

2017-10-25

TJÄNSTESKRIVELSE
KFKS 2017/563

Kommunstyrelsen

Revisionsrapport nr 3/2017 IT- och informationssäkerhet

Yttrande till kommunfullmäktiges revisorer

Förslag till beslut

Kommunstyrelsen antar stadsledningskontorets förslag till yttrande över revisionsrapport nr 3/2017, IT-och informationssäkerhet.

Sammanfattning

Kommunens revisorer har gjort en granskning av kommunens arbete med IT- och informationssäkerhet. Kommunstyrelsen har fått en skrivelse med ett antal områden där brister identifierats. I detta ärende föreslår stadsledningskontoret hur kommunstyrelsen ska yttra sig över rapporten och en redovisning om hur bristerna åtgärdats. Sedan granskningen genomfördes i maj-juni har fem av sju brister åtgärdats. Det gäller bland annat att genomföra utbildningsinsatser och att göra penetrationstester. Bristerna inom de återstående två områdena kommer att vara åtgärdade innan nyår. Det gäller att förtydliga rutiner och processer för arbetet med informationssäkerhet samt att utveckla rutinerna vid incidenter.

Ärendet

Kommunstyrelsen har fått en revisionsskrivelse från kommunfullmäktiges revisorer angående kommunens arbete med IT- och informationssäkerhet. I skrivelsen finns sju förbättringsområden som revisorerna vill ha svar på senast 25 november. Skrivelsen bygger på en revisionsrapport från EY.

EY har genomfört en granskning under maj och juni. Den gjordes genom att studera dokument och intervjua en handfull nyckelpersoner med ansvar för informationssäkerhet. Utifrån detta har sedan kommunens arbete bedömts inom ett 60-tal områden utifrån en modell som EY själv tagit fram. Detta har sedan sammanställts i en revisionsrapport. Det är utifrån den rapport som sedan revisorerna formulerat den skrivelse som kommunstyrelsen nu ska yttra sig över.

I rapporten från EY konstateras att kommunen har goda förutsättningar för det fortsatta arbetet med informationssäkerhet. I samband med granskningen redovisades att kommunen kommer att förstärka arbetet inom informationssäkerhet under denna höst. Det finns noterat i skrivelsen men eftersom det inte fanns på plats vid granskningen i maj och juni så blev resultatet i bedömningen lågt på vissa områden.

De förbättringsområden som tas upp i revisionsskrivelsen berör otydlighet kring vem som är den centralt ansvariga personen, avsaknad av standardiserade och definierade rutiner och processer och att informationssäkerhetspolicyn inte formellt uppdaterats på tre år. Vidare tas upp att kommunen inte genomför några utbildningsinsatser, att det saknas tydliga incidenthanteringsrutiner och att det borde finnas en central grupp som ansvarar för informationssäkerhetsarbetet. Slutligen tas upp att kommunen inte genomför några penetrationstester. Med penetrationstester avses att man testar hur pass väl system motstår olika former av attacker mot dem.

Inom fem av områdena finns i förslaget till yttrande att frågan är löst eller på god väg att lösas. Den centralt ansvarige är administrativa direktören, förslag på informationssäkerhetsstrategi (ersätter den nuvarande informationssäkerhetspolicyn) läggs fram vid samma sammanträde som detta ärende. Utbildningsinsatser pågår, det finns en central grupp och kommunen har påbörjat penetrationstester. Vad gäller incidenthantering och standardiserade processer och rutiner kommer dessa att tas fram före nyår.

Ekonomiska konsekvenser

Kostnader för att åtgärda de brister som nämns i revisionsskrivelsen hanteras inom fastställd budgetram.

Konsekvenser för barn

Inga direkta konsekvenser för barn.

Bilagor

Förslag till yttrande till revisorerna

Revisionsskrivelse

Revisionsrapport

Mats Bohman
Administrativ direktör
Stadsledningskontoret

Anneli Sagnérius
Enhetschef
Juridik och kansliheten

Johan Höge
Tf enhetschef
Digitaliseringsenheten