§ 23 2023.546 KS

Granskning av informations- och IT-säkerhet

Ärendebeskrivning

På uppdrag av de förtroendevalda revisorerna i Alingsås kommun har KPMG genomfört en granskning av kommunens arbete för att upprätthålla en god informations- och IT-säkerhet. Granskningen har syftat till att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt informationssäkerhetsarbete.
KPMG:s samlade bedömning utifrån granskningens syfte är att kommunstyrelsen vid tid för granskningen bedriver ett systematiskt informationssäkerhetsarbete men att nämndernas arbete är i behov av utveckling för att vara systematiskt i enlighet med beslutade styrdokument.
KPMG:s granskning rekommenderar kommunstyrelsen att:

- Revidera och aktualisera informationssäkerhetspolicyn mot bakgrund av att den kan riskera att vara föråldrad i förhållande till nuvarande hot, risker och krav.
- Tillse att informationssäkerhetsutbildning genomförs i högre grad inom samtliga verksamheter.
- Tillse att egna informationstillgångar klassas och riskbedöms samt följa upp att samtliga kommunens verksamhetskritiska system samt system som hanterar skyddsvärd information och personuppgifter har en aktuell klassning och riskbedömning.
- Följa upp att säkerhetsåtgärder vidtagits som informationsklassning och riskbedömning visat behov av.
- Säkerställa att kommunövergripande incidenthanteringsrutiner upprättas och etableras.
- Anpassa och stärka uppföljningsmetoder och kontroll av efterlevnad av beslutade styrdokument inom informationssäkerhet i takt med att kommunens mognadsgrad i informationssäkerhetsarbetet ökar.

Beredning

Kommunledningskontoret har i skrivelse den 16 månad 2024 lämnat följande yttrande:

Kommunledningskontoret har tagit del av rapporten och delar de slutsatser som framkommer i rapporten. Arbetet med informations- och IT-säkerhet har pågått strukturerat i tre år med en medveten strategi att utvecklas i rimlig takt över lång tid. Bedömning gjordes inledningsvis att det skulle bli svårt att implementera ett heltäckande arbetssätt omgående då arbetet skulle bli för stort för att få genomslagskraft. Istället har arbetet varit långsiktigt med mindre utvecklingar och förbättringar varje år. Med en engagerad kommunledning har frågorna givits tillträde till ledningsgrupper och dagordningar, detta tillsammans med nödvändiga politiska beslut har varit avgörande för den positiva förflyttning som skett i kommunen inom områdena.

Kommunfullmäktige har fastställt en informationssäkerhetspolicy vilken anger kommunens långsiktiga målsättningar och grundläggande principer. I policyn framgår att kommunstyrelsen årligen ska fastställa en handlingsplan där aktiviteter som ska genomföras

under året ska framgå. Dessa aktiviteter ska bidra till att verksamheten över tid uppnår fullmäktiges målsättningar.

Under de senaste åren har stort fokus i handlingsplanerna varit att implementera olika metoder som utgör kommunens ledningssystem för informations- och IT-säkerhet:

- verksamhetsanalys - kartläggning av verksamhetens information
- riskanalys
- informationsklassning
- genomförande av säkerhetsåtgärder
- uppföljning och revision

Precis som KPMG påpekar behöver fokus framgent vara att säkerställa genomförandet av metoder i verksamhet. I vissa delar av kommunkoncernen har ledningssystemets olika delar införts till fullo, i andra delar finns förbättringspotential.

Nedan redogörs för några av de insatser som är planerade att genomföras under kommande år för att möta påpekandena i genomförd granskning och fortsatt utveckling av arbetet med informations- och IT-säkerhet.

- Ett förslag på reviderad informationssäkerhetspolicy är framtaget och väntas för politisk behandling under våren 2024. I revideringen ingår bland annat ett förtydligande mellan centrala och lokala roller. Därigenom väntas det bli tydligare vem som ansvarar för att driva och genomföra arbete i respektive verksamhet. Detta väntas medföra positiv förflyttning för arbetet i respektive nämnd/bolag/förbund.
- En riktad uppföljning gällande genomförande av digitala lektioner kommer tillställas chef. Sikte tas på de arbetsgrupper som har lägst genomförandegrad av lektionerna och tillsammans med centrala stöttningsfunktioner identifieras lösningar för att öka andelen medarbetare som tar del av lektionerna.
- Arbetet med informationsklassning och riskanalys är numer en del av kommunkoncernens arbetssätt och ska genomföras årligen. Andelen genomförda klassningar och analyser väntas öka för varje år, centrala stöttningsfunktioner hjälper till vid genomförande om så behövs, likaså följs arbetet upp årligen.
- En incidenthanteringsprocess ska under 2024 implementeras vilken inbegriper flera delar av incidenthantering (exempelvis personuppgiftsincident, IT-incident osv).

Aktiviteter för 2024 kan läsas i sin helhet i kommunstyrelsen Handlingsplan för informations- och IT-säkerhet 2024.

Kommunledningskontoret föreslår med ovan kommentarer att kommunstyrelsen antar kommunledningskontorets yttrande som svar på granskning av informations- och IT-säkerhet i Alingsås kommun.

Beslut

Förslag till beslut i kommunstyrelsen

Kommunledningskontorets yttrande i tjänsteskrivelse antas som kommunstyrelsens eget yttrande som svar på granskning av informations- och IT-säkerhet i Alingsås kommun.

Beslutsunderlag

- Tjänsteskrivelse - Svar på granskning av informations- och IT-säkerhet i Alingsås kommun
- Missiv - Granskning av informations- och IT-säkerhet
- Revisionsrapport - Granskning av informations- och IT-säkerhet