Kommunstyrelsen

**Handläggare**
Peter Callsen | Administrativ chef/Kommunjurist
Klas Höglund | IT-ansvarig/IT-strateg

Dnr : KS2018/86-4

Kommunrevisionen

# Yttrande - granskning av IT- och informationssäkerhet i Bollebygds kommun

## Sammanfattning av ärendet

Revisorerna i Bollebygds kommun har gett PWC i uppdrag att granska kommunens IT- och informationssäkerhet. Rapporten ger vissa rekommendationer på åtgärder för vidare utveckling vilket med detta yttrande beaktas och besvaras.

## Yttrande

Revisorerna har punktvis framställt rekommendationer vilket härmed

*Kommunstyrelsen bör upprätta instruktioner och rutinbeskrivningar för IT-organisationen för att säkerställa att nuvarande kompetens i IT-organisationen kan tillvaratas av andra personer än enbart nuvarande nyckelpersoner.*

kommenteras och besvaras punkt för punkt.

Det bör förtydligas att berörd verksamhet har jobbat aktivt en längre period för att minska sårbarheten med en relativt liten organisation. Bl.a. har personalstyrkan nyligen utökats med en person och inom IT-kontoret finns nu tre personer som kan avropa externt konsultstöd utöver administrativ chef samt kommunchef. Det finns ett antal befintliga leverantörer med god kännedom om kommunens driftmiljö vilken dessutom är mycket väl dokumenterad och följer branschstandards och best practice för dylika

uppsättningar. I och med att miljön är väl dokumenterad samt följer standards finns det även gott om externa leverantörer vilka enkelt skulle kunna verkställa kontinuerlig drift i händelse av att befintlig IT-personal faller bort vid exakt samma tidpunkt. Därmed är den operativa driftsituationen mycket trygg, med eller utan egen personal.

Dock finns osäkerhet på det taktiska och strategiska planet vilket inte är ett område som är enkelt att ta extern hjälp utav. På grund av detta jobbar IT-kontoret kontinuerligt med kompetensvidgande insatser och en hög intern transparans vid olika överväganden. Under en längre period har även en aktiv kunskapöverföring på det strategiska och taktiska området skett från IT-kontor till Administrativ chef, bl.a. för att säkerställa en långsiktigt hållbar situation vid eventuellt oplanerat kompetensbortfall.

Sammantaget är vi trots framförda synpunkter medvetna om vikten av övergripande instruktioner och rutinbeskrivningar när detta är tillämpligt och kostnadsmässigt försvarbart att alls hantera. Kommunen håller på att bereda en helt ny digitaliseringsstrategi (preliminärt till kommunfullmäktige juni 2018) vilken bl.a. omfattar ett större omtag av organisationen för IT, Tillämpning samt Förändringsledning. Under förutsättning att digitaliseringsstrategin blir formellt beslutad bör det finnas goda förutsättningar att lägga uppgift på ett ”Tillämpningskontor” att dokumentera rutiner för såväl IT som verksamhetstillämpningar. Vidare skulle nämnda Tillämpningskontor kunna få i uppdrag att arbeta fram ett förslag till lämplig förvaltningsmodell (instruktioner och rutiner) samt aktivt verka för en samordning av kommunens informationssäkerhet.

Tanken om ett Tillämpningskontor baseras främst på de brister kommun idag inom området förvaltning av verksamhetstillämpningar. Rent generellt råder stor sårbarhet där då tunga verksamhetstillämpningar i bästa fall har en dedikerad resurs med avsatt tid för systemförvaltning. Dock uppstår allvarliga problem när dylika kompetenser slutar då det är svårt att ersätta dessa på ett bra vis. Vi noterar även att det finns en allvarlig sårbarhet för skolornas pedagogiska tillämpning då endast en person vid förvaltningen har teknisk kunskap om alla deras tillämpningar.

*Kommunstyrelsen bör införa en formaliserad rutin för behörighetshantering. Rutinen bör säkerställa att nya, ändrade eller borttagande av behörigheter baseras på en formell ansökan som är attesterad av närmaste chef och/eller systemägare. Slutligen bör rutin även inkludera periodiska genomgångar av befintliga behörigheter för att säkerställa att behörigheter är uppdaterade över tid. Rutinbeskrivningen bör delas med både IT-personal och systemansvariga för verksamhetssystem för att säkerställa att rutinerna implementeras för samtliga system.*

Det finns en plan att införskaffa en e-tjänsteplattform kopplat till ett kommungemensamt ärendesystem. Planen var att detta skulle finnas på plats hösten 2017 men det har av beslutstekniska skäl kommit att senareläggas. E-tjänster ska byggas för såväl externt som internt bruk och bl.a. IT-kontoret har en plan för att alla former av beställningar (konton, behörigher, borttag m.m.) ska gå via en kommungemensam intern e-tjänst där vi enkelt kan lägga en kontrollprocess så att t.ex. en ansvarig chef godkänner detta. Vi hoppas att nämnda plattform kommer på plats innan utgången av år 2018.

Avseende rutiner får vi huvudsak hänvisa till det som besvaras under punkt 1 då ett upprättande av dylika rutiner och rutinbeskrivningar med fördel skulle

*Vi rekommenderar kommunstyrelsen att upprätta en avbrottsplan avseende IT och systemstöd. Kommunstyrelsen bör dokumentera åtgärder som behöver vidtas, i vilken ordning och av vem, för att effektivt återställa system och applikationer vid en eventuell incident. Baserat på verksamhetens riskanalyser bör kritiska system definieras och få en tydlig prioritering i avbrottsplanen. Vidare bör ansvarsområden beskrivas och kommuniceras till alla berörda, exempelvis genom träning samt testning av planen.*

kunna hanteras av ett Tillämpningskontor.
IT-kontoret är medvetet om vikten av en kontinuitets och avbrottsplan då det finns en hel del externa avskräckande exempel på större IT-haverier. IT-kontoret jobbar aktivt med en plan för att utveckla kommunens möjligheter till kontinuerlig drift även vid riktigt omfattande haverier bl.a. för pågående planering av framtida IT-plattform. En avbrottsplan kommer att tas fram i anslutning till detta. När det gäller avbrottsplanering för respektive verksamhetstillämpning ligger det praktiska ansvaret hos respektive systemägare, ytterst hos respektive nämnd. Möjligen kan det framtida Tillämpningskontoret säkerställa en bättre samordning för drift och kontinuitet av verksamhetstillämpningar om detta samordas centralt i kommunen.

*För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi även kommunstyrelsen att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i appendix till bifogad revisionsrapport.*

Vi tackar revisionen för den strukturerade och överskådliga sammanställningen i appendix och kommer aktivt verka för att åtgärda punkterna så snart det är möjligt. Som en notering till revisorerna kan härmed informeras om att en ny informationssäkerhetspolicy (anm. 3.2) blev beslutad i kommunfullmäktige 2018-04-26 samt att ett förslag till ny IT-strategi (anm. 3.2.) är under beredning för eventuellt beslut innan sommmaren. Kommunens omfattande systemsäkerhetsanalyser är nu sammanfattade i en kommungemensam registerförteckning och där har verksamheterna klassificerat tillgänglighetskrav (anm. 3.3) enligt ISO 27001 vilket kommer att ligga till grund för kommande avbrottsplanering.

BOLLEBYGDS KOMMUN
Kommunstyrelsen

Peter Rosholm
Kommunstyrelsens ordförande

Anders Einarsson
Kommunchef

Denna skrivelse har godkänts digitalt och saknar därför underskrifter.