Hedemora välkomnar

Kommunrevisionen 2023-03-13

Till:
Kommunfullmäktige

För kännedom:
Kommunstyrelsen
Omsorgsnämnden
Bildningsnämnden
Miljö- samhällsbyggnadsnämnden

Granskning av informationssäkerhet

KPMG har på uppdrag av Hedemora kommuns revisorer genomfört en granskning om kommunstyrelsen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen. Uppdraget ingår i revisionsplanen för år 2022.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen till viss del har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Kommunen har en dokumenterad styrning inom området där roller, funktioner och ansvar finns beskrivet men det finns behov av att implementera detta i organisationen för att säkerställa att aktiviteter genomförs i den utsträckning som krävs för att uppnå en god informationssäkerhet. Vår uppfattning är därtill att den ansvarsfördelning som anges för IT-säkerhet inte är korrekt, detta då styrande dokument anger att ansvaret för IT-säkerhet följer linjeansvaret. Vanligtvis innehar inte förvaltningschefer kompetens eller förutsättningar att ansvara för den it-tekniska säkerheten och vår bedömning är därför att ansvarsfördelningen bör justeras och det IT-tekniska ansvaret bör ligga inom IT-avdelningen på IT-chef eller på annan utsedd funktion inom IT-avdelningen.

Aktiviteter som informationsklassning och riskbedömning genomförs i kommunen, däremot kan systematiken i arbetet stärkas ytterligare i syfte att efterleva styrande dokument samt för att säkerställa att brister i systemsäkerhet samt felaktig hantering av information identifieras i tillräcklig utsträckning.

För att säkerställa medarbetarnas medverkan i de utbildningsinsatser som genomförs bör kommunstyrelsen och nämnderna säkerställa att uppföljning av utbildningarna genomförs. En uppföljning kan även visa om det finns behov av ytterligare åtgärder, som exempelvis informationsinsatser på arbetsplatsträffar.

Utöver detta anser vi att kommunstyrelsen bör säkerställa att åtgärder vidtas utifrån det som framkommit av genomförda sårbarhetsskanningar samt att uppföljning genomförs av IT-säkerhetsåtgärder genomförs på ett systematiskt sätt i syfte att följa upp åtgärdernas effekt. Som en del i det förebyggande arbetet bör kommunen även se över möjligheterna att möta

verksamheternas behov av säkerhetskopiering samt se över möjligheterna att införa tvåfaktorautentisering.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen i sitt övergripande ansvar för styrning och uppföljning att:

- Säkerställa att roller, funktioner och ansvar kommuniceras i organisationen så att var en och upprätthåller sitt ansvar i enlighet med styrande dokument.
- Justera det dokumenterade ansvaret för IT-säkerhet från verksamhetsansvariga till IT-avdelningen/utsedd funktion så att lämplig kompetens innehar det it-tekniska säkerhetsansvaret.
- Säkerställa att riktlinjer för incidenthantering implementeras i organisationen.
- Säkerställa att incidenter analyseras på en kommunövergripande nivå i syfte att identifiera eventuella behov av åtgärder
- I uppföljningsarbetet inkludera efterlevnad av styrande dokument.
- Säkerställa att åtgärder vid behov beslutas utifrån den uppföljning och rapportering av det övergripande säkerhetsarbetet som styrelsen tar del av.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen och nämnderna inom sitt verksamhetsansvar för informationssäkerhet att:

- Säkerställa att informationstillgångar klassificeras samt att omklassningen genomförs i enlighet med styrande dokument.
- Säkerställa att former för kontroller av behörighetstilldelning upprättas samt att kontroller genomförs i syfte att undvika otillbörlig informationstillgång.
- Vidta åtgärder i syfte att öka medvetenhet och kunskap avseende säker hantering av information samt vad som definierar en incident i syfte att nå ett förändrat beteende hos kommunens medarbetare.
- Säkerställa att IT-säkerhetsarbetet utgår från genomförda riskanalyser.
- Säkerställa att åtgärder vidtas utifrån genomförda sårbarhetsskanningar i syfte att upprätthålla ett tillräckligt fysiskt och digitalt skydd.
- Se över möjligheterna att möta verksamheternas behov av säkerhetskopiering.

Revisionen rekommenderar fullmäktige att begära in ett yttrande avseende de förbättringsområden och rekommendationer som framgår av revisionsrapporten från kommunstyrelsen och berörda nämnder till fullmäktiges sammanträde den 27 juni år 2023.

Yttrandet bör även lämnas till revisionen för kännedom.

För de förtroendevalda revisorerna i Hedemora kommun.

DocuSigned by:
Jan Erik Ohlans
7FD128E8BEBB47C...
Jan-Erik Ohlans
Ordförande i kommunrevisionen

Granskning av informationssäkerhet

Rapport
Hedemora kommun

KPMG AB

2023-02-28

Antal sidor 23

Hedemora kommun
Granskning av informationssäkerhet

2023-02-28

Innehållsförteckning

1 Sammanfattning

KPMG har av Hedemora kommuns revisorer fått i uppdrag att granska om kommunstyrelsen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen. Uppdraget ingår i revisionsplanen för år 2022.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen till viss del har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Kommunen har en dokumenterad styrning inom området där roller, funktioner och ansvar finns beskrivet men det finns behov av att implementera detta i organisationen för att säkerställa att aktiviteter genomförs i den utsträckning som krävs för att uppnå en god informationssäkerhet. Vår uppfattning är därtill att den ansvarsfördelning som anges för it-säkerhet inte är korrekt, detta då styrande dokument anger att ansvaret för it-säkerhet följer linjeansvaret. Vanligtvis innehar inte förvaltningschefer kompetens eller förutsättningar att ansvara för den it-tekniska säkerheten och vår bedömning är därför att ansvarsfördelningen bör justeras och det it-tekniska ansvaret bör ligga inom it-avdelningen på it-chef eller på annan utsedd funktion inom it-avdelningen.

Aktiviteter som informationsklassning och riskbedömning genomförs i kommunen, däremot kan systematiken i arbetet stärkas ytterligare i syfte att efterleva styrande dokument samt för att säkerställa att brister i systemsäkerhet samt felaktig hantering av information identifieras i tillräcklig utsträckning.

För att säkerställa medarbetarnas medverkan i de utbildningsinsatser som genomförs bör kommunstyrelsen och nämnderna säkerställa att uppföljning av utbildningarna genomförs. En uppföljning kan även visa om det finns behov av ytterligare åtgärder, som exempelvis informationsinsatser på arbetsplatsträffar.

Utöver detta anser vi att kommunstyrelsen bör säkerställa att åtgärder vidtas utifrån det som framkommit av genomförda sårbarhetsskanningar samt att uppföljning genomförs av it-säkerhetsåtgärder genomförs på ett systematiskt sätt i syfte att följa upp åtgärdernas effekt. Som en del i det förebyggande arbetet bör kommunen även se över möjligheterna att möta verksamheternas behov av säkerhetskopiering samt se över möjligheterna att införa tvåfaktorautentisering.

Då säkerhetsrapporten för år 2022 sammanställs under granskningsperioden kan vi inte göra bedömning om det uppföljningsarbete som sker är ändamålsenligt.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen i sitt övergripande ansvar för styrning och uppföljning att:

- Säkerställa att roller, funktioner och ansvar kommuniceras i organisationen så att var en och upprätthåller sitt ansvar i enlighet med styrande dokument.
- Justera det dokumenterade ansvaret för it-säkerhet från verksamhetsansvariga till it-avdelningen/utsedd funktion så att lämplig kompetens innehar det it-tekniska säkerhetsansvaret.
- Säkerställa att riktlinjer för incidenthantering implementeras i organisationen.
- Säkerställa att incidenter analyseras på en kommunövergripande nivå i syfte att identifiera eventuella behov av åtgärder
- I uppföljningsarbetet inkludera efterlevnad av styrande dokument.
- Säkerställa att åtgärder vid behov beslutas utifrån den uppföljning och rapportering av det övergripande säkerhetsarbetet som styrelsen tar del av.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen och nämnderna inom sitt verksamhetsansvar för informationssäkerhet att:

- Säkerställa att informationstillgångar klassificeras samt att omklassningen genomförs i enlighet med styrande dokument.
- Säkerställa att former för kontroller av behörighetstilldelning upprättas samt att kontroller genomförs i syfte att undvika otillbörlig informationstillgång.
- Vidta åtgärder i syfte att öka medvetenhet och kunskap avseende säker hantering av information samt vad som definierar en incident i syfte att nå ett förändrat beteende hos kommunens medarbetare.
- Säkerställa att it-säkerhetsarbetet utgår från genomförda riskanalyser.
- Säkerställa att åtgärder vidtas utifrån genomförda sårbarhetsskanningar i syfte att upprätthålla ett tillräckligt fysiskt och digitalt skydd.
- Se över möjligheterna att möta verksamheternas behov av säkerhetskopiering.

2 Bakgrund

KPMG har av Hedemora kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används om informationssäkerhet för information som hanteras i kommunens IT-system. Alltmer information hanteras idag med olika tekniska lösningar och aldrig förr har kommunerna hanterat sådana mängder information som görs idag. Informationssäkerhet innebär att skydda information utifrån dess krav på konfidentialitet, riktighet och tillgänglighet i alla kommunens system. För att kunna hantera detta på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget. Informationssäkerhet är inte en IT-fråga utan en fråga om att säkra och trygga driften av kommunens kärnverksamheter.

Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd.

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

2.1 Syfte, revisionsfrågor och avgränsning

Granskningens syfte har varit att bedöma om kommunstyrelsen har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Granskningen har besvarat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhet?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?
- Sker en kravställning av IT-säkerhetsåtgärder utifrån genomförd riskbedömning och klassning av informationstillgångar som hanteras i system?
- Finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.)?
- Finns incidenthanteringsrutiner och sker en tillräcklig rapportering av inträffade incidenter?

- Görs systematiska uppföljningar av implementerade säkerhetsåtgärder för att kontinuerligt förbättra informationssäkerheten?
- Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?

Granskningen omfattar kommunstyrelsen, omsorgsnämnden, bildningsnämnden samt miljö- och samhällsbyggnadsnämnden.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- 6 kap. 6 § kommunallagen (2017:725)
- Tillämpbara interna regelverk, policys och beslut
- MSB[1]:s rekommendationer avseende Ledningssystem för informationssäkerhet och säkerhetsåtgärder

2.3 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

- Informationssäkerhetspolicy och dataskyddsstrategi
- Riktlinje för informationssäkerhet- och dataskydd
- Handlingsplan för informationssäkerhet, dataskydd och digitalisering
- Riktlinje för GDPR
- Rutiner för rapportering av informationssäkerhetsincident
- Mall för systemdokumentation
- Informationssäkerhetsinstruktion för ett verksamhetssystem
- Uppföljning informationssäkerhet 2020
- Internkontrollplan, Kommunstyrelsen, 2022

[1] Myndigheten för samhällsskydd och beredskap. MSB har på uppdrag av regeringen ansvar att vara råd- och stödgivande i informationssäkerhetsarbetet och hantera samt förebygga IT-incidenter.

Intervjuer har skett med följande:

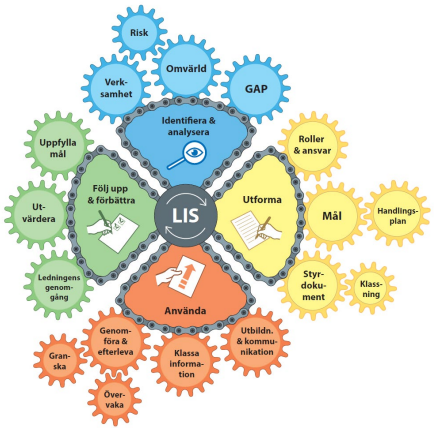
- Kommundirektör
- Informationssäkerhetssamordnare
- It-chef
- Förvaltningschef barn- och utbildningsförvaltningen
- Förvaltningschef och systemförvaltare inom miljö- och samhällsbyggnadsförvaltningen
- Förvaltningschef och systemförvaltare inom omsorgsförvaltningen

Samtliga intervjuade har fått möjlighet att faktakontrollera rapporten.

2.4 Metodstöd för systematiskt informationssäkerhetsarbete

MSB har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet baserat på den internationella standardserien för informationssäkerhet, ISO/IEC 27000, och ämnar till att förtydliga hur informationssäkerhetsarbetet kan utformas.

Metodstödet består av fyra olika metodsteg för informationssäkerhetsarbetet vilka illustreras i nedanstående figur.



2.4.1 Identifiera och analyser

Syftet med att analysera informationssäkerhetsarbetet är enligt MSB att säkerställa att informationssäkerheten utformas utifrån verksamhetens rådande förutsättningar. Det ska även leda till att väsentliga informationstillgångar identifieras, vilka risker de ska skyddas mot, samt valda säkerhetsåtgärder.

2.4.2 Utforma

Enligt MSB:s metodstöd behövs följande delar för ett systematiskt informationssäkerhetsarbete:

- Organisation
- Informationssäkerhetsmål
- Styrdokument
- Klassningsmodell
- Handlingsplan
- Kontinuitetshantering för informationstillgångar

2.4.3 Använda

När verksamheten har utformat styrningen enligt avsnitt 2.4.2 ska det tillämpas. Det innebär:

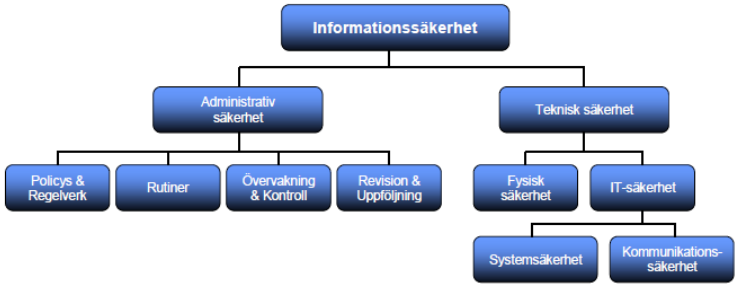
- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet.
- Utbilda och kommunicera informationssäkerhetsfrågor till organisationens medarbetare. Det är ständigt pågående arbete som är nödvändigt för att skapa ett systematiskt informationsarbete.

2.4.4 Följa upp och förbättra

Informationssäkerhetsarbetet ska utvärderas och följas upp för att säkerställa att arbetets fortsatta lämplighet, tillräcklighet och verkan. Det kan enligt MSB ske genom övervakning, mätning och måluppföljning.

2.4.5 Roller och ansvar

Informationssäkerhetsbegreppet och dess innehåll kan översiktligt beskrivas i nedanstående skiss:



Informationssäkerhetsarbetet kan struktureras i ett Ledningssystem för informationssäkerhet, kallat LIS. I ett sådant har verksamheten tydliggjort krav som ställs genom styrande dokument och hur ansvaret är fördelat.

En central del i ett ledningssystem, är enligt MSB, ledningens uttalade stöd. Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledningen till chefer och övriga medarbetare. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenhet visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete. En stor del av arbetet med att driva ett ledningssystem handlar därför om att informera medarbetare om de regler som ingår i ledningssystemet.

Den svenska och internationella standardserien SS-ISO/IEC 27000 visar på ett sådant ledningssystem där säkerhetsnivån tar sin utgångspunkt i en verksamhetsanpassad riskanalys, och där informationssäkerhetsarbetet följer en tydlig process. Tillämpning av standarderna enligt denna serie underlättar arbetet med informationssäkerhet inom organisationer och förbättrar också möjligheterna att externt bedöma säkerhet och revidera denna på ett enhetligt sätt.

Enligt MSB:s metodstöd för hur ett systematiskt informationssäkerhetsarbete kan bedrivas framgår det hur ansvaret för arbetet med informationssäkerhet bör fördelas. 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, verksamhetschefer 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.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men bör generellt vara placerad nära ledning, exempelvis i ledningsstaben. Vanliga organisatoriska placeringar, enligt MSB:s metodstöd är exempelvis:

- Säkerhet
- Kvalitet
- Juridik

I de fall rollen är placerad i en strategisk IT-funktion bör funktionen vara åtskilda från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetssamordnaren både ska granska och vara kravställande gentemot IT-drift och riskerar annars att brista i opartiskhet.

3 Resultat av granskningen

3.1 Organisation

3.1.1 Styrande dokument

Kommunfullmäktige har i ett gemensamt dokument antagit en Informationssäkerhetspolicy och Dataskyddsstrategi. Syftet med dokumentet är bland annat att tydliggöra mål, principer och arbetssätt för informationssäkerhet- och dataskyddsarbetet i kommunen. Utöver detta regleras även uppföljning och utvärdering samt definition av information, informationssäkerhet och dataskydd.

Därtill har kommunstyrelsen antagit en riktlinje för informationssäkerhet och dataskydd[2]. Syftet med dokumentet är att konkretisera informationssäkerhetspolicyn och dataskyddsstrategin med mer detaljerad information och regler för hur information får hanteras inom kommunen. Av dokumentet framgår att det utgör ledningssystem för informationssäkerhet. Dokumentet innehåller även en introduktion till informationssäkerhet och dataskydd.

Kommunstyrelsen har därtill antagit en handlingsplan[3] som beskriver kommunens informationssäkerhets- och dataskyddsorganisation samt digitaliseringsutvecklingsorganisation. I handlingsplanen redogörs att ansvaret för information, informationssäkerhet och dataskydd följer det ordinarie verksamhetsansvaret. Det innebär att den som är ansvarig för en viss verksamhet också är ansvarig för information, informationssäkerhet och dataskydd inom verksamhetsområdet.

I syfte att organisera kommunens dataskyddsarbete och reglera kommunens förhållningssätt gentemot dataskyddsförordningen har kommunstyrelsen antagit en riktlinje för GDPR[4] (General Data Protection Regulation). Av dokumentet framgår att all verksamhet i kommunen ska arbeta utifrån principerna inbyggt dataskydd samt dataskydd som standard. Inbyggt dataskydd innebär att verksamheterna ska ha ett ständigt tekniskt och organisatoriskt förbättringsarbete. Dataskydd som standard innebär att personuppgiftsansvarige i standardfallet inte ska behandla personuppgifter utan att det är nödvändigt. Vidare framgår att syftet med GDPR-arbetet är att stärka integritetsskyddet för enskilda personer.

Utöver detta finns en framtagen mall för systemdokumentation. Mallen är en del av kommunens it-säkerhetsarbete och ska fyllas i för de system som kommunen

[2] Riktlinje för informationssäkerhet och dataskydd, kommunstyrelsen, 2022-05-17

[3] Handlingsplan, kommunstyrelsen, 2022-05-17

[4] Riktlinje för GDPR, kommunstyrelsen, 2022-05-17

införskaffar. Syftet med dokumentet är att systemets användare på ett enkelt sätt ska hitta information och rutiner rörande systemet. Information som efterfrågas i mallen är bland annat klassning av information, styrning av åtkomst, driftsäkerhet, logghantering, kontinuitetshantering, incidentrapportering samt förvaltningsplan.

3.1.2 Roller och ansvar

Av handlingsplanen framgår att kommunstyrelsen innehar det yttersta ansvaret för säkerheten i kommunen. Varje nämnd har sedan det yttersta ansvaret inom sin verksamhet och de är även personuppgiftsansvarig.

Som tidigare nämnts är grundprincipen att ansvaret för informationssäkerhetsarbetet följer det ordinarie verksamhetsansvaret. Det är därigenom förvaltningschef eller motsvarande som är informationsägare och som innehar ansvar att säkerställa att informationshanteringen sker på ett korrekt sätt utifrån interna styrdokument och lagkrav.

Av handlingsplanen framgår även att det är informationsägaren som är systemägare. Det är sedan systemägaren som utser systemförvaltare och enligt uppgift är dessa etablerade på kommunens förvaltningar. Systemförvaltaren har enligt handlingsplanen ansvaret för den dagliga användningen av objektet (it-systemet) och samverkar med systemadministratör för att säkerställa en säker och rationell daglig drift av it-systemet och andra it-resurser. Systemförvaltaren ansvarar även för hantering av tekniska sårbarheter. Intervjupersoner uppger att det finns behov av att tydliggöra systemförvaltaren och systemägarens roll samt att det finns ett behov av att införa ställföreträdande systemägare då förvaltningschefer som innehar den rollen utifrån arbetsbelastning inte har möjlighet att fullfölja sitt ansvar som systemägare.

Som stöd till verksamheterna att fullfölja sitt ansvar för informationssäkerhetsarbetet finns en centralt placerad informationssäkerhetssamordnare. I Hedemora kommun är det säkerhetschefen som även innehar funktionen informationssäkerhetssamordnare. Funktionen har enligt handlingsplanen i uppdrag att samordna, leda och styra informationssäkerhetsarbetet utifrån ett strategiskt perspektiv i organisationen. Vidare har funktionen även ansvar för att samordna informationsklassningsarbetet samt genomförda risk- och sårbarhetsanalyser. Samordnaren ska även i sin roll utforma och förvalta arbetssätt och processer för informationssäkerhetsarbetet, till exempel riskhantering, informationsklassning och incidenthantering. Intervjupersoner lyfter att det finns ett behov av en informationssäkerhetssamordnare med förutsättningar att lägga större andel av sin arbetstid för att de uppgifter som samordnaren har ansvar för ska kunna etableras fullt ut.

Av riktlinjerna för informationssäkerhet framgår att ansvaret för it-säkerheten i Hedemora kommun följer verksamhetsansvaret, likt ansvaret för informationssäkerhet. It-chefen i kommunen har enligt handlingsplanen det övergripande ansvaret inför kommunstyrelsen för kommunens it-infrastruktur och för att it-system, applikationer och plattformars tekniska delar fungerar.

Enligt handlingsplanen ansvarar driftansvarig tillsammans med systemförvaltaren för att den dagliga driften av objektet upprätthålls enligt överenskommelse mellan informationsägaren och it-chef samt informationsägarens instruktioner.

Kommunen har även upprättat ett informationssäkerhets- och dataskyddsråd. I rådet ingår följande funktioner: säkerhetschef (tillika informationssäkerhets- och dataskyddssamordnare), it-chef, kommunsekreterare, arkivarie, digitaliseringsledare, digitaliseringsutvecklare från vardera bolagen, Hedemora Energi AB med dotterbolags it-ansvarig, kommunjurist och dataskyddsombud). Rådet träffas ca en gång i kvartalet.

Kommunen har även en dataskyddssamordningsgrupp, dataskyddsspecialist samt ett dataskyddsombud.

I intervjuer får vi en delad bild om ansvarsfördelningen mellan roller och funktioner är etablerad i kommunen och att det kan finnas behov av att detta förtydligas ytterligare. Vidare uppges att det finns en viss otydlighet vilken typ av stöd som centrala funktioner ska bistå verksamheterna med.

3.1.3 Bedömning

Vår bedömning är att kommunstyrelsen har beslutat om styrande och stödjande dokument avseende informationssäkerhetsarbetet. Kommunen har ett dokumenterat ledningssystem men vår bedömning är att detta till viss del inte är etablerat i organisationen.

Vår bedömning är att det saknas ett tydliggörande av it-avdelningens ansvar och uppdrag avseende it-säkerheten i nuvarande styrdokument. Vår uppfattning är därtill att den ansvarsfördelning som anges för it-säkerhet inte är korrekt, detta då styrande dokument anger att ansvaret för it-säkerhet följer linjeansvaret. Vanligtvis innehar inte förvaltningschefer kompetens eller förutsättningar att ansvara för den it-tekniska säkerheten och vår bedömning är därför att ansvarsfördelningen bör justeras och det it-tekniska ansvaret bör ligga inom it-avdelningen på it-chef eller på annan utsedd funktion inom it-avdelningen.

Vidare är vår bedömning att det är tydliggjort i styrdokument vilka funktioner och roller som är centrala i informationssäkerhetsarbetet. Vår bedömning av det som framkommer i granskningen är att rollerna är etablerade i kommunen men kan samtidigt konstatera att ansvar inte upprätthålls fullt ut då informationssäkerhetsarbetet

inte når upp till att vara systematiskt. Vi ser att roller och ansvar skulle behöva kommuniceras ytterligare inom organisationen.

Vi kan konstatera att kommunen följer MSB:s rekommendation om att ha en utsedd informationssäkerhetssamordnare. Dock gör vi bedömningen att kommunstyrelsen bör utvärdera om de uppgifter som samordnaren enligt styrdokument har i ansvar att genomföra står i relation till nuvarande förutsättningar att lägga tid på arbetet. Detta för att säkerställa att funktionen kan upprätthålla ansvar i enlighet med den beskrivning som ges i den fastställda handlingsplanen.

3.2 Analys av behov och risker för informationssäkerhet

Eftersom skadeverkningarna av bristande säkerhet i system även medför risker hos andra informationsägare och verksamheter behöver riskbedömning och kravställningar om åtgärder ske med samsyn och med delaktighet från olika funktioner i kommunen.

3.2.1 Riskhantering och informationsklassning

I riktlinjer för informationssäkerhet framgår att all information som hanteras av kommunen ska genomgå informationsklassificering. Klassningen ska enligt dokumentet ske utifrån konfidentialitet, riktighet, tillgänglighet samt informationens värde och genomföras innan hantering av informationen har påbörjats. Uppföljning av genomförd klassning ska enligt riktlinjerna genomföras minst vartannat år.

Vidare framgår att det är informationsägaren som ansvarar för att alla informationstillgångar är klassificerade och är ytterst ansvarig för att genomföra risk- och sårbarhetsanalyser. Kommunen använder sig av SKR:s modell för genomförande av klassningen.

I riktlinjerna framgår även att underliggande it-resurser i form av infrastruktur, stödsystem och så vidare ska ges motsvarande klassning som vid informationsklassningen. I det fall det saknas en klassning eller av annan orsak saknas en koppling mellan it-resurs och klassade verksamhetssystem klassas it-resursen utifrån en bedömning enligt konsekvensbeskrivningarna i den klassningsmodell som används.

Riktlinjerna tar även upp att kommunen redan vid upphandling av nya it-resurser exempelvis system och applikationer ska tydliggöra kravställning av informationssäkerhet. I intervjuer framgår att kommunen de senaste åren har arbetat mot att informationssäkerhetskrav ska finnas med redan vid upphandlingsförfarandet, men att det inte är etablerat fullt ut i kommunens organisation.

Intervjupersoner uppger att det hos systemförvaltarna är etablerat att verksamhetens system ska genomgå en informationsklassning. Vi får i intervjuer till oss att

omklassningar genomförs men det ges en delad bild av hur ofta det sker. Det uppges att förändringar i organisationen har varit bakomliggande orsaker till att omklassningar har genomförts. I intervjuer lyfts även att modellen som kommunen har använt vid klassningen har uppdaterats vilket innebär att samtliga system behöver genomgå en omklassning.

Intervjupersoner uppger att stora delar av kommunens system har genomgått en informationsklassning och att det är de senast införskaffade systemen som i dagsläget saknar klassning. Klassningarna genomförs utifrån SKR:s modell och intervjuuppgifter gör gällande att dessa sparas men inte diarieförs. Kravställan uppges ske indirekt utifrån den informationsklassning som verksamheten har genomfört, utöver detta har verksamheten inte lämnat över någon formell kravställan angående it-säkerhetsåtgärder som behöver vidtas utifrån informationsklassningen.

Enligt uppgift genomförde kommunen i början av 2022 en kommunövergripande riskanalys som omfattade samtliga av kommunens verksamheter. Vi har i granskningen efterfrågat riskanalysen, dock uppges att den är muntligt genomförd. Riskanalysen syftade bland annat till att kartlägga molnbaserade tjänster och resulterade i en lista med åtgärder som behöver vidtas i syfte att stärka informationssäkerhetsarbetet. Utifrån riskanalysen har förvaltningarna upprättat kontinuitetsplaner i syfte att kunna bedriva verksamhet vid en eventuell störning eller ett avbrott. Intervjupersoner uppger att delar av planerna har testats, exempelvis uppges att bildningsförvaltningen har testat analog hantering av specialkost.

Intervjupersoner uppger vidare att it-avdelningen har upprättat en turordningslista både avseende vilka system som ska stängas ned först samt vilka system som ska startas upp först i samband med en incident eller misstanke om incident. Enligt uppgift ska detta finnas beskrivet i den systembeskrivning som ska upprättas för respektive system.

Vi har i granskningen tagit del av ett exempel på systemdokumentation. Dock följer den en tidigare form av mall som vid tid för granskningen har ersatts av en ny mall (se avsnitt 3.1.1). Intervjupersoner uppger att informationssäkerhetssamordnaren har genomfört insatser och informerat systemförvaltarna om mallen, men det finns ytterligare behov av att etablera den nya mallen samt rutiner inför införande av nytt system.

Som en del i kommunens riskhantering regleras styrning av åtkomst i riktlinjer för informationssäkerhet och det framgår att grundprincipen för behörighetstilldelning baseras på respektive användares behov till information eller it-system. Intervjupersoner uppger att kommunen avser att upprätta särskilda riktlinjer för behörighetstilldelning där bland annat processen för behörighetstilldelning framgår. Vid tid för granskningen är det systemförvaltaren som utarbetar ett förslag till beslut och

sedan är det ansvarig chef som beslutar om behörigheten. Det genomförs ingen systematisk kontroll av tilldelade behörigheter.

3.2.2 Medvetenhet och förståelse

En viktig del i ett systematiskt informations- och it-säkerhetsarbete är att det finns en tillräcklig medvetenhet hos de som har tillgång till kommunens information. I en kommun utgör det exempelvis förtroendevalda, medarbetare, elever samt externa konsulter.

Intervjupersoner uppger att intresset för informationssäkerhetsfrågor tidigare har varit lågt i kommunens ledning. Med anledning av detta har det enligt uppgift funnits svårigheter med att upprätta och implementera styrande dokument som exempelvis riktlinjer för informationssäkerhet. Dock uppges att intresset har ökat under senare år, bland annat med anledning av att en ny kommundirektör har tillträtt (den nuvarande kommundirektören är en tillförordnad tjänst fram till 1 mars). Tjänstepersoner uppger att det finns en medvetenhet hos politiken angående vikten av att ha ett bra informations- och it-säkerhetsarbete samt förståelse för att det är ett resurskrävande arbete.

I intervjuer framgår att det finns en varierad grad av it-mognad samt en varierade kunskapsnivå angående hantering av personuppgifter hos kommunens medarbetare. I syfte att stärka medarbetarnas kunskap och medvetenhet har kommunen genomfört en digital utbildning via ett utbildningsföretag. Utbildningen är obligatorisk för samtliga medarbetare, men det genomförs ingen formaliserad uppföljning av deltagandet. Ansvaret för att följa upp deltagandet åligger respektive verksamhetschef. Intervjupersoner uppger att deltagandet varit relativt lågt och att det upplevs ha funnits en inställning att det saknas behov av att gå utbildningen då medarbetaren har genomfört den vid ett tidigare tillfälle. Vi får dock till oss att resultatet från utbildningen visar att det finns teoretisk kunskap angående hur information ska hanteras, men att det fortfarande finns brister i den praktiska hanteringen.

Utöver detta uppger intervjupersoner att även om utbildning erbjudits och genomförts av medarbetare lätt faller tillbaka i gamla mönster och rutiner, vilket innebär en fortsatt osäker hantering av information trots insatser.

Det finns en checklista som ska användas av samtliga verksamheter vid introduktion av nyanställda eller avslut av en medarbetares anställning. Vid introduktion framgår av dokumentet att ansvarig chef ska fylla i en behörighetsanmälan till de aktuella system som medarbetare behöver ha behörighet till. Checklistan innehåller även en systemdokumentation där ansvarig chef ska fylla i till vilka system som behörighet har beställts. Vid avslut av anställning eller vid byte av tjänst finns en checklista för avslut

av behörighet. Vidare framgår att medarbetaren vid introduktion ska ta del av informationssäkerhetspolicy, riktlinje för informationssäkerhet samt grundläggande information om informationssäkerhet och GDPR.

3.2.3 Bedömning

Vi gör bedömningen att det i kommunen finns en dokumenterad styrning för hur riskbedömning och informationsklassning ska genomföras i kommunen. Vi anser även att det till viss del finns ett systematiskt arbetssätt, men att det kan stärkas ytterligare för att den dokumenterade styrningen ska efterlevas samt för att säkerställa att riskbedömning, klassning och omklassning genomförs i syfte att upprätthålla en tillräcklig säkerhet utifrån behov.

Vidare är vår bedömning att det till viss del sker en kravställning mellan verksamheterna och it-avdelningen. Vi anser dock att kravställningen kan stärkas genom att verksamheterna upprättar en handlingsplan utifrån genomförd riskbedömning och klassning som omfattar vilka it-säkerhetsåtgärder som verksamheterna har behov av.

Vi ser positivt på att kommunen har för avsikt att upprätta ett särskilt styrande dokument där bland annat processen för behörighetstilldelning framgår. Utöver detta anser vi att kommunen bör upprätta och dokumentera former för hur kontroll av tilldelade behörigheter ska hanteras samt säkerställa att denna typ av kontroller genomförs.

Vi kan konstatera att kommunen vidtagit åtgärder i syfte att öka medarbetarnas medvetenhet om säker hantering av information. Vår bedömning är dock att det finns ytterligare behov av insatser med anledning av det som framkommer i granskningen. För att säkerställa medarbetarnas medverkan i utbildningarna bör kommunstyrelsen och nämnderna säkerställa att uppföljning av utbildningarna genomförs. En uppföljning kan även visa om det finns behov av ytterligare åtgärder, som exempelvis informationsinsatser på arbetsplatsträffar.

3.3 It-säkerhetsåtgärder

I riktlinjer för informationssäkerhet regleras informationssäkerhet i it-miljön, nedan kallat it-säkerhet. Enligt dokumentet ska det finnas rutiner i syfte att information om it-tekniska sårbarheter erhålls i tid så att sårbarheter kan analyseras och att lämpliga åtgärder kan vidtas för att behandla de risker som sårbarheter medför.

Det it-säkerhetsarbetet som i dagsläget sker i kommunen grundas till stora delar i ett omvärldsbevakningsarbete och utifrån det görs en bedömning om det finns behov av att vidta säkerhetsåtgärder. Arbetet inkluderar även genomgång av incidenter som

inträffat i kommunen. Som en del i it-avdelningens omvärldsbevakning och utvecklingsarbete medverkar it-chefen i ett samverkanforum med it-chefer från andra kommuner samt regionen. Syftet med forumet är bland annat att lyfta uppstådd problematik som de medverkande har erfarenhet av samt lyfta om det finns möjlighet att genomföra gemensamma upphandlingar inom området. I arbetet ingår även vidareutbildning och intervjupersoner uppger att systemförvaltare på it-avdelningen vid tid för granskningen genomgår kompetensutveckling.

It-avdelningen ser i dagsläget över möjligheter för att stärka säkerheten i nätverk. En åtgärd som kommunen vidtagit är att inte tillåta okända enheter att ansluta till nätverken. Därtill pågår ett arbete med att höja säkerheten genom segmentering av nätverk och stärka säkerheten i publika nät. Segmentering av nätverk bidrar till att minska risken för intrång då det ger en tydligare överblick över antal vägar in till exempelvis en skyddsvärd information.

I syfte att identifiera sårbarheter i nätverken är det vanligt att genomföra fysiska och digitala sårbarhetsscanningar. Intervjupersoner uppger att de fysiska skanningarna av det fysiska skyddet för kommunens datahallar har genomförts i närtid och resultatet uppges visa ett behov av att förstärka skalskyddet något. Som en del i att skydda datahallarna från intrång har hallarna ett skalskydd med bland annat behörighetsstyrd inpassering. Det framgår i intervjuer att digital sårbarhetsskanning har genomförts men utan systematik i uppföljningen. Intervjupersoner uppger att it-avdelningen har för avsikt att upprätta en plan för genomförande av sårbarhetsskanningar.

I syfte att säkerställa att information inte går förlorad vid ett eventuellt avbrott använder sig kommunen av säkerhetskopiering. Dock uppger intervjupersoner att det finns behov av åtgärder för att säkra att informationen återställs i den utsträckning som är nödvändigt för kommunens verksamheter.

För att upptäcka eventuella intrångsförsök eller hot mot nätverk och it-system har kommunen digital övervakning som larmar då det sker en avvikelse i vissa nätverk och it-system. It-avdelningen saknar i dagsläget resurser för att kunna upprätta en jourfunktion med bevakning dygnet runt. Intervjupersoner uppger dock att det inom avdelningen finns en lojalitet där medarbetare vid behov ställer upp i det fall det sker en större incident utanför it-avdelningens ordinarie arbetstid.

3.3.1 Bedömning

Vår bedömning är att kommunstyrelsen via it-avdelningen har vidtagit åtgärder i syfte att upptäcka eventuella hot om intrång eller andra incidenter i it-system. Vi anser att arbetet som bedrivs kan utvecklas genom att ha utgångspunkt i upprättade och dokumenterade riskanalyser. Riskanalyserna kan sedan ligga till grund för mål- och handlingsplaner där åtgärder prioriteras utifrån sårbarhet och behov över tid. Dokumentationen kan även bidra till att förenkla det uppföljande arbetet.

Vidare är vår bedömning att kommunstyrelsen bör säkerställa att åtgärder vidtas utifrån det som framkommit av genomförda sårbarhetsskanningar. Det fysiska skyddet är av vikt både i syfte att stänga obehöriga ute och i syfte att skydda mot exempelvis brand. Vi anser även att det finns behov från kommunstyrelsen sida att säkerställa att uppföljning av införda it-säkerhetsåtgärder genomförs på ett systematiskt sätt i syfte att följa upp åtgärdernas effekt.

Utöver detta anser vi att kommunstyrelsen bör se över vilka möjligheter som finns för att möta verksamheternas behov av säkerhetskopiering. En kontinuerlig säkerhetskopiering av information kan bidra till en minskad förlust av information vid en incident som exempelvis intrång eller elavbrott.

3.4 Incidenthantering

I riktlinjerna för informationssäkerhet regleras hur en incident ska hanteras inom Hedemora kommun. I riktlinjerna finns förtydligande angående vad som är en informationssäkerhetsincident samt att brister ska rapporteras, exempelvis olåsta dörrar och fönster, larm som inte fungerar etc.

Incidenter och brister ska enligt riktlinjerna rapporteras till säkerhetschefen. Då det i kommunen har saknats rutiner för incidentrapportering har säkerhetschefen tagit fram ett utkast på rutiner daterat 2021-11-22. Intervjupersoner uppger att rutinerna inte alltid efterlevs. Vidare uppges att kommunen planerar för att införa incidentrapportering via e-tjänst, men att detta vid tiden för granskningen är i planeringsstadiet.

Enligt riktlinjerna för informationssäkerhet är det säkerhetschefen som leder hanteringen av incidenter i samverkan med berörda ägare av informationen. Av dokumentet framgår även att kunskaper baserade på analyser av hanterade incidenter ska nyttjas som underlag för beslut om åtgärder i syfte att minska risken för att liknande incidenter sker framgent. Större incidenter ska enligt dokumentet sammanställas i incidentrapporter som respektive informationsägare ansvarar för att ta fram i

samverkan med säkerhetschef. Vi får i intervjuer delade bilder avseende om inträffade incidenter sammanställs och diarieförs på kommunövergripande nivå.

Intervjupersoner uppger att kunskapen för att upptäcka och anmäla en misstanke om eller en inträffad incident varierar i kommunen och lyfter samtidigt att det kan finnas behov av utbildnings- och informationsinsatser inom området. Vidare uppges att de framtagna rutinerna i dagsläget inte är implementerade i organisationen fullt ut och därmed inte alltid efterlevs då anmälan om incidenter kan inkomma på annat sätt än upprättade eskaleringsvägar.

Antalet anmälda incidenter uppges ha minskat i kommunen och det finns en uppfattning att anmälningarna bör vara fler, bland annat med tanke på den mängd personuppgifter som hanteras i kommunens verksamheter.

3.4.1 Bedömning

Vi gör bedömningen att det i kommunen finns upprättade riktlinjer för hur en incident ska hanteras. Då riktlinjerna i dagsläget inte efterlevs till fullo bör kommunstyrelsen säkerställa att riktlinjerna implementeras i kommunens organisation, exempelvis genom det upprättade rutindokumentet som vid tid för granskningen är i form av ett utkast.

Vidare är vår bedömning att kommunstyrelsen bör säkerställa att inträffade incidenter analyseras på en kommunövergripande nivå i syfte att kunna identifiera eventuella behov av åtgärder.

Vi ser även att kommunstyrelsen bör säkerställa att det genomförs utbildningsinsatser inom området incidenter. Att öka kunskap och medvetenhet kring vad en incident är bidrar till att minska risken för att en incident sker samt att medarbetarna anmäler inträffade händelser.

3.5 Uppföljning, intern kontroll och rapportering

3.5.1 Uppföljning och intern kontroll

Enligt handlingsplan för informationssäkerhet, dataskydd och digitalisering ansvarar informationssäkerhet- och dataskyddsrådet för att en årlig översyn genomförs av ledningssystemet. Översynen ska enligt dokumentet fungera som underlag för koncernledningsgruppen/kommunledningsgruppen årliga uppföljning och utvärdering av arbetet med informationssäkerhet, dataskydd och digitaliseringsutveckling.

Säkerhetschefen upprättar årligen en uppföljningsrapport av det säkerhetsarbete som bedrivits i kommunen där informationssäkerhetsarbetet inkluderas. I intervjuer uppges att det för år 2021 inte upprättades någon plan med anledning av pandemin. Vi har i granskningen efterfrågat uppföljning för år 2022, vilket uppges vara under upprättande vid tid för granskning.

Utöver detta har dataskyddsombudet som uppföljning av kommunens dataskyddsarbete genomfört intervjuer med representanter från förvaltningen. Intervjuerna syftar till att följa upp förvaltningarnas dataskyddsarbete. Detta sammanställs i en rapport tillsammans med bland annat inträffade personuppgiftsincidenter som skett under året.

I den av kommunstyrelsen antagna internkontrollplanen finns kontrollmomenten personuppgiftsbehandlingar samt säker åtkomst till kommunens it-miljö. Vi har i granskningen efterfrågat uppföljning av internkontrollplanen men har inte delgetts denna.

3.5.2 Rapportering

Intervjupersoner uppger att säkerhetschef och it-chef lämnar en redogörelse till följande funktioner i kommunledning: kommundirektör, förvaltningschefer samt kommunstyrelsens arbetsutskott.

3.5.3 Bedömning

Vår bedömning är att det finns en dokumenterad styrning avseende uppföljning av ledningssystemet. Med anledning av att vi i granskningen inte tagit del av år 2022 års säkerhetsrapport kan vi inte bedöma om det uppföljningsarbete som sker är ändamålsenligt. Utöver detta anser vi att kommunstyrelsen bör säkerställa att de i återrapportering från tjänstepersoner tar del av den upprättade uppföljningsrapporten och att åtgärder vidtas utifrån behov.

Vidare är vår bedömning att kommunstyrelsen fortsatt bör beakta informationssäkerhet i det riskanalysarbetet som ligger till grund för den kommunövergripande internkontrollplanen i syfte att bedöma om området behöver inkluderas ytterligare i planen.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen till viss del har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Kommunen har en dokumenterad styrning inom området där roller, funktioner och ansvar finns beskrivet men det finns behov av att implementera detta i organisationen för att säkerställa att aktiviteter genomförs i den utsträckning som krävs för att uppnå en god informationssäkerhet.

Aktiviteter som informationsklassning och riskbedömning genomförs i kommunen, däremot kan systematiken i arbetet stärkas ytterligare i syfte att efterleva styrande dokument samt för att säkerställa att brister i systemsäkerhet samt felaktig hantering av information identifieras i tillräcklig utsträckning.

Utöver detta anser vi att kommunstyrelsen bör säkerställa att åtgärder vidtas utifrån det som framkommit av genomförda sårbarhetsskanningar samt att uppföljning genomförs av it-säkerhetsåtgärder genomförs på ett systematiskt sätt i syfte att följa upp åtgärdernas effekt. Som en del i det förebyggande arbetet bör kommunen även se över möjligheterna att möta verksamheternas behov av säkerhetskopiering samt se över möjligheterna att införa tvåfaktorautentisering.

Då säkerhetsrapporten för år 2022 sammanställs under granskningsperioden kan vi inte göra bedömning om det uppföljningsarbete som sker är ändamålsenligt.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen i sitt övergripande ansvar för styrning och uppföljning att:

- Säkerställa att roller, funktioner och ansvar kommuniceras i organisationen så att var en och upprätthåller sitt ansvar i enlighet med styrande dokument.
- Justera det dokumenterade ansvaret för it-säkerhet från verksamhetsansvariga till it-avdelningen/utsedd funktion så att lämplig kompetens innehar det it-tekniska säkerhetsansvaret.
- Säkerställa att riktlinjer för incidenthantering implementeras i organisationen.
- Säkerställa att incidenter analyseras på en kommunövergripande nivå i syfte att identifiera eventuella behov av åtgärder
- I uppföljningsarbetet inkludera efterlevnad av styrande dokument.

— Säkerställa att åtgärder vid behov beslutas utifrån den uppföljning och rapportering av det övergripande säkerhetsarbetet som styrelsen tar del av.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen och nämnderna inom sitt verksamhetsansvar för informationssäkerhet att:

— Säkerställa att informationstillgångar klassificeras samt att omklassningen genomförs i enlighet med styrande dokument.

— Säkerställa att former för kontroller av behörighetstilldelning upprättas samt att kontroller genomförs i syfte att undvika otillbörlig informationstillgång.

— Vidta åtgärder i syfte att öka medvetenhet och kunskap avseende säker hantering av information samt vad som definierar en incident i syfte att nå ett förändrat beteende hos kommunens medarbetare.

— Säkerställa att it-säkerhetsarbetet utgår från genomförda riskanalyser.

— Säkerställa att åtgärder vidtas utifrån genomförda sårbarhetsskanningar i syfte att upprätthålla ett tillräckligt fysiskt och digitalt skydd.

— Se över möjligheterna att möta verksamheternas behov av säkerhetskopiering.

Datum som ovan

KPMG AB

Ida Larsson

Kommunal revisor

Linnéa Grönvold

Certifierad kommunal revisor