# Granskning av kommunens informationssäkerhet

Rapport

Nora kommun

KPMG AB

Datum 2022-11-14

Antal sidor 22

# Innehållsförteckning

# 1 Sammanfattning

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

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

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

Vår bedömning bygger bland annat på att det i kommunen inte har genomförts riskbedömning eller informationsklassning av informationen som hanteras. Det arbete som bedrivs genomförs på verksamhetsnivå och det saknas en kommunövergripande bild över de mål och krav som ställs i informationssäkerhetspolicyn.

Kommunen har till viss del aktuella styrande dokument. Vi ser ett behov av att kommunen upprättar riktlinjer för informationssäkerhet, som konkretiserar policyn. Utöver detta anser vi att kommunen bör se över IT-policyn och reviderar den utifrån behov, då den är antagen år 2013.

Vi ser även att det finns en risk att det saknas kunskap angående vad en incident är samt hur en incident ska anmälas inom kommunen. Vi ser därför ett behov av utbildningsinsatser. Insatserna bör även omfatta övergripande information om informationssäkerhet som en del i att säkerställa medvetenhet, kunskap och förståelse för området hos medarbetare och förtroendevalda.

Vi ser positivt på att kommunen arbetar med att upprätta kontinuitetsplaner för samtliga verksamheter. Utifrån detta rekommenderar vi att kommunstyrelsen säkerställer att planerna regelbundet testas utifrån ändamålsenlighet.

I syfte att kommunen ska kunna säkerställa en säker IT-infrastruktur är vår bedömning att det arbete som bedrivs behöver systematiseras och bör utgå från genomförda riskanalyser. Utifrån riskanalyser kan mål- och handlingsplaner upprättas och utgöra en prioriteringsordning utifrån sårbarhet och behov över tid. Denna dokumentation kan även bidra till att förenkla det uppföljande arbetet.

Vår bedömning är vidare att kommunstyrelsen bör beakta informationssäkerhet i det riskanalysarbete som ligger till grund för kommande internkontrollplan samt efterfråga en samlad uppföljning av det informationssäkerhetsarbete som bedrivs i kommunen.

Utifrån vår slutsats och bedömning rekommenderar vi kommunstyrelsen att:

- Säkerställa att riktlinjer för informationssäkerhetsarbetet upprättas och implementeras som kan konkretisera policyns intentioner.
- Se över och utifrån behov revidera kommunens IT-policy.
- Säkerställa att uppföljning av efterlevnaden av styrande dokument sker.

- Utreda möjligheten att utse alternativt tillsätta en informationssäkerhetssamordnare. Samordnarens roll bör omfatta en samordnande funktion av det informationssäkerhetsarbete som bedrivs i kommunen, utöver sin roll i personuppgiftshanteringen.
- Upprätta former för genomförande av riskbedömning och informationsklassning samt säkerställa att momenten genomförs.
- Säkerställa att riskanalyser genomförs som kan ligga till grund för eventuella tekniska säkerhetsåtgärder som behöver vidtas samt säkerställa att en mål- och handlingsplan upprättas utifrån genomförs riskanalys.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera en medvetenhet och kunskap om informationssäkerhet.
- Ställa krav om uppföljning och återrapportering av kommunens samlade informationssäkerhetsarbete så att beslut kan tas om mål och handlingsplan över åtgärder som behöver vidtas för att förbättra informationssäkerheten.

# 2 Bakgrund

KPMG har av Nora kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av styrelsens rutiner för sitt 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.

Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod. Många verksamheter inom kommunen är idag helt beroende av väl fungerande IT. För flera verksamheter handlar ett väl fungerande IT-stöd såväl om säkerhet som möjlighet till en fungerande verksamhet utan driftstörningar. 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 arbetet med informationssäkerheten 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 besvarar 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. Granskningen avser år 2022.

## 2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

— Kommunallagen 6 kap. 6 §
— Tillämpbara interna regelverk, policys och beslut
— MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
— NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

## 2.3 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

— Informationssäkerhetspolicy
— IT-säkerhetspolicy
— Riktlinjer för personuppgiftshantering
— Verksamhetsspecifika rutiner

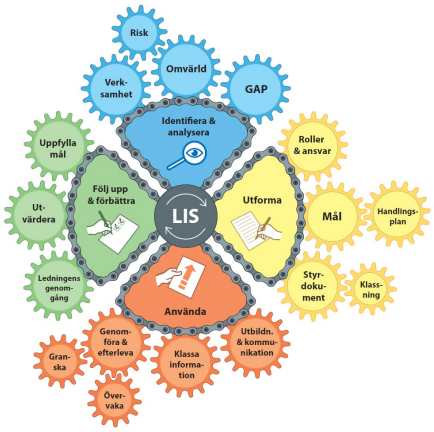
Intervjuer har genomförts med berörda tjänstepersoner samt kommunstyrelsens presidium.

Rapporten är faktakontrollerad av intervjupersoner.

## 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:

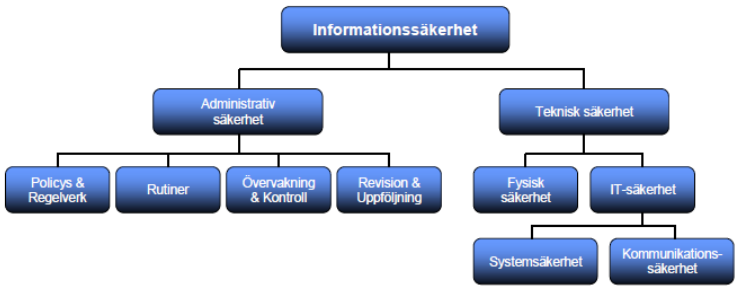
- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet.
- Utbilda och kommunicera informationssäkerhetsfrågor 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

Nora kommuns kommunfullmäktige antog år 2020 en informationssäkerhetspolicy[1]. Av dokumentet framgår att policyn är giltig till och med 1 juni 2023 och att revidering av dokumentet sker i samband med ny mandatperiod. Vidare framgår att kommundirektören har det yttersta ansvaret för informationssäkerheten inom förvaltningen. Det är säkerhetsskyddschef som innehar dokumentansvar för policyn och som regelbundet ska ompröva dokumentet för att kontrollera om det finns ett behov av revidering.

Utöver detta framgår i policyn att målet med informationssäkerhetsarbetet är att hantera och skydda information i verksamheterna på ett sådant sätt att rättsliga och verksamhetsmässiga krav samt invånarintressen kan tillgodoses.

År 2022 antog kommunstyrelsen riktlinjer för behandling av personuppgifter för Nora kommun[2]. Av riktlinjerna framgår roller och ansvar, hur en personuppgiftsincident ska hanteras samt exempel på vad som anses vara en incident. Utöver detta finns även ett exempel på konsekvensbedömning.

Kommunfullmäktige antog 2013 en IT-säkerhetspolicy[3]. Av policyn framgår att det övergripande ansvaret för säkerheten i organisationens IT-verksamhet vilar på kommunchefen. I övrigt framgår att samtliga IT-system ska vara identifierade och förtecknade och att det är kommunchefen som utser systemägare för dessa.

Det framgår av policyn att uppföljning av IT-säkerhetsarbetet ska ske i syfte att bevaka att beslutande åtgärder är genomförda, årliga mål är uppfyllda, att riktlinjer följs samt att systemsäkerhetsplaner och policydokument vid behov revideras.

Utöver detta har kommunen upprättat IT-säkerhetsinstruktioner[4] som innehåller regler och riktlinjer för användare. Dokumentet syftar till att ge kunskap och riktlinjer om hur man på ett säkert sätt använder IT-stöden. Det framgår att dokumentet kan användas som ett uppslagsverk och en viktig källa om hur IT-systemen och informationen får användas. Det framgår inte om dokumentet är antaget av kommunstyrelsen.

Av instruktionerna framgår att IT-systemet är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt informationen. Vidare framgår att det är ansvarig chef som beslutar om behörighetstilldelning. I övrigt saknas kommunövergripande riktlinjer.

---

[1] Policy för informationssäkerhet, kommunfullmäktige 2020-10-21, senast revidering 2021-04-28

[2] Riktlinjer för behandling av personuppgifter för Nora kommun[2], kommunstyrelsen, 2022-04-06

[3] IT-policy, kommunfullmäktige, 2013-12-16

[4] IT-säkerhetsinstruktion: Regler och riktlinjer för användare i Nora kommun, IT-chef, 2007-01-29

Socialtjänsten i Nora kommun har upprättat interna rutiner för behörighetstilldelning samt loggkontroller. Intervjupersoner uppger att dessa är upprättade utifrån vad andra myndigheter ställer för krav på verksamheten utifrån myndighetsutövning samt vårdgivare. Rutinerna uppges inte vara upprättade utifrån kommunen informationssäkerhetspolicy.

Av IT-policyn framgår även att det inom kommunen ska finnas IT-säkerhetsinstruktioner för förvaltning samt drift. Vi har i granskningen efterfrågat dokumenten men inte mottagit dessa.

Intervjupersoner uppger att det inte sker någon samlad uppföljning angående att styrande dokument efterlevs.

### 3.1.2 Roller och ansvar

Av policy för informationssäkerhet framgår att grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Vidare tydliggörs bland annat att fullmäktige, styrelse samt övriga nämnder har det yttersta ansvaret för informationssäkerheten i respektive verksamhetsområde. Verksamhetsansvariga, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet.

Utöver detta beskrivs följande roller med tillhörande ansvar:

- **Systemägare** – Informationsansvarig för all data i, eller exporter från, informationskällan. Ansvarar för att besluta om källans informationssäkerhetsnivå genom att klassning sker enligt beslutad modell.
- **Systemansvarig** – De som ansvarar för den dagliga användningen av det digitala verksamhetsstödet.
- **IT-avdelningen** – Ansvarar för att säkerheten i kommunens IT-miljö är tillförlitlig och motsvarar verksamhetens och legala krav.
- **Driftsansvarig** – Ska inneha den tekniska kompetensen och ansvarar tillsammans med systemansvarig för att den dagliga driften upprätthålls enligt avtal.

Av riktlinjen för behandling av personuppgifter framgår roller och ansvarig inom området. Det är personuppgiftsansvarig, exempelvis styrelse och nämnd, som bestämmer ändamålen och medlen med en behandling. Personuppgiftsansvarig ansvarar även bland annat för att riktlinjerna efterlevs samt för att ta fram en handlingsplan för hur de ska arbeta med personuppgifter inom sitt område. Utöver detta beskrivs följande roller:

- **Informationssäkerhetssamordnare** – Ansvarar för att leda arbetet med framtagandet av ett inbyggt dataskydd vid behandling av personuppgifter som en del av informationssäkerhetsarbetet.
- **Objektägare** – ska finnas för alla system som behandlar personuppgifter.

- **Förvaltningsledare** – förvalta systemet och kontinuerligt informera objektägaren och dataskyddsombudet om händelser och behandlingar som kan påverka den registrerades rättigheter på ett negativt sätt.
- **Dataskyddsombud** – i intervjuer framgår att dataskyddsombudet är en extern tjänst där kommunerna som ingår i samverkansnätverket KNÖL[5] innehar samma dataskyddsombud.
- **Personuppgiftssamordnare** – förvaltningens huvudsakliga kontaktperson vid frågor rörande personuppgifter och dataskydd och en förmedlande länk till dataskyddsombudet.
- **Dataskyddsgruppen** – kommunkoncernens gemensamma nätverk för personuppgifts- och dataskyddsfrågor. Gruppen består av personuppgiftssamordnare i kommunen och de kommunala bolagen, informationssäkerhetssamordnaren samt dataskyddsombud i kommunen och de kommunala bolagen som deltar som rådgivare.

Intervjupersoner uppger att det finns utsedda systemansvariga i kommunen, men det saknas en förteckning över detta. Det finns även som nämnts ett dataskyddsombud samt en utsedd personuppgiftssamordnare. I övrigt saknas nämnda funktioner i kommunen, däribland en informationssäkerhetssamordnare.

IT-avdelningen består i nuläget av sex medarbetare, men avses utökas med ytterligare en medarbetare. Samtliga arbetsuppgifter är fördelade på samtliga medarbetare, däribland bemanning av avdelningens servicedesk.

Det uppges i intervjuer att det finns en aktiv dialog gällande säkerhet och kontinuitet inom kommunen och att informationssäkerhet är en del av det. Med anledning av pandemin, situationen i Ukraina samt en vattenläcka inom kommunen valde kommunen att gå från stabsläge till ett så kallat ”mitt-emellan-läge”. Läget innebär att kommunen fortsatt har ett stabsläge med en något höjd beredskap.

Intervjupersoner uppger att det saknas en tydlighet avseende att det med linjeansvaret följer med ansvar för informationssäkerhet inom verksamhetsområdet. Det uppges att nya chefer inte har fått en överlämning eller introduktion där den här typen av information anses bör ha ingått. Vidare uppges att det finns kunskap om var styrande dokument finns, men att det hade underlättat om det hade genomförts en tydligare introduktion. Vidare uppges att ansvaret för informationssäkerheten upplevs som intetsägande och att det saknas en upplevd förpliktelse.

### 3.1.3 Bedömning

Vi gör bedömningen att kommunen till viss del har aktuella styrande dokument som tydliggör ansvar, krav samt hur informationssäkerhetsarbetet ska bedrivas. Vår bedömning bygger på att det finns en antagen informationssäkerhetspolicy, IT-policy samt riktlinjer för personuppgiftshantering. Vi saknar dock riktlinjer för

[5] Kommunerna i Norra Örebro Län. Kommunerna som ingår är Nora, Lindesberg, Hällefors och Ljusnarsberg.

informationssäkerhet, vilket nämns i informationssäkerhetspolicyn ska finnas, och anser att kommunstyrelsen bör upprätta denna typ av styrande dokument som en del i sin styrning.

Då kommunens IT-policy är antagen 2013, är vår bedömning att kommunstyrelsen bör se över denna i syfte att säkerställa att den överensstämmer med kommunens nuvarande organisation samt de mål och krav som kommunstyrelsen har angående kommunens tekniska säkerhet.

I IT-policyn finns riktlinjer för behörighet, vi gör dock bedömningen att det finns behov av att komplettera dessa med exempelvis reglering om systematisk kontroll av tilldelade behörigheter.

Av det som framkommer i granskningen gör vi även bedömningen att kommunen brister i att följa upp efterlevnaden av styrande dokument och att kommunstyrelsen i sin styrning bör säkerställa att sådan uppföljning sker.

Vidare gör vi bedömningen att det finns behov av att tydliggöra att ägare av information samt ansvar för hur informationen skyddas, hanteras och sprids följer linjeansvaret.

Utöver detta är vår bedömningen att det till viss del finns en ändamålsenlig organisation i kommunen avseende informationssäkerhet. Vi saknar ett antal funktioner som benämns i informationssäkerhetspolicyn samt riktlinjer för personuppgiftshantering. Vi gör därför bedömningen att det finns behov av att utse dessa funktioner i kommunen som en del i att säkerställa att samtliga delar i informationssäkerhetsarbetet genomförs. Främst ser vi ett behov av att kommunen utser alternativt tillsätter en informationssäkerhetssamordnare i syfte att vara en drivande samt en samordnande funktion i det informationssäkerhetsarbete som bedrivs i kommunen, utöver sin roll inom personuppgiftshanteringen.

## 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 syfte att få kunskap om informationens skyddsvärde och utifrån det kunna ställa krav gentemot aktörer som hanterar informationen ska enligt informationssäkerhetspolicyn metoden informationsklassning tillämpas. Det framgår att klassningen ska baseras på interna och externa krav på informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Intervjupersoner uppger att IT-avdelningen i dagsläget inte samverkar med verksamheterna angående informationssäkerhetsarbete. Det uppges även att det i dagsläget saknas en nära samverkan mellan centrala funktioner, IT-avdelningen och verksamhetschefer kring system och krav av dessa. Det uppges även att det saknas samverkan kring upphandling av nya system och att det inte genomförs klassningar vid upphandling.

Det saknas i dagsläget vetskap angående vilka system i kommunen som har klassats, men det pågår ett kommunövergripande arbete av kartläggning av systemen. Kartläggningen uppges mynna ut i upprättande av en förvaltningsmodell för samtliga system som används i kommunen. I det fall det finns en förteckning sedan innan uppger intervjupersoner att de saknar vetskap om detta.

Inom socialtjänstens verksamhetsområde uppges att en systemgenomgång genomfördes i samband med att dataskyddsförordningen (GDPR[6]) infördes. Dock uppges även att det inte har genomförts en fullständig riskbedömning och informationsklassning utifrån krav som konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Det uppges finnas ett behov av att kommunen arbetar utifrån en klassningsmodell som är tolkad och anpassad utifrån ett kommunövergripande perspektiv samt utifrån respektive verksamhets behov.

Inom kultur- och fritidsverksamheten uppges att det främst är bibliotekets verksamhet som berörs av informationssäkerhet. Intervjupersoner uppger att det genomfördes en riskbedömning tillsammans med kommunens dataskyddsombud utifrån att verksamheten använder ett integrerat verksamhetssystem där flera verksamheter har tillgång till samma system. Arbetet ledde till att behörigheter till systemet begränsades.

Enligt uppgift saknas det genomförda riskbedömningar och informationsklassningar inom verksamhetsområdet kultur och fritid. Dock lyfter intervjupersoner att det finns upprättade rutiner för hantering av personuppgifter och att detta är en aktuell fråga inom biblioteksverksamheten.

Enligt intervjupersoner är det respektive chef som beslutar om behörighetstilldelning vilket kommuniceras till IT-avdelningen via systemansvarig för genomförande. Det uppges att rutiner finns upprättade för vissa verksamhetsområden i kommunen. Intervjupersoner lyfter även att det inom socialtjänsten genomförs en riskanalys inför varje behörighetstilldelning.

Inom socialtjänsten genomförs även regelbundna loggkontroller. Kontrollerna genomförs 10 gånger per år utifrån manuellt upptäckta avvikelser. Ett exempel på avvikelser som uppges är om dagpersonal har gjort sökningar i verksamhetssystemet nattetid, eller vice versa. Enligt uppgift är det systemansvarig som genomför utskick av loggkontroller. Det är sedan enhetschef som ansvarar för att följa upp och utreda loggkontrollerna och i nästa steg förvaltningschefen som kontrollerar enhetschefens utredning. Det uppges att arbetet är tidskrävande och att det därför önskas ett automatiserat sätt att upptäcka avvikelser. I syfte att kunna urskilja systemleverantörens inloggningar i systemet har socialtjänsten ställt krav på leverantören att upprätta personliga inloggningar. Detta för att kunna följa upp även dessa loggningar och syftet med dem.

[6] General Data Protection Regulation

Utöver detta pågår även ett kommunövergripande arbete med att införa tvåfaktorsautentisering, som innebär att inloggning med användarnamn och lösenord kompletteras med ytterligare verifieringslösning.

### 3.2.2 Medvetenhet och förståelse

Enligt informationssäkerhetspolicyn åligger det varje verksamhetsansvarig att ansvara för att egna medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap så att nödvändig informationssäkerhet kan uppnås.

Det framgår i intervjuer att kommunikationsavdelningen tillsammans med IT-avdelningen har genomfört en kommunövergripande utbildning i syfte att skapa medvetenhet om nätfiske[7]. I samband med utbildningen genomfördes ett test. I testet uppmanades medarbetaren att klicka på en länk för att uträtta ett ärende, där länken ledde till utbildningen. Det genomfördes ingen strukturerad uppföljning av deltagandet mer än antalet medarbetare som genomförde den.

Inom socialtjänsten genomförs en introduktion av nya medarbetare där bland annat utbildning inom GDPR, dataintrång samt loggning och loggkontroller ingår. Det uppges i intervjuer att utbildningarna finns tillgängliga genom samma externa leverantör som dataskyddsombudet tillhör. Utöver detta ingår även information angående sekretess och sekretessförbindelse.

Inom biblioteksverksamheten genomgår samtliga anställda utbildning inom GDPR och hantering av personuppgifter. Medarbetarna har även genomgått en utbildning hos Region Örebro län för biblioteksutveckling, där personuppgiftshantering ingick.

Det genomförs ingen uppföljning över medarbetarnas medverkan i utbildningarna.

De förtroendevalda i kommunen genomgår en utbildning i samband med ny mandatperiod och däribland ingår utbildning inom GDPR, men det uppges att det saknas återkommande utbildningstillfällen under mandatperioden.

Med anledning av kommunens förhöjda beredskap och stabsläge uppges att medarbetare inom staben kommer att genomgå en utbildning inom övergripande säkerhet.

### 3.2.3 Bedömning

Vi gör bedömningen att kommunen saknar ett systematiskt och ändamålsenligt arbetssätt för att riskbedöma och klassa informationen som hanteras i kommunen. Vi gör bedömningen att informationssäkerhetspolicyn bör kompletteras med riktlinjer och rutiner för hur informationsklassningen ska genomföras. Vi gör även bedömningen att riktlinjerna med fördel kan innehålla en för kommunen anpassad klassningsmodell.

Vidare är vår bedömning att vissa verksamheter har genomfört riskbedömningar och utifrån detta vidtagit åtgärder. Däremot ser vi ett behov av att system och den

[7] Nätfiske, också kallat phishing, är vanligtvis en uppmaning att kicka på en felaktig länk som kan leda till exempelvis ett dataintrång.

information som hanteras i systemen har behov av att klassas utifrån en etablerad klassningsmodell. Vi gör även bedömningen att det finns behov av att upprätta rutiner för att regelbundet ompröva de genomförda informationsklassningarna och riskbedömningar som gjorts för att möta nya risker och behov när systemen är i drift.

Vi ser positivt på att det inom vissa verksamheter finns upprättade rutiner för behörighetshantering, men som vi har nämnt tidigare ser vi ett behov av att riktlinjerna kompletteras med reglering avseende kontinuerliga kontroller.

Av det som framkommer i granskningen gör vi bedömningen att det till viss del och inom vissa verksamhetsområden har vidtagits åtgärder i syfte att informera och sprida kunskap om informationssäkerhetsarbetet.

Vi ser positivt på att kommunen har genomfört en kommunövergripande interaktiv utbildning, men gör bedömningen att åtgärderna kan utökas ytterligare med återkommande utbildningstillfällen med inriktning mot informationssäkerhet. Utbildningarna bör vara obligatoriska för samtliga medarbetare och förtroendevalda i kommunen. Vi ser även att det i samband med utbildningarna genomförs en strukturerad uppföljning i syfte att kunna vidta riktade åtgärder eller utbildningsinsatser.

## 3.3 IT-säkerhetsåtgärder

Intervjupersoner uppger att det finns en aktuell och uppdaterad dokumentation av de IT-komponenter som utgör kommunens IT-miljö. Vidare uppges att det bland annat pågår ett arbete med att byta ut nätverksutrustning vilket kommer generera bättre möjligheter till att övervaka och upptäcka eventuella hot. Det finns i dagsläget inget etablerat arbetssätt eller metod för att regelbundet bevaka nya hot och risker.

I syfte att minimera förlust eller skada av information vid ett intrång genomför kommunen regelbundna backuper. Det framgår även att kommunen i dagsläget arbetar med andra typer av lösningar i syfte att säkerställa informationen.

Vidare uppges att kommunen har vidtagit vissa åtgärder i syfte att ge kommunen motståndskraft mot intrång eller cyberhot.

Enligt policyn ska systemsäkerhetsplan upprättas för de samhällsviktiga IT-systemen. Policyn hänvisar till dåvarande Krisberedskapsmyndighetens rekommendationer. Intervjupersoner uppger att det inte har genomförts någon bedömning över vilka system och komponenter som är samhällsviktiga/verksamhetskritiska och det saknas därmed en tydlighet angående vilka system som behöver prioriteras vid en särskild händelse. Intervjupersoner lyfter att det finns planer på att starta upp detta arbete i början av nästkommande år.

Vi får i intervjuer delade bilder angående om det finns upprättade SLA-avtal. Intervjupersoner uppger att det har överlämnats en SLA till IT-avdelningen över den tillgänglighet och åtkomst som verksamhetens system har behov av och att åtgärderna inte har kunnat genomföras på grund av resursbrist. Detta delas inte av samtliga intervjupersoner som lyfter att det saknas upprättade avtal.

### 3.3.1 Bedömning

Av det som framkommer i granskningen är vår bedömning att det i kommunen saknas ett systematiskt arbetssätt avseende tekniska säkerhetsåtgärder. IT-enheten har till viss del vidtagit åtgärder i syfte att säkerställa att information som hanteras i kommunen skyddas från digitala intrång, men vår bedömning är att åtgärderna inte är tillräckliga.

I syfte att kommunen ska kunna säkerställa en säker IT-infrastruktur är vår bedömning att det arbete som bedrivs behöver systematiseras. Arbetet kan utvecklas genom genomförda riskanalyser som ligger till grund för de tekniska säkerhetsåtgärder som genomförs. Utifrån riskanalyser kan mål- och handlingsplaner upprättas och utgöra en prioriteringsordning utifrån sårbarhet och behov över tid. Denna dokumentation kan även bidra till att förenkla det uppföljande arbetet.

## 3.4 Incidenthantering

Som tidigare nämnts har Nora kommun upprättat riktlinjer för behandling av personuppgifter. I riktlinjerna beskrivs vad en personuppgiftsincident är samt hur anmälan ska ske internt i kommunen. Det framgår i intervjuer att det finns en upplevelse av att riktlinjerna inte efterlevs fullt ut. Intervjupersoner ser därför ett behov av att verksamheterna upprättar kontaktpersoner då detta inte finns i dagsläget. Syftet med kontaktpersonerna uppges vara en naturlig kommunikationsväg för centrala funktioner för att nå ut med riktad information angående exempelvis efterlevnad av rutiner samt även resultat av genomförda analyser på inträffade incidenter.

Enligt intervjupersoner har dataskyddsombudet rapporterat att kommunen har ett lågt antal anmälda incidenter och det uppges att det därmed finns en oro över att det saknas kunskap om vad en incident är, alternativt att det saknas vetskap om hur en incident ska anmälas inom kommunen.

Intervjupersoner uppger att det är kommunsekreteraren tillsammans med dataskyddsombudet som analyserar anmäld personuppgiftsincident utifrån följande perspektiv: anledningen till att incidenten uppstått samt vilka åtgärder som kan vidtas för att förhindra att liknande incidenter sker igen. I nästa steg är det kanslichef tillsammans med HR-chef som tar ställning om det ska ske en anmälan till IMY och vid behov även gör en anmälan. Incidenterna dokumenteras och diarieförs.

Inom verksamheterna genomförs enligt uppgift analys över de incidenter som har skett i syfte att kunna vidta åtgärder. Incidenterna dokumenteras inte på verksamhetsnivå.

Intervjupersoner uppger att andra typer av incidenter anmäls på samma sätt som personuppgiftsincidenter. Det sker ingen sammanställning eller övergripande analys av dessa incidenter.

Intervjupersoner uppger att samtliga verksamhetsansvariga i kommunen har fått i uppdrag att upprätta kontinuitetsplaner. Arbetet är pågående vid tid för granskningen.

### 3.4.1 Bedömning

Vi gör bedömningen att det i kommunen finns upprättade riktlinjer och rutiner för hantering av personuppgiftsincidenter. Vi gör dock bedömningen utifrån uppgifter från intervjupersoner att det finns en risk att det saknas kunskap om vad en incident är samt om upprättade riktlinjer och rutiner. Därmed anser vi att det finns ett kommunövergripande behov av utbildnings- och informationsinsatser angående incidenthantering.

Vi ser positivt på att kommunen arbetar med att upprätta kontinuitetsplaner för samtliga verksamheter. Utifrån detta rekommenderar vi att kommunstyrelsen säkerställer att planerna regelbundet testas utifrån ändamålsenlighet.

## 3.5 Uppföljning, intern kontroll och rapportering

### 3.5.1 Intern kontroll

I kontakt med kommunen framgår att det saknas en fastställd internkontrollplan för år 2022. På grund av personalomsättning har arbetet med intern kontroll blivit eftersatt. Intervjupersoner uppger att kommunen arbetar mot att framgent inkludera internkontrollarbetet i ledningssystemet Stratsys.

I 2021 års internkontrollplan finns kontrollområde IT-säkerhet. Det framgår att kontrollmomentet syftar till att säkerställa att IT-avledningen bedriver ett systematiskt säkerhetsarbete och att verksamheten följer de regler och riktlinjer som beslutats. Det framgår i kontakt med kommunen att uppföljning av internkontrollplanen för 2021 ännu inte är genomförd.

Vidare uppges i intervjuer att informationssäkerhet inte har beaktats i det riskanalysarbete som ligger till grund för upprättande av internkontrollplan.

### 3.5.2 Uppföljning och rapportering

I intervjuer framgår att det inte genomförs någon samlad uppföljning angående det informationssäkerhetsarbete som bedrivs i kommunen.

Det informationssäkerhetsarbete som bedrivs inom respektive verksamhet följs upp utifrån enskilda insatser, men återrapporteras inte till centrala funktioner.

Med anledning av att kommunen har valt att aktivera stabsläge till ett ”mitt-emellan-läge” träffas staben en gång i månaden. Avstämningen syftar bland annat till att ge en nulägesbeskrivning i förhållande till omvärldsförändringar. I dagsläget förs inga minnesanteckningar från avstämningen.

I intervjuer uppges att kommundirektören både i kommunstyrelsen och i utskotten genomfört regelbundna återrapporteringar angående säkerhetsarbetet i kommunen. Det har inte skett någon särskild återrapportering av specifikt informationssäkerhetsarbetet, utan det har inkluderats i det övergripande säkerhetsarbetet som skett i kommunen.

### 3.5.3 Bedömning

Av det som framkommer i granskningen kan vi konstatera att det i kommunen saknas systematiska uppföljningar av de säkerhetsåtgärder som vidtagits. Vår bedömning utifrån detta är att kommunstyrelsen bör kräva en samlad uppföljning av samtliga verksamheters informationssäkerhetsarbete. Detta då uppföljningen kan utgöra ett beslutsunderlag för åtgärder som behöver vidtas.

Då det i tid för granskningen saknas en internkontrollplan för 2022 är vår bedömning att det finns behov från kommunstyrelsens sida att beakta informationssäkerhet i det

riskanalysarbete som ligger till grund för kommande internkontrollplan. Detta utifrån kommunstyrelsens styrning och uppsiktsplikt, men även som en del i uppföljningsarbetet.

Vi ser positivt på att kommundirektören kontinuerligt återrapporterar till kommunstyrelsen och utskott. Vi rekommenderar kommunstyrelsen att utifrån säkerhetsläge och behov bedöma hur kontinuerlig återrapporteringen bör vara samt ställa krav på att den är dokumenterad. Även detta i syfte att utgöra underlag för beslut om åtgärder.

# 4 Slutsats och rekommendationer

## 4.1 Slutsats

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

Vår bedömning bygger på att det i kommunen inte har genomförts riskbedömning eller informationsklassning av informationen som hanteras. Det arbete som bedrivs genomförs på verksamhetsnivå och det saknas en kommunövergripande bild över de mål och krav som ställs i informationssäkerhetspolicyn.

Vi ser även att det finns en risk att det saknas kunskap angående vad en incident är samt hur en incident ska anmälas inom kommunen. Vi ser därför ett behov av utbildningsinsatser. Insatserna bör även omfatta övergripande information om informationssäkerhet som en del i att säkerställa medvetenhet, kunskap och förståelse för området hos medarbetare samt förtroendevalda.

Vår bedömning är vidare att kommunstyrelsen bör beakta informationssäkerhet i det riskanalysarbete som ligger till grund för kommande internkontrollplan samt efterfråga en samlad uppföljning av det informationssäkerhetsarbete som bedrivs i kommunen.

## 4.2 Rekommendationer

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen att:

- Säkerställa att riktlinjer för informationssäkerhetsarbetet upprättas och implementeras som kan konkretisera policyns intentioner.
- Se över och utifrån behov revidera kommunens IT-policy.
- Säkerställa att uppföljning av efterlevnaden av styrande dokument sker.
- Utreda möjligheten att utse alternativt tillsätta en informationssäkerhetssamordnare. Samordnarens roll bör omfatta en samordnande funktion av det informationssäkerhetsarbete som bedrivs i kommunen, utöver sin roll i personuppgiftshanteringen.
- Upprätta former för genomförande av riskbedömning och informationsklassning samt säkerställa att momenten genomförs.
- Säkerställa att riskanalyser genomförs som kan ligga till grund för eventuella tekniska säkerhetsåtgärder som behöver vidtas samt säkerställa att en mål- och handlingsplan upprättas utifrån genomförs riskanalys.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera en medvetenhet och kunskap om informationssäkerhet.

— Ställa krav om uppföljning och återrapportering av kommunens samlade informationssäkerhetsarbete så att beslut kan tas om mål och handlingsplan över åtgärder som behöver vidtas för att förbättra informationssäkerheten.

Datum som ovan

KPMG AB

Karin Helin Lindkvist
*Certifierad kommunal yrkesrevisor*
*Kundansvarig*

Jenny Thörn
*Kommunal yrkesrevisor*

Ida Larsson
*Kommunal yrkesrevisor*