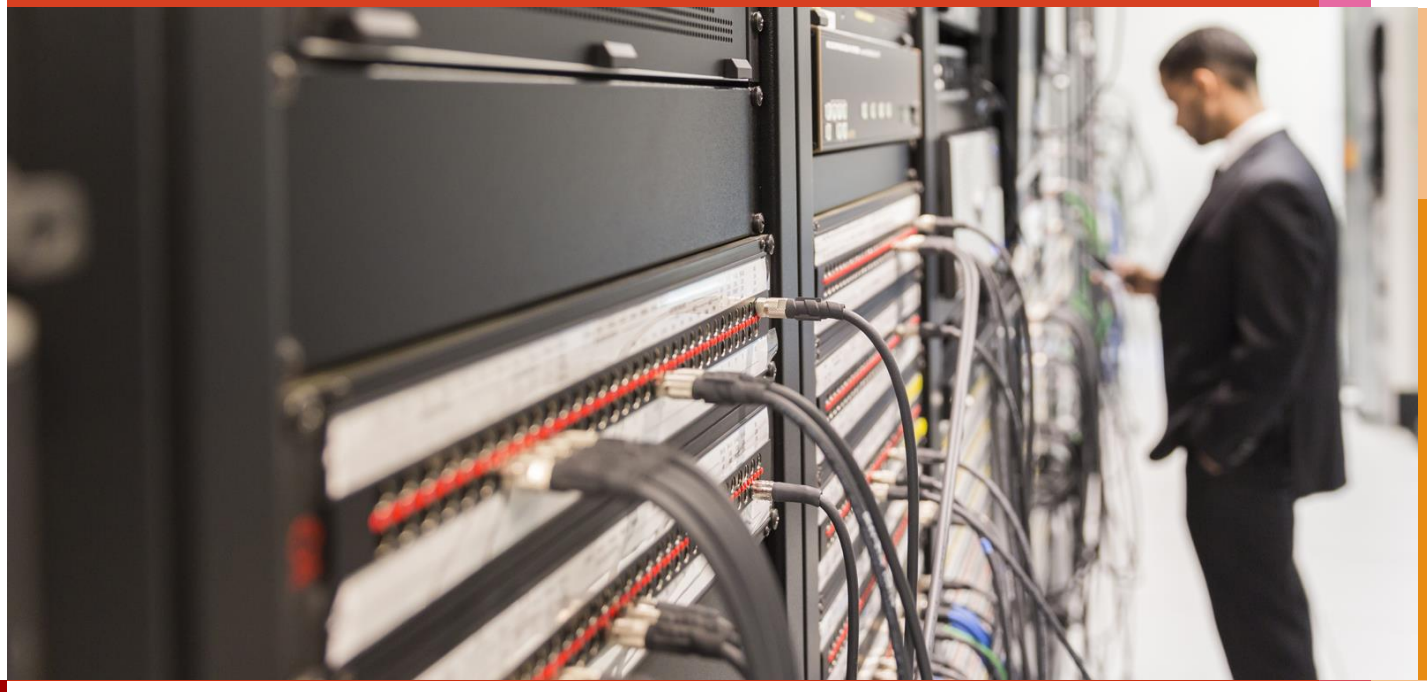
www.pwc.com/se

# *Emmaboda kommun*

## Granskning av Informationssäkerheten inom Emmaboda kommun

November 2017



*28 november 2017*

*Strängt personlig och konfidentiell*

# Innehåll

# Sammanfattning

*Under perioden juni till augusti 2017 har PwC på uppdrag av revisionen i Emmaboda kommun genomfört en* granskning av kommunstyrelsens arbete med IT- och informationssäkerhet*. *Syftet har varit att granska om kommunstyrelsen på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera informationssäkerhet.*

- Vår övergripande bedömning är att kommunstyrelsens arbete med informationssäkerhet till viss del uppfyller revisionsfrågans innebörd. Dokumentation kring policys, rutiner och processer brister men ett strukturerat arbete har påbörjats kring informationssäkerhet och det finns god medvetenhet inom kommunledningen för att säkerställa ett effektivt arbete med informationssäkerhet.
- Arbetet med dokumentationen bör förutom policys innefatta även processer, riktlinjer och roller/ansvar varför det bedöms vara relativt omfattande.
- Kommunstyrelsen bör också upprätta ett strukturerat arbete med risk- och sårbarhetsanalyser.

**Se bilaga 2 för definitioner*

# Bakgrund och syfte

## Inledning

Under perioden juni till augusti 2017 har PwC på uppdrag av revisionen i Emmaboda kommun genomfört en översiktlig granskning av kommunstyrelsens arbete med informationssäkerhet. Resultatet av granskningen presenteras i denna rapport.

## Syfte

Uppdraget innebar att inom ramen för revisionsarbetet inom Emmaboda kommun genomföra en granskning av kommunens arbete med informationssäkerhet för att förstå och analysera huruvida kommunstyrelsen på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera informationssäkerhet. Granskningen har översiktligt fokuserat på; styrning och ledning av informationssäkerhet, strategifrågor, teknologi och funktionalitet, projekt och processer, uppföljning, samt personalaspekter såsom kompetens och bredd.

Syftet med granskningen är att klargöra vilka eventuella områden som kommunstyrelsen behöver utveckla för att uppnå en i förhållande till jämförbara verksamheter ändamålsenliga rutiner och processer för att hantera informationssäkerhet.

## Övergripande revisionsfrågor

Rapporten avser att belysa följande övergripande revisionsfråga:

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

För att besvara den övergripande revisionsfrågan, har nio kontrollmål definierats, se nästa sida.

# Kontrollmål

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

## Kontrollmål

1. Finns beslutade styrande dokument inom området informationssäkerhet? Är dessa kommunicerade?
2. Kontrolleras efterlevnaden av riktlinjer för informationssäkerhet?
3. Har informationssäkerhetsarbetet organiserats på ett ändamålsenligt sätt?
4. Genomförs riskanalyser för informationssäkerhetsarbetet? Har systemsäkerhetsanalyser genomförts för verksamhetskritiska system?
5. Sker informationsklassning enligt en systematisk metod?
6. Finns det rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till informationssäkerhet?
7. Finns kontinuitetsplaner för att hantera bortfall av information i verksamhetskritiska processer?
8. Beaktas informationssäkerhetsrelaterade aspekter vid upphandling/anskaffning?
9. Sker utbildning av medarbetare i informationssäkerhet?

# Metod

## Metod

PwC har baserat granskningen på följande arbetssätt och metodik.

- Intervjuer med identifierade nyckelpersoner i kommunen, (se intervjulista, bilaga 1) samt inläsning och genomgång av tillgänglig dokumentation och styrande dokument.
- Granskningen baseras dels på metod för informationssäkerhet i form av ett internationellt etablerat ramverk för Informationssäkerhet från National Institute of Standards and Technology och dels på PwC:s metod för bedömning av IT-mognad.

## Avgränsning

- Erhållet material har granskats på en övergripande nivå.
- PwC har endast granskat den information som tillgängliggjorts för oss.
- Verksamhet inom olika kommunala bolag har inte granskats specifikt.

# Revisionell bedömning

## Övergripande revisionsfråga

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

## Bedömning

Vår övergripande bedömning är att kommunstyrelsens arbete med informationssäkerhet till viss del uppfyller revisionsfrågans innebörd. Dokumentation kring policys, rutiner och processer brister men ett strukturerat arbete har påbörjats kring informationssäkerhet och det finns god medvetenhet inom kommunledningen för att säkerställa ett effektivt arbete med informationssäkerhet.

Arbetet med dokumentationen bör förutom policys innefatta även processer, riktlinjer och roller/ansvar varför det bedöms vara relativt omfattande. Kommunstyrelsen bör också upprätta ett strukturerat arbete med risk- och sårbarhetsanalyser.

- Styrande dokument i form av exempelvis en tydlig och uppdaterad integritetspolicy samt IT-strategi och riktlinjer kopplade till dessa styrdokument bör fastställas och kommuniceras till verksamheten för att skapa en samsyn kring informationssäkerhetsarbetet inom Emmaboda kommun.
- Processer och rutiner kopplade till informationssäkerhets- och integritetsfrågor eller incidenter finns till viss del men bör dokumenteras på ett tydligt sätt.
- Roller och ansvar kopplade till informationssäkerhet och integritet bör tydliggöras, särskilt i ljuset av kommande dataskyddsförordning som ersätter PUL.
- Vidare bedöms det finnas ett generellt stort behov av utbildning inom området för att säkerställa god kunskap om vad informationssäkerhet och integritet omfattar, vilket ansvar man har som anställd och hur man bör hantera incidenter kopplade till detta. Ett undantag från detta är socialförvaltningen där man kontinuerligt utbildar sina medarbetare.

# Kontrollmål 1

***Finns beslutade styrande dokument inom området informationssäkerhet? Är dessa kommunicerade?***

*Styrande dokument kring informationssäkerhet är tätt sammankopplade med policys och strategier för bland annat IT, vi har därför valt att ta med även dessa för att förstå helheten.*

## Observationer

- Kommunen har en informationssäkerhetspolicy innehållande bland annat övergripande mål för arbetet med informationssäkerhet, generella långsiktiga mål, roller och ansvar samt instruktioner för användare och förvaltning men den är i behov av uppdatering vilket planeras göras i samarbete med andra kommuner i länet.
- Utöver informationssäkerhetspolicyn finns en IT säkerhetsinstruktion för användare. Det finns även annan information av instruktionskaraktär, dessa avsnitt planeras lyftas ut från policyn.
- Befintlig IT-strategi är ej aktuell utan  från 2003, en ny IT-strategi ska upprättas.
- Det framkommer att ett omfattande arbete pågår med att revidera samtliga policys inom kommunen där målet är att arbetet ska vara klart till hösten.
- I samband med uppdatering av policys har checklistor skickat ut till förvaltningschefer för att gå igenom säkerhetsrutiner.

## Rekommendationer

Kommunstyrelsen bör ta fram en plan för att komplettera IT-relaterade styrande dokument enligt följande:

- Ta fram en övergripande strategi och plan för IT-verksamheten i kommunen. Denna ska ta utgångspunkt i kommunens vision, övergripande strategi eller fokusområden och beskriva hur kommunen avser att dra nytta av digitalisering och modern teknik över en längre period.
  - Strategin bör kompletteras med en handlingsplan med prioriterade aktiviteter.
  - Strategin bör beslutas av fullmäktige och ägas av IT-chef.
- Slutför och fastställ policys och riktlinjer för IT såsom
  - IT-policy
  - IT- och Informationssäkerhetspolicy
  - Integritetspolicy
  - Kontinuitetsplan
- Instruktioner bör separeras från informationssäkerhetspolicyn i enlighet med kommunens plan.

# Kontrollmål 2

***Kontrolleras efterlevnaden av riktlinjer för informationssäkerhet?***

## Observationer

- Socialförvaltningen har en process för uppföljning av anställdas efterlevnad av riktlinjer inom informationssäkerhet, området berörs också i de internkontrollplaner som görs av varje förvaltning men vi har inte kunnat bedöma omfattningen av kontrollerna.
- I intervjuerna framkommer att andra förvaltningar muntligen har informerat personal men inte i vilken utsträckning, vid hur många tillfällen eller om detta gäller samtliga förvaltningar.
- Ett exempel på god efterlevnad framkom under intervjuerna. En medarbetare på kommunledningskontoret hade under sommaren uppmärksammat ett inkommande bluffmail och agerade enligt satta riktlinjer genom att meddela närmaste chef samt IT avdelningen varvid polisanmälan kunde genomföras.

## Rekommendationer

- Informationssäkerhetspolicyn och tillhörande instruktioner bör uppdateras och tydligt kommuniceras till verksamheten.
- Kommunen bör ta fram processer och en plan för att säkerställa efterlevnaden av riktlinjer och styrande dokument inom informationssäkerhet hos de anställda, samt andra berörda personer (t ex förtroendevalda).

# Kontrollmål 3

***Har informationssäkerhetsarbetet organiserats på ett ändamålsenligt sätt?***

## Observationer

- Kommunchefen är ytterst ansvarig tjänsteman för informationsarbetet. Det framkommer att det finns ett stort intresse och engagemang från både kommunchefens och IT chefens sida. Detta har uppmärksammas av förvaltningar som anser att det finns ett strukturerat och bra stöd i arbetet med informationssäkerhet.
- IT-chefen är formellt utsedd informationssäkerhetsansvarig men det saknas en tydlig befattningsbeskrivning.
- Målsättningen för arbetet med informationssäkerhet finns i *Informationssäkerhetspolicyn*. I maj 2008 antogs policyn (reviderad mars 2014) och i den framgår att ett aktivt arbete kring informationssäkerhet ska genomföras inom kommunen. Policyn är i behov av ytterligare revidering.
- I informationssäkerhetspolicyn framgår roll- och arbetsbeskrivningar inom IT-verksamheten, dock är det inte formellt dokumenterat vem som innehar respektive roll inom förvaltningarna.
- Det ska enligt uppgifter i intervjuer finnas personuppgiftsansvarig både centralt och i respektive förvaltning.

## Rekommendationer

- En tydlig strategi samt riktlinjer kopplade till denna bör upprättas och kommuniceras till verksamheten för att skapa en samsyn kring informationssäkerhetsarbetet inom Emmaboda kommun.
- En roll som informationssäkerhetssamordnare bör utses eller tillsättas för att säkerställa att arbete med informationssäkerhet samordnas på en övergripande nivå. Denna bör rapportera till kommunledningen.
- Säkerställ att de resurser som arbetar med informationssäkerhet får tillräckligt med tid avsatt för att bl a ta fram den dokumentation som krävs för det praktiska arbetet med informationssäkerhet.
- Säkerställ att roller med koppling till personuppgifter är tydligt dokumenterade och kommunicerade.

# Kontrollmål 4

***Genomförs riskanalyser för informationssäkerhetsarbetet? Har systemsäkerhetsanalyser genomförts för verksamhetskritiska system?***

## Observationer

- I intervju framkommer att det finns en medvetenhet och aktivt tänk rörande informationssäkerhet inom verksamheten och kunskap om vilka system som hanterar kritisk information.
- Respektive systemägare är ansvarig för genomförande av systemsäkerhetsanalyser. Det saknas tydligt kommunicerade riktlinjer för genomförandet av dessa och med undantag för vård och omsorg är det oklart om sådana analyser utförts i verksamheten.
- Det framkommer under granskningen att det saknas tydliga processer och riktlinjer rörande genomförandet av risk- och systemsäkerhetsanalyser kommunicerade till verksamheten. Det finns en målsättning om att strukturera arbetet med riskanalyser i och med projektet som pågår inom informationssäkerhet.

## Rekommendationer

- Kommunen bör fastställa en process för genomförande av regelbundet återkommande risk- och systemsäkerhetsanalyser.
- Tydliggör roller och ansvar såväl på IT- som på verksamhetssidan kring ansvaret för riskanalyserna.
- Vi rekommenderar att kommunstyrelsen tillser att snarast uppdatera de befintliga risk- och systemsäkerhetsanalyserna för att säkerställa att system och IT-infrastrukturen inte är exponerad för risker som kan innebära väsentlig påverkan vid allvarliga händelser.

# Kontrollmål 5

***Sker informationsklassning enligt en systematisk metod?***

## Observationer

- Granskningen visar att ett projekt nyligen initierats för informationsklassning av alla större system i enlighet med KLASSA*. Projektet är ett första steg i arbetet för anpassning till den kommande dataskyddsförordningen.
- Informationsklassning har sedan tidigare skett för samtliga samhällskritiska system men kommer nu även ske för övriga större system.
- Enligt uppgift pågår ett projekt i samarbete med Nybro och Torsås inför den kommande dataskyddsförordningen som ersätter PUL och som träder i kraft i maj 2018. Initiala initiativ har tagits i det pågående arbetet med informationsklassning. I intervjuerna framkommer det att projektets existens inte är fullt ut kommunicerad.

## Rekommendationer

- Säkerställ att arbetet med informationsklassningen kan slutföras enligt uppsatta mål.
- Information om projektet med anpassning mot GDPR bör kommuniceras ut tydligare från kommunledningen till förvaltningarna för att säkerställa att dessa är medvetna om vilka åtgärder de behöver vidtaga.

*) **KLASSA** – En metod framtagen av SKL för att hjälpa verksamheten välja rätt åtgärder som skyddar informationen.
**) **GDPR** – (General Data Protection Regulation). Ny dataskyddsförordning som är gemensam inom EU och ersätter Personuppgiftslagen. GDPR träder i kraft 25 maj 2018. I Sverige kommer Datainspektionen att vara tillsynsmyndighet.

# Kontrollmål 6

***Finns det rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till informationssäkerhet?***

## Observationer

- Det framkommer att enklare rutiner specifika för informationssäkerhet finns i dokumentet ”Säkerhetsinstruktioner IT”. Utöver det finns informella rutiner för incidenthantering inom förvaltningarna men det är otydligt om dessa tar hänsyn till incidenter och säkerhetsbrister kopplade till informationssäkerhet eller integritetsfrågor.
- Ett nytt intranät har implementerats under juni 2017, dock är det fortfarande under utveckling och en sida för incidenthanteringsrapportering kommer finnas. Det tidigare intranätet hade också en sida för incidentrapportering.
- Vidare framkommer att respektive förvaltning har rutiner för att hantera säkerhetsbrister och incidenter. Det är dock osäkert om det finns specifika rutiner för rapportering av incidenter kopplade till informationssäkerhet eller integritetsfrågor inom vissa förvaltningar.
- Det framkommer att det inom socialförvaltningen finns en hög grad av medvetenhet för hantering av känslig information och även dokumenterade rutiner och beskrivningar kring incidenter som grundar sig i sekretesslagar.

## Rekommendationer

- Kommunstyrelsen bör säkerställa att incidentrapporteringsverktyget på intranätet aktiveras snarast möjligt.
- Incidenthanteringsprocessen bör omgående uppdateras till att omfatta incidenter kopplade till integritetsfrågor och persondata i ljuset av kommande dataskyddsdirektiv där höga krav ställs på inrapportering till tillsynsmyndighet för dessa.
- Rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till informationssäkerhet bör upprättas, dokumenteras och anpassas till samtliga förvaltningar, samt kommuniceras till verksamheten. Rutinerna ska inkludera hantering av både elektronisk och fysisk information.

# Kontrollmål 7

***Finns kontinuitetsplaner för att hantera bortfall av information i verksamhetskritiska processer?***

## Observationer

- Det framkommer under granskningen att det saknas en tydlig och dokumenterad kontinuitets- eller katastrofplan som klargör vilka åtgärder som ska vidtas för att skydda och bibehålla integriteten hos information och/eller känslig data. Dock framgår det att det till viss del finns rutiner på plats inom förvaltningarna och att dokumentation kommer upprättas i och med informationsklassningsprojektet.
- Enligt informationssäkerhetspolicyn ska krav på avbrotts- och katastrofplanering för IT-system finnas i systemsäkerhetsanalyserna.
- IT-infrastrukturen upplevs vara modern med två speglade serverhallar, batteribackup samt dieselaggregat. Ett serverrum är beläget i kommunhuset och ett hos IT-avdelningen. Skulle journalsystemet gå ner finns en reservserver som aktiveras.
- Återläsningstest av backuper sker ad hoc. IT-avdelningen önskar genomföra återläsningstester mer regelbundet. I och med nyligen ökade resurser till IT-avdelningen kommer detta möjliggöras.
- Manuella rutiner till viss del finns på plats inom verksamheten om systemavbrott skulle inträffa, dock genomförs inga återkommande katastrofövningar kopplat till informationssäkerhetsincidenter, endast en kärnkraftsövning genomförs.
- All IT inom kommunen ligger under IT-avdelningen och jourberedskap finns dygnet runt.

## Rekommendationer

- Kommunstyrelsen bör i samband med projektet för informations-klassning och revidering av policys se över och uppdatera befintliga planer och dokumentation för att säkerställa att de är direkt användbara vid en kris. I samband med denna uppdatering bör styrelsen säkerställa att aspekten ”skydda och bibehålla integriteten hos informationen” finns med.
- Kommunstyrelsen bör dokumentera en kontinuitets- eller katastrofplan samt genomföra systemsäkerhetsanalyser, för samtliga kritiska system, där avbrotts- och katastrofplanering framgår i samband med informations-klassningsprojektet som planerat och säkerställa att dokumenten kommuniceras till verksamheten.
- Vi rekommenderar att man planerar återkommande katastrofövningar kopplade till informationssäkerhet och integritet för att säkerställa en god beredskap för intrång med förlust av t ex känsliga persondata samt identifiera och rätta fel i processerna.

# Kontrollmål 8

***Beaktas informationssäkerhetsrelaterade aspekter vid upphandling/anskaffning?***

## Observationer

- Upphandling av system hanteras av IT-avdelningen och riskanalyser genomförs i samband med detta.
- Målet är att använda metoden KLASSA* även vid upphandling framgent.
- Ingen upphandling av systemstöd sker separat av verksamheten utan att IT konsulteras.

## Rekommendationer

- Säkerställ att det finns tydliga kriterier för utvärdering av integritets- och informationssäkerhet i samband med systemupphandlingar. Dessa kriterier bör utformas på ett sådant sätt att de även kan användas vid andra typer av upphandling, t ex outsourcing av tjänster eller liknande.

*) **KLASSA** – är en metod framtagen av SKL för att hjälpa verksamheten välja rätt åtgärder som skyddar informationen.

# Kontrollmål 9

***Sker utbildning av medarbetare i informationssäkerhet?***

## Observationer

- Utbildning i informationssäkerhet sker inte strukturerat i någon större omfattning. Det noterades att vissa förvaltningar inte har någon process för utbildning av nyanställda inom informationssäkerhet med undantag för socialförvaltningen där utbildning sker riktad mot informationssäkerhet i och med reglering av sekretesslagar.
- Vidare framkommer att personer som arbetar aktivt med informationssäkerhet både på strategisk och operativ nivå bedöms ha goda kunskaper inom området.
- Kunskapsnivån hos de medarbetare som inte har säkerhet som primärt arbetsområde varierar kraftigt.
- Inom IT-verksamheten bedöms medvetenheten kring informationssäkerhet generellt som god.
- Det finns instruktioner för användare och förvaltning i informationssäkerhetspolicyn och ett separat dokument för säkerhetsinstruktioner inom IT tillgängliga via kommunens hemsida.
- Det saknas fastställd utbildningsplan för utbildning inom informationssäkerhet. Kommunen har verktyget Nano-learning* som fungerar som hjälpmedel vid utbildning och informationsspridning. Verktyget skickar mail två gånger i veckan med informationsfilmer och frågor inom informationssäkerhet till samtliga anställda.
- Det framkommer att en övergripande utbildning inom den nya dataskyddsförordningen planeras att genomföras i och med införandet av den. Arbete pågår med att äska pengar till genomförandet av utbildningen.

## Rekommendationer

- Kommunstyrelsen bör tydliggöra målsättning och tidsplan för arbetet med informationssäkerhet.
- Kommunstyrelsen bör prioritera arbetet med att ta fram en tydlig utbildningsplan rörande informationssäkerhet. Utbildningsplanen bör innehålla information om vilken kunskapsnivå en viss roll/tjänst kräver, samt vilken typ av kunskapshöjande aktiviteter som bör genomföras
- Tydliggör ansvar för att utbildning och fortbildning sker fortlöpande. I ett initialt skede kan detta ansvar ligga på informationssäkerhetssamordnaren.
- Säkerställ att utbildning kring regelverket i dataskyddsförordningen, hur denna skiljer sig från PUL och vilka krav det ställer på hantering av personuppgifter genomförs snarast.

*) **NanoLearning** – En inlärningsmetod baserad på en serie av moduler som levereras via mail över en bestämt tidsperiod.

# Avslutning

Vi vill avslutningsvis ta tillfället i akt och tacka de personer som deltagit i intervjuer och bidragit med underlag till denna översyn för ett vänligt bemötande och ett gott samarbete.

Vid frågor om översynen kan Mikael Carinci eller Jesper Östling kontaktas.

Stockholm, oktober 2017

Kontakt:

Mikael Carinci
E-post: mikael.carinci@pwc.com
Tel: 072 - 980 90 35

Jesper Östling
E-post: jesper.oestling@pwc.com
Tel: 072 - 980 94 11

# Bilaga

Bilaga 1, Intervjulista
Bilaga 2. Vad innebär en god informationssäkerhet och teknisk IT-säkerhet?

# Bilaga 1. Intervjulista

| Namn | Roll | Verksamhet |
|---|---|---|
| Henrik Andersson | IT chef | IT-avdelningen |
| Lennart Werner | Bildningschef | Bildningsförvaltningen |
| Michael Börjesson | Socialchef | Socialförvaltningen |
| Anette Strömblad | Kommunchef | Kommunledningskontoret |
| Ann-Marie Fagerström | Kommunalråd och ordförande kommunstyrelsen | Kommunstyrelsen |

# *Bilaga 2. Vad innebär en god informationssäkerhet och teknisk IT-säkerhet?*

God informationssäkerhet syftar till att säkra en effektiv informationsförsörjning och att undgå allvarlig fel som påverkar möjligheten att bedriva en ändamålsenlig verksamhet.

### *En ändamålsenlig informationssäkerhet innebär:*

- *Vidta preventiva åtgärder för att undvika att information kan förvanskas eller för att förhindra informationsläckage.*
- *Säkerställa att man alltid har tillgång till den information organisationen behöver för sin dagliga verksamhet, även om kris eller katastrof föreligger.*
- *Informationssäkerhetsnivån är helt avhängig den riskaptit man har, samt den bedömda hotbilden.*
- *En organisation som hanterar mycket känslig information, exempelvis i form av personuppgifter i kundregister, lönelistor eller liknande, kan behöva mer skydd än en organisation som inte hanterar och lagrar liknande information.*

En god teknisk IT-säkerhet innebär att organisationen har rutiner, processer och uppsatta kontrollpunkter som löpande följs upp och att organisationen har rutiner för att hålla sig uppdaterad kring omvärldshot och förändringar som kan påverka kritiska resurser.

### *En god teknisk IT-säkerhet innebär:*

- *att ha hög tillgänglighet till information och tjänster,*
- *att säkerställa informationens riktighet genom skydd mot oavsiktlig och avsiktlig förvanskning,*
- *att ha en behörighetskontroll baserad på klassificering av informationens känslighet, spårbarhet och konfidentialitet, samt möjlighet till skyddad kommunikation,*
- *ett aktivt arbete för att så tidigt som möjligt upptäcka och åtgärda intrångsförsök och identifiera eventuella sårbarheter i den interna och externa IT-miljön.*