Sollefteå kommun

SAMMANFATTNING REVISIONSRAPPORT

IT-säkerhet

Vi har av Sollefteå kommuns revisorer fått i uppdrag att granska kommunens arbete med IT-säkerhet.

Vår sammanfattande bedömning utifrån granskningens syfte är att det finns brister i kommunstyrelsens arbete för att säkerställa en tillräcklig kontroll över kommunens Informations- och IT-säkerhet.

Vår bedömning baseras på att kommunstyrelsen inte har tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas. Dialog och samverkan mellan förvaltningarna och IT behöver utvecklas gällande systemförvaltning och informationsklassning för att säkerställa informationssäkerheten och underliggande IT-säkerhetsåtgärder.

I nuläget baseras inte säkerhetsåtgärderna på risker och behov som ansvariga för informationen har fastställt. Utan det underlaget anordnas åtgärderna på ett sätt som IT-enheten upplever som nödvändigt utifrån sina förutsättningar. Det finns olika former att säkerställa att efterlevnad av beslutad IT-säkerhet sker. I de fall det inte går att säkerställa är det näst bästa att se till att incidenter upptäcks och kan åtgärdas. Vi bedömer att detta arbete inte är tillräckligt och att kommunen behöver utveckla sitt arbete med riskanalys i syfte att tydliggöra vilka hot och brister som finns i kommunens IT-miljö och avseende informationssäkerheten.

Trots alla maskinella skydd och varningssystem är det medarbetarna som ska efterleva den beslutade IT-säkerheten. För detta krävs en viss kunskapsnivå och en medvetenhet inom Informations- och IT-säkerhet. Det finns instruktioner på användarnivå men det har inte genomförts någon utbildning för att säkerställa efterlevnaden av en god informationssäkerhet.

Det saknas politiska beslut och uppdrag till verksamheten för att säkerställa arbetet och ingen rapportering sker kring incidenter eller åtgärder för att upprätthålla en tillräcklig säkerhetsnivå.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att det finns aktuella, kända och tillämpade styrdokument med tillhörande instruktioner som lägger en grund för en god informationssäkerhet och tillhörande IT-säkerhet. Dessa bör även tydliggöra ansvar och roller för arbetet.
- Säkerställa att informationsklassning av de datoriserade verksamhetssystemen genomförs för att verksamhetsansvariga ska kunna bedöma vilka säkerhetsåtgärder som behöver vidtas för att skydda de informationstillgångar som de ansvarar för.
- Utveckla arbetet med systemförvaltning så att en dialog förs mellan verksamhetens systemägare/systemförvaltare och IT-enheten.
- Ge IT-enheten i uppdrag att ta fram kontinuitetsplaner som beskriver de reserv-, återställnings- och återgångsrutiner som används för att säkerställa kontinuiteten i en prioriterad verksamhet eller process.

Eventuella frågor besvaras av Bertil Falkerby, telefon 070-679 32 53.

Rapporten i sin helhet finns att hämta på Sollefteå kommuns hemsida:

https://www.solleftea.se/kommunpolitik/kommunens organisation/revisorer

Bertil Falkerby, revisorernas ordförande, telefon 070-679 32 53
Leif Ågren, revisorernas vice ordförande, telefon 070-518 71 84
Martin Nilsson
Jens Lindman,
Susanne Nordgren