LESSEBO KOMMUN
Kommunens revisorer

2019-06-13

Till
Kommunstyrelsen
Kommunfullmäktige för kännedom

Förstudie av kommunens organisation och ansvarsfördelning i arbetet med informationssäkerhet

Revisorerna i Lessebo Kommun har givit EY i uppdrag att genomföra en förstudie med syfte att på en övergripande nivå kartlägga kommunens rutiner och arbete med informationssäkerhet.

Förstudien visar på att det har inletts ett arbete med att förbättra och tydliggöra styrningen av informationssäkerhetsarbetet, exempelvis i form av att avtalet mellan Lessebo kommun och Växjö kommun har reviderats och därmed tydliggjort ansvarsfördelningen och kostnadsmodeller.

Det finns ett antal styrdokument avseende informationssäkerhetsarbetet. Dessa är dock antagna 2008 respektive 2009 och överensstämmer inte på flera punkter med nuvarande arbetssätt. Som exempel ges att det inte finns några utsedda systemägare, att det saknas klassificering av IT-systemen samt att det inte genomförs riskanalyser för samtliga system. Det finns ambitioner att revidera samtliga styrdokument.

IT-enheten i Lessebo kommun är bemannad kontorstid. Respektive förvaltning ansvarar för att ha en rutin för hur verksamheten ska hantera eventuella störningar som kan uppstå i verksamhetssystemen, om verksamhet bedrivs utanför kontorstid. I förstudien poängteras särskilt att det är allvarligt för de systemen som har berörts i förstudien, inte finns några separata supportavtal för att hantera driftstörningar utanför kontorstid.

Mot bakgrund av förstudiens resultat görs bedömningen att det är av vikt att det avsätts tillräckliga resurser för att i ett första läge revidera styrdokumenten och därefter säkerställa att de implementeras i verksamheterna. I detta ingår att upprätta rutiner för hur de störningar som inträffar utanför kontorstid ska hanteras.

Revisorerna önskar svar senast den **3 september 2019** på i första hand nedanstående frågor men också i övrigt de påpekande som finns i förstudien.

- Kommunstyrelsens tidsplan för uppdatering och implementering av styrdokumenten.
- Hur säkerställer Kommunstyrelsen It-verksamheten utanför ”kontorstid”?
- Hur genomförs och vad är inriktningen på riskanalyserna inom prioriterade It-områden?

För kommunens revisorer

Örjan Davoust
Ordförande

Per-Anders Johansson
Vice ordförande

Förstudie av kommunens organisation och ansvarsfördelning i arbetet med informationssäkerhet

Lessebo kommun

Kristina Lindstedt och Anna Färdig

Juni 2019

The better the question. The better the answer.
The better the world works.

Building a better working world

Inledning

Bakgrund

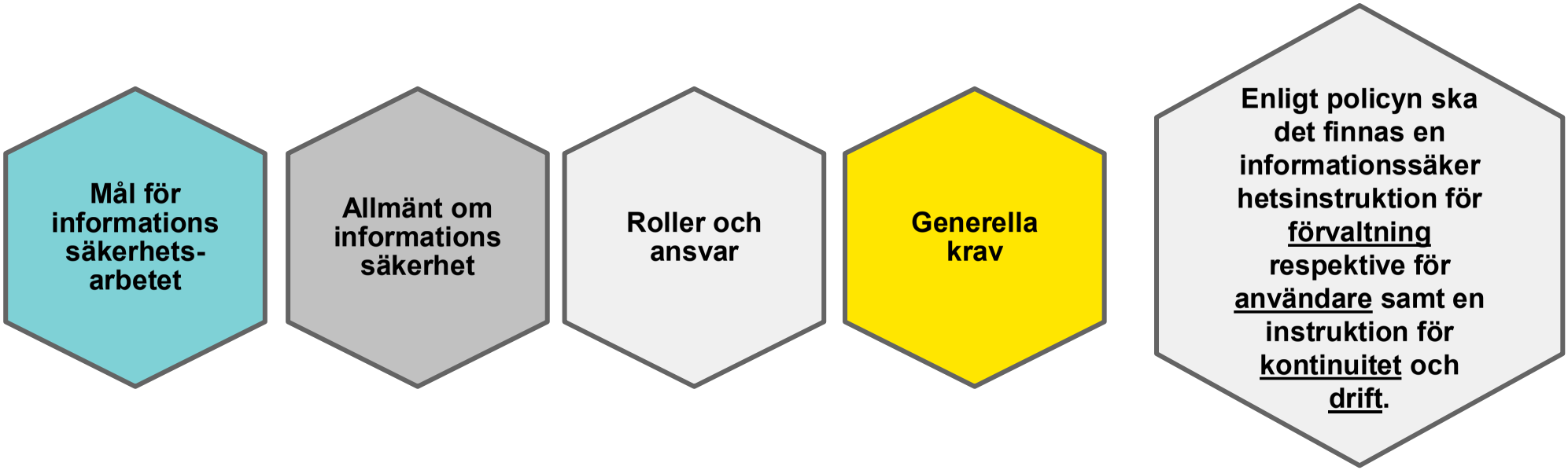
Kommunerna blir alltmer beroende av sina system för informationshantering och drift. Ny teknik innebär nya möjligheter men medför även nya risker.

Syfte

Att kartlägga kommunens rutiner och processer för en ändamålsenlig informationssäkerhet ur ett övergripande perspektiv.

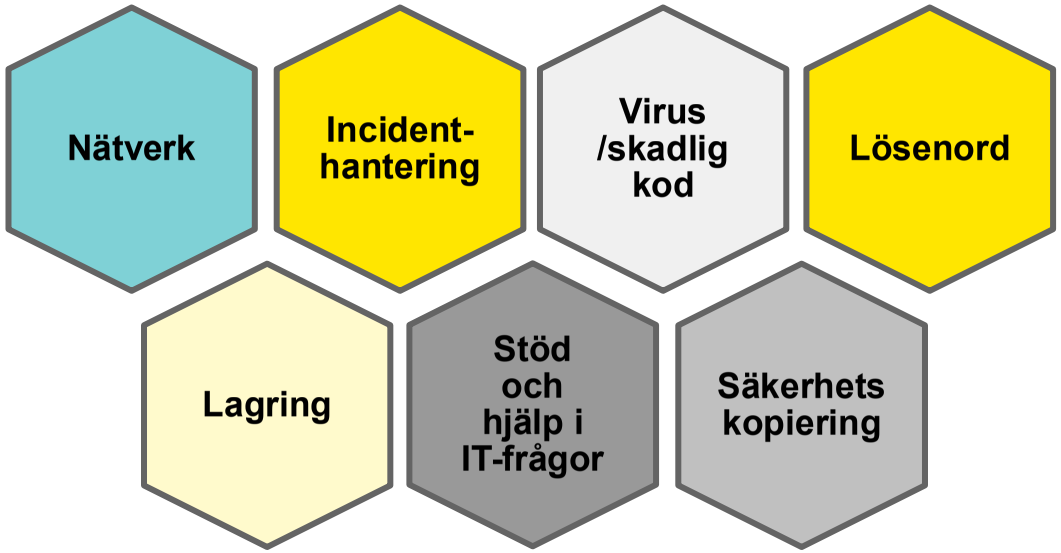
Styrdokument

- Informationssäkerhetspolicy. *Antagen av kommunfullmäktige 2008-04-21*
  - Policyn syftar till att redovisa ledningens viljeriktning och mål för informationssäkerhetsarbetet.
  - Policyn innehåller information om följande:



Styrdokument

- Informationssäkerhetsinstruktion-användare. *Antagen av kommunstyrelsen 2009-02-10* [1].
  - Instruktionen syftar till att hjälpa medarbetare att leva upp till gällande säkerhetskrav samt upplysa om deras ansvar. Dokumentet innehåller exempelvis information om följande områden:

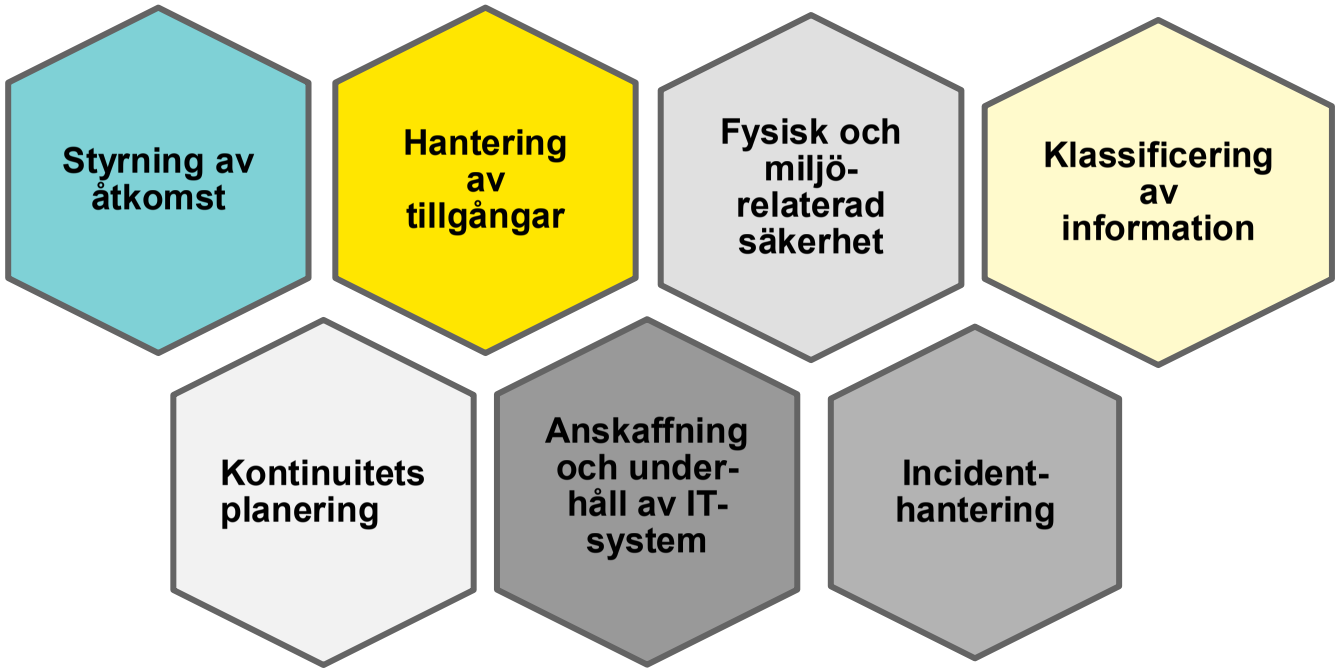


Samtliga medarbetare ska skriva under en bilaga där de bekräftar att de har tagit del av informationen samt förbinder sig att följa instruktionen.

1 Senast ändrad av kommunstyrelsen 2016-02-09

Styrdokument

- Informationssäkerhetsinstruktion-förvaltning. *Antagen av kommunstyrelsen 2009-05-05.*
  - Instruktionen syftar till att utgöra ett stöd för systemägare, systemansvariga, IT-chef, informationssäkerhetsansvarig och systemtekniker inom kommunen. Dokumentet innehåller exempelvis information om följande områden:



Styrdokument

- Enligt informations-säkerhetspolicyn ska det finnas en instruktion för kontinuitet och drift som riktar sig till IT-driftsansvariga.
  - Det finns ingen instruktion för kontinuitet och drift.

Organisation

- Kommunen har en IT-enhet. Enheten består av en IT-chef och tre IT-tekniker. Tjänstepersonen som är IT-chef är även kanslichef.
- Lessebo kommun har tecknat ett avtal med Växjö kommun som innebär att Lessebo köper tjänsten ”Datorarbetsplatsen”.
- Samtliga ärenden som anmäls av medarbetare i Lessebo kommun skickas till Växjö kommuns Service desk. Växjö kommun hanterar de ärenden som omfattas av avtalet och resterande ärenden skickas till Lessebo kommuns IT-enhet.

Organisation

Lessebo kommuns IT-enhets ansvarsområden:

- Drift av merpaten av kommunens system (ett fåtal driftas av annan aktör)
- Utföra backuper
- Elektronisk kommunikation som exempelvis internet
- Inköp av hårdvara

Växjö kommun har bl.a. följande ansvarsområde:

- Service desk
- Klienthantering (inkl. virusskydd)
- E-post
- Kontohantering
- Licenser
- Att hårdvara konfigureras enligt Växjö kommuns standard

Ansvarsfördelning

- Vid intervju uttrycks att det pågår ett arbete med att tydliggöra avtalet mellan Lessebo kommun och Växjö kommun.
  - Revideringen av avtalet syftar till att förtydliga förutsättningarna för samarbete framöver samt fastställa kostnadsmodellen.
  - Vid intervju uppges att revideringen av avtalet är i slutskedet.

Revidering av styrdokument

- Vid intervju uppges att det ska påbörjas ett arbete med att revidera styrdokumenten, då dessa är antagna 2008 respektive 2009.
- I det kommande arbetet med att revidera styrdokumenten ska hänsyn tas till motsvarande dokument i Växjö kommun för att på så sätt skapa en tydligare och mer enhetlig struktur.

Ansvarsfördelning

- Vid intervju uttrycks en ambition om att upprätta avtal mellan kommunens IT-enhet och samtliga nämnder och bolag.
  - Avtalet ska tydliggöra vilka tjänster som IT-enheten erbjuder samt till vilket pris.
  - I dagsläget finns det inget dokument som tydligt fastställer detta.
- I informationssäkerhetsinstruktion-förvaltning framgår att IT-chefen ska upprätta driftsavtal med respektive systemägare.

Systemägare

- En systemägare kan definieras som en person som har det överordnade ansvaret för administration och drift av ett eller flera system.
  - I kommunens förteckning över verksamhetssystem har respektive system en systemansvarig/kontakt. Benämningen systemägare återfinns inte.
- I kommunens informationssäkerhetspolicy framgår att systemansvarig ska utses av systemägaren. Systemansvarig ska enligt policyn ansvara för den dagliga användningen av systemet.
  - Vid kontakt med systemansvariga för två verksamhetssystem uppges att det inte finns någon som är uttalad systemägare.

Systemförteckning

- I informationssäkerhetspolicyn framgår att samtliga informationssystem ska vara identifierade och förtecknade.
  - Vid intervju framkommer att det finns en lista över system som används i kommunen. Det uttrycks en osäkerhet huruvida denna lista är komplett.
  - I listan framgår vilken nämnd som använder respektive system, vem som är systemansvarig samt kontaktuppgifter till systemansvarig.
  - Det framgår även vad systemet används för, exempelvis schemaläggning och övervakningssystem.

Riskanalyser

- I policyn framgår att systemägarna ska genomföra risk- och sårbarhetsanalyser för prioriterade IT-system.
  - Vid intervju med en av kommunens systemansvariga framkommer att det varierar i vilken utsträckning som riskanalyser har genomförts. För 2018 finns det färdigställda riskanalyser för tre av de fem systemen som den systemansvariga ansvarar för.
    - Den nuvarande systemansvariga fick vid tillträdandet ingen information om hur resultatet av riskanalyserna ska tillämpas.
    - Riskanalyserna innehåller information om: risk, skadeverkan, sannolikhet, konsekvens, riskvärdet och förslag på åtgärder/kommentar.
  - Vid intervju med systemansvarig för ytterligare ett av kommunens system framkommer att det genomfördes en riskanalys för ett par år sedan.

Kontinuitetsplan

- I informationssäkerhetsinstruktion förvaltning kan utläsas att respektive systemägare ska besluta om den längsta tiden som IT-systemet bedöms kunna vara ur funktion innan verksamheten äventyras.
  - Det finns ingen längsta acceptabla tid som informationssystemen bedöms kunna vara ur funktion innan verksamheten äventyras.
- I informationssäkerhetsinstruktionen för förvaltningen framgår att det för prioriterade IT-system ska finnas en kontinuitetsplan. Det framgår även att systemägaren ska identifiera IT-utrustning som kräver avbrottsfri elkraft.
  - Vid intervju med IT-chef och två systemansvariga uppges att de inte känner till några kontinuitetsplaner.

Skapa användare

- Respektive verksamhet ansvarar för att lägga upp användare inom de olika verksamhetssystemen.
  - Vid intervju med en av kommunens systemansvariga framkommer att systemansvarig skapar nya användare genom att den aktuella medarbetarens närmsta chef meddelar vilken behörighet som ska läggas upp.

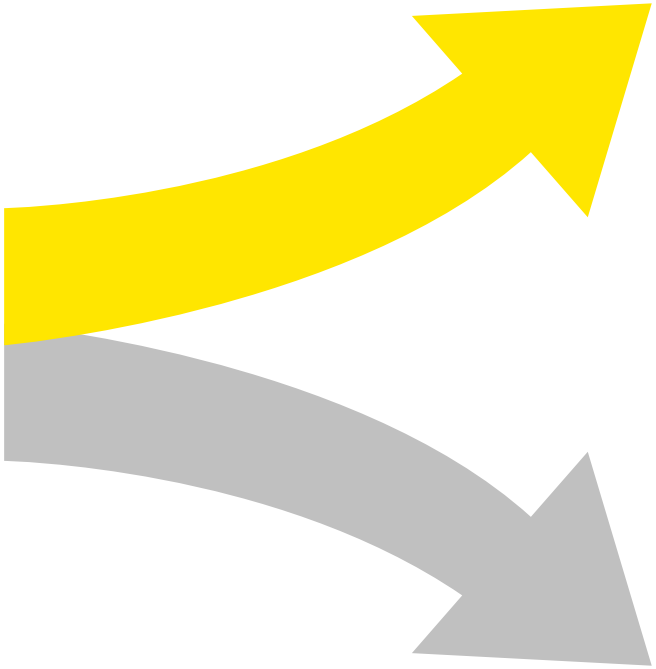
Gallring av behörighet

- IT-enheten ansvarar inte för att kontrollera vilka medarbetare som har behörighet till verksamhetssystemen.
- Det åligger respektive verksamhet att kontrollera att inga obehöriga har tillgång till systemen.
  - Vid intervju med en systemansvarig framkommer att det har påbörjats ett arbete med att kontrollera vilka som har behörighet till systemet. Systemansvarig har mailat samtliga chefer för att be dem kontrollera om det finns medarbetare som inte ska ha behörighet till systemet.

Support vid driftsstopp

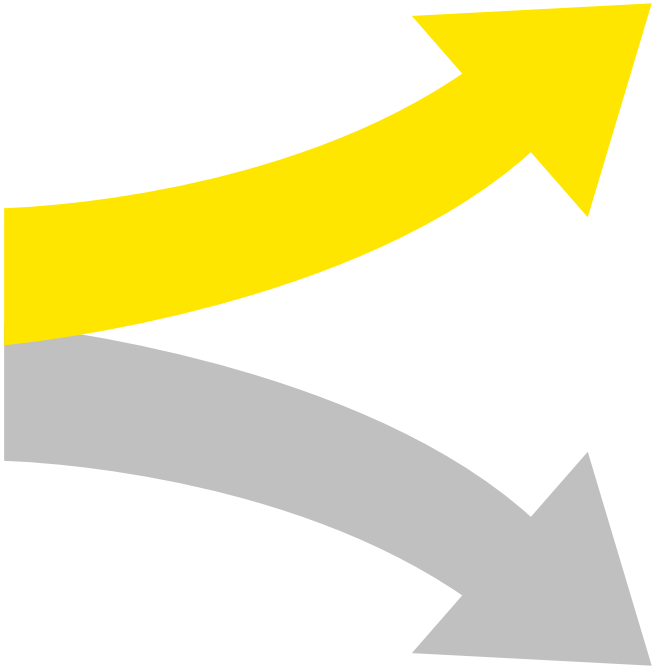
- IT-enheten i Lessebo kommun är bemannad kontorstid.
- Respektive förvaltning ansvarar för att ha en rutin för hur verksamheten ska hantera eventuella störningar som kan uppstå i exempelvis verksamhetssystem, om verksamhet bedrivs utanför kontorstid.
  - Vid intervju med en systemansvarig för ett av kommunens system uppges att det för det aktuella systemet inte finns något separat supportavtal som täcker upp för den tid som IT-enheten inte är bemannad.

Bedömning



- Kommunen har inlett ett arbete för att förbättra och tydliggöra styrningen.
- Det finns ett antal styrdokument. Dessa är dock antagna 2008 respektive 2009 och efterlevs inte fullt ut.
- Vi ser särskilt allvarligt på att det, för de systemen som har berörts i förstudien, inte finns några separata supportavtal för att hantera driftstörningar utanför kontorstid.
- Mot bakgrund av förstudiens resultat gör vi bedömningen att det är av vikt att det avsätts tillräckliga resurser för att i ett första läge revidera styrdokumenten och därefter säkerställa att de implementeras i verksamheterna.

Slutsats



- Utifrån de brister och utvecklingsområden som har identifierats i förstudien ser vi ett behov av att genomföra en uppföljande granskning av IT- och informationssäkerheten. Granskningen bör dock invänta det kommande förbättringsarbetet.

EY

Building a better
working world