KOMMUNENS REVISORER
ALE KOMMUN

Kommunstyrelsen
Ale kommun

2018-09-12

Rapport – Granskning av informations- och IT-säkerhet

KPMG AB har på uppdrag av kommunens revisorer granskat hur kommunen arbetar med informations- och IT-säkerhet baserat på styrande policydokument och rutiner för generella IT-kontroller.

Vi har i granskningen kunnat fastställa att Ale kommun har implementerat styrande dokument och riktlinjer som behandlar informationssäkerhet. Kommunen arbetar aktivt med informationssäkerhetsfrågor och de dokument och det löpande arbete som pågår indikerar att det är ett prioriterat område. Vid revisionstillfället höll en utbildning i informationssäkerhet på att rullas ut, men dessförinnan har det saknats strukturer för att på ett enhetligt sätt utbilda personal i informationssäkerhetsfrågor. Vår bedömning är att styrande dokument överlag är fullständiga utifrån de krav och den praxis som finns gällande informationssäkerhet.

Flertalet krav och generella IT-kontroller som har granskats och som återfinns i informationssäkerhetspolicyns riktlinjer har blivit implementerade i verksamheten. Undantag finns då periodisk genomgång av användarkonton och behörigheter inte har blivit fullständig implementerad. Rutinen för behörighetsadministration är i stor utsträckning automatiserad, undantag finns i verksamhetssystemen och för de granskade systemen finns effektiva manuella processer. Kommunen har en restriktiv inställning till höga behörigheter och ansvaret är tydligt angivet i både styrdokument och för granskade system. Lösenordskraven i AD (Active Directory, Microsofts katalogtjänst) är starka och i linje med KPMGs rekommendationer, där det inte är möjligt att ha starka lösenord finns riktlinjer att tillgå.

Vid upphandlingar av nya IT-stöd ska alltid IT-avdelningen involveras. Det saknas tydliga instruktioner i relation till upphandlingspolicyn som tar hänsyn till de krav på informationssäkerhet som ställs på informationssystem och molnbaserade systemlösningar.

Det finns en tydlig incidenthanteringsprocess på plats som bör säkerställa att incidenter hanteras, åtgärdas och förebyggs på strukturerat sätt. Det finns flera olika modeller på plats för katastrofhantering såsom It-tekniker i beredskap, återställningsrutiner och backuplösningar. Det saknas dock fullständiga kontinuitetsplaner för samtliga verksamheter och återläsningstester av säkerhetskopierad data genomförs inte utefter ett fastställt schema.

Vid granskningen har nedanstående förbättringsområden identifierats varför vi rekommenderar kommunstyrelsen att:

- Säkerställa att en formaliserad rutin för inköp och upphandling av IT implementeras eller kompletteras till upphandlingsrutinen.
- Säkerställa att utbildningarna i informationssäkerhet genomförs och att en strategi för löpande utbildning tas fram.

- Säkerställa efterlevnaden av informationssäkerhetskraven i informationssäkerhetspolicyn och dess riktlinjer genom en underskrift av den anställde.
- Säkerställa att en periodisk genomgång av användare och dess behörigheter implementeras och nyttjas i samtliga verksamhetssystem.
- Säkerställa att lösenordskraven för politiker är lika starka som för anställda avseende iPAD:s.
- Säkerställa att samtliga mobila enheter (datorer, telefoner och iPAD:s) omfattas av samtliga säkerhetskrav.
- Säkerställa att återläsningstester genomförs på löpande basis i syfte att säkerställa att backuper är återläsningsbara.
- Säkerställa att kontinuitetsplaner tas fram för samtliga verksamheter.

I övrigt hänvisas till biträdets rapport.

Vi önskar delta vid det AU-sammanträde där kommunstyrelsens svar på granskningsrapporten ska beredas. Vi önskar delta i ett sådant möte senast under november månad 2018. Vi önskar även före ovan nämnda möte ta del av förvaltningens tjänsteutlåtande som lämnas inför styrelsen respektive nämndens behandling av rapporten.

Ale som ovan

Leif Andersson
Ordf. i kommunrevisionen

Irene Hellekant
Vice ordf. i kommunrevisionen