

Granskning av informationssäkerhet

Granskningens inriktning

KPMG har av Kramfors kommuns revisorer fått i uppdrag att granska kommunstyrelsens och samtliga nämnders rutiner för informationssäkerhetsarbetet. Uppdraget ingår i revisionsplanen för år 2021.

Granskningen syftar till att bedöma om kommunstyrelsen har säkerställt att det finns ett ändamålsenligt arbete med informationssäkerhet och en tillräcklig intern kontroll. Syftet är därtill att följa upp de åtgärder som bistånds-, arbetsmarknad- och socialnämnden vidtagit avseende behörighetshantering och loggkontroll utifrån rekommendationer i tidigare genomförd granskning 2017 där ett flertal förbättringsområden identifierades.

Sammanfattning

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnderna inte har säkerställt ett ändamålsenligt och systematiskt arbete med kommunens informationssäkerhet.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelse och nämnder att:

- Göra en översyn av styrande dokument så att dessa utgör en sammanhållen helhet för styrningen av kommunens informationssäkerhetsarbete.
- Säkerställa att informationsägarna är medvetna om sitt ansvar och vidtar de åtgärder och aktiviteter som krävs för ett systematiskt informationssäkerhetsarbete för den information de ansvarar för.

- Upprätta en årlig handlingsplan med prioriterade åtgärder och aktiviteter för att utveckla informationssäkerhetsarbetet.
- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- Säkerställa att rutiner och regler finns för behörighetshantering på kommunövergripande nivå. Rutiner bör om möjligt utvecklas genom en mer automatiserad process som kvalitetssäkrar hantering, uppföljning samt kontroll av tilldelade behörigheter.
- Säkerställa att nya och befintliga medarbetare får del av utbildning och information om informationssäkerhet så att en tillräcklig medvetenhet och kunskap finns över enskildas hantering och för att upptäcka incidenter.
- Besluta om kommunövergripande rutin för hantering av informationssäkerhetsincidenter och säkerställa att inträffade incidenter dokumenteras på övergripande nivå samt analyseras och följs upp som en del i det systematiska förbättringsarbetet.
- Säkerställa att uppföljning av beslutad handlingsplan och kommunens informationssäkerhetsarbete sker genom att etablera en årlig rapportering i form av ledningens genomgång till kommunstyrelsen.

Revisorernas rapport ”Granskning av informationssäkerhet” kan i sin helhet läsas på www.kramfors.se (sökväg via kommun och demokrati, resultat och kvalitet, revisionsrapporter).

För ytterligare information kontakta:
Revisionens ordförande
Bertil Wiklund, tfn 070 – 627 27 37