2006. Vi uppfattar att det reviderats 2009-03-09 av kommunens före detta ekonomichef. Vad som reviderats framgår inte. Enligt dokumentets första punkt sägs det vara en policy. Av dokumentet framgår det *inte* att det är antaget av KF eller någon annan beslutande instans. Dokumentet innehåller inget som styr eller informerar om informationssäkerhet i kommunen.

- **Koncernövergripande IT-plan för 2010 samt perioden 2011-2012**. Dokumentet är odaterat och det framgår inte vem som upprättat det. Vilken beslutande instans som antagit dokumentet framgår inte. Dokumentet innehåller inget som styr eller informerar om informationssäkerhet i kommunen.

Kommentarer

De dokument som idag finns och redovisas ovan kan inte anses vara så fullständiga och riktiga att de bidrar till att styra, upplysa och upprätthålla en adekvat informationssäkerhet i kommunen. Enlig uppgift har det startats ett arbete för att ändra på den situationen. Målsättning som vi förstår den är att det skall finnas en informationssäkerhetspolicy för kommunen antagen av kommunfullmäktige innan 2014 års slut. Det fortlöpande arbetet skall även resultera i att nya tillämpningsföreskrifter skall komplettera denna policy.

Vi noterar därmed att det finns förståelse och engagemang för informationssäkerhet hos de personer som har ett övergripande ansvar. Det redogörs för planer hur fortsatt arbete skall bedrivas. Vi saknar dock dokumentation om vad som skall ske när och vilka mål som skall nås på kort och lång sikt. Vilka ytterligare skall mer konkret involveras och hur skall ansvar och arbete fördelas? Vem skall styra och följa upp att målen nås så att kommun får optimal nytta av ansträngningen. Det är positivt att få höra att man engagerar sig på länsnivån för att tillsammans med ansvariga i andra kommuner inhämta kunskap och inspiration. Notera dock att det är det konkreta dokumenterade och kommunicerade arbetet i den egna kommunen som säkerställer att beslutad informationssäkerhet förstås och efterlevs. När nu ett högst nödvändigt arbete efter en väl känd, prioriterad och finansierad plan startas (för att i princip aldrig avslutas). Se vidare våra rekommendationer om planer under avsnittet 10 nedan.

8.2 Anses de kommungemensamma styrdokument väl kända?

Nej. När vi väger samman erhållna svar gör vi bedömningen att alla som omfattas av styrdokumenten redovisade ovan inte känner till dess existens samt syfte och hur de skall användas.

Kommentarer

Vi bedömer att man historiskt inte lyckats med att göra styrdokumenten kända hos alla som berörs. När nya dokument finns på plats överväg då att tillämpa en metod som dokumenterar att medarbetaren mottagit, förstått samt intygar att man kommer att efterleva innebörden av dem. Vi rekommenderar att ett e-postformulär skapas och används för att få en effektiv hantering av det momentet. Hanteringen blir för de allra flesta snabbare än med en pappersburen metod och möjlighet till uppföljning och kontroll förbättras avsevärt.

8.3 Är det kommungemensamma kompletterat med förvaltningsspecifika styrdokument?

Nej. vi kan inte identifiera att några sådana finns i någon förvaltning. Det övervägande motivet till detta uppfattas vara att ett vare sig kunskap om nyttan, krav eller behov funnits för detta.

Kommentarer

Vi bedömer att anledningen kan vara att informationssäkerhetsarbetet kommunen och den allmänna kunskapen om informationssäkerhet inte avancerat så långt att analyser identifierat nytta och behov av förvaltningsspecifika styrdokument.

8.4 Är styrdokumenten konkretiserade i systemsäkerhetsplaner/-analyser eller motsvarande?

Nej. Det finns inga sådana planer och analyser i drift eller under framtagande.

Kommentarer

Det är i konkretiseringarna som det skall framgå hur respektive datoriserat systemstöd skall hanteras utifrån vad policy och vägledningar anger. Här anges i detalj hur systemägaren/-ansvarig och –förvaltare skall förhålla sig så att optimal informationssäkerhet för det specifika systemet uppnås. Det är här som det även skall framgå hur ansvarspersonerna hanterar informationssäkerheten i förhållande till en utkontrakteringspartner. Alla ingångna avtal skall därför rimligen vara avstämda mot rådande policy och vad som framgår av de särskilda förhållanden som framkommer i en systemsäkerhetsanalys.

MSB stöder och utvecklar inte längre det system (BITS) som tidigare använts i kommuner när sådana planer/analyser upprättats och införts. Idag förordar MSB användandet av LIS (Ledningssystem för informationssäkerhet) vilket avhandlas i avsnitt nedan samt beskrivs i bilaga 1.

8.5 Styrs informationssäkerhetsarbetet på något annat sätt än efter gemensamma styrdokument i någon förvaltning?

Svaret vi får när vi ställer frågan är ett tydligt nej.

8.6 Finns eller förbereds införandet av ett LIS i kommunen?

Det som beskrivs som inte fastställda planer för fortsatt informationssäkerhetsarbete i avsnitt ovan kan, vad vi förstår, komma att bedrivas med ett LIS (Ledningssystem för informationssäkerhet) som stöd. Inga formella beslut finns dock om ett införande.

Kommentarer

Vi rekommenderar att kommunen överväger att införa ett LIS med följande motiveringar: Systemet är skalbart och kan därför införas anpassat. Det finns gott om kostnadsfritt stöd att tillgå. Kunskap om ledningssystem som metod finns redan i kommunen i och med att socialtjänsten använder ett sådant i sin verksamhet.

8.7 Ligger förekommande styrdokument till grund för regelbundet återkommande information och utbildning?

Vad vi förstår har det aldrig bedrivits någon regelbundet återkommande informations- och/eller utbildningsverksamhet i och om informationssäkerhet för kommunens anställda.

Kommentarer

För att lyckas med informationssäkerhetsarbetet som en naturlig del av ansvaret i linjen behöver respektive funktion kunskap som korresponderar till ansvaret. Säkerställ i pågående arbete att beslutsfattare, särskilt ansvariga och samordnare över tid har relevant kunskap för sitt uppdrag och inte enbart för sin roll som användare av datoriserade verksamhetsstöd.

Regelbundet återkommande information om hur omtaget med informationssäkerheten fortskrider och hur det arbetet påverkar den enskilde är ett lika enkelt som effektivt sätt att hålla ämnet levande och intressant Överväg att uppmuntra/uppmana kommunmedarbetare att genomgå ”Säkerhetsutbildning IT-test på intranätet (DISA[1]/ISA)”

[1] DISA är MSB:s informationssäkerhetsutbildning för användare och erbjuds alla organisationer kostnadsfritt. Syftet med DISA är att på ett enkelt och kostnadseffektivt sätt höja nivån på informationssäkerheten inom en organisation genom att säkerställa att samtliga medarbetare har förståelse för grunderna med informationssäkerhet. Utbildningen vänder sig till alla på en arbetsplats och kan användas som introduktion för nyanställda, vikarier, konsulter och annan inhyrd personal.

8.8 Kontrolleras det återkommande att de styrande dokumenten eller motsvarande efterlevs?

Inga särskilda kontroller uppges finns införda än mindre utförda. Vad vi förstår så innehåller inte internkontrollplanen för kommunen som helhet för 2014 några kontrollmål och följaktligen inga kontrollåtgärder som omfattar informationssäkerhet.

Kommentarer

Med MSB: s material som stöd och kommunintern kunskap om hur den skall hanteras finns möjlighet att utforma, införa och utföra kontroller för att säkerställa hela kommunens efterlevnad av beslutade styrdokument. Informationssäkerhetsmål har en given plats i internkontrollplanen. Kommunen bör ha ambitionen att få med något eller några kontrollmål och -åtgärder omfattande informationssäkerheten under 2014. Ett lämpligt mål torde vara att kontrollera att det finns kunskap bland kommunens medarbetare att det pågår ett arbete med att införa informationssäkerhet i kommunen och vad målsättningen är med detta arbete.

9. Sammanfattning av svar på konkreta frågor om informationssäkerhetsåtgärder i kommunen.

Syftet med dessa frågor är att, med bakgrund av frånvaron av moderna, fullständiga och helt riktiga styrdokument, bland de ”gruppintervjuade” undersöka status för informationssäkerhetsläget och -kunskapen om detsamma. Frågorna framgår av bilaga 3 och vi gör inte anspråk på att de fullständigt redovisar/berör allt vad som behöver styras inom informationssäkerheten i en kommun. Nedan redovisas en sammanfattning av svar och kommentarer från gruppintervjun.

9.1 Informationsklassificering

Är inte utfört och nämns inte i de äldre styrdokumenten som beskrivs under avsnittet 8.1 ovan. Det borde vara möjligt att utgå från de dokumentationsplaner som utförts på respektive förvaltning när klasser beslutats och klassificering påbörjas. Att ansvaret för att fortlöpande klassa information som skapas ligger på den enskilda användaren var inte väl känt.

9.2 Lagar

Att det finns en stor mängd lagar, särskilt inom det område där socialtjänsten har ansvaret, som påverkar hur informationssäkerheten utformas och styrs var inte obekant för de flesta. Vi uppfattar det som att förteckningen i bilagan kommer till användning i det pågående omtaget vad gäller informationssäkerhet i kommunen.

9.3 Installation/Anslutning

Flera men inte alla frågorna får sitt svar i *IT-säkerhetshandledningen* som avhandlas avsnitt 8.1 ovan. Det är i sammanhanget oklart i vilken omfattning detta dokument har efterlevts. Den del av IT-säkerhetshandledningen som omfattar internet säger inget om hur Facebook, Twitter,

Instagram etc. får och inte får användas. Enligt en inte bekräftad uppgift skall Facebook inte kunna nås av användarna oavsett vilken utrustning (dator, platta, telefon) man har ansluten.

9.4 Drift

Inte alla system testas och får ett formellt godkännande innan det sätts i drift. Det verkar tveksamt om de tester som utförs dokumenteras. Det finns inga regler för hur systemleverantörer och/eller konsulter får tillgång till system. Det vanligaste verkar vara att de släpps in när behov uppstår. Några sekretessavtal med dessa verkar inte vara upprättade. Gjorda anslutningar loggas inte. Det kan inte uteslutas att flera olika konsulter kan komma åt systemet vid varje enskild anslutning.

Kunskapen om säkerhetseffekter och risker med användning molntjänster upplever vi som svag. Inom utbildningsverksamheten uppfattar vi att molntjänster används. Vad vi förstår så finns inte en fullständig kunskap om vad som framgår av Personuppgiftslagen vad gäller hantering och lagring av personinformation när denna driftform används. Det är oklart om förvaltningens/ kommunens personuppgiftsansvarig är informerad och har godkänt avtalad driftlösning. De styrdokument som avhandlas under avsnitt 8.1 ovan hanterar inte denna problematik. Vi uppfattar det som att leverantören av systemet över tid inte kontrolleras leva upp till vad som eventuellt avtalats om nivå och omfattning av informationssäkerheten.

9.5 Behörighet

Flera men inte alla frågorna får sitt svar i *IT-säkerhetshandledningen* som avhandlas avsnitt 8.1. Att en kombination av tilldelade behörigheter för en enskild användare kan innebära informationssäkerhetsbrister är inte allmän kunskap. I närtid har kommunen kontrollerat i vilken omfattning personer som avslutat sin anställning fortfarande kvarstår med behörigheter i en av kommunens katalogtjänster (AD). Kontrollen visade på en mycket stora mängd av personer som fanns kvar i AD. Detta är en tydlig indikation på att det inte funnits/finns regler och rutiner som fungerat vad gäller förändring och avveckling av personer när det gäller behörigheter. Det torde vara högaktuellt att även kontrollera status i verksamhetssystemen.

Det förekommer enligt uppgift s k ”super users” (personer med omfattande administratörsrättigheter) i de flesta av kommunens datoriserade verksamhetsstöd. Hur många de är, var de är verksamma och vilka rättigheter de innehar finns inte centralt förtecknade.

9.6 Säkerhetskopiering

Kommunen har inte dokumenterat kommunens alla system på ett sådant sätt att de viktigaste finns identifierade. Det är i dokumentet *IT-strategi* avhandlat avsnitt 8.1 ovan som det angetts hur lång tid man ska klara sig utan vad man benämner ”övergripande system”. Vi ställer oss frågande till de tider som anges i dokumentet samt förvånas över att man inte nämner de mest väsentliga verksamhetssystemen. Man anser sig inte kunna vara utan ekonomi- och personalsystem längre än två timmar. De system som understödjer socialtjänsten och skolan nämns över huvud taget inte.

Säkerhetskopiering verkar inte vara anpassad efter systemägarnas krav/önskemål. Vi bedömer att det är få utöver teknikerna knutna till IT-funktionen som vet hur säkerhetskopieringen utförs. Än

mindre verkar man känna till eller ha styrt hur säkerhetskopiorna skall förvaras och kontrolleras. Att media för säkerhetskopior inte skall användas efter bäst-före-datum och destrueras under säkra former upplevdes var en nyhet för alla.

9.7 Skalskydd/Fysisk säkerhet

Flera men inte alla frågorna får sitt svar i *IT-säkerhetshandledningen* som avhandlas avsnitt 8.1. Det finns skäl att misstänka att information på utrustning som avvecklas inte hanteras på ett informationssäkert sätt. Hur redundans för kommunikation och elkraft säkerställs är inte allas kunskap, än mindre har man varit med och påverkat. Kontinuitetsplaner verkar saknas helt även för de mest västliga systemen.

9.8 ”Blandade frågor”

Informationssäkerhet rör inte endast den som lagras elektroniskt. Vi noterar att ingen spontant kan svara på vilken information som får distribueras via brev utan att det rekommenderas. Det är ingen som säkert kan säga vad som får kommuniceras via mobiltelefon och under vilka omständigheter det är tillåtet att använda telefax.

Ingen kunde fullständigt berätta vad som gäller för hantering och lagring av ljud, bilder och ritningar. Ingenstans verkar det heller gå att läsa sig till beslutet om hur sekretessbelagd pappersburen information skall förvaras.

9.9 Sammanfattande kommentar till avsnitt 9

Den styrande dokumentation som redovisas under avsnitt 8.1, och som inte många ens visste att den fanns, skall inte användas om den inte först revideras och uppdateras. Detta torde inte vara ett svårt beslut att fatta då dokumentation inte förefaller vara formellt beslutad.

Frågorna och svaren anser vi däremot kan ge ett inte oväsentligt stöd när tillämpningsföreskrifterna till, en vad vi förstår kommande, informationssäkerhetspolicy skall produceras.

10. Informationssäkerhetsarbetet i kommunen 2014

Det framgår av avsnitten ovan att kommunen historiskt sett inte aktivt arbetat med och infört en ändamålsenlig och känd informationssäkerhet för kommunens verksamhet. För att det arbete vi nu förstår ha initierats och till viss del även påbörjats skall bli lyckosamt och generera styrande dokument som förstås och efterlevs behövs en organisation. Förutom att driva arbetet framåt måste organisationen även medverka till att hantera (identifiera och minimera) de risker som föreligger när kommunen nu rimligtvis fått insikt om att styrningen av informationssäkerheten kan vara om inte obefintlig så bristfällig. Vi rekommenderar:

- Besluta och dokumentera en plan för åtgärder på både kort och lång sikt.
- Specificera vilka åtgärder planen omfattar.

- Ange vem som tagit beslut om planen och dess innehåll.
- Ange med vilka motiv åtgärderna i planerna har prioriterats.
- Ange tidsomfattning för åtgärderna i planen besluta om när de skall vara färdigställda, beslutade, kommunicerade och införda (milstolpar).
- Ange och kommunicera vem/vilka som är operativt ansvariga för planernas genomförande.
- Ange och kommunicera vilka som skall delta operativt med de olika delarna i planerna.
- Tillsätt externa resurser om det behövs och kan motiveras.
- Till vilka (styrgrupp) skall operativt ansvarig fortlöpande rapportera till.
- Budgetera arbetet.

KPMG, dag som ovan

Lars Anteskog
Projektansvarig

Camilla Karlsson
Kundansvarig

Frågekomplex vid granskning av informationssäkerhet i Hofors kommun 2014.

Svaren på nedanstående frågor bildar tillsammans med dokumentstudier och intervjuer grund för vår rapport till kommunrevisionen. Urval för intervjuer görs med ledning av de svar vi får. Vi hänvisar nedan till Myndigheten för samhällsskydd och beredskaps (MSB) dokument ”Kommunens informationssäkerhet – en vägledning” (Vägledningen) när vi vill beskriva eller förklara informationssäkerhet. Vi rekommenderar att vägledningen läses en gång innan frågorna börjar besvaras.

Frågorma är löpnumrerade så att svaren kan numreras korresponderande. Vi är tacksamma om svaren kan produceras och överföras elektroniskt.

Vad omfattar kommunens informationssäkerhetsarbete?

Vad omfattar förvaltningens informationssäkerhetsarbete? Se de tre första styckena på sidan 9 i vägledningen.

Vi önskar få en kortare beskrivning av hur de kommungemensamma styrdokumenten (informationssäkerhetspolicy med därtill hörande tillämpningsföreskrifter) används i informationssäkerhetsarbetet. Med används menar vi att de:

1. Finns?

2. Anses vara väl kända?

3. Är kompletterade med förvaltningsspecifika styrdokument?

4. Är konkretiserade i systemsäkerhetsplaner/-analyser eller motsvarande?

5. a) Styrs ***inte*** informationssäkerhetsarbetet i förvaltningen på ett sätt så att fråga 1 till 4 enkelt och kortfatta kan besvaras hur säkerställs då den nytta med informationssäkerhet som beskrivs i vägledningen punkt 1.4 sidan 11? b) Med kortfattad motivering anses det i avsaknad av styrdokument enligt ovan att förvaltningens informationssäkerhetsarbete i någon utsträckning ***ändå*** överensstämmer med vad som framgår av vägledningens avsnitt 2 på sidan 15 till 19?

Finns eller förbereds ett ledningssystem?

Ledningssystem för informationssäkerhet (LIS) beskrivs i vägledningens avsnitt 3 sidan 21 till 24

6. Finns eller förbereds införandet av ett LIS i kommunen? Om ja vänligen bifoga dokument som beskriver detta.

Policys och tillämpningsföreskrifter samt processer och åtgärder

Om styrdokument ***finns*** behöver vi:

7. En förteckning av de styrande dokumenten som ***särskilt*** finns beslutade för förvaltningen. Vänligen ange namnet på dokumentet, vad det innehåller samt var och när det beslutats gälla. Det går även utmärkt översända de styrdokument som är upprättade och används?

Hur införs de styrande dokumenten och hur kontrolleras efterlevnaden?

Oavsett hur förvaltningen organiserar informationssäkerhetsarbetet (med eller utan styrdokument i gängse mening beskrivet ovan) eller tillämpar/inför ett LIS:

8. Vad ligger till grund för regelbundet återkommande information och utbildning om informationssäkerhet?

9. Kontrolleras det återkommande att de styrande dokumenten eller motsvarande efterlevs? Finns kontrollåtgärderna och resultaten av dem dokumenterade? Förekommer informationssäkerhet som ett kontrollmål i internkontrollplanen och vilka kontrollåtgärder skall utföras?

Informationssäkerhetsfrågor.

Informationsklassificering

1. Har kommunen och/eller förvaltningarna en fastställd dokumenthanteringsplan?

2. Framgår informationsklassningen av dessa? Vilken typ av information har kommunen/förvaltningen beslutat vara:

    a. Öppen

    b. Intern

    c. Konfidentiell

    d. Sekretessbelagd

3. Om vi indexerar innehållet i allmänt tillgängliga volymer/mappar på filservrar kommer vi då att finna konfidentiell och/eller sekretessbelagd information i de dokument som sparats/lagrats där?

4. Vem har ansvaret för att besluta om informationsklasser?

5. Vem har ansvaret för att klassa information?

6. Hur skall olika klassad information förvaras? Elektroniskt och pappersburet?

7. Kan felaktig klassning och hantering orsaka kommunen kostnader och/eller dåligt renommé?

Lagar

8. Hur hanterar kommunen lagkraven omgärdande information inom vård och omsorg?

9. 26 lagar/förordningar omgärdande information inom vård och omsorg omfattar sammanlagt över 200 informationskrav!

    a. Arkivlagen (1990:782)

    b. Lagen (2002:297) om biobanker i hälso- och sjukvården m.m.

    c. Hälso- och sjukvårdslagen (1982:763)

    d. Lagen (1990:1404) om kommunernas betalningsansvar för viss hälso- och sjukvård

    e. Lagen (1993:389) om assistansersättning

f. Lagen (2003:460) om etikprövning av forskning som avser människor

g. Lagen (1998:543) om hälsodataregister

h. Lagen (2005:258) om läkemedelsförteckning

i. Lagen (1993:387) om stöd och service till vissa funktionshindrade

j. Lagen (1988:870) om vård av missbrukare i vissa fall

k. Lagen (1990:52) med särskilda bestämmelser om vård av unga

l. Lagen (1998:531) om yrkesverksamhet på hälso- och sjukvårdens område

m. Patientdatalagen (2008:355)

n. Personuppgiftslagen (1998:204)

o. Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) RA-FS 2009:1

p. Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling) (RA-FS 2009:2)

q. Socialtjänstlagen (2001:453)

r. Socialstyrelsens föreskrifter om ansvar för remisser för patienter inom hälso- och sjukvården, tandvården mm (SOSFS 2004:11)

s. Föreskrift om ledningssystem för kvalitet och patientsäkerhet (SOSFS 2005:12)

t. Socialstyrelsens föreskrifter om utfärdande av intyg inom hälso- och sjukvården m m (SOSFS 2005:29)

u. Socialstyrelsens föreskrifter och allmänna råd om dokumentation vid handläggning av ärenden och genomförande av insatser enligt SoL, LVU, LVM och LSS (SOSFS 2006:5)

v. Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för kvalitet i verksamhet enligt SoL, LVU, LVM och LSS (SOSFS 2006:11)

w. Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)

x. Smittskyddslagen (2004:168)

y. Tryckfrihetsförordningen (1949:105)

z. Tandvårdslagen (1985:125)

10. Ytterligare lagar och förordningar ställer direkt eller indirekt krav på informationssäkerheten i kommun. Några exempel:

    a. Offentlighets- och sekretesslagen

    b. Säkerhetsskyddslagen

    c. Förvaltningslagen

    d. Lag om offentlig upphandling

    e. Lag om kommunal redovisning

    f. Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

    g. Kommunallagen

Installation/Anslutning

11. I vilken omfattning har anställda användare möjlighet att installera program/applikationer på den egna datorn?

12. Använder icke anställda (uppdragstagare, arvodister etc.) kommunens datorer utan att efterleva skriftligt överenskomna informationssäkerhetskrav?

13. Får utomstående på något sätt ansluta egen utrustning till kommuns nät utan att efterleva skriftligt överenskomna informationssäkerhetskrav?

14. Har kommunen/förvaltningen sådan kontroll att användarlicenser finns för de program som används/installeras av enskild användare?

15. Har kommunen/förvaltningen sådan kontroll att användarlicenser för kommunövergripande program/applikationer/system inte över- eller felutnyttjats? Är kommunen förberedd på att licensutgivare enligt avtal kan komma att kräva att via tredje part kontrollera efterlevnaden av ingångna licensavtal?

16. Finns det fungerande och kontinuerligt uppdaterad antivirusprogram på kommunens alla enheter som kan och får anslutas till kommunens nät?

17. Är det förenat med några restriktioner hur kommunanställda kommunicerar via e-post, chatt och sociala medier (Facebook, Twitter, Instagram etc.)?

Drift

18. Testas system i särskild testmiljö innan de driftsätts?

19. Dokumenteras tester?

20. Bildar dokumenterade testresultat underlag till skriftliga driftgodkännanden?

21. Används även driftgodkännanden vid ändringar, felrättningar, uppdateringar, versionsbyten etc?

22. Hur säkerställer kommun över tid kapacitet för att systemen kan användas effektivt? Med andra ord är systemen ur ett prestandatekniskt perspektiv tillgängliga i ändamålsenlig omfattning?

23. Kommer systemleverantörer och/eller konsulter åt system utan att särskilt, dokumenterat och tidsbegränsat getts tillträde?

24. Upprättar kommunen sekretessavtal eller motsvarande med systemleverantörer och konsulter?

25. Hur säkerställs informationssäkerheten när drift och/eller data utkontrakteras och/eller köps som ”molntjänst” i någon omfattning och form?

Behörighet

26. Vem och under vilka former tilldelas en medarbetare i kommunen behörighet till de datoriserade verksamhetsstöd som behövs för hens arbetsuppgifter och ansvar?

27. Vem ansvarar för att behörighetens omfattning motsvarar hens arbetsuppgifter och ansvar?

28. Om fler än en person är ansvarig för enskilds behörighet vem ser då till att kombinationen av behörigheter systemen sammantaget inte innebär att informa- tionssäkerhetsrisker i ett eller flera system?

29. Vem har ansvar för att behörigheter som ändras dokumenteras och kontrolleras inte att informationssäkerhetsrisker uppstår?

30. Vem ansvarar för att behörigheter avvecklas på ett informationssäkert sätt? När kontrollerades innehållet i AD mot anställningsregistret?

31. Vem ansvarar för att antalet ”super users”(personer med omfattande administratörsrättigheter) hålls på en effektiv och säker nivå? Hur många finns och vilka är de per system?

32. I vilken omfattning och under vems ansvar används s k funktionsbehörigheter?

33. Vad får det kosta kommunen i pengar och/eller renommé om personer haft tillgång till information de inte är behöriga att ta del av?

Säkerhetskopiering

34. Vilka är kommunens fem (5) viktigaste datoriserade verksamhetsstöd?

35. Kan man starta alla kommunens viktiga (får inte vara otillgängliga längre än två arbetsdagar) från de säkerhetskopior som tas?

36. När kontrollerades det senast, av någon utanför IT-avdelningen/-funktionen, att tagna säkerhetskopior går att återläsa till full funktion för berörda system?

37. Vem har beslutat att säkerhetskopior skall tas och kontrolleras på det sätt som görs idag?

38. Känner systemägaren, -ansvarig och –förvaltaren samt informationsägaren till hur säkerhetskopior:

    a. Förvaras?

    b. Kontrolleras?

    c. Medier inte har passerat sitt bäst-före-datum?

    d. Destrueras?

39. Vad får det kosta och hur lång tid får det ta att återställa ett datoriserat verksamhetsstöd vars säkerhetskopieringshantering inte fungerat? Budgeteras det för denna typ av kostnader?

40. Vem har ansvaret för att en förvaltnings datoriserade verksamhet fungerar ändamålsenligt och informationssäkert?

Skalskydd/Fysisk säkerhet

41. På vilket sätt skyddas/hanteras informationsbärande utrustning när:

    a. Den placeras?

    b. Den lämnas obevakad?

    c. När personal slutar?

    d. När utrustning avvecklas?

42. Hur säkerställs att inte obehöriga får tillgång till utrustning/lokaler där särskilt klassad information hanteras/förvaras?

43. Hur säkerställs skydd mot eld, rök och vatten?

44. Hur säkerställs skydd av kommunikationsutrustning inklusive kablar och kopplingspunkter samt möjlighet till redundanta kommunikationsvägar? Omfattar skyddet både avlyssning och åverkan?

45. Hur säkerställs ordinarie elkraft inklusive redundans och reservkraft?

46. Vad kostar det kommunen om ett system inte är tillgängligt i ett dygn? Två i två dygn o s v?

47. Finns det kontinuitetsplaner och är de testade och övade?

”Blandade frågor”

48. Finns det dokumenterade regler/anvisningar om vilken information som får kommuniceras hur?

    a. Vad måste skickas med brev rekommenderat eller inte?

    b. Vad får inte avhandlas via mobiltelefon?

    c. När, hur och under vilka omständigheter får fax användas eller inte?

49. Vilka dokumenterade regler/anvisningar finns för hantering och förvaring av:

    a. Ljud

    b. Bild

    c. Ritningar

    d. Sekretessbelagd pappersburen dokumentation