Kommunstyrelseförvaltningen
Kansli
Carl Björnberg, digitaliseringssamordnare
carl.bjornberg@arboga.se

Kommunstyrelsen

Svar på revisionens skrivelse avseende IT-verksamheten

Förslag till beslut

1. Kommunstyrelseförvaltningens förslag till svar på revisionens skrivelse avseende IT-verksamhet godkänns.

Bakgrund

De förtroendevalda revisorerna i Arboga kommun har den 20 februari 2024 inkommit med en skrivelse till kommunstyrelsen avseende IT-verksamheten daterad 2024-01-26.

I skrivelsen efterfrågar de förtroendevalda revisorerna svar på ett antal frågor senast 30 april 2024. Svar redovisas nedan.

Hur har kommunstyrelsen beaktat informationssäkerhetsrisker som kommunen skulle kunna drabbas av?

Informationssäkerhet begränsas inte till säkerhet i IT-system utan omfattar information i alla dess former och oavsett hur information lagras, transporteras, bearbetas och kommuniceras. Information kan till exempel vara i form av text, ljud, bilder och film och kan hanteras med stöd av IT, papper eller direkt av människor i form av tal. Det är därför sannolikt att alla risker en kommun skulle kunna drabbas av involverar någon form av information och därmed per definition är en informationssäkerhetsrisk. Riskbedömningar görs som en naturlig del av arbetet kontinuerligt i alla kommunens verksamheter.

Hur har kommunstyrelsen kravställt och följt upp att informations-klassning och riskbedömning av informationstillgångar har genomförts?

Kravställning

I den antagna informationssäkerhetspolicyn framgår att en riskbedömning eller en informationssäkerhetsklassificering ska ske.

Uppföljning

Informationssäkerhetspolicyn är antagen av Kommunfullmäktige 2023-11-23 § 117. Någon uppföljning har ännu inte skett.

Hur har resultat från dessa kommunicerats till VMKF så att erforderliga it-säkerhetsåtgärder har vidtagits för att skydda tillgångarna?

Se föregående svar. Informationssäkerhetspolicyn innehåller två principer för informationssäkerhet. Den första är riskorienterad informationssäkerhet, vilken har besvarat de två första av revisorernas frågor. Den andra principen är verksamhetsdriven informationssäkerhet, vilket innebär att verksamheter utifrån informationens skyddsvärde ställer krav på de aktörer som hanterar informationen. VMKF är en av många av dessa aktörer. Krav på informationssäkerhet ställs kontinuerligt, företrädelsevis redan i upphandlingsfas och säkras upp genom avtal, som till exempel drift- och serviceavtal (SLA) och PUB-avtal.

Hur har kommunen tagit ställning till hur informationssäkerhets-arbetet ska ledas och samordnas för att nå upp till att vara systematiskt och riskbaserat?

Informationssäkerhetspolicyn anger att ansvaret för informations-säkerhet följer det ordinarie verksamhetsansvaret. Kommun-direktören har det övergripande ansvaret och förvaltningschef eller VD ansvarar för att ge förutsättningar så att lämplig informations-säkerhet upprätthålls för den information som finns i det egna verksamhetsområdet. Någon utsedd samordnade roll finns inte i den meningen. Notera också att det inte finns några formella krav på ett systematiskt informationssäkerhetsarbete så länge inte verksamheten definieras som samhällsviktig av Myndigheten för samhällsskydd och beredskap. Vid ett eventuellt införande av ett systematiskt informationssäkerhetsarbete, vilket ska baseras på ISO 27.000 så krävs en samordnande roll för detta.

Riktlinje för systemförvaltning som beslutats är en viktig utgångs-punkt för ansvarsfördelning mellan medlemskommunerna och förbundet kring de verksamhetssystem som nyttjas. Hur har kommunstyrelsen säkerställt att riktlinjen efterlevs och är implementerad tillräckligt i kommunens samtliga verksamheter?

Riktlinje för systemförvaltning antogs av kommunstyrelsen 2018-08-28 § 218. Den har bidragit till förbättrad ledning och styrning

av de resurser som krävs för att upprätthålla system och den har ökat verksamhetsnyttan av gjorda IT-investeringar, men den är fortfarande inte helt implementerad i kommunens samtliga verksamheter. Arbete pågår med att ta fram en ny riktlinje för systemförvaltning som bygger på de facto-standarden pm3 i syfte att förbättra och samtidigt förenkla systemförvaltningen. Antagande av den nya riktlinjen förväntas ske under 2024. I samband med antagandet planeras aktiviteter för att förankra och implementera riktlinjen på nytt.

Informationssäkerhetspolicyn förtydligar också systemförvaltarens ansvar gällande informationssäkerhet och vem som har denna roll om utsedd systemförvaltare saknas.

På vilket sätt finns det dokumenterat vem som är systemägare för de IT-system som kommunen använder?

Det finns en systemkatalog innehållandes alla system som kommunen använder. I den pekas inte systemägare ut med namn, men både informationssäkerhetspolicyn och riktlinjen för system-förvaltning pekar ut IT-chef, om VMKF ansvarar för driften, annars verksamhetsansvarig. På så sätt går det att läsa ut vem som är systemägare för respektive system.

Anders Neuman
Kommundirektör

Carl Björnberg
Digitaliseringssamordnare

Skickas till:
Revisorerna i Arboga kommun
Karin Helin Lindkvist, KPMG