# Granskning av kommunens IT-säkerhet

Rapport

Östhammars kommun

KPMG AB

2019-10-30

Antal sidor 14

Antal bilagor 1

**Östhammars kommun**
Granskning av kommunens IT-säkerhet

2019-10-30

# Innehållsförteckning

# 1 Sammanfattning

Vi har av Östhammars kommuns revisorer fått i uppdrag att granska kommunens arbete med IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2019.

Granskningen har syftat till att konstatera om kommunen har erforderlig kontroll över att de bedömningar och beställningar som införd IT-säkerhet grundar sig på är baserade på de risker och behov som ansvariga för informationen har identifierat och kommunicerat.

Vår sammanfattande bedömning utifrån granskningens syfte är att det finns brister i kommunstyrelsens arbete för att säkerställa en tillräcklig kontroll över kommunens Informations- och IT-säkerhet. Vår bedömning baseras på att kommunstyrelsen inte har tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas. Arbetet med informations- och IT-säkerhet baseras inte på risker och behov som ansvariga för informationen har fastställt. Utan det underlaget anordnas IT-säkerhetsåtgärderna på ett sätt som IT-avdelningen upplever som nödvändigt utifrån sina förutsättningar. Det finns olika former att säkerställa att efterlevnad av beslutad IT-säkerhet sker. I de fall det inte går att säkerställa är det näst bästa att se till att incidenter upptäcks och kan åtgärdas. Vi bedömer att detta arbete inte är tillräckligt och att kommunen behöver utveckla sitt arbete med riskanalys i syfte att tydliggöra vilka hot och brister som finns i kommunens IT-miljö och avseende informationssäkerheten.

Trots alla maskinella skydd och varningssystem är det medarbetarna som ska efterleva den beslutade IT-säkerheten. För detta krävs en viss kunskapsnivå och en medvetenhet inom Informations- och IT-säkerhet. Vi ser det som positivt att kommunen har genomfört utbildning i Informationssäkerhet för alla medarbetare samt följt upp deltagandet på enhetsnivå.

I granskningen har framkommit att ett övergripande säkerhetsarbete pågår i kommunen som har påbörjats genom att göra en säkerhetsskyddsanalys och att den är utgångspunkten för kommande åtgärder som även inkluderar Informations- och IT-säkerhet. Det finns en medvetenhet om behovet av ett utvecklingsarbete inom granskningens område men organisationsförändringar och resursbrist anges som några anledningar till att arbetet inte har kunnat genomföras.

Det saknas politiska beslut och uppdrag till verksamheten för att säkerställa arbetet med kommunens informations- och IT-säkerhet och ingen rapportering sker kring incidenter eller åtgärder för att upprätthålla en tillräcklig säkerhetsnivå.

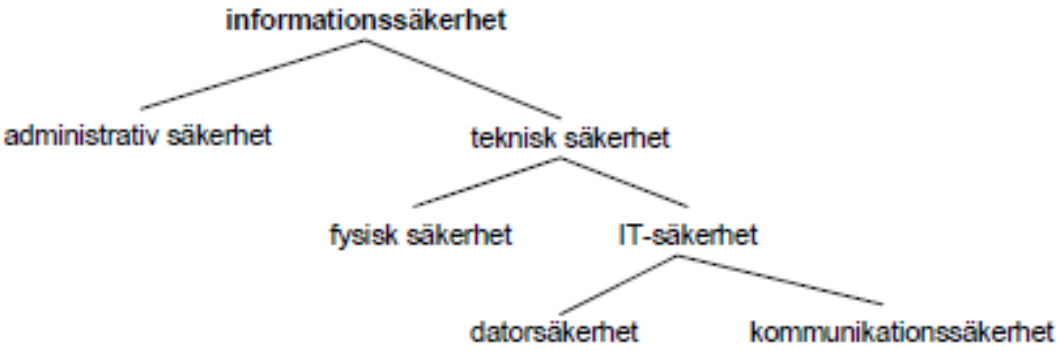
Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- säkerställa att det finns aktuella, kända och tillämpade styrdokument med tillhörande instruktioner som lägger en grund för en god informationssäkerhet och tillhörande IT-säkerhet. Dessa bör även tydliggöra ansvar och roller för arbetet.
- säkerställa att informationsklassning av de datoriserade verksamhetssystemen genomförs för att verksamhetsansvariga ska kunna bedöma vilka säkerhetsåtgärder som behöver vidtas för att skydda informationstillgångar de ansvarar för
- ge IT-enheten i uppdrag att ta fram kontinuitetsplaner som beskriver de reserv-, återställnings- och återgångsrutiner som används för att säkerställa kontinuiteten i en prioriterad verksamhet eller process
- se till att utbildning i informationssäkerhet finns med som en del i introduktion av nyanställda, samt logga vilka som slutfört den för att säkerställa att medarbetarna får grundläggande kunskap inom informationssäkerhet och sitt ansvar i IT-användandet.

# 2 Inledning/bakgrund

Vi har av Östhammar kommuns revisorer fått i uppdrag att granska hur kommunen med underlag av sina styrande dokument avseende informationssäkerhetsrutiner anordnat sin IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2019.

Med IT-säkerhet avses en väl avgränsad del av det större begreppet informationssäkerhet och består av delarna datorsäkerhet och kommunikationssäkerhet. Bilden nedan illustrerar förhållandet mellan informationssäkerhet och IT-säkerhet.




Av standarderna i ISO 27000-serien kan utläsas att IT-säkerhet är underordnad informationssäkerheten. Placeringen innebär att beslut om IT-säkerhet styrs av de beslut som tas av system och/eller objektägare som har att efterleva beslutad informationssäkerhetspolicy med tillhörande tillämpningsföreskrifter. Alternativt tillämpar kommunen ett LIS[1]

Revisorerna utesluter inte att det finns risk för att införda IT-säkerhetsåtgärder inte står i relation till hur verksamhetsansvariga klassificerat den information de har ansvar för. Det kan i sin tur innebära att ansvarsförhållandena avseende kommunens informationstillgångar inte är tillräckligt kända och respektive ansvariga inte beställer/styr den IT-säkerhet som tillhandahålls.

Uppdraget ingår i revisionsplanen för år 2019.

## 2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att konstatera om kommunen har erforderlig kontroll över att de bedömningar och beställningar som införd IT-säkerhet grundar sig på är baserade på de risker och behov som ansvariga för informationen har identifierat och kommunicerat.

Granskningen ska besvara följande revisionsfrågor:

[1] Ledningssystem för informationssäkerhet

- Har kommunstyrelsen tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
- Har kommunstyrelsen tillsett att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet?
- Finns det former för att säkerställa efterlevnaden av beslutad IT-säkerhet?

Granskningen avser kommunstyrelsen.

## 2.2 Revisionskriterier

Vi har bedömt om etablerad IT-säkerhet uppfyller interna regelverk samt policys med tillhörande tillämpningsföreskrifter.

## 2.3 Metod

Granskningen har genomförts genom inledande dokumentstudier och därefter en utfrågning (hearing) med deltagande av tjänstemän på förvaltningsledningsnivå och inom IT och säkerhetsarbete.

I bilaga 1 redovisas det frågekomplex som har använts vid utfrågningen.

Rapporten är faktakontrollerad av IT-chef och kundansvarig.

# 3 Resultat av granskningen

## 3.1 Organisation

Ansvarig för Informationssäkerhetsarbetet är kommunens säkerhetsskyddschef. Övriga medarbetare inom säkerhet och beredskap samt kommunens utsedda dataskyddsombud är viktiga funktioner i arbetet. Dessa är organiserade under kommunledningsförvaltningen som lyder under kommunstyrelsen.

Östhammar kommuns IT-verksamhet ingår från 1 januari 2019 i en samverkan om IT-funktion i en gemensam IT-nämnd, kallad Cassiopeia. Samverkansavtalet gäller mellan kommunerna Heby, Knivsta, Tierp, Älvkarleby och Östhammar, med en gemensam IT-nämnd som styrs av ett särskilt reglemente.

Av reglementet framgår att ansvaret för kommunernas förvaltning, inklusive t ex krisberedskap och informationssäkerhet samt den digitala utvecklingen, i sin helhet ligger inom respektive kommuns ansvar. Nämnden kan dock efter överenskommelse i digitaliseringsrådet ges i uppdrag av en eller flera kommuner att ta fram beslutsunderlag och medverka i dessa frågor. Det framgår i reglementet att nämnden särskilt bör arbeta för att se över möjligheter till gemensamma lösningar som stöd vid allvarlig samhällsstörning. Nämnden ansvarar för den tekniska och produktmässiga säkerheten som är ett stöd för kommunernas förvaltningsarbete.

Samverkan inom Cassiopeia gäller strategiska och dagliga, operativa IT-frågor. Tierps kommun är arbetsgivare för medarbetarna inom IT men dessa är lokalt placerade i kommunerna. IT-chef finns anställd inom nämnden och varje kommun har en kundansvarig som är kontakt mellan kommunen och nämnden med ansvar för vissa processer i samarbetet.

Inom systemförvaltningsarbetet finns en uppbyggd struktur av objektägare och förvaltningsledare som är utsedda från verksamheterna samt från IT-avdelningen där utvecklingsarbetet för systemförvaltning bedrivs.

Ett IT-styrningsråd bildades 2014 i syfte att tydliggöra kommunens IT-styrning, detta har utvecklats till ett e-styrningsråd med ovan representanter från systemförvaltningsmodellen. Även dataskyddsombud är med i e-styrningsrådet. Dessa träffas även i ett regionalt digitaliseringsråd för att diskutera gemensamma utvecklingsfrågor.

#### *Bedömning*

Vår bedömning är att det inte är helt tydliggjort hur uppdraget för att säkerställa en god IT-säkerhet ser ut då den nya IT-organisationen fortfarande är under uppbyggnad.

I systemförvaltningsuppdraget finns en uppbyggd struktur för dialog mellan förvaltningarna och IT som kan utgöra en bra grund för utvecklingsarbetet kring Informations- och IT-säkerhetsfrågorna.

## 3.2 Styrande dokument

### 3.2.1 Informationssäkerhetspolicy

IT-säkerhet är underordnat informationssäkerhet. Av detta följer att beslut om IT-säkerhet styrs av de beslut som tas av system som har att efterleva beslutad informationssäkerhetspolicy med tillhörande tillämpningsföreskrifter. Av denna anledning har vi utvidgat granskningen till att även omfatta informationssäkerheten.

Östhammars kommun har en informationssäkerhetspolicy som antogs av kommunfullmäktige 2016-06-14 § 65/2016.

Kommunens informationssäkerhetspolicy är ett huvuddokument som ska ligga till grund för rutiner, planer och instruktioner. Dessa informationssäkerhetsinstruktioner ska enligt policyn revideras och fastställas årligen av kommunstyrelsen.

I policyn framgår att målet med Östhammars kommuns informationssäkerhetsarbete är:

- att samtlig personal har kunskap om gällande informationssäkerhetsregler
- att informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- att ingångna avtal är kända och följs

- att krishanteringsförmågan upprätthålls
- att alla investeringar både i form av information och teknisk utrustning har skydd i tillräcklig grad
- att det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- att hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet fortlöpande analyseras och hanteras
- att händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs
- att årliga mål för informationssäkerhetsarbetet beslutas gemensamt i kommunens IT-råd, och beskrivs i Informationssäkerhetsobjektets förvaltningsplan (PM3).

För de årliga målen anges:

- vad som ska göras under året och hur
- tidplan
- behov av personella och ekonomiska resurser
- när och hur uppföljning, utvärdering och avrapportering ska ske
- när och hur våra medarbetare ska informeras och utbildas

I Informationssäkerhetspolicyn framgår att övergripande ansvarig för informationssäkerhetsarbetet är IT-chefen som också ansvarar för att uppfylla kommunens kontinuitetsplan för IT-stödet. Respektive systemägare ansvarar för att det/de informationssystem denne har ägandeskap för, uppfyller de krav på informationssäkerhet som Östhammars kommun ställer samt att systemförvaltaren ansvarar för den dagliga användningen av informationssystemen. Ett förtydligande av roller ska finnas i tillämpningsföreskriften *Informationssäkerhetsinstruktion för Förvaltning* men denna och övriga instruktioner som finns benämnda i policyn saknas.

Det finns därmed inga dokument som tydliggör hur Informationssäkerheten och IT-säkerheten ska säkerställas.

### 3.2.2 IT-policy

En IT-policy finns som är beslutad i kommunfullmäktige 2002-11-14. Av den framgår att kommunens hantering av IT ska förtydligas med hjälp av en dokumenthierarki bestående av policy, strategi, riktlinjer och handlingsplaner.

Kommunens IT-verksamhet styrs av dokument där IT-policyn är det mest övergripande och långsiktiga dokumentet. IT-strategin utgår från visionen och lägger fast hur

kommunens IT-stöd ska byggas upp, underhållas och förnyas. IT-strategin lägger också fast organisation och ansvarsfördelning för arbetet med IT. Riktlinjer inom IT förtydligar och beskriver mer i detalj områden i IT-strategin som behöver klarläggas, exempelvis valda applikationer och tekniska lösningar. Handlingsplaner inom IT tas fram av alla förvaltningar i samband med budgetprocessen. Handlingsplanerna ger överblick över önskade/planerade förändringar.

Avsnitt 2.2 i IT-policyn avser säkerhet. Kommunen betraktar information och processer förknippade med IT som en väsentlig del av verksamheten och det är därför viktigt att förhindra störningar och oönskade händelser i IT-stödet. Informationen ska vara tillgänglig under överenskomna tider, den ska endast vara åtkomlig för behöriga personer, den ska vara riktig och det ska vara möjligt att spåra vem som har skapat eller förändrat informationen.

Vi har i granskningen inte tagit del av några strategier, riktlinjer eller handlingsplaner för IT.

### 3.2.3 IT-styrningsmodell

I samband med projektet Ny IT-styrningsmodell som avslutades 2017 togs dokumentet IT-styrningsmodell i Östhammars kommun fram.

Av dokumentet framgår att IT-styrningsmodellen styr och planerar aktiviteter för förvaltning av det stöd som verksamheten behöver. Detta inkluderar aktiviteter som syftar till att vidmakthålla och vidareutveckla det stöd verksamheten behöver för att kunna arbeta effektivt i sina processer och arbetsflöden. Stödet inkluderar såväl arbetsprocesser, utbildningar och support såväl som relaterade verksamhetssystem, applikationer och tekniska infrastruktur m.m.

Som utgångspunkt i utformningen av IT-styrningsmodellen har kommunen valt pm3[2] som ger stöd för styrning av förvaltningen av verksamhetens stöd. Förvaltning av IT-stöd inom ramen för kommunens IT-styrningsmodell är uppdelad i åtta områden s.k. förvaltningsobjekt (i samband med hearing 2019-10-21 framkommer att det nu finns sex förvaltningsobjekt i kommunen). Dessa utgör den samlade förvaltningsportföljen gällande resurser och kostnader för att vidmakthålla och vidareutveckla kommunens IT-stöd. Förvaltningsobjekten är uppdelade i tre typer; stöd för kärnverksamhet, stöd för stödverksamhet samt stöd för IKT-verksamhet (Information, Kommunikation, Teknik).

Vad gäller säkerhetsaspekter finns en kort skrivelse att minsta möjliga insats för att vidmakthålla IT-stödet är att vidta säkerhetsrelaterade åtgärder för att upprätthålla befintliga säkerhetskrav.

#### Bedömning

Vår bedömning är att kommunstyrelsen inte har tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka

[2] pm3 är en styrmodell med sin grund i systemförvaltningen men som över tid utvecklats till en modell som används för styrning av verksamhetsutveckling i stort.

krav som ställs och hur arbetet för att säkerställa kommunens informations- och IT-säkerhet ska organiseras.

Den informationssäkerhetspolicy som är beslutad behöver revideras enligt nuvarande organisation och de instruktioner som ska förtydliga arbetet saknas. Vi ser det som allvarligt att den beslutade IT-policyn inte reviderats sedan 2002. De dokument som finns beskrivna i policyn som avser att tydliggöra arbetet saknas.

Kommunstyrelsen har inte gett några uppdrag till verksamheten för att säkerställa arbetet med kommunens informations- och IT-säkerhet. Det sker inte heller någon rapportering avseende incidenter eller behov av åtgärder för att upprätthålla en tillräcklig säkerhetsnivå.

## 3.3 Redovisning av förberedande frågor

I bilaga 1 finns de frågor som vi använt i denna granskning. IT-chef, kundansvarig samt kommunens säkerhetsskyddschef har svarat skriftligt på samtliga frågor och vi (KPMG) har också diskuterat utvalda frågor vid den hearing som genomfördes 2019-10-21 i Östhammar.

### 3.3.1 Roller och ansvar för IT-säkerheten

Under hearingen bad vi att få en beskrivning över hur kommunen byggt upp sitt arbete och sin organisering av Informationssäkerheten. Den beskrivning som gjordes var att denna fråga har lyfts in i det övergripande skydds- och säkerhetsarbetet som ligger under säkerhetsskyddschefens ansvar. I kommunens gällande Informationssäkerhetspolicy framgår att IT-chef ansvarar för arbetet, vilket med andra ord inte stämmer överens med nuvarande organisation.

Det övergripande säkerhetsarbetet har påbörjats genom att ta fram en säkerhetsskyddsanalys, som är ett nationellt uppdrag till alla aktörer som bedriver säkerhetskänslig verksamhet, däribland kommuner. Det finns inget politiskt beslut i Östhammar att genomföra arbetet och det sker inte heller någon löpande återrapport till kommunstyrelsen om hur arbetet fortlöper. Säkerhetsskyddsanalysen beräknas vara klar under 2020 och är starten på ett större säkerhetsarbete där även IT-säkerheten finns med.

Det finns en medvetenhet om behovet av ett utvecklingsarbete inom granskningens område men organisationsförändringar (bildande av en gemensam IT-nämnd) och resursbrist anges som anledningar till att arbetet inte har kunnat genomföras fullt ut.

Det är planerat en registerkontroll och säkerhetsklassning av medarbetare men är inte påbörjad ännu. Det ska ske en särskild klassning av IT-personal för att bedöma behörighetsnivå och säkerställa att rätt personer har insyn i rätt system.

Efter en presentation om de olika delarna för att säkerställa arbetet med Informationssäkerheten reflekterar deltagarna på hearingen över att kommunen lägger för lite resurser på den administrativa säkerheten och det i stora delar fastnar på administratörsnivå.

Enligt svaren finns det inte någon uppdragsbeskrivning för IT-enheten som anger eget och kommungemensamt ansvar för IT-säkerheten. IT-enheten upplever själva att de har ett stort ansvar för IT-säkerheten, men att det ibland är svårt att hålla isär skillnaden mellan informationssäkerhet samt IT-säkerhet.

IT-driftschef har påbörjat en utredning för att tydliggöra ansvaret. Frågeställningar som ska besvaras i utredningen är bland annat hur organisationerna ser ut och vad som behöver utvecklas. Vad som finns dokumenterat och vad förvaltningarna har för behov vad gäller systemförvaltning samt IT-säkerhet. Det framgår i svaren på frågorna att målet är att få en mer likartad syn i kommunerna för att kunna bli mer effektiva och göra rätt saker i den nya IT-organisationen vad gäller IT-säkerheten. Detta förstärks under hearingen då ytterligare aspekter av vinster vid ett mer likartat arbetssätt och IT-infrastruktur skulle leda till effektiviseringar och en mer kvalitativ IT-drift.

Eventuell rapportering inom IT-säkerheten sker till kommundirektören men utan att detta dokumenteras och inte med någon kontinuerlig periodicitet. Det finns ingen planerad avrapportering för 2019.

Under hearingen ställdes kompletterande frågor om vilka uppdrag som finns politiskt beslutade och vilken rapportering som skett till kommunstyrelsen avseende IT-säkerhet och svaret i dessa blev att det inte finns några politiska uppdrag och att rapportering främst sker om det krävs ekonomiska beslut.

IT-enheten upplever inte att de har tillräckliga resurser (ekonomi och kompetens internt och/eller extern personal) som behövs för att uppnå den IT-säkerhet som erfordras den kommunala verksamheten.

### 3.3.2 Styrande dokument och annan dokumentation

En aktuell informationssäkerhetspolicy finns. Men de tillhörande tillämpningsföreskrifter som anges i policyn saknas. Se kapitel 3.2.1.

Vi har ställt frågan om det finns systemförvaltningsplaner (baserat på pm3, ITIL eller egenutvecklad organisation) för de verksamhetssystem som kommunen använder. Kommunen svarar att det finns som baseras på pm3. I hearing uppges att målet med arbetet är att skapa nytta, ordning och reda, kostnadseffektivitet och säkerställa att man gör rätt. Det har genom arbetet skett en stor förändring från att se systemförvaltningen som en IT-fråga till att verksamheten tar ett större ansvar.

Vi har i granskningen tagit del av ett exempel på en systemförvaltningsplan, för Barn- och utbildningsförvaltningen. Enligt dokumentet är syftet med förvaltningsplanen att klargöra vad som ska göras i förvaltningsarbetet och hur förvaltningen ska styras. Målgrupp för dokumentet är dels de som ansvarar för nämnda objekt och de som bedriver förvaltningen av detta objekt. Dokumentet ägs av objektsägaren och förvaltas av förvaltningsledaren.

I informationssäkerhetspolicyn framhålls några delar som ska dokumenteras i systemförvaltningsplanen samt att den ska fastställas i IT-rådet. Vi anser att dokumentet i stora delar innehåller denna information.

Av dokumentet vi tagit del av framgår att det saknas objektägare IT samt systemspecialist IT medan det för de verksamhetsnära rollerna finns namngivna personer för samtliga roller.

Kommunen har svarat att det delvis finns en systemförteckning där kommunens IT-komponenter (bland annat system) har identifierats utav verksamheternas förvaltningsledare. Det framgår av svaret att flera av dessa system/IT-komponenter dock saknar utsedda systemförvaltare/systemadministratörer. Fokus har hittills varit på att identifiera alla IT-komponenter och ingen informationsklassning har genomförts.

IT-chefen uppger att Ledningssystem för informationssäkerhet (LIS) saknas. Det finns för närvarande inga planer på att certifiera kommunens arbete efter standarder i ISO 27000-serien. En implementering av Digframe som är en modul i kvalitetsledningssystemet Stratsys, planeras. Denna motsvarar kraven som ställs enligt ISO 27000-serien. Under hearingen diskuteras detta och det framkommer att denna implementering är stoppad tillsvidare då man identifierat begränsningar i Digframe som kan innebära en säkerhetsrisk.

Vad gäller NIS-direktivet och GDPR har inte IT-nämnden fått något uppdrag eller ansvar för att vidta åtgärder för att hantera dessa frågor för kommunen i stort men har vidtagit åtgärder för sitt interna arbete. Östhammars kommun har genomfört ett flertal åtgärder som en del i sin anpassning till GDPR.

Alla medarbetare har genomgått utbildningen DISA som erbjuds via Myndigheten för säkerhet och beredskap, MSB. Deltagandet följdes upp på enhetsnivå och enligt medverkande på hearing så var deltagandet stort och många medarbetare har därmed fått kunskap i informationssäkerhet.

Några beslut och åtgärder kring NIS-direktivet framkommer inte.

Personuppgiftsansvariga, PUA har gått ett flertal utbildningar och dataskyddsombudet håller interna presentationer och utbildningar för att fortbilda medarbetare och enheter i kommunen.

### 3.3.3 IT-säkerhetsåtgärder

#### *Rutiner och processer*

Kommunen har ett flertal av de vanliga åtgärderna för skydd av IT och system. Bland annat brandvägg, backuper, övervakning, antivirus, spamskydd (externt). Samt för att säkerställa en kontinuerlig drift, automatisk utskjutning av uppdateringar till klienter och servrar via SCCM. Det finns även fysiskt skydd för serverhallar.

Det finns ingen kontinuitetsplan eller katastrofplan framtagen och kommunen arbetar inte med några löpande kontroller av sin säkerhet för att på så sätt identifiera eventuella brister för att ha möjlighet att åtgärda dessa innan det skadar kommunens informationstillgångar. Viss incidenthantering hanteras men dokumenteras inte idag. IT löser de problem som uppstår men det pågår ett arbete med att ta fram en instruktion för incidenter och rapportering.

En särskild riktlinje för att rapportera personuppgiftsincidenter enligt dataskyddsförordningen (GDPR) är upprättad. Syftet med den är att skapa en systematisk och samlad rapportering av personuppgiftsincidenter för Östhammars kommun. Till riktlinjerna finns även en checklista för vad som behöver utföras i händelse av en incident. På kommunens intranät finns en utförlig beskrivning över hantering och efterlevnad av dataskyddsförordningen.

I granskningen har vi tagit del av ett stort antal processer och rutinbeskrivningar över aktiviteter inom IT-verksamheten som sker i samverkan mellan kommunerna och IT-nämnden. Dessa sker enligt ITIL[3]-ramverket. Det pågår ett arbete att ta fram fler sådana processer. Dessa utgör en grund för att förtydliga hur beställningar och uppdrag fungerar och avser bland annat inköp, systemprocesser, inställningar för konton mm. De fungerar främst för att tydliggöra och kvalitetssäkra IT-enhetens processer men kan i sin tur ligga till grund för att genomföra riskbedömningar.

Det finns enligt svaren på utskickade frågor ingen utbildningsplan för anställda på IT-enheten utan kompetensbehov utgår från individerna i enskilda möten, exempelvis medarbetarsamtal. Då IT-branschen är i ständig utveckling är det viktigt att anställda inom främst IT-avdelningen får löpande utbildning och information över åtgärder för att säkerställa kommunens IT-säkerhet.

### Bedömning

Kommunens arbete med informationssäkerhet och IT-säkerhet baseras inte på risker och behov som ansvariga för informationen har fastställt. Vår bedömning är att kommunen behöver utveckla sitt arbete med riskanalys i syfte att tydliggöra vilka hot och brister som finns i kommunens IT-miljö och informationssäkerhet.

Det finns framtagna rutiner och processer enligt ITIL-ramverket som tydliggör och kvalitetssäkrar IT-enhetens processer.

Vi ser det som positivt att kommunen har genomfört utbildning i Informationssäkerhet för alla medarbetare samt följt upp deltagandet på enhetsnivå.

# 4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att det finns brister i kommunstyrelsens arbete för att säkerställa en tillräcklig kontroll över kommunens Informationssäkerhet och IT-säkerhet. Vi baserar detta på att kommunstyrelsen inte har tillsett att det finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet ska bedrivas.

Kommunens arbete med informationssäkerhet och IT-säkerhet baseras inte på risker och behov som ansvariga för informationen har fastställt.  De datoriserade verksamhetsstöden har inte informationsklassats och utan det underlaget anordnas IT-

[3] ITIL=IT Infrastructure Library och består av en uppsättning bästa praxis för att leverera IT-tjänster.

säkerhetsåtgärderna på ett sätt som IT-avdelningen upplever som nödvändigt utifrån sina förutsättningar. Verksamhetsansvariga har följaktligen ingen kontroll över om den information de ansvarar för hanteras med relevanta säkerhetsanordningar.

Det finns olika former för att säkerställa att efterlevnad av beslutad IT-säkerhet sker. I de fall det inte går att säkerställa är det näst bästa att se till att incidenter upptäcks och kan åtgärdas. Vi bedömer att detta arbete inte är tillräckligt och att kommunen behöver utveckla sitt arbete med riskanalys i syfte att tydliggöra vilka hot och brister som finns i kommunens IT-miljö och informationssäkerhet.

Trots alla maskinella skydd och varningssystem är det medarbetare som ska efterleva den beslutade IT-säkerheten. För detta krävs en viss kunskapsnivå och en viss insikt i vikten av IT- och informationssäkerhet. Vi ser det som positivt att kommunen har genomfört utbildning i Informationssäkerhet för alla medarbetare samt följt upp deltagandet på enhetsnivå.

Det har under hearingen framkommit att det finns en medvetenhet och vilja att utveckla arbetet med säkerhetsfrågor överlag och att första steget har varit att ta fram en säkerhetsskyddsanalys för att sedan utveckla planer mm utifrån denna. Den gemensamma organisationen för IT är fortfarande under uppbyggnad och roller och ansvar inte helt tydliggjort. Den samverkansmodell som finns uppbyggd mellan förvaltningarna och IT i systemförvaltningsarbetet kan komma att utgöra en bra grund för dialog i utvecklingsarbetet kring Informations- och IT-säkerhetsfrågorna.

Det saknas politiska beslut och uppdrag till verksamheten för att säkerställa arbetet med kommunens informationssäkerhet och IT-säkerhet och ingen rapportering sker kring incidenter eller åtgärder för att upprätthålla en tillräcklig säkerhetsnivå.

## 4.1 Svar på revisionsfrågorna

***Har kommunstyrelsen tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?***

Vår bedömning är att kommunstyrelsen inte har tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas.

Det finns en beslutad Informationssäkerhetspolicy där det framgår att tillhörande informationssäkerhetsinstruktioner ska revideras och fastställas årligen av kommunstyrelsen. Detta har inte verkställts sedan policyn antogs av kommunfullmäktige 2016. Därmed finns inte en strukturerad helhet av styrdokument för att säkerställa en tillräcklig Informations- och IT-säkerhet.

Den IT-policy som beslutades 2002 är på en övergripande nivå och de dokument som finns beskrivna i policyn som ska tydliggöra arbetet saknas.

### *Har kommunstyrelsen tillsett att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet?*

Arbetet med IT-säkerheten är ett kontinuerligt arbete som till sin struktur beskrivs i styrdokument som utgår från kommunens informationssäkerhetspolicy eller liknande policydokument för säkerhet och beredskap. Då stora delar av denna helhet saknas för att kunna tillämpa i verksamheten bedömer vi att arbetet inte är ändamålsenligt.

Oavsett om styrande dokument finns i någon utsträckning eller inte är det nödvändigt att de datoriserade verksamhetsstöden informationsklassas. Utan det underlaget anordnas IT-säkerhetsåtgärderna på ett sätt som IT-avdelningen upplever som nödvändigt utifrån sina förutsättningar. Verksamhetsansvariga har följaktligen ingen kontroll över om den information de ansvarar för hanteras korrekt enligt externa och interna regler. Vid utfrågningen uppfattar vi att inget av de verksamhetssystem som är i drift har informationsklassats och det går därför inte att bedöma om tillräckliga och relevanta säkerhetsåtgärder är vidtagna.

Det saknas politiska beslut och uppdrag till verksamheten för att säkerställa arbetet med kommunens informationssäkerhet och IT-säkerhet. Det går inte att följa upp på vilket sätt och i vilka delar kommunstyrelsen är delaktiga i kommunens säkerhetsarbete.

### *Finns det former för att säkerställa efterlevnaden av beslutad IT-säkerhet?*

Det finns olika former för att säkerställa att efterlevnad av beslutad IT-säkerhet sker. I de fall det inte går att säkerställa är det näst bästa att se till att incidenter upptäcks och kan åtgärdas. Av denna anledning har kommunen ett antal säkerhetsanordningar för att försvåra intrång och om det ändå sker, att upptäcka och åtgärda. De säkerhetsanordningar som finns på plats i nuläget är i form av brandväggar, antivirus, spam-filter mm. Inga regelbundna penetrationstester eller intrångsförsök är genomförda för att se om en tillräcklig säkerhet för kommunens informationstillgångar är vidtagen.

Det saknas även kontinuitetsplan som beskriver de reserv-, återställning- och återgångsrutiner som krävs för att säkerställa kontinuiteten i en prioriterad verksamhet eller process, utifrån vad som har inträffat.

Trots alla maskinella skydd och varningssystem är det människor som ska efterleva den beslutade IT-säkerheten. För detta krävs en viss kunskapsnivå och en viss insikt i vikten av IT- och informationssäkerhet. Detta har man tagit fast på i Östhammars kommun vad gäller informationssäkerhet och alla anställda i kommunen har uppmanats att genomföra DISA, en utbildning i informationssäkerhet. Det saknas däremot rutiner och anvisningar på användarnivå för att ge medarbetarna förutsättningar att agera på ett säkert sätt avseende informationssäkerhet och IT-säkerhet.

## 4.2 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- säkerställa att det finns aktuella, kända och tillämpade styrdokument med tillhörande instruktioner som lägger en grund för en god informationssäkerhet och tillhörande IT-säkerhet. Dessa bör även tydliggöra ansvar och roller för arbetet.
- säkerställa att informationsklassning av de datoriserade verksamhetssystemen genomförs för att verksamhetsansvariga ska kunna bedöma vilka säkerhetsåtgärder som behöver vidtas för att skydda informationstillgångar som de ansvarar för
- ge IT-enheten i uppdrag att ta fram kontinuitetsplaner som beskriver de reserv-, återställnings- och återgångsrutiner som används för att säkerställa kontinuiteten i en prioriterad verksamhet eller process
- se till att utbildning i informationssäkerhet finns med som en del i introduktionen av nyanställda, samt logga vilka som slutfört den för att säkerställa att medarbetarna får grundläggande kunskap inom informationssäkerhet och sitt ansvar i IT-användandet.

Datum som ovan

KPMG AB

Jenny Thörn
*Kommunal revisor*

# Bilaga 1

# Förberedande frågor inför hearing om IT-säkerhet

## Styrande dokument och annan dokumentation

1. Finns det en aktuell informationssäkerhetspolicy för kommunen med tillhörande tillämpningsföreskrifter?
2. Finns det särskilda tillämpningsföreskrifter avseende IT-säkerheten?
3. Finns det ett ledningssystem för informationssäkerhet (LIS) infört eller planeras det för ett sådant?
4. Är LIS certifierat eller finns det planer på att certifiera sig efter standarder i ISO 27000-serien?
5. Finns det en uppdragsbeskrivning för IT-avdelningen som anger eget och kommungemensamt ansvar för IT-säkerheten?
6. Om ovan nämnda dokument inte finns framtagna, vilka styrdokument anser IT-enheten att man verkar utifrån vad gäller IT-säkerheten?
7. Finns det systemförvaltningsplaner (baserad på pm3, ITIL eller egenutvecklad organisation) för de datoriserade verksamhetsstöd kommunen använder?
8. Finns det en systemförteckning som redovisar driftsatta system där det framgår vem som innehar de olika ansvar som identifierats?
9. Vilket ansvar anser/upplever IT-enheten sig ha för informationssäkerheten och IT-säkerheten? Finns detta ansvar dokumenterat och kommunicerat?
10. Har kommunen utfört någon informationsklassning och på vilket sätt har den påverkat de IT-säkerhetsåtgärder som införts?
11. Finns det servicenivåöverenskommelser (SLA) mellan IT-avdelningen och verksamhetsansvariga? På vems/vilkas initiativ är de framtagna? Vi önskar få ett eller flera exempel på ett SLA om detta finns.
12. Både NIS-direktivet och GDPR gäller från och med första halvåret 2018. Vilka instruktioner/uppdrag/ansvar har IT-avdelningen erhållit för att anpassa verksamheten för att säkerställa att kommunen efterlever dessa?
13. Har IT-enheten tagit stöd/involverats av kommunens dataskyddsombud (ett eller flera) under anpassningen till GDPR?
14. Finns det kunskap om och etablerade rutiner för:
    a. Incidenthantering som innefattar rapportering till överordnade, politiken, berörd verksamhet, anställda och kommunmedborgare?

b. Incidenthantering som innefattar rapportering till berörda myndigheter så som Datainspektionen (Integritetsskyddsmyndigheten), Myndigheten för samhällsskydd och beredskap (MSB).

15. Finns det dokumenterade manuella rutiner/kontinuitetsplaner/katastrofplaner innefattande IT-säkerhetsåtgärder som testats någon gång(er) under de senaste två åren?

## IT-säkerhetsåtgärder

16. Vi behöver en beskrivning av samt motivet (analysen) för de IT-säkerhetsåtgärder som vid utfrågningstillfället:
    a. Är i drift.
    b. Planeras sättas i drift innan årsskiftet 2019.
    c. Planeras sättas i drift efter årsskiftet 2019.
    d. Planeras förändras och/eller avvecklas.
17. Finns det vid utfrågningstillfället IT-säkerhetsrisker där åtgärder inte är i drift eller där befintliga åtgärder är bristfälliga?
18. Har det identifierats något intrångsförsök till kommunens infrastruktur och/eller system under 2018-2019? Vilken form av intrång och vad blev effekten?
19. Vilka åtgärder har vidtagits efter detta?
20. Har det utförts eller planeras det för penetrationstest av kommuns skydd mot intrång?
21. Anser IT-avdelningen att de har de resurser (ekonomi och kompetens internt och/eller extern personal) som behövs för att uppnå den IT-säkerhet som erfordras den kommunala verksamheten?
22. Vem/Vilka rapporterar IT-enheten till avseende IT-säkerheten? Med vilken periodicitet? Finns rapportering för 2018-2019 dokumenterad tar vi gärna del av den.
23. I vilka grupperingar (arbets- samordning-, samverkans- etc.) medverkar personer från IT-avdelningen när informationssäkerhet diskuteras/planeras/införs?
24. Finns det en dokumenterad och fastställd utbildningsplan för IT-avdelningen där IT-säkerhet ingår och är den fullföljd?
25. Finns det en fastställd utbildningsplan för kommunens övriga medarbetare avseende deras ansvar för kommunens IT-säkerhet på en grundläggande nivå?