HÖGSBY KOMMUN
KANSLIET
2016 -02- 03

# *Revisionsrapport*

## Granskning av Informationssäkerhet

## *Högsby Kommun*

*Quentin Authelet*
*Aydin Altun*

*3 februari 2016*

pwc

Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161

# *Innehållsförteckning*



Ankom: 2016-02-03 Ärende: KU 2016 30 Handling: 204161

# 1. Revisionell Bedömning

Vi bedömer att kommunstyrelsen till viss del har ändamålsenliga rutiner och processer för att hantera informationssäkerhet. Detta grundar vi på det samordningsarbete och utförande av riskanalyser som skett. Det saknas en tydlig kravställning för informationssäkerhet med hänsyn till lagstiftning, förordningar, allmänna råd, relevanta standarder, interna regler och verksamhetsbehov. Om detta finns ges möjlighet att göra uppföljning för att säkerställa att gällande krav upprätthålls samt att samhällstjänster kan levereras till medborgarna.

Sammanfattningsvis bör kommunstyrelsen genomföra förbättringar inom följande områden:

- Kravställning avseende informationssäkerhet
- Koordinering av informationssäkerhetsarbete
- Klassificering av informationstillgångar
- Hantering av incidenter och förändringar
- Uppföljningsprocessen
- Kontinuitetshantering

Baserat på ovanstående bedömer vi på övergripande nivå att processer och rutiner för informationssäkerhet inte är i enlighet med "leading practice" för informationssäkerhet och kommunstyrelsen rekommenderas att genomföra föreslagna förbättringar.

För samtliga observationer som noterats i samband med granskningen, se Appendix.

Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161

# 2. Inledning

## 2.1. Bakgrund

Kommuner blir allt mer beroende av sina informationssystem. Ny teknik utgör en viktig komponent för fungerande och effektiva verksamhetsprocesser men introducerar även nya risker. Kommunikation med omvärlden ökar i omfattning och systemen blir mer integrerade såväl inom kommunen som med externa intressenter. Detta ställer krav på ett balanserat risktagande och ett funktionellt säkerhetsarbete. Informationen måste skyddas mot obehörig åtkomst samtidigt som den skall finnas tillgänglig och dessutom vara tillförlitlig – *rätt information i rätt tid och för rätt personer*.

En ändamålsenlig IT-verksamhet som baseras på grundläggande styrprinciper och en väl fungerande teknisk och funktionell plattform är en viktig förutsättning för en effektiv verksamhet.

Inom ramen för revisionsarbetet har revisorerna uppmärksammat informationssäkerhet i sin risk- och väsentlighetsbedömning.

## 2.2. Revisionsfråga

Har kommunstyrelsen på en övergripande nivå ändamålsenliga rutiner och processer för att hantera informationssäkerhet?

### 2.2.1. Revisionskriterier

Relevanta styrdokument avseende informationssäkerhet samt IT-rutiner.

### 2.2.2. Kontrollmål

Den övergripande granskningen ska utgå från bland annat följande kontrollmål:

- Det finns ett strukturerat arbete för att säkerställa en god informationssäkerhet.
- Det finns erforderliga styrande dokument framtagna som är kommunicerade till intressenterna (t ex verksamheten).
- Hantering av behörigheter (tillägg, förändring, borttag) sker strukturerat.
- Behörigheter till applikationer granskas periodiskt.
- Applikationen skyddas med lösenord som efterlever satta policys och ”leading practice”.
- Loggfunktionalitet finns aktiverad i kritiska applikationer.
- Regelbundna logguttag och analys av genomförd aktivitet för de centrala enheterna görs.
- Ändamålsenlig förändringshanteringsrutin finns på plats.
- Rutiner för backup och avbrottshantering finns definierade.
- Utbildning av personal sker i informationssäkerhet.

Ankom: 2016-02-03 Ärende: KU 2016.30 Handling: 204161

Granskningen genomförs enligt följande:

- Genomgång av tillgänglig dokumentation, policys och riktlinjer.
- Interjuver med berörda personer inom IT samt eventuellt utvalda verksamhetspersoner inom ledning och systemförvaltning/utveckling.

Den interna kontrollen över informationssäkerhet bedöms utifrån följande kriterier:

- Det finns en övergripande informationssäkerhetspolicy för kommunen.
- Det finns tydliga processer och riktlinjer definierade för tilldelning och utnyttjande av applikationer och system.
- Det finns kontroller, kontrollmoment och definierade uppföljningsprocesser för uppföljning av vad tredjepartleverantörer gör i systemen, där syftet är att säkerställa fullständighet och riktighet.

Brister inom något av dessa områden kan påverka tillgänglighet, riktighet och konfidentialitet för både finansiell och icke finansiell information.

Granskningen utförs genom intervjuer med nyckelpersoner inom Högsby kommun, samt IT-personal ansvariga för informationssäkerhet. Vidare granskas även stödjande dokument för informationssäkerhet.

### *2.2.3. Avgränsning*

Granskningen ska främst fokusera på central hantering för att säkerställa att den interna kontrollen avseende informationssäkerhet är tillräcklig. Granskningen avser inte att vara:

- Bestyrkande
- Tredjeparts bekräftelse (s k ”Third Party Assurance”)
- Intyg av drift/processer/intern kontroll.

Granskningens innehåll har sakgranskats av Maria Oscarsson, IT-strateg och Anders Johansson, kommunchef/IT-chef.

Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161

# 3. Summering av rekommendationer

Baserat på de risker som är förknippade med observerade brister sammanställs här de rekommendationer som bedöms nödvändiga för att åtgärda det mest prioriterade bristerna.

I enlighet med ledande praxis rekommenderar vi kommunstyrelsen att upprätta en informationssäkerhetsfunktion. Rollen bör ansvara för kravställning mot verksamheten, inklusive IT, projekt, användare samt leverantörer. Informationssäkerhetsfunktionen bör vidare ansvara för att samordna krav avseende lagstiftning, förordningar, allmänna råd, relevanta standarder samt interna regler i ledningssystemet för informationssäkerhet. Rollen skulle därmed i praktiken koordinera krav, utbildnings- och kunskapsnivå samt uppföljning och rapportering till kommunstyrelsen.

Verksamhetens krav på skyddsnivå bör förtydligas avseende tillgänglighet, integritet, spårbarhet och konfidentialitet. Detta kan uppnås i två steg: Steg ett: vi rekommenderar kommunstyrelsen att i samarbete med respektive utskott definiera en lämplig kravställningsnivå avseende informationssäkerhet med hänsyn till hotbilden. Steg två: Vi rekommenderar att systematiska riskanalyser i enlighet med risk- och sårbarhetsmetodiken genomförs för kritiska verksamhetsprocesser, tjänster och system utifrån informationssäkerhetsaspekter.

Vi rekommenderar kommunstyrelsen att genomföra en regelbunden översyn av framtagna styrdokument och krav för att säkerställa efterlevnaden av informationssäkerhet och rådande hotbild mot informationssäkerhet.

Vi rekommenderar även kommunstyrelsen att formalisera informationssäkerhetskrav i avtal med sina leverantörer samt upprätta processer för uppföljning av leverantörers efterlevnad av informationssäkerhetskrav.

Vi rekommenderar kommunstyrelsen att samordna, upprätta och underhålla ett gemensamt register över informationstillgångar för samtlig kritisk information och dess ägare, lokalisering, säkerhetskrav samt kontroller som appliceras på informationen under dess livscykel.

Avslutningsvis rekommenderar vi att en IT-strategi upprättas som ligger i linje med långsiktiga och kortsiktiga verksamhetsmål och prioriteringar.

Ankom: 2016-02-03 Ärende: KU 2016 30 Handling: 204161

# 4. Sammanfattning

Revisionen har genomfört en övergripande granskning av informationssäkerhet. Utgångspunkten för granskningen har varit att förstå om det finns ändamålsenliga processer och rutiner för att säkerställa att väsentlig information behandlas och förvaras på ett säkert sätt.

Granskningen har utgått från den centrala IT-organisationen, vilken består av kommunchef tillika IT-chef och IT-strateg. IT-driften hanteras av Högsbynät AB, vilket bland annat omfattar service och drift av servrar och infrastruktur.

Det finns ingen funktion som är formellt utsedd till att vara informationssäkerhetsansvarig för hela kommunen. Det finns inget formellt uppdrag från kommunstyrelsen att avsätta resurser till att arbeta med frågor kring informationssäkerhet.

I granskningen framkom att det på senare tid påbörjats flertalet förbättringar avseende informationssäkerhet. Bland annat har loggning av olika aktiviteter införts. Det har inte genomförts några kontroller av den information som samlats in via loggningen. Det bör införas rutiner för kontroll och uppföljning av loggar. Ur ett proaktivt uppföljningsperspektiv kommer kommunen under år 2017 att äska medel från kommunstyrelsen till anskaffning av ett verktyg för att kunna upptäcka skadlig kod och intrång i kommunens infrastruktur och IT-system.

Det finns ett samarbete med Regionförbundet i Kalmar län genom en informationssäkerhetssamordnare och med kommunerna Oskarshamn och Hultsfred (H2O) där det finns två personer som arbetar med verksamhetsutveckling med stöd av IT. Det finns även ett länsgemensamt projekt där Myndigheten för samhällsskydd och beredskap (MSB) har tilldelat 1,7 MSEK för kompetenshöjande åtgärder inom informationssäkerhet, vilket anses vara positivt.

**IT-styrning, ansvarsfördelning och förvaltningsrutiner**

Enligt nuvarande ansvarsfördelning står IT-strategen som ansvarig för kommunens IT-organisation och innehar det största ansvaret, men viss delning av ansvar sker med kommunchefen. Informationssäkerhetssamordnaren på Regionförbundet har anlitats för att bland annat stötta IT-strategen samt uppdatera en informationssäkerhetspolicy.

Under året har en vägledning för informationssäkerhet tagits fram i samarbete med informationssäkerhetsamordnaren på Regionförbundet i Kalmar län. Vid en övergripande granskning av policyn bedöms den hålla god kvalitet och kan vara ett steg i att få styrande dokument på plats.

Det finns även en kontinuitetsplan där applikationer kopplade till HSA (risktäckande katalogtjänst med kvalitetssäkrade uppgifter om personer, funktioner och

Ankom: 2016-02-03 Ärende: KU 2016 30 Handling: 204161

enheter i Sveriges kommuner, landsting och privata vårdgivare) ingår. I projektet "Home Care" har klassificering av denna typ av information gjorts.

Information och applikationer ägs primärt av systemägare, men ägandeskapet kan delegeras till systemförvaltare. Ansvaret för dessa kan därmed också ses som att de ligger på respektive systemförvaltare. Systemförvaltare har även ansvaret att se till att lagkrav och samordning följs av respektive system.

Det sker inte någon utbildning i informationssäkerhet. Vid anställningstillfället får den nyanställde en genomgång av vilka styrande dokument som gäller för dennes område, vilket den anställde skriftligen intygar att den tagit del av.

**Behörighetshantering**

En regelbunden genomgång av behörigheter och användare genomförs, men det saknas formell kontroll av hur och när genomgången ska göras. Då det saknas en formaliserad kontroll finns heller ingen riskbedömning för vilka risker som minskas genom att utföra genomgången.

Denna brist blir tydligare då det saknas en riskanalys för vem som kommer åt vilken information och om det finns personer med åtkomst kopplad till flertalet roller. Roller som registreras i systemen baseras istället på standardiserade roller, men är i vissa fall justerade för att lägga till eller ta bort funktioner. Även den geografiska behörigheten, till exempelvis roller relaterade till omvårdnadssystemen, justeras baserat på om användaren har ett fast arbetsställe, är tillsvidareanställd eller vikarie inom flertalet vårdområden.

För tilldelning, förändring och borttag av behörigheter till IT-infrastrukturen (nätverk, e-post etc) är ansvaret begränsat till IT-strateg som mottagit beställning från verksamhetsansvarig chef. Det är också verksamhetsansvarig chef som tillser att tilldelad behörighet ändras eller återkallas vid behov. För tilldelning eller förändring av behörighet till applikationer ligger ansvaret hos respektive system-förvaltare.

Nedan har observationer för granskningen sammanställts på aggregerad nivå. Observationerna har bedömts efter dess väsentlighet, graderingen illustreras med hjälp av följande definition:

**Hög** – En brist med stor påverkan på system, processer eller intern kontroll vilken kan medföra att verksamheten exponeras för betydande förluster eller väsentliga fel i rapporteringen. Brister med prioritet *hög* bör hanterats snarast.

**Mellan** – En brist med påverkan på system, processer eller intern kontroll som kan medföra att verksamheten exponeras för förluster eller ett betydande fel i rapporteringen. Brister med prioritet *mellan* bör hanteras inom ett år.

**Låg** – Mindre brister eller fel där risken för otillbörlig användning och/eller felaktigheter är lägre, men där det ändå bedöms finnas utrymme för förbättringar. Brister med prioritet *låg* bör hanteras inom två år.

Ankom: 2016-02-03 Ärende: KU 2016 30 Handling: 204161

| Ref. | Observation | Prioritet |
|---|---|---|
| **2015.1** | Bristande koordinering av informationssäkerhetsarbete | **Mellan** |
| **2015.2** | Bristande uppdatering av ledningssystem för informationssäkerhet | **Hög** |
| **2015.3** | Otydliga säkerhetskrav i projekt | **Mellan** |
| **2015.4** | Otydlig säkerhetskravställning och uppföljning av leverantörer | **Hög** |
| **2015.5** | Bristande rutiner för klassificering och hantering av information | **Mellan** |
| **2015.6** | Avsaknad av IT-strategi | **Hög** |
| **2015.7** | Bristande rutiner för förändringshantering | **Låg** |
| **2015.8** | Bristande rutiner för incidenthantering | **Mellan** |
| **2015.9** | Bristande uppföljningsprocess | **Hög** |
| **2015,10** | Bristande kontinuitetsplanering | **Mellan** |

För mer information och detaljer gällande respektive observation, se sektionen "Observationer" i Appendix.

Ankom: 2016-02-03 Ärende: KU 2016 30 Handling: 204161

# Appendix

## Observationer

### 2015.1 Bristande koordinering av informationssäkerhetsarbete

**Observation**

Granskningen visade att IT-strategen informellt utsetts att ansvara för informationssäkerhetsarbetet, inklusive ansvar för styrande dokument, d v s ledningssystemet för informationssäkerhet. Det saknas dock en formulerad ansvarsroll för informationssäkerhet, som kravställare mot verksamheten, inklusive IT, projekt, användarna och leverantörerna. I dagsläget är detta ansvar utfördelat på respektive verksamhet och det saknas tydliga informationssäkerhetskrav som är kopplade till legala krav, standarder och allmänna råd samt interna regler. Risker relaterade till illegitim användning eller otillgänglighet av information hanteras av respektive verksamhet och sammanställs inte, vilket innebär att det saknas en gemensam hotbild gällande informationssäkerhet och en process för hantering av informationsrisker.

Regionförbundet i Kalmar län har en regionövergripande resurs som jobbar med informationssäkerhetsfrågor. Dock har arbetet främst fokuserat på uppföljning av efterlevnad av informationssäkerhetskrav enligt standarden för informationssäkerhet, ISO/IEC 27001, vägledning för kommunens informationssäkerhet från Myndigheten för samhällsskydd och beredskap (MSB) och föreskrifter från Socialstyrelsen, SOSFS 2008:14. Det framkom dock att kravbilden är ofullständig då direkt koppling till övriga legala krav så som personuppgiftlagen, offentlighets- och sekretesslagen, säkerhetsskyddslagen, arkivlagen och patientdatalagen är otydlig.

**Risk**

Avsaknad av en övergripande ansvarsroll för informationssäkerhet medför en risk för att säkerhetskravställning inte är fullständig och att implementerade kontroller i infrastruktur, system och applikationer inte är ändamålsenliga. Vidare riskerar verksamheten att inte identifiera eller hantera informationsrisker.

**Rekommendation**

Enligt ledande praxis rekommenderar vi kommunstyrelsen att upprätta en informationssäkerhetsfunktion. Informationssäkerhetsfunktion bör ansvara för att samordna kravställning mot verksamheten, inklusive IT, projekt, användarna och leverantörerna. Vidare bör informationssäkerhetsfunktionen ansvara för att samordna säkerhetskrav från gällande lagstiftningar, förordningar, lagar, allmänna råd, relevanta standarder och interna regler, samt formalisera dessa krav i ledningssystemet för informationssäkerhet. Rollen bör även ansvara för att koordinera hanteringen av informationsrisker. Det bör också vara informations-

Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161

säkerhetsfunktionens ansvar att koordinera utbildnings- och medvetandearbete gällande informationssäkerhet. Sedan bör rollen ansvara för att säkerställa spårbarhet av krav, koordinera uppföljning och mätning av regelefterlevnad samt rapportering till kommunledningen.

**Prioritet:** Mellan

### *2015.2 Bristande uppdatering av ledningssystem för informationssäkerhet*

#### Observation

Granskningen visar att det finns en formaliserad informationssäkerhetspolicy. Dokumentet innehåller kortfattad information om organisation, rollfördelning och mål. Ansvaret för informationssäkerhetspolicyn har delegerats till IT-strategen. Dock har informationssäkerhetspolicyn inte uppdaterats sedan den antogs år 2010.

I ledningssystemet finns instruktioner för förvaltning, kontinuitet och drift samt för användare som ska beaktas.

#### Risk

Bristen på uppdaterade styrdokument relaterade till informationssäkerhet kan resultera i bristande kravställning vad gäller förändrad teknik och verksamhetsverktyg, så som användning av molntjänster, digitalisering och mobilitet. Då IT-området förändras snabbt är det viktigt att policys och underliggande styrdokument adresserar nya informationsrisker.

#### Rekommendation

I syfte att samordna informationssäkerhetsarbetet och säkerställa en tydlig kravbild rekommenderar vi att ledningssystemet för informationssäkerhet uppdateras. Ledningssystemet bör förtydliga verksamhetens krav genom att beskriva skyddsnivå avseende såväl tillgänglighet, integritet, spårbarhet som konfidentialitet.

Som första steg i detta arbete rekommenderar vi att kommunstyrelsen tillsammans med utskotten definierar en lämplig kravställningsnivå avseende informationssäkerhet med hänsyn till hotbilden. Ett förslag är att exempelvis följa MSB:s vägledning för kommunens informationssäkerhet som pekar på områden i standarden för informationssäkerhet, SS-ISO/IEC 27001. Vägledningen och standarden erbjuder bäst praxis-orientering för att tillhandahålla krav för att upprätta, införa, underhålla och ständigt förbättra ett ledningssystem för informationssäkerhet.

Som nästa steg rekommenderar vi att systematiska riskanalyser i enlighet med risk- och sårbarhetsanalysmetodik genomförs för kritiska verksamhetsprocesser, tjänster och system, samt att dessa görs med hänsyn till ovannämnda informationssäkerhetsaspekter.

Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161

För väsentliga informationssäkerhetsrisker som identifieras och för att säkerställa att åtgärder vidtas, rekommenderar vi även att befintliga policydokument kompletteras med informationssäkerhetskrav.

Rutiner för kontinuerlig utvärdering av framtagna krav bör upprättas. Därtill bör en översyn av framtagna styrdokument genomföras regelbundet.

**Prioritet:** Hög

### *2015.3 Otydliga säkerhetskrav i projekt*

#### Observation

Informationssäkerhetskrav finns delvis definierade i informationssäkerhetspolicyn, dock saknas för närvarande instruktioner för hantering av säkerhetskrav i projekt, så som vid utveckling av e-tjänster. Vidare saknas vem som är ansvarig för säkerheten i projekt. Vi har inte heller kunnat observera att kvalitetskontroll avseende säkerhet har genomförts för projekt.

#### Risk

Det föreligger en risk för att säkerhetsaspekter inom projekt inte tas i beaktande samt att verksamheten inte är medveten om säkerhetsrelaterade risker i projekt samt att hot inte identifieras och åtgärdas inom rimlig tid.

#### Rekommendation

Vi rekommenderar att en kontrollkatalog (eller checklista) för att redovisa samtliga informationssäkerhetskrav som bör beaktas i projektcykeln upprättas. Den bör inkludera överlämning från projekt till förvaltning. Exempel på kontroller är säker hantering av testdata, härdning av system, kodgranskning och intrångstester.

Vi rekommenderar projektet att vid relevanta beslutspunkter återrapportera eventuella informations- och IT-säkerhetsbrister samt risker till lämplig instans, så som informationssäkerhetsfunktion eller informationsägare, detta för att möjliggöra utvärdering av implementerade säkerhetskontroller. Inför överlämning till förvaltning bör säkerhetskontroller finnas implementerade i driftmiljö.

**Prioritet:** Mellan

### *2015.4 Otydliga säkerhetskravställning och uppföljning av leverantörer*

#### Observation

Informationssäkerhetskrav definieras inte i avtal med leverantör och avtalade tjänster varken utvärderas eller kontrolleras regelbundet. En struktur för

Ankom: 2016-02-03 Ärende: KU 2016 30 Handling: 204161

uppföljning av kravefterlevnad hos leverantörer saknas, liksom en plan för systematisk utvärdering av leverantörer.

**Risk**

Avsaknad av en formell kravställning och uppföljning av informationssäkerhetsaspekter kan föranleda att risker kopplade till leverantörernas hantering av kommunens information inte upptäcks och åtgärdas inom rimlig tid. Detta kan i sin tur leda till driftstörningar, obehörig åtkomst till och manipulering av information.

**Rekommendation**

Vi rekommenderar att informationssäkerhetskrav formaliseras i avtal med leverantörer, samt att en plan för att utföra uppföljningar av leverantörernas efterlevnad av fastställda informationssäkerhetskrav upprättas.

**Prioritet:** Hög

### *2015.5 Bristande rutiner för klassificering och hantering av information*

**Observation**

Det finns utsett ett personuppgiftsombud. Det är dock otydligt vad rollen och arbetsuppgifterna innebär, både ur ett kravställnings- och uppföljningsperspektiv. Vi noterade att information om vad personuppgiftslagen (1998:204) reglerar och vilka krav som ställs utifrån lagen inte ges i någon större utsträckning till verksamheten, medarbetarna och leverantörer. Det saknas även en definition om vad personuppgifter eller känsliga personuppgifter innebär för kommunen.

Utöver personuppgifter som är styrda av personuppgiftslagen har övriga väsentliga informationstyper inte identifierats fullständigt. Detta innebär att det saknas övergripande kunskap i organisationen om vilken information som finns i verksamheten. Bristande kravställning avseende klassificering och hantering av information innebär en utmaning för verksamheten att ändamålsenligt prioritera information och därmed en utmaning för IT att prioritera, ur ett kontinuitetsperspektiv, stödsystem och applikationer där information hanteras.

Informationsägare är inte heller tydligt definierade. Det är ägarens uppgift att informationen skyddas ändamålsenligt, d v s att endast behörig personal har åtkomst till informationen, att informationen lagras på lämplig arbetsyta samt att den transporteras enligt fastställda krav. Dock har vi noterat att ägarskapet inte är förankrat i verksamheten och i dagsläget föreligger otydligheter kring vem som ansvarar för övervakning av informationshanteringen. I och med att det är otydligt för verksamheten vilka informationstyper som finns är det också svårt att bedöma efterlevnad av önskat skydd.

Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161

### Risk

Detta innebär en risk för att implementerade kontroller för att skydda tillgångar inte reflekteras av säkerhetskrav. Icke ändamålsenliga kontroller kan medföra risk för informationsläckage, driftstörningar och otillåten datamanipulering.

### Rekommendation

Enligt rekommendation 2015.1 ovan föreslår vi att en informationssäkerhetsfunktion utses. Rollen bör bland annat ansvara för att följa upp att verksamheten identifierar och beaktar befintliga informationstyper. Informationssäkerhetsfunktionen bör ur ett regelverksperspektiv specificera krav på skyddsnivå för informationstyper som verksamheten bedömer relevanta. Därefter bör informationssäkerhetskrav brytas ner till IT-säkerhetsinstruktioner, -rutiner och -kontroller som skall appliceras för dessa informationstyper. Informationsägarerollen bör också förtydligas. Ansvar kan i praktiken ligga hos systemförvaltare, förvaltningschef eller övergripande inom kommunen för generella informationstyper så som personuppgifter.

Vi rekommenderar även att informationssäkerhetsfunktionen samordnar initiativ inom verksamheten för att upprätta och underhålla ett gemensamt register över information som redovisar samtlig kritisk information och dess ägare, lokalisering samt vilka kontroller som bör appliceras under hela informationslivs-cykeln (från att information skapas till att den lagras, bearbetas, transporteras, arkiveras och till sist gallras).

Vi rekommenderar att en kontrollkatalog upprättas som beskriver säkerhetskrav som bör appliceras på respektive informationstyp beroende på klassificeringen. Säkerhetskrav bör baseras på konfidentialitet, integritet, spårbarhet och tillgänglighet av information i syfte att säkerställa en ändamålsenlig skyddsnivå i enlighet med kraven i den styrande dokumentationen. Därefter bör informationsägare skapa rutiner för att säkerställa efterlevnad av fastställda krav, exempelvis genom årliga genomgångar.

**Prioritet:** Mellan

## *2015.6 Avsaknad av IT-strategi*

### Observation

Granskningen visar att IT-relaterade åtgärder hanteras ad hoc och att det saknas ett strategiskt tillvägagångssätt för att prioritera långsiktiga IT-förändringar och stödja verksamheten i utvecklingsprojekt av exempelvis e-tjänster. Vi noterade dock att två verksamhetsutvecklare har anlitats av H2O kommunerna för att i ett första steg kartlägga utvecklingsbehov i form av e-tjänster och sedan definiera målbilden ur ett arkitekturperspektiv.

Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161

### Risk

Avsaknad av en IT-strategi försvårar styrningen av IT-verksamheten och kan leda till onödiga kostnader genom sämre grundande beslut av IT-investeringar och resursallokering.

### Rekommendation

För att stödja verksamhetsutveckling rekommenderar vi att kommunstyrelsen beslutar om en strategi för IT-verksamheten i linjen med verksamhetsstrategi, mål och prioriteringar, med hänsyn till resultatet från det pågående arkitekturarbetet. Detta bör inkludera båda en kortsiktig och en långsiktig handlingsplan som tydliggör vilka projekt och aktiviteter som ska genomföras inom IT.

**Prioritet:** Hög

## *2015.7 Bristande rutiner för förändringshantering*

### Observation

Det saknas tydliga rutiner för förändringshantering.

IT-avdelning består av IT-strategen och Högsbynät AB. IT-strategen deltar i den dagliga operativa driften tillsammans med Högsbynät. Det sker en dialog mellan IT-avdelningen och aktuell systemförvaltare i verksamheten innan en förändring införs. Det saknas dock en formell process för hantering av förändringar. Avstämning med systemförvaltare sker för närvarande muntligt. Spårbarhet över genomförda förändringar saknas då förändringen inte dokumenteras vilket kan försvåra uppföljning och felsökning vid incident.

### Risk

Avsaknad av tydliga förändringsrutiner innebär en risk för obehörig åtkomst, obehörig förändring av data och läckage av kritisk information, vilket kan orsaka konsekvenser för hela verksamheten, till exempel rykterisker och legala risker.

### Rekommendation

För att säkerställa att alla ändringar som görs i produktionsmiljön är kontrollerade rekommenderar vi att processen för hantering av förändringar i system och applikationer formaliseras. Processen och underliggande rutiner bör säkerställa att alla moment har genomförts innan förändringar implementeras i produktionsmiljön.

Kontrollstegen i förändringshanteringsprocessen bör åtminstone hantera:

- En dokumenterad förändringsförfrågan med godkännande,
- Godkännande av testresultat,
- Godkännande av produktionssättning,
- Plan för återrullning av genomförd ändring.



Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161

**Prioritet:** Låg

### *2015.8 Bristande rutiner för incidenthantering*

#### Observation

Enligt uppgifter saknas rutiner för att rapportera, dokumentera och följa upp incidenter. Det finns planer på att införskaffa ett stödsystem som kan identifiera inskränkning och driftincidenter. Målet är att kunna upptäcka och hantera diverse incidenter effektivare än i nuläget.

#### Risk

Bristande rutiner för hantering av incidenter kan leda till:

- försämrad möjlighet till upptäckt och åtgärd,
- att personalen inte vet hur de skall hantera onormala situationer,
- att tillräckligt med bevismaterial inte samlas in,
- att informationssäkerhetsrelaterade incidenter inte rapporteras eller följs upp,
- att lärdomar och erfarenhetsåterföring inte fungerar, vilket kan leda till att problem återkommer.

#### Rekommendation

Vi rekommenderar att rutiner för att hantera incidenter införs. Rutinerna bör innehålla en tydlig mottagare av incidentlarm, hanteringsregler för olika typer av incidenter, ett verktyg för att samla alla incidenter samt instruktioner för eventuell eskalering av ärenden. En del i incidenthanteringen är att informera/utbilda användarna i att kunna identifiera och rapportera incidenter. Detta bör beskrivas i informationssäkerhetsinstruktion för användare. Vi föreslår att alla incidenter som rapporteras ska registreras i ett ärendehanteringssystem för att säkerställa spårbarhet samt göra uppföljning lättare.

**Prioritet:** Mellan

### *2015.9 Bristande uppföljningsprocess*

#### Observation

Det finns rutiner på plats för uppföljning av loggaktivitet i applikationer. Detta gäller dock inte alla applikationer då kontroller inte hunnit implementeras för samtliga system. Uppföljning sker periodiskt och avser att identifiera avvikelser i aktivitet som exempelvis att endast behöriga är aktiva i systemet och att aktivitet är kopplad till arbetsspecifika uppgifter.

Ankom: 2016-02-03 Ärende: KU 2016 30 Handling: 204161

Enligt uppgift har dock uppföljningsrutiner tydliga brister då ingen hanterings-process av avvikelser finns implementerad. Trots att loggkontroll omfattar kontroll av behörigheter så framkom ingen formaliserad process för hantering av övriga avvikelser. Det finns ingen procedur på plats som larmar vid avvikelser. Avvikelser identifieras primärt när loggkontroll genomförs och en längre tidsperiod kan därmed ha förflutit från att avvikelser uppstår tills att identifikation sker.

**Risk**

Brister i uppföljningsprocess riskerar att leda till inkonsekvent hantering av avvikelser i loggkontroll.

**Rekommendation**

Vi rekommenderar att uppföljningsprocessen formaliseras för att minska risken för ofullständig hantering av avvikelser i loggkontroll.

**Prioritet:** Hög

### *2015.10 Bristande kontinuitetsplanering*

Kontinuitetsplanering är en metod för organisationen att säkerställa fortsatt operativ förmåga genom att planera för händelser som kan komma att påverka verksamhetens leverans.

Det saknas en process och ansvarsfördelning för kontinuitetshantering, inklusive kris- och katastrofhantering, för att hantera händelser som kan orsaka avbrott i den operationella verksamheten.

Detta beror delvis på avsaknad av tydligt ägarskap och ansvarsfördelning för kontinuitetsarbetet samt avsaknad av en process som beskriver hur ett riskbaserat kontinuitetsarbete ska bedrivas och styras ur en informationssäkerhetssynpunkt. Vi har noterat att det finns en ambition att ta fram en sådan process i form av en informationssäkerhetsinstruktion för kontinuitet och drift.

**Risk**

Avsaknad av en formell process för kontinuitetshantering ökar risken för att organisationen inte kan hantera avbrott i den operationella verksamheten på ett ändamålsenligt sätt.

**Rekommendation**

Vi rekommenderar att det upprättas en process för kontinuitetshantering. Processen bör ägas, förvaltas och vidareutvecklas av verksamheten. Vi rekommenderar därför att ansvaret över processen tydliggörs. Därtill bör processen innefatta en beskrivning av hur organisationen löpande ska hantera identifierade risker och ta fram åtgärdsplaner eller krisberedskapsplaner för dessa. Krisberedskapsplanerna bör innefatta reservrutiner som beskriver alternativa arbetssätt under pågående krissituation.

Ankom: 2016-02-03 Ärende: KU 2016.30 Handling: 204161

Dessutom bör processen etablera eskalerings- och rapporteringskanaler. Vidare behöver framtagna planer hanteras enligt en fastställd livscykel. Samtliga berörda bör involveras för att säkerställa att planerna utvärderas och testas regelbundet. Krisövningar bör genomföras årligen och kan variera i omfattning, t ex skrivbordstest eller fullskalig simulering.

Ur ett tillgänglighetsperspektiv rekommenderar vi att regelbundna tester genomförs av återskapande av systemen som stödjer verksamhetskritiska processer, samt att rutiner och instruktioner för säkerhetskopiering, återläsning och test formellt dokumenteras.

**Prioritet:** Mellan

Ankom: 2016-02-03 Ärende: KU 2016 30 Handling: 204161

## *Granskat material*

1. Långsiktig plan Högsby kommun 2016-2020.pdf
2. Bild gemensam kalender support.
3. Systemförteckning Högsby kommun.xlsx
4. KRAVSPECIFIKATION DRIFTMILJÖ itsystemprogramvarawebbtjänst.pdf
5. Mall Avbrottsrapport.docx
6. Högsby Rutinbibliotek.xlsx
7. Checklista produktionssättning.docx
8. Anställda tv 150926.xlsx
9. Tidsbegränsade anst 150926.xlsx
10. Slutat under året.xlsx
11. procapitaTSSadmin
12. BESTÄLLNING AVBESTÄLLNING inloggning dator skyddad utökad.pdf
13. Infosäk A Högsby.pdf
14. Infosäk B Högsby.pdf
15. Viktig Info om känslig info Högsby.pdf
16. Riktlinjer för information och kommunikation i Högsby kommun.pdf
17. Informationsäkerhetspolicy Högsby kommun.pdf
18. Avtal underhåll 2009.pdf
19. Avtal underhåll 2007.pdf
20. Avtal Leverans.pdf
21. Lösen SSA.txr
22. Systemsäkerhetsanalys Högsby v1.0.docx
23. SU Hby 4 juni 15 v1.0
24. Rutiner för tillträde och arbete i servicerummet Högsby kommun.docx
25. Bilaga 7 åtgärdsplan v1.0.docx
26. Bilaga 5 RSA_Serverhall_2012_v1.0.docx
27. Bilaga 6 RSA ver 20150601 v1.0.docx
28. Bilaga 4 grundskyddsanalys v1.0.docx
29. Bilaga 3 Säkerhet i IT-utrymmen v1.0.docx
30. Bilaga 2 SOSFS v1.0.docx
31. Bilaga 1 verksamhets och systembeskrivning v1.0.dox
32. Lösenord.txt
33. RSA_Serverhall.docx

Ankom: 2016-02-03 Ärende: KU 2016.30 Handling: 204161

## *Intervjuade personer*

Fredrik Sandqvist, Informationsansvarig

Maria Oscarsson, IT-strateg

Lennart Engström, Systemansvarig ProCapita

Anders Johansson, Kommunchef

Steven Dorch, Systemsäkerhetssamordnare, Regionförbundet i Kalmar län

Malin Hanson, Verksamhetsutvecklare

Jens Fridsén, Verksamhetsutvecklare/IT-arkitekt

Ankom: 2016-02-03 Ärende: KU.2016.30 Handling: 204161