Åmåls kommun **2018-11-20**

Revisorerna

Till: Kommunstyrelsen

För kännedom: Kommunfullmäktige

Revisionsrapport

Vi har granska hur kommunen arbetar med informations- och IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2018. Vid granskningen har vi biträtts av KPMG.

Det övergripande syftet med granskningen är att fastställa om styrning finns av informationssäkerheten.

Sammanfattningsvis konstateras i rapporten att kommunen vid granskningstillfället i allt väsentligt saknar styrande och stödjande dokument för hur informationssäkerheten ska hanteras.
Mot bakgrund av vår granskning rekommenderar vi kommunen att inte underprioritera arbetet med att upprätta styrning och stöd för en ändamålsenlig informationssäkerhet. Enskilda specialister kommer inte att utan stöd och aktiv medverkan från ansvariga nå nödvändig verkanshöjd i ett arbete som behöver startas omgående.

I övrigt hänvisar vi till rapporten i sin helhet. Vi önskar att kommunstyrelsen senast den 15 februari 2019 inkommer med kommenterar till ovanstående iakttagelser och rekommendationer.

För kommunrevisionen

Lennart Hansson
Ordförande/ revisor

Informations- och IT-säkerhet

Rapport

Åmåls kommun

KPMG AB

2018-12-04

Antal sidor 10

Åmåls kommun
Informations- och IT-säkerhet

2018-12-04

Innehållsförteckning

1 Sammanfattning

Vi har av Åmåls kommuns revisorer fått i uppdrag att granska hur kommunen arbetar med informations- och IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2018.

Samtlig IT-verksamhet behöver utföras på ett säkert sätt där informationen som bearbetas skyddas mot extern och intern missanvändning. En stor mängd viktig information, varav en del är sekretessbelagd, hanteras i IT-systemen. Utvecklingen går mot att än mer information hanteras elektroniskt och därmed minskar den fysiska kontrollen på informationen. Det övergripande syftet med granskningen är att fastställa om styrning finns av informationssäkerheten.

Sammanfattningsvis kan vi konstatera att kommunen vid granskningstillfället i allt väsentligt saknar styrande och stödjande dokument för hur informationssäkerheten ska hanteras.

Mot bakgrund av vår granskning rekommenderar vi kommunen att inte underprioritera arbetet med att upprätta styrning och stöd för en ändamålsenlig informationssäkerhet. Enskilda specialister kommer inte att utan stöd och aktiv medverkan från ansvariga nå nödvändig verkanshöjd i ett arbete som behöver startas omgående.

2 Bakgrund

Vi har av Åmåls kommuns revisorer fått i uppdrag att granska hur kommunen arbetar med informations- och IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2018.

All verksamhet är i dagsläget beroende av IT och det IT-stöd som används. IT-verksamheten måste fungera för att kommunen ska kunna utföra den samhällsviktiga funktionen. IT-verksamheten behöver utföras på ett effektivt sätt där nyttan med IT-relaterade beslut alltid finns i åtanke.

Molntjänster för bl.a. applikationer och lagring av data blir allt mer vanligt förekommande i både privata och offentliga organisationer. En molntjänst kan utformas på ett antal olika sätt men kortfattat så är en molnlösning en färdigpaketerad tjänst där lagring, datorkapacitet, programvara eller liknande levereras över Internet (beskrivning från Sveriges Kommuner och Landsting, SKL). Molntjänster innebär därmed att applikationer och underliggande data inte längre hanteras inom den egna organisationen.

Samtlig IT-verksamhet behöver utföras på ett säkert sätt där informationen som bearbetas skyddas mot extern och intern missanvändning. En stor mängd viktig information, varav en del är sekretessbelagd, hanteras i IT-systemen. Utvecklingen går mot att än mer information hanteras elektroniskt och därmed minskar den fysiska kontrollen på informationen. IT-säkerhet är därmed ett väsentligt område och det krävs en tydlig hantering för att säkerställa skyddet kring viktig information. Säkerhetsaspekter som bör existera inkluderar bland annat åtkomsthantering och drifthantering. Kommunens arbete med behörigheter och lösenord utgör en väsentlig vikt i säkerhetsarbetet då bristande rutiner och riktlinjer kan leda till att obehöriga personer får tillgång till känslig information. Driftssäkerheten är ytterligare ett område som är av vikt att säkerställa för att tillse att viktiga samhällsfunktioner inte äventyras.

Åmåls kommuns revisorer drar i sin riskanalys slutsatsen att området för informations- och IT-säkerhet behöver granskas.

3 Syfte, revisionsfråga och avgränsning

3.1 Syfte och revisionsfråga

Det övergripande syftet med granskningen är att fastställa om riktlinjer finns kring informationssäkerhet samt IT-säkerhet med bäring på ny teknisk utveckling och driftsäkerhet är ändamålsenlig.

Vi kommer därmed belysa följande revisionsfrågor:

- Finns en informationssäkerhetspolicy med tillhörande informationssäkerhetsrutiner och regelverk som tar i beaktande säkerhetsfrågor med avseende på ny IT-teknisk utveckling såsom molntjänster, mobila enheter och hantering av sociala medier?

- Hur säkerställs informationssäkerheten vid användandet av mobila enheter såsom läsplattor, datorer och mobiltelefoner? Vad gäller avseende IT-utrustning vid avslut av behörigheter och anställningar?

- Finns riktlinjer för åtkomsthantering för väsentliga IT-system inklusive riktlinjer för beställning av behörighetsförändringar, lösenordshantering, begränsning kring höga behörigheter och säkerhet relaterad till att endast behöriga personer har åtkomst till relevanta IT-system?

- Beaktas informationssäkerhetskrav vid upphandling av nya IT-tjänster så som exempelvis molntjänster?

- Finns kontroller, kontrollmoment och definierade uppföljningsprocesser för uppföljning av aktivitet i IT-systemen? Exempelvis regelbundna logguttag och analys av genomförda aktiviteter.

- Finns riktlinjer och rutiner för katastrof- och incidenthantering? Finns rutiner för att säkerställa driftsäkerheten vid datorstyrda samhällsviktiga funktioner (till exempel vattenförsörjning eller liknande)?

3.2 Avgränsning

Granskningen kommer att fokuseras på verksamheten kring IT och identifiering av eventuella förbättringsområden. Granskningen omfattar inte en utvärdering av lämpligheten i befintliga system eller hårdvara som kommunen använder. Granskningen inkluderar inte implementering av de rekommendationer som lämnas.

4 Revisionskriterier

Vi kommer att bedöma om rutinerna uppfyller:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk och policys avseende informationssäkerhet
- Jämförbar praxis avseende informationssäkerhet

5 Ansvarig nämnd

Granskningen avser huvudsakligen kommunstyrelsen.

6 Metod

Granskningen har genomförts genom:

- Dokumentstudier av relevanta dokument
- Faktainsamling av underlag
- Intervjuer med berörda tjänstemän

IT-chefen har samordnat faktakontrollen av rapporten.

7 Resultat av granskningen

7.1 Generellt styrande och stödjande dokument

Vi har erhållit *"IT-policy med strategier Dalsland 2009 – 2013"*. Informationssäkerhet och den underordnade IT-säkerheten nämns i detta dokument som i inledande text anger att: *"Dokumentet har tagits fram på uppdrag av Dalslandskommunernas kommunalförbund (DKF) och har genomförts med en styrgrupp bestående av de sex IT-cheferna i Dalsland."* Vidare framgår att: *"Dokumentet är att betrakta som en avrapportering av detta uppdrag."* Dokumenten är minst fem år gammalt omfattar inte informationssäkerhet och är inte formellt antaget i någon instans och fyller därför vid granskningstillfället ingen funktion för informationssäkerheten i kommunen. Av kompletterande information framgår att en *"digitaliseringsstrategi ska tas fram"*. Det uppges att detta eventuellt ska ske i ett samverkansprojekt med övriga Dalslandskommuner.

Erhållen informationssäkerhetspolicy är enligt den inledande texten *"beslutad och ägd av kommunfullmäktige"*. Vidare framgår i det odaterade dokumentet att: *"Policyn skall tillämpas inom alla kommunens nämnder, förvaltningar, bolag och stiftelser. Tillämpningen ska stödjas av riktlinjer och konkreta rutiner. Kommunchefens ledningsgrupp ska årligen ha en genomgång av kommunens informationssäkerhetsarbete och vid behov föreslå uppdatering av denna policy."* Bristen på datering och dokumenterade genomgångar att ta del av antyder att dokumentet inte varit föremål för några förändringar. Till detta ska läggas en uppgift som når oss att den *"tyvärr inte"* är helt känd i våra verksamheter.

"IT-säkerhet på användarnivå" är rubriken på ett tresidigt dokument som tillsammans med två ensidiga dokument *"IT-Användaravtal"* och blanketten *"Beställning till IT-enheten"* anges användas som informationssäkerhetsstyrning vid nyanställningar. Dokumenten är alla odaterade, det framgår inte vem som upprättat dem och ansvarar för innehållet och inte något av dem refererar till informationssäkerhetspolicyn. I *"IT-säkerhet på användarnivå"* hänvisas det till *"IT-policy med strategier Dalsland 2009 – 2013"* som vi redan konstaterat inte är en policy och inte omfattar informationssäkerhet. Att förstå den kommunövergripande styrningen av informationssäkerheten kompliceras även av det i dokumentet redovisas följande: *"Följ lokala föreskrifter för arbete med itstöd. Om din arbetsplats eller skola har egna föreskrifter eller avtal för arbete med itstöd skall du även följa dessa. I de fall föreskrifterna är motstridiga gäller det här dokumentet."*

Blanketten *"Beställning till IT-enheten"* innehåller, förutom de uppgifter IT-enheten behöver för sin administration och åtgärder, en informationsruta med följande text: *"Beställning ska vara inkommen två veckor innan användarens första arbetsdag. För att konto ska kunna skapas krävs det att ett anställningsavtal är påskrivet. Du är ansvarig för att kontakta IT-enheten om någon personal slutar som har behörighet till något datasystem på din enhet/förvaltning."*

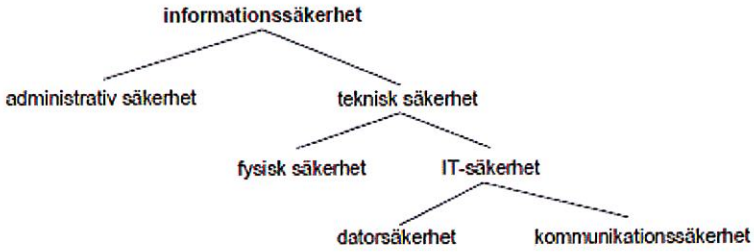
Kommentarer

Revisionsfrågan: *"Finns en informationssäkerhetspolicy med tillhörande informationssäkerhetsrutiner och regelverk som tar i beaktande säkerhetsfrågor med avseende på ny IT-teknisk utveckling såsom molntjänster, mobila enheter och hantering av sociala*

medier" besvaras med ja delvis. Policyn finns och indikerar medvetenhet vad gäller informationssäkerhet. Den är dock i princip praktiskt verkningslös när den inte bedöms vara känd och saknar därtill hörande konkreta och väl dokumenterade tillämpningsföreskrifter. Policyn behöver en allmän uppdatering inte minst med i vilken omfattning kommunen avser följa standarderna i den så kallade 27000-serien[1].

Revisionsfrågan: *"Hur säkerställs informationssäkerheten vid användandet av mobila enheter såsom läsplattor, datorer och mobiltelefoner?"* Svaret blir inte alls. Det utifrån det faktum att det inte finns tydligt konkreta och dokumenterade instruktioner kopplad till informationssäkerhetspolicyn som anger hur det ska gå till och hur efterlevnaden sedan kontrolleras. Om dokumentet *"IT-säkerhet på användarnivå"* ska behållas krävs omfattande justeringar, uppdateringar samt förtydliganden. Det inte minst vad gäller förhållandet mellan informationssäkerhet och IT-säkerhet samt hur kontrollen av efterlevnaden kommer att genomföras.

Av standarderna i 27000 serien kan utläsas att IT-säkerhet är underordnad informationssäkerheten. Placeringen innebär att beslut om IT-säkerhet styrs av de beslut som tas av system och/eller objektägare som tillämpar det LIS[2] som kommunfullmäktige enligt antagen informationssäkerhetspolicy beslutat om. Ett LIS som vi förmodar är och ska vara en del av kommunens samlade ledningssystem.



Revisionsfrågan: *"Vad gäller avseende IT-utrustning vid avslut av behörigheter och anställningar?"* Vi kan i erhållna dokument i inte finna några tillämpningsföreskrifter som anger svaret på revisionsfrågan. Det som framgår av blanketten *"Beställning till IT-enheten"* är inte tillräckligt för att kunna bedöma att det finns åtgärder för att säkerställa att en känd metod används för avveckling av behörigheter och data. Känd så till vida att den med verksamhetsansvaret känner till den och kan kontrollera att resultatet blir det beställda när den efterlevs.

Revisionsfrågan: *"Finns riktlinjer för åtkomsthantering för väsentliga IT-system inklusive riktlinjer för beställning av behörighetsförändringar, lösenordshantering, begränsning kring höga behörigheter och säkerhet relaterad till att endast behöriga personer har åtkomst till relevanta IT-system?"* Vi har inte erhållit någon styrande eller stödjande dokumentation som övergripande gäller för kommunen. Kommunen saknar därmed grundläggande lägstanivåer för åtkomsthanteringen vilket innebär att detta ansvar ligger hos verksamhetsledningen i respektive förvaltning. Mer om detta i avsnitt nedan.

---

[1] Överväg att i ett första steg anta SS-ISO/IEC 27001 Ledningssystem för informationssäkerhet – Krav, SS-ISO/IEC 27002 Riktlinjer för styrning av informationssäkerhet, SS-ISO/IEC 27003 Vägledning för införande av ledningssystem för informationssäkerhet, SS-ISO/IEC 27004 Vägledning för mätning av informationssäkerhet och SS-ISO/IEC 27005 Riskhantering för informationssäkerhet.

[2] Ledningssystem för informationssäkerhet. Nämns under rubriken "Mål och principer för informationssäkerhetsarbetet" i informationssäkerhetspolicyn.

7.2 Styrande och stödjande dokument vid upphandling

Kommunen har vid granskningstillfället inga dokumenterade krav och/eller instruktioner för hur beslutad informationssäkerhet ska säkerställas vid någon form av upphandling.

Kommentarer

Revisionsfrågan: *"Beaktas informationssäkerhetskrav vid upphandling av nya IT-tjänster så som exempelvis molntjänster?"* Frågan besvaras med ett nej. Vi kan notera att vid den nyligen utförda upphandlingen av e-Arkiv[3], vilken enligt uppgift gjorts gemensamt med andra kommuner, hade ansvariga tillgång till den säkerhetsanalys som upprättats av Uddevalla kommun. Av den framgår inledningsvis att: *"Riskanalysen tar inte ställning till de ingående systemens skydd mot åtkomst eller förvrängning av information utan begränsar sig till användandet av E-arkivet som lagringsmedia."* Analysen redovisar även informationssäkerhetsrisker som kommunen inte har styrande och stödjande dokument för att hantera.

7.3 Kontroller och uppföljning av informationssäkerheten.

Kommunen saknar kommunövergripande styrande och stödjande dokument för kontroll av att beslutad informationssäkerhet är känd och efterlevd.

Kommentarer

Revisionsfrågan: *"Finns kontroller, kontrollmoment och definierade uppföljningsprocesser för uppföljning av aktivitet i IT-systemen? Exempelvis regelbundna logguttag och analys av genomförda aktiviteter?"* Frågan besvaras med ett nej. Vi kan dock notera verksamhetsspecifik dokumentation. Mer om det i avsnitt nedan.

7.4 Kontinuitetsplaner och NIS-direktivet

För kommunen övergripande styrande och/eller stödjande dokument som vägleder om hur kontinuitetsplaner ska upprättas och övas finns inte. Vid granskningstillfället har kommunen inte undersökt i vilken omfattning och på vilket sätt NIS-direktivet[4] ska efterlevas.

Kommentarer

Revisionsfrågan: *"Finns riktlinjer och rutiner för katastrof- och incidenthantering? Finns rutiner för att säkerställa driftsäkerheten vid datorstyrda samhällsviktiga funktioner (till exempel vattenförsörjning eller liknande)?"* Frågan besvaras med ett nej. Vad vi förstår så har kommunen från och med 2018-08-28 en nyanställd säkerhetssamordnare som kommer att ansvara för utveckling av informationssäkerhetsarbetet inkluderat anpassningen till NIS-direktivet. Av vad som uppges kommer hen att ha ett visst stöd i det arbetet i form av resultatet av det arbete som lagts ned i samband med anpassningen till

[3] Alla kommuner och landsting har ansvar för att bevara sin information, oavsett om den finns i pappersform eller digital form. Det krävs ett e-arkiv för att kunna bevara organisationens digitala information för all evighet. Det framgår i tryckfrihetsförordningen, arkivlagen och annan lagstiftning.

[4] *"Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen."*

GDPR[5]. Säkerhetssamordnaren kommer, vad vi förstår, att bidra med att införa en ändamålsenlig styrning av informationssäkerheten i och med sitt ansvar att upprätta kommunens risk- och sårbarhetsanalys[6] för 2019. Informationssäkerheten är en inte oväsentlig del av det arbetet. Kommunen ska rapportera sin RSA till länsstyrelsen senast den 31 oktober 2019.

7.5 Verksamhetsspecifika styrande och stödjande dokument

Av erfarenhet känner vi till att det kan finnas styrande och stödjande dokument avseende informationssäkerhet omfattande avgränsade delar av kommunens verksamhet. Denna typ av dokumentation saknar inte sällan en dokumenterad koppling till en kommunövergripande policy och tillämpningsföreskrifter. Vi har som exempel efterfrågat styrande dokument vad gäller:

- Hanteringen av skyddad identitet inom barn- och utbildningsförvaltningen samt vård- och omsorgsförvaltningen.
- Loggkontroller inom vård- och omsorgsförvaltningen.
- Behörighetshantering i lönesystemet.

7.5.1 Skyddad identitet

Det finns en odaterad *"Checklista för hantering av klienter med skyddad identitet"* som utan att det anges mest troligt är upprättad inom vad som idag benämns vård- och omsorgsförvaltningen. Att den finns visar på medvetenhet om vikten av en säker hantering. Våra intervju indikerar en osäkerhet i vilken omfattning den är känd och efterlevd och enligt uppgift finns inget motsvarande för barn- och utbildningsförvaltningen. Det saknas inte insikt om att dokumentet behöver revideras, göras känt samt att det utförs kontroller för att säkerställa efterlevnaden.

7.5.2 Loggkontroller

Förvaltningschef inom vård- och omsorgsförvaltningen har med en angiven giltighetstid från 2014-02-01 till 2019-01-31 upprättat dokumentet *"Rutiner för loggning inom vård- och omsorgsförvaltningens verksamhetssystem Procapita samt Nationell Patientöversikt, NPÖ"*. Det fyrsidiga dokumentet visar på medvetenhet om att detta är ett väsentligt inslag i arbetet med informationssäkerhet. Vi noterar att dokument är efterlevt i så motto att det utförts loggkontroller. När giltighetstiden nu går ut i början av 2019 och det är dags för en översyn så bedömer vi att innehållet behöver uppdateringar och förtydliganden. Dokumentet behöver anpassas och hänsyn tas till nya lagar och föreskrifter.

---

[5] *"Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)."*

[6] Risk- och sårbarhetsanalyser (RSA) är ett första steg i en kedja som syftar till att reducera risker, minska sårbarheter i samhället och att förbättra förmågan att förebygga, motstå och hantera kriser och extraordinära händelser. Kommuner ska göra en RSA enligt lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och under höjd beredskap.

7.5.3 Behörigheter i lönesystem

Dokumenterade rutiner för hur hantering av behörigheter i lönesystemet finns enligt uppgift inte. Det är väsentligt att sådana finns, är väl kända och efterlevda. Det ska inte råda någon osäkerhet om vilka och varför som över tid påverkar förutsättningarna för hur löner och ersättningar betalas.

7.6 Slutsats och rekommendationer

Sammanfattningsvis kan vi konstatera att kommunen vid granskningstillfället i allt väsentligt saknar styrande och stödjande dokument för hur informationssäkerheten ska hanteras.

Mot bakgrund av vår granskning rekommenderar vi kommunen att inte underprioritera arbetet med att upprätta styrning och stöd för en ändamålsenlig informationssäkerhet. Enskilda specialister kommer inte att utan stöd och aktiv medverkan från ansvariga nå nödvändig verkanshöjd i ett arbete som behöver startas omgående.

2018-12-04

KPMG AB

Lars Anteskog
Projektansvarig