Diarienummer: KS.2018.264
Datum: 2018-10-09
Utvecklingschef Gunilla Dörner Buskas
E-post: gunilla.dorner-buskas@ale.se

Kommunstyrelsen

Svar på granskningsrapport om IT- och informationssäkerhet

KPMG har på uppdrag av kommunens revisorer genomfört en granskning av hur Ale kommun arbetar med informations- och IT-säkerhet. Granskningen har genomförts genom intervjuer med nyckelpersoner samt genom dokumentanalys. Syftet med granskningen har varit att fastställa om riktlinjer kring informationssäkerhet och IT-säkerhet med bäring på ny teknisk utveckling är implementerade och ändamålsenliga.

Förvaltningens beslutsförslag till kommunstyrelsen

Kommunstyrelsen beslutar att anteckna revisionsrapporten och godkänna förvaltningens förslag till åtgärder med anledning av de rekommendationer som ges.

Gunilla Dörner Buskas
Tf kommunchef

Beslutsunderlag

- Tjänsteutlåtande, 2018-10-09
- Granskningsrapport
- Missiv

Ärendet expedieras efter beslut till:

För vidare hantering
IT-chef

Administrativ chef

För kännedom
Förvaltningsledningen

Sektor KS ledningsgrupp

Bakgrund

KPMG har på uppdrag av kommunens revisorer genomfört en granskning av hur Ale kommun arbetar med informations- och IT-säkerhet. Granskningen har genomförts genom intervjuer med nyckelpersoner samt genom dokumentanalys. Syftet med granskningen har varit att fastställa om riktlinjer kring informationssäkerhet och IT-säkerhet med bäring på ny teknisk utveckling är implementerade och ändamålsenliga.

Revisionen har omfattat följande frågor:

- Finns en informationssäkerhetspolicy med tillhörande rutiner 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 IT-utrustning vid avslut av behörigheter och anställningar?
- Finns riktlinjer föråtkomsthantering 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 vi upphandling av nya IT-tjänster såsom 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?

Samråd/samverkan

Granskningsrapporten har hanterats i styrgruppen för Digital Agenda.

Ekonomisk bedömning/konsekvens

Förslaget bedöms inte ha några ekonomiska konsekvenser.

Barnperspektivet

Förslaget påverkar inte barnperspektivet.

Miljöperspektivet

Förslaget påverkar inte miljöperspektivet.

Funktionshinderperspektivet

Förslaget påverkar inte funktionshinderperspektivet.

Övriga i kommunen förekommande styrdokument som påverkar ärendet

- Informationssäkerhetspolicy

- Informationssäkerhet - riktlinje för användare
- Informationssäkerhet - riktlinje för förvaltning, kontinuitet och drift
- Strategi, policy och riktlinjer för Ale kommuns närvaro i sociala medier
- Upphandlingspolicy

Förvaltningens bedömning och motivering

KPMG har på uppdrag av kommunens revisorer genomfört en granskning av hur Ale kommun arbetar med informations- och IT-säkerhet. Granskningen har genomförts genom intervjuer med nyckelpersoner samt genom dokumentanalys. Syftet med granskningen har varit att fastställa om riktlinjer kring informationssäkerhet och IT-säkerhet med bäring på ny teknisk utveckling är implementerade och ändamålsenliga.

Granskningen konstaterar att Ale kommun väl lever upp på de krav som kan ställas för informations- och IT-säkerhet. Kommunen har implementerat styrande dokument och riktlinjer samt arbetar aktivt med informationssäkerhetsfrågor. En obligatorisk utbildning i informationssäkerhet rullas ut.

Flertalet krav och generella IT-kontroller som finns i informationssäkerhetspolicyn har implementerats i verksamheten. Rutinen för behörighetsadministration är i hög utsträckning automatiserad och där det saknas finns effektiva manuella processer. Ale kommun har en restriktiv inställning till höga behörigheter och detta finns tydligt angivet i styrande dokument. Lösenordskraven är starka.

Vid upphandlingar av nya IT-stöd ska alltid IT-avdelningen involveras. Det saknas dock tydliga instruktioner i relation till upphandlingspolicyn som tar hänsyn till kraven på informationssäkerhet.

Det finns flera modeller på plats för katastrofhantering men det saknas fullständiga kontinuitetsplaner för samtliga verksamheter.

KPMG lämnar rekommendationer inom fem områden:

1. Det saknas en formaliserad upphandlingsprocess avseende IT- och molntjänster.
    a. En formaliserad rutin för inköp och upphandling av IT implementeras eller kompletteras till upphandlingsrutinen. Rutinen bör inkludera beaktanden som är väsentliga i samband med upphandling av molntjänster.
2. Medvetenheten och utbildning i informationssäkerhet inom kommunen kan stärkas ytterligare.
    a. Kommunen säkerställer att utbildningarna i informationssäkerhet genomförs och att en strategi för löpande utbildning tas fram.
    b. Anställda skriver på att de ska efterleva informationssäkerhetskrav som återfinns i informationssäkerhetspolicyn och dess riktlinjer.
3. Det saknas en formaliserad rutin för periodisk genomgång av användarkonton och behörigheter i kommunens verksamhetssystem.
    a. En central rutin för periodisk genomgång av användare och dess behörigheter implementeras.

4. Samtliga mobila enheter omfattas inte av säkerhetskraven och säkerhetskraven är inte enhetliga mellan politiker och anställda.
    a. Säkerställa att lösenordskraven för politiker är lika starka som för anställda.
    b. Säkerställa att samtliga mobila enheter omfattas av samtliga säkerhetskrav.
5. Återläsningstester av applikationer genomförs inte på löpande basis och det saknas fullständiga kontinuitetsplaner för samtliga verksamheter.
    a. Kommunen säkerställer att återläsningstester genomförs på löpande basis i syfte att säkerställa att backuper är återläsningsbara.
    b. Kontinuitetsplaner tas fram för samtliga verksamheter.

Förvaltningen välkomnar granskningsrapporten och anser att en utgör ett bra stöd för förbättringsarbetet inom IT- och informationssäkerhet. Avseende flera av rekommendationerna är arbetet påbörjat. Här redovisas kommunens åtgärder med anledning av rekommendationerna:

Det saknas en formaliserad upphandlingsprocess avseende IT och molntjänster.

Ett förslag till rutin avseende upphandling av IT-stöd och molntjänster har tagits fram. Förslaget hanteras i förvaltningsledningen den 15 oktober för att därefter fastställas av kommunchefen. Rutinen kompletterar upphandlingspolicyn och omfattar vägledning, kravbibliotek och checklista.

Medvetenheten och utbildning i informationssäkerhet inom kommunen kan stärkas ytterligare.

En obligatorisk utbildning i informationssäkerhet har startats i september. En ny rutin tas fram så att användare kvitterar att de tagit del av "Informationssäkerhet för användare" när de får nya enheter eller nytt konto.

Det saknas en formaliserad rutin för periodisk genomgång av användarkonton och behörigheter i kommunens verksamhetssystem.

Rutinerna skärps för att sätta rätt behörighet till rätt användare vid förändringar i verksamheten. Rutinen tas fram tillsammans med objektsledarna. Möjligheterna att inaktivering i AD också leder till inaktivering i system som har Single Sign On utreds.

Samtliga mobila enheter omfattas inte av säkerhetskraven och säkerhetskraven är inte enhetliga mellan politiker och anställda.

Alla nya enheter kommer att hanteras av Microsoft Intune vilket ger möjligheter till managering och fjärradering. Samma lösenordskrav kommer att ställas på alla användare, dvs politiker och anställda kommer att ha samma krav på lösenord.

Återläsningstester av applikationer genomförs inte på löpande basis och det saknas fullständiga kontinuitetsplaner för samtliga verksamheter.

Rutin för återläsningstester tas fram. Administrativa chefen, som tillika är säkerhetschef, säkerställer att objektsägarna tar fram kontinuitetsplaner för respektive verksamhet.