

---

Kommunrevisionen

## Revisionsgranskning avseende informationssäkerhet

Kommunrevisionen har begärt att kommunstyrelsen redovisar vilka åtgärder man ämnar vidta med anledning av vad som framkommit i den granskning av informationssäkerhet som gjorts. Nedan redovisas vad som genomförts, vad som pågår och vad som planeras utifrån revisorernas rekommendationer. Rekommendationerna redovisas i punktform och efter varje punkt anges vilka åtgärder som vidtagits.

- Kommunstyrelsen ska ge kommundirektören i uppdrag att, utifrån MSB:s rekommendationer och metodstöd, vidta åtgärder i enlighet med dessa så att kommunen etablerar ett systematiskt och riskbaserat informationssäkerhetsarbete

Kommunstyrelsen har den 11 april beslutat om en *Policy för informationssäkerhet* (bilaga). Antagandet av policyn innebär ett uppdrag till förvaltningen att genomföra åtgärder för att stärka informationssäkerheten enligt de strategiska målsättningar som anges i policyn. Kommundirektören har sedan tidigare tillsatt en informationssäkerhetsgrupp bestående av administrativ chef, kommunjurist och representanter för förvaltningarna. Förslaget till policy har tagits fram av informationssäkerhetsgruppen. Policyn anger bland annat att kommunen ska ha ett ledningssystem för informationssäkerhet, att det ska finnas en hållbar organisation, att utbildning ska genomföras, att informationstillgångar ska informationssäkerhetsklassas, att incidenter ska rapporteras och att kommunen ska ställa relevanta krav på Sydnärke IT och leverantörer vad gäller fysisk och teknisk informationssäkerhet. Informationssäkerhetsgruppens uppdrag är vidta åtgärder för att uppnå de målsättningar som anges i policyn.

- Kommunstyrelsen ska säkerställa att det etableras organisation/funktion med ansvar för att leda och samordna informationssäkerhetsarbetet.

Informationssäkerhetsgruppen har samtidigt som man lämnat förslag på *Policy för informationssäkerhet* också lämnat förslag på *Riktlinjer för informationssäkerhet – organisation och roller*. Kommunstyrelsen beslutade om dessa riktlinjer den 11 april samtidigt som beslut om policyn. Av riktlinjerna framgår att på övergripande nivå ska finnas en informationssäkerhetssamordnare = Chief Information Security Officer (CISO), som tillhör kommunledningsförvaltningen och utgör stödfunktion till förvaltningarna. Rollen kommer tills vidare att upprätthållas av administrativa chefen. På varje förvaltning ska det finnas en informationssäkerhetshandläggare som samordnar informationssäkerhetsarbetet inom respektive förvaltning samt är ett operativt stöd till förvaltningen. Informationssäkerhetshandläggarna bildar tillsammans med informationssäkerhetssamordnaren en informationssäkerhetsgrupp.

- Kommunstyrelsen ska etablera incidenthanteringsrutiner för informationssäkerhet där ansvar och process för hanteringen tydliggörs

Det är en åtgärd som anges i policyn. Förvaltningen har uppdraget och arbetet med att etablera en sådan rutin har påbörjats.



- Kommunstyrelsen ska tydliggöra ansvarsfördelning mellan kommunen och gemensam IT-nämnd inom informationssäkerhetsområdet och fastställa vilka tjänsten som ingår i förvaltningens uppdrag till kommunerna.

Sydnärke IT-nämnd håller på att ta fram ett dokument som ska tydliggöra ansvarsfördelningen mellan kommunen och IT-nämnden inom olika områden. Frågor kring ansvarsfördelning mellan kommunen och nämnden inom informationssäkerhetsområdet bör kunna hanteras i det sammanhanget.

Utgångspunkten är att det är kommunen som äger sina informationstillgångar och ansvarar för informationssäkerheten för dessa. Kommunen behöver därför tydligt gentemot Sydnärke IT kravställa vilken skydds nivå olika informationstillgångar ska ha. Det kan göras först efter det att olika informationstillgångar klassats efter genomförda riskanalyser. Sydnärke IT bör dock oavsett detta ansvara för att upprätthålla en generellt hög grundläggande säkerhetsnivå.

- Kommunstyrelsen ska efterfråga riskanalys och nulägesbeskrivning av den tekniska säkerhet som it-nämnden har etablerat för kommunen för att säkerställa att nuvarande skyddsåtgärder är tillräckliga i förhållande till aktuella hot och risker

Kommunstyrelsen kommer att efterfråga uppgifterna som ett led i den uppsiktskyldighet styrelsen har över nämnderna. Informationssäkerhetsgruppen för en dialog med Sydnärke IT-förvaltning om ansvarsfördelningen och kravställning från kommunen mot förvaltningen vad gäller teknisk säkerhet.

Informationssäkerhetsgruppen har ett tidsbegränsat uppdrag. Kommunledningsgruppen är styrgrupp. De åtgärder som genomförs initialt rapporteras under hösten till styrgruppen. Därefter kommer beslut tas om hur det fortsatta informationssäkerhetsarbetet ska bedrivas.

---

Caroline Dieker (M)  
Kommunstyrelsens ordförande