Kramfors kommun

Kommunrevisionen informerar

2023-09-20

Uppföljande granskning av informationssäkerhet

Granskningens inriktning

KPMG har av Kramfors kommuns revisorer fått i uppdrag att följa upp resultatet av tidigare genomförda granskning av informationssäkerhet från 2021. Uppdraget ingår i revisionsplanen för år 2023.

Det övergripande syftet har varit att bedöma om kommunstyrelse och nämnder har vidtagit åtgärder i enlighet med lämnade rekommendationer för att etablera ett systematiskt och riskbaserat informationssäkerhetsarbete.

Sammanfattning

Vår sammanfattande bedömning är att kommunstyrelsen och de nämnder som ingick i den tidigare granskningen inte i tillräcklig omfattning hörsammat de rekommendationer som lämnades vid granskningen av informationssäkerhet från år 2021.

Vi konstaterar att samtliga rekommendationer som lämnades vid den tidigare granskningen kvarstår helt eller delvis, vilket vi betraktar som mycket allvarligt utifrån de informationssäkerhetsrisker som kommunen därvid exponeras för. Flera av de tidigare rekommendationerna avsåg grundläggande aktiviteter för att kommunen ska bedriva ett systematiskt arbete med informationssäkerhet. Att dessa inte hörsammats utsätter kommunen både för ekonomiska risker men även risk för förtroendeskada om det skulle visa sig att nuvarande skyddsnivåer inte är tillräckliga för att skydda kommunens informationstillgångar.

Vid den uppföljande granskningens genomförande pågick en organisationsförändring med syfte att stärka arbetet inom säkerhet och beredskap, däribland informationssäkerhet. I intervjuer beskrivs den nya organisationen som en förutsättning för att kommunen ska kunna arbeta vidare med åtgärder inom informationssäkerhet, bland annat de rekommendationer som den tidigare granskningen identifierat.

Mot bakgrund av detta ser vi det som väsentligt att kommunstyrelsen följer utvecklingsarbetet och att tillkommande resurser får i uppdrag att påbörja ett förbättringsarbete i enlighet med de rekommendationer och andra åtgärder som kommunen bedömer som nödvändiga för att etablera ett systematiskt och riskbaserat informationssäkerhetsarbete.

Rekommendationer

Mot bakgrund av genomförd uppföljning konstaterar vi att samtliga rekommendationer kvarstår. Vi rekommenderar därför kommunstyrelsen och att prioritera nedanstående:

- 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.
- 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.

Postadress
Kramfors kommun
Revisionen
872 80 Kramfors

E-post
kramfors@kramfors.se

Besöksadress
Torggatan 2

Telefon
0612-800 00

Fax
0612-157 57

Hemsida
www.kramfors.se

Organisationsnr
212000-2429

- 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.

Mot bakgrund av genomförd uppföljning tillkommer följande rekommendation till kommunstyrelsen:

- Säkerställa att den planerade organisationsförstärkningen påbörjar ett strukturerat förbättringsarbete inom informationssäkerhet. Exempelvis genom att inkludera informationssäkerhetsrisker i arbetet med internkontroll och löpande följa upp att arbetet leder till önskat resultat.

Mot bakgrund av genomförd uppföljning konstaterar vi att samtliga rekommendationer kvarstår. Vi rekommenderar därför nämnderna att prioritera nedanstående:

- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- 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.

Mot bakgrund av genomförd uppföljning rekommenderar vi produktionsnämnden att prioritera:

- Om möjligt utveckla rutiner genom en mer automatiserad process som kvalitetssäkrar hantering, uppföljning och kontroll av tilldelade behörigheter.

Revisorernas rapport ”Uppföljande 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 Böhlin, tfn 070 – 555 15 46