Granskning av Informationssäkerhet

Rapport

Salems kommun

KPMG AB

2023-09-20

Antal sidor: 13

Innehållsförteckning

Salems kommun
Granskning av Informationssäkerhet

2023-09-20

1 Sammanfattning

KPMG har av Salems kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens, socialnämndens samt barn- och utbildningsnämndens informationssäkerhetsarbete. Granskningen ingår i revisionsplanen för år 2023.

Syftet med granskningen har varit att bedöma om kommunstyrelsen och berörda nämnder bedriver ett systematiskt informationssäkerhetsarbete.

Utifrån genomförd granskning gör vi den samlade bedömningen att kommunstyrelsen och de berörda nämnderna inte fullt ut bedriver ett systematiskt informationssäkerhetsarbete.

Vi bedömer att det i nuläget saknas aktuella styrande dokument som tydliggör ansvar, krav och hur informationssäkerhetsarbetet ska bedrivas. Vi bedömer därför att kommunstyrelsen inte etablerat en tillräcklig styrning av kommunens informationssäkerhetsarbete. Detta tar sig uttryck genom att det vid tid för granskningen inte finns en tydliggjord och dokumenterad ansvarsfördelning, eller kravställning av det operativa informationssäkerhetsarbetet i kommunens verksamheter. I avsaknad av ovanstående bedömer vi att kommunstyrelsen inte har etablerat en ändamålsenlig organisation för informationssäkerhetsarbetet.

Vid tid för granskningen pågår ett aktivt arbete med informationssäkerhet i kommunen där exempelvis riskanalyser och informationsklassningar genomförts. Det är dock av vikt att informationssäkerhetsarbetet systematiseras ytterligare, för att säkerställa att informationsklassningar och riskanalyser genomförs rutinmässigt och att skyddsåtgärder vidtas som klassningar och analyser visar behov av.

Kommunen har etablerade incidenthanteringsrutiner för informationssäkerhetsincidenter. Det är emellertid inte tydligt hur förankrade dessa är i kommunens verksamheter. Kommunen har genomfört kunskapshöjande insatser inom informationssäkerhetsområdet men granskningen visar att det kan finnas ytterligare behov av att höja kunskapen om informationssäkerhet bland medarbetarna samt att förtroendevalda inkluderas vid utbildningsinsatser.

Vi bedömer att uppföljning och rapportering av kommunens samlade informationssäkerhet och det arbete som bedrivs saknas. Således bedömer vi att uppföljningen av informationssäkerhetsarbetet inte är tillräcklig och riskerar att leda till att förbättringsbehov inte identifieras i tillräcklig grad och erforderliga åtgärder inte genomförs i syfte att stärka informationssäkerheten.

Kommunstyrelsen rekommenderas att:

- Fastställa styrande dokument för informationssäkerhetsarbetet
- Tillse att incidenthanteringsrutiner för informationssäkerhetsincidenter är förankrade och kända i kommunens verksamheter
- Etablera en årlig uppföljning av det samlade informationssäkerhetsarbetet
- Säkerställa att informationsklassning och riskbedömningar genomförs avseende den information som styrelsen har ansvar över och som hanteras i system för att säkerställa att informationen har tillräckliga skyddsåtgärder
- Säkerställa att informationssäkerhetsutbildningar genomförs regelbundet för medarbetare och förtroendevalda och att deltagandet följs upp

Salems kommun
Granskning av Informationssäkerhet

2023-09-20

Socialnämnden och barn- och utbildningsnämnden rekommenderas att:

- Säkerställa att informationssäkerhetsarbetet genomförs systematiskt i enlighet med rekommendationer från MSB samt interna styrdokument när dessa fastställts
- Säkerställa att informationsklassning och riskbedömningar genomförs avseende den information som nämnden ansvarar över och som hanteras i system för att säkerställa att informationen har tillräckliga skyddsåtgärder
- Säkerställa att informationssäkerhetsutbildningar genomförs regelbundet och att deltagandet följs upp

2 Bakgrund

KPMG har av Salems kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens och utvalda nämnders informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2023.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete.

Informationssäkerhet innebär att all skyddsvärd information ska vara tillgänglig, konfidentiell och spårbar. Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för kommunen. Det är således väsentligt att kommunen har en tillräcklig intern styrning och kontroll av sitt informationssäkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att arbetet med informationssäkerheten behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningen har syftat till att bedöma om kommunstyrelsen och berörda nämnder bedriver ett systematiskt informationssäkerhetsarbete.

Granskningen har besvarat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
- Har riskanalyser och informationsklassning genomförts för de informationstillgångar som verksamheten ansvarar för?
  - Har säkerhetsåtgärder vidtagits som ett resultat av dessa?
  - Har säkerhetsåtgärderna följts upp?
- Finns etablerade incidenthanteringsrutiner för informationssäkerhetsincidenter?
  - Finns tillräcklig kunskap och medvetenhet hos medarbetare för att identifiera och anmäla incidenter?
  - Inkluderar rutiner eskaleringsvägar och krav på hur incidenter ska dokumenteras och följas upp?
- Finns en etablerad uppföljning av informationssäkerhetsarbetet och rapporteras denna till styrelse och nämnder så att beslut om förbättringsåtgärder kan beslutas?

2.2 Revisionskriterier

I granskningen har vi utgått från följande revisionskriterier:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policyer och beslut
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet

2.3 Ansvarig nämnd/styrelse

Granskningen omfattar kommunstyrelsen, socialnämnden samt barn- och utbildningsnämnden.

2.4 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer/avstämningar med berörda tjänstepersoner.

Vi har granskat följande styrande dokument:

- IT-strategi
- IT-säkerhetsplan
- Riskanalyser och informationsklassningar

Vi har intervjuat följande funktioner:

- Kommundirektör
- Dataskyddsombud
- IT-chef
- Förvaltningschef socialförvaltning
- Förvaltningschef barn- och utbildningsförvaltning
- Medarbetare från respektive förvaltning med insyn i informationssäkerhetsarbetet

3 Inledning

3.1 Metodstöd för systematiskt informationssäkerhetsarbete och säkerhetsåtgärder

Som revisionskriterium i granskningen utgår vi från MSB:s metodstöd och rekommendationer för ett systematiskt informationssäkerhetsarbete och säkerhetsåtgärder med fokus på nedanstående områden.

Standard och krav

Metodstödet bygger på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien och då främst på SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 om ledningssystem för informationssäkerhet.

Ledningssystem för informationssäkerhet

Ett ledningssystem för informationssäkerhet (ofta förkortat LIS) är den del av ledningssystemet som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, som planering och uppföljning. Det innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och kontroller samt ser över styrdokumenten med jämna mellanrum.

Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare om vilka krav som ställs i arbetet. Det är viktigt att alla i en organisation känner till och förstår innehållet i policyer och riktlinjer.

Ansvar och organisation

Metodstödet beskriver hur ansvaret för arbetet med informationssäkerhet bör fördelas i organisationen samt tydliggör betydelsen av ledningens förståelse och engagemang i informationssäkerhetsarbetet för att det ska lyckas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, chefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten. Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Utbildning och kommunikation

MSB:s metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet. Utbildning och kommunikation ökar också acceptansen av och förståelsen för de säkerhetsåtgärder som implementeras.

Riskanalys och informationsklassning

Genom en riskanalys ska verksamheten identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen. Riskanalyser kan göras verksamhetsövergripande, för en process eller för ett enskilt objekt. Risker och potentiella händelser som kan leda till negativa konsekvenser beskrivs och bedöms sedan avseende sannolikheten att de inträffar samt potentiella konsekvenser.

Metodstödet anger vidare att informationsklassning är en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet. Skyddsnivåerna beskriver säkerhetsåtgärder som informationens värde kräver. Identifierat behov av säkerhetsåtgärder utgör ett viktigt underlag vid exempelvis kravställning av tjänster, som interna och externa it-tjänster. De identifierade behoven av säkerhetsåtgärder bör dokumenteras i en åtgärdsplan. IT-säkerhetsåtgärder rent tekniskt kan vara en del men klassningen kan även ha identifierat behov av kompletterande risk- och konsekvensanalyser, förbättrade rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Skyddsåtgärder

Informationstillgångar består av information och resurser som används för att hantera information. Själva informationen är den primära tillgången som ska klassas. Resurser som används för att hantera informationen, till exempel it-system och fysiska tillgångar, samt rutiner i verksamheten ska sedan utformas enligt skyddsnivåer som matchar klassningens resultat. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

I MSB:s föreskrift för säkerhetsåtgärder i informationssystem framgår att systemägaren behöver ha en dialog med berörda informationsägare inom organisationens olika verksamheter för att införa de säkerhetsåtgärder som ger rätt nivå av skydd för informationssystemet. Behovet av säkerhetsåtgärder identifieras utifrån de informationsklassningar och riskbedömningar som informationsägaren har genomfört, samt systemägarens egna riskbedömningar för informationssystemet.

MSB:s metodstöd beskriver att övervakning anger status för ett system, en process eller en aktivitet. Övervakning sker ofta kontinuerligt genom exempelvis att loggar i ett it-system övervakas och avvikelser automatiskt rapporteras. Övervakning och mätning görs för att bedöma om implementerade säkerhetsåtgärder har avsedd verkan och fungerar tillfredsställande.

Uppföljning och förbättringsarbete

För att ledningen ska hållas informerad om informationssäkerhetsarbetets status och därmed kunna besluta om åtgärder utifrån föreslagna förbättringsområden är uppföljning av vikt. Informationssäkerhetssamordnaren bör presentera det samlade informationssäkerhetsarbetet årligen.

3.2 Interna styrdokument

Enligt MSB bör ledningen se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan ledningen ge vägledning till chefer och övriga medarbetare över de krav och förhållningssätt som gäller i informationssäkerhetsarbetet.

I riktlinjer är det vanligt att det förs in bestämmelser om till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet
- incidenthantering
- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning

Det är viktigt att alla i en organisation känner till och förstår innehållet i policyer och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.

4 Resultat

4.1 Styrning och organisering av informationssäkerhetsarbetet

4.1.1 Styrning och ansvarsfördelning

De politiskt antagna styrdokumenten vid tid för granskningen är IT-säkerhetsplan[1] och IT-strategi.[2] Dessa styrdokument är emellertid inte aktuella i nuläget enligt intervjupersoner. I nuläget saknas därigenom en dokumenterad ansvarsfördelning för informationssäkerheten i kommunen.

Av intervjuer framgår att det för arbetet med personuppgiftshanteringen finns etablerade styrdokument med tillhörande mallar och rutiner.

Kommunen har identifierat behov av att upprätta nya styrdokument vilka vi har tagit del av i utkastform. Av intervjuer framgår att utkast till ny IT-policy, IT-strategi samt en informationssäkerhetspolicy med tillhörande riktlinjer i stort är färdigställda. De intervjuade uppger även att utkast för olika stödjande dokument inom informationssäkerhetsområdet är nära färdigställande.

Intervjupersoner menar att de nya styrdokumenten kommer tydliggöra styrning, organisation och ansvarsfördelning av informationssäkerhetsarbetet. Vi har tagit del av utkasten som styrker intervjupersonernas beskrivning.

Ansvar för informationssäkerhet ingår i linjeansvaret. Detta betyder att ansvarig chef för en verksamhet även är ansvarig för den information som hanteras. Intervjupersoner uppger emellertid att det finns utmaningar i att ansvaret etableras hos ansvariga chefer och att informationssäkerhetsarbetet kan genomföras på ett systematiskt sätt. Anledningen uppges främst vara att kommunens chefer har en hög arbetsbelastning, vilket försvårar att aktiviteter och utbildningar prioriteras.

Av intervjuer framgår att samordning och stöd i informationssäkerhetsarbetet i huvudsak utgår från funktionen dataskyddsombud. Även IT-chef och andra funktioner inom IT är involverade i informationssäkerhetsarbetet, exempelvis vad gäller tekniska krav vid upphandling. I nuläget finns inte informationssäkerhetssamordnarrollen etablerad inom kommunen. Intervjupersoner lyfter att de ser ett behov av att rollen inrättas.

4.1.2 Bedömning

Vi bedömer att det i nuläget saknas aktuella styrande dokument som tydliggör ansvar, krav och hur informationssäkerhetsarbetet ska bedrivas. Vi bedömer därför att kommunstyrelsen inte etablerat en tillräcklig styrning av kommunens informationssäkerhetsarbete. Detta tar sig uttryck genom att det vid tid för granskningen inte finns en tydliggjord och dokumenterad ansvarsfördelning, eller kravställning av det operativa informationssäkerhetsarbetet i kommunens verksamheter. I avsaknad av ovanstående bedömer vi att kommunstyrelsen inte har etablerat en ändamålsenlig organisation för informationssäkerhetsarbetet men uppfattar att ansvar i enlighet med linjeansvaret är känt och accepterat. Däremot lyfts en

[1] KF, 2010-09-30, §§ framgår ej.
[2] 2011-10-26, beslutsinstans och §§ framgår ej.

risk med att alltför hög arbetsbelastning påverkar ansvariga chefers förutsättningar att säkerställa ett systematiskt informationssäkerhetsarbete. Avsaknaden av en informationssäkerhetssamordnare är inte i enlighet med MSB:s rekommendationer för informationssäkerhet. Därtill upplever även intervjupersoner att informationssäkerhetssamordnarrollen bör etableras inom kommunen, varför vi anser att kommunen bör undersöka huruvida befintliga avsatta resurser för informationssäkerhetsarbetet är tillräckliga för det skall ske med systematik.

Vad gäller arbetet som bedrivs utifrån dataskyddsförordningen finns en tydligare styrning, vilket gett effekt på arbetet med personuppgiftshantering som vi bedömer sker utifrån en tydligare ansvarsfördelning och med en högre grad av systematik.

Vi noterar att det finns flera framtagna utkast på styrande dokument som vi bedömer skapar förutsättningar för en mer ändamålsenlig styrning och organisering av informationssäkerhetsarbetet.

4.2 Riskbedömning och åtgärder

4.2.1 Informationsklassning

Enligt MSB:s metodstöd är informationsklassning en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Nuvarande styrdokument saknar reglering och krav på genomförande av informationsklassningar. Intervjuade beskriver dock att det pågår ett aktivt arbete med informationsklassning och att modellen KLASSA används i arbetet.[3] Dataskyddsombud är den som initierat arbetssättet med klassningar och håller även regelbundna utbildningar för att sprida kunskap om hur klassningar går till och hur verktyget fungerar. Kopplat till klassningsarbetet genomför dataskyddsombudet skrivarstugor där förvaltningarna får stöd och hjälp i det operativa arbetet.

Intervjupersoner från social- och barn- och utbildningsförvaltningarna uppger att de i nuläget arbetar med att klassa sina verksamhetssystem. Vidare har båda förvaltningarna inlett arbete med riskanalys och genomför sådana i viss utsträckning vid anskaffning av nya verksamhetssystem. Vi har tagit del av genomförda informationsklassningar och riskanalyser som styrker intervjupersonernas beskrivning.

Arbetet med riskanalys och informationsklassning uppges i huvudsak ske med systematik, men intervjupersoner ser vissa förbättringsområden då det finns exempel på när detta inte har gjorts vid upphandling med resultatet att system köpts in som sedan inte har kunnat nyttjats på grund av att de inte uppnår säkerhetskraven.

Kommunens dataskyddsombud stödjer i hög utsträckning förvaltningarna i arbetet med informationsklassningar. Att dataskyddsombudet aktivt deltar i informationsklassningar lyfts som en risk för att det kan påverka dennes oberoende i tillsynen. Detta då ombudet varit delaktig i det operativa arbetet som sedan funktionen har i uppdrag att utöva tillsyn mot.

4.2.2 Bedömning

[3] KLASSA är ett verktyg för informationsklassning som tillhandahålls av SKR och används av kommunen.

Det saknas i styrdokument reglering över krav på riskanalyser och informationsklassning. Vi bedömer att informationsklassning och riskanalyser till stor del har gjorts för de informationstillgångar som förvaltningarna ansvarar för och att arbete pågår för att samtliga system ska vara klassade. Vi bedömer dock att arbetet ytterligare kan stärkas genom att verksamheten säkerställer genom regelbunden uppföljning att de skyddsåtgärder som klassning visat behov och krav på etableras och utvärderas.

4.3 Säkerhetsmedvetenhet och incidenthantering

4.3.1 Säkerhetsmedvetenhet och kunskapshöjande insatser

Intervjuade beskriver att kommunen i hög grad är i en förändringsresa där medvetenheten stärkts kontinuerligt de senaste åren. Dels som ett resultat av nyanställningar på vissa funktioner som etablerat ett mer systematiskt arbetssätt, främst inom dataskyddsfrågor. Dels utifrån omvärldsläget med större fokus på risker och säkerhetsarbete på en övergripande nivå. Kommunchef och kommunstyrelsens ordförande får bland annat information genom deltagande i regionala rådet.

Kommunen har genomfört ett antal kunskapshöjande insatser inom informationssäkerhet som riktar sig till chefer och medarbetare. Förtroendevalda har inte inkluderats i utbildningsinsatser.

MSB:s digitala utbildning inom informationssäkerhet, DISA[4], genomförs löpande sedan 2021 och finns tillgänglig på intranätet. Vid introduktion av nyanställda ingår också stående punkter rörande informationssäkerhet. Andra utbildningar som genomförts är genomgång av informationsklassningsverktyget KLASSA till chefer och berörda medarbetare.

Som vi nämnt tidigare så finns en uppfattning att chefer inte i tillräcklig grad har förutsättningar att prioritera utbildningar inom informationssäkerhet vilket kan riskera att påverka hur arbetet bedrivs och hur säkerhetsmedvetenheten etableras inom respektive verksamhet. Intervjupersoner lyfter även en önskan om att ytterligare insatser genomförs i syfte att höja kunskapsnivån hos medarbetare rörande informationssäkerhet för att säkerställa en säkerhetsmedvetenhet.

4.3.2 Incidenthanteringsrutiner

Intervjupersoner uppger att kommunen har två huvudsakliga rutiner för incidenthantering. En avser personuppgiftsincidenter och den andra avser IT-ärenden och incidenter. Båda dessa incidenthanteringsrutiner finns tillgängliga för medarbetare på kommunens intranät. Till rutinen för IT-ärenden och incidenter finns en eskaleringsfunktion som medarbetare har möjlighet att nyttja beroende på incidentens allvarsgrad. Av intervjuer framgår att personuppgiftsincidenter dokumenteras och analyseras, samt presenteras för kommunstyrelsen.[5] Detta gäller dock inte informationsincidenter, utan endast incidenter avseende personuppgifter.

[4] Digital informationssäkerhetsutbildning för alla
[5] Personuppgiftsincidenter rapporteras till den nämnd/styrelse som är personuppgiftsansvarig samt i förekommande fall även till tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY). Detta enligt bestämmelserna i Dataskyddsförordningen.

4.3.3 Bedömning

Vi bedömer att det finns etablerade incidenthanteringsrutiner med tillhörande eskaleringsvägar för informationssäkerhetsincidenter.

Vi bedömer att det till viss del finns en tillräcklig kunskap och medvetenhet hos medarbetare för att identifiera och anmäla incidenter. Utbildningar har genomförts i viss utsträckning i syfte att etablera en säkerhetsmedvetenhet samt för att etablera kunskap om informationsklassning och riskanalyser inom området. Vi ser dock att utbildningar bör följas upp regelbundet samt att förtroendevalda i kommunen inkluderas.

Vi har däremot inte utifrån den information och underlag vi fått del av kunnat bedöma om incidenthanteringsrutinerna är kända av medarbetare eller om säkerhetsmedvetenheten är tillräcklig i syfte att hindra att incidenter sker eller upptäcks i tillräckligt hög grad.

Vi bedömer att incidenter förvisso dokumenteras och sammanställs för analys vad gäller personuppgiftsincidenter, men att detta inte görs för informationsincidenter i stort. Det är av vikt att informationsincidenter dokumenteras så att de samlat kan analyseras och återrapporteras till kommunledning och/eller förtroendevalda.

4.4 Uppföljning och återrapportering

Styrande dokument reglerar inte hur uppföljning och återrapportering av informationssäkerhetsarbetet ska ske. Intervjuade uppger att kommunstyrelsen i nuläget inte erhåller någon samlad uppföljning och rapportering avseende kommunens informationssäkerhet eller det arbete som genomförs.

Dataskyddsombudet har däremot en årlig rapportering rörande nämndernas personuppgiftsarbete. Vi har tagit del av rapporteringen för kommunstyrelsens personuppgiftsarbete. Av kommunstyrelsens tillsynsrapport framgår att det finns brister i kommunstyrelsens personuppgiftshantering. Exempelvis framgår brister i den samlade registerförteckningen, då förvaltningar inte fyllt i förteckningen fullt ut, inte förstått vilken information som efterfrågas, angett en kontaktperson som inte längre är anställd, etcetera. Av protokoll[6] framgår att kommunstyrelsen tagit del av rapporten och godkänt kommunstyrelseförvaltningens åtgärdsplan med anledning av de brister som noterats.

4.4.1 Bedömning

Vi bedömer att uppföljning och rapportering av kommunens samlade informationssäkerhet och det arbete som bedrivs saknas. Vi kan konstatera att den rapportering som genomförs i nuläget främst avser nämnders och styrelsers personuppgiftsansvar.

Således bedömer vi att uppföljningen av informationssäkerhetsarbetet inte är tillräcklig och riskerar att leda till att förbättringsbehov inte identifieras i tillräcklig grad och erforderliga åtgärder inte genomförs i syfte att stärka informationssäkerheten.

[6] KS 2023-03-06 § 19.

Salems kommun
Granskning av Informationssäkerhet

2023-09-20

5 Slutsats och rekommendationer

Utifrån genomförd granskning gör vi den samlade bedömningen att kommunstyrelsen och de berörda nämnderna inte fullt ut bedriver ett systematiskt informationssäkerhetsarbete.

Vi bedömer att det i nuläget saknas aktuella styrande dokument som tydliggör ansvar, krav och hur informationssäkerhetsarbetet ska bedrivas. Vi bedömer därför att kommunstyrelsen inte etablerat en tillräcklig styrning av kommunens informationssäkerhetsarbete. Detta tar sig uttryck genom att det vid tid för granskningen inte finns en tydliggjord och dokumenterad ansvarsfördelning, eller kravställning av det operativa informationssäkerhetsarbetet i kommunens verksamheter. I avsaknad av ovanstående bedömer vi att kommunstyrelsen inte har etablerat en ändamålsenlig organisation för informationssäkerhetsarbetet.

Vid tid för granskningen pågår ett aktivt arbete med informationssäkerhet i kommunen där exempelvis riskanalyser och informationsklassningar genomförts. Det är dock av vikt att informationssäkerhetsarbetet systematiseras ytterligare, för att säkerställa att informationsklassningar och riskanalyser genomförs rutinmässigt och att skyddsåtgärder vidtas som klassningar och analyser visar behov av.

Kommunen har etablerade incidenthanteringsrutiner för informationssäkerhetsincidenter. Det är emellertid inte tydligt hur förankrade dessa är i kommunens verksamheter. Kommunen har genomfört kunskapshöjande insatser inom informationssäkerhetsområdet men granskningen visar att det kan finnas ytterligare behov av att höja kunskapen om informationssäkerhet bland medarbetarna samt att förtroendevalda inkluderas i utbildningsinsatser.

Vi bedömer att uppföljning och rapportering av kommunens samlade informationssäkerhet och det arbete som bedrivs saknas. Således bedömer vi att uppföljningen av informationssäkerhetsarbetet inte är tillräcklig och riskerar att leda till att förbättringsbehov inte identifieras i tillräcklig grad och erforderliga åtgärder inte genomförs i syfte att stärka informationssäkerheten.

Kommunstyrelsen rekommenderas att:

- Fastställa styrande dokument för informationssäkerhetsarbetet
- Tillse att incidenthanteringsrutiner för informationssäkerhetsincidenter är förankrade och kända i kommunens verksamheter
- Etablera en årlig uppföljning av det samlade informationssäkerhetsarbetet
- Säkerställa att informationsklassning och riskbedömningar genomförs avseende den information som styrelsen har ansvar över och som hanteras i system för att säkerställa att informationen har tillräckliga skyddsåtgärder
- Säkerställa att informationssäkerhetsutbildningar genomförs regelbundet för medarbetare och förtroendevalda och att deltagandet följs upp

Socialnämnden och barn-och utbildningsnämnden rekommenderas att:

- Säkerställa att informationssäkerhetsarbetet genomförs systematiskt i enlighet med rekommendationer från MSB samt interna styrdokument när dessa fastställts

- Säkerställa att informationsklassning och riskbedömningar genomförs avseende den information som nämnden över och som hanteras i system för att säkerställa att informationen har tillräckliga skyddsåtgärder
- Säkerställa att informationssäkerhetsutbildningar genomförs regelbundet och att deltagandet följs upp

2023-09-20

KPMG AB

Anders Peterson

Certifierad kommunal yrkesrevisor

Jenny Thörn

Verksamhetsrevisor

William Andreasson

Verksamhetsrevisor