Magnus Widén
Handläggare
033 357142

Datum
2017-12-18

Instans
**Kommunstyrelsen**
Dnr KS 2017-00679
007

# Revisionsrapport - Informationssäkerhet

## Förslag till beslut

Kommunstyrelsen lämnar upprättat svar på revisionsrapporten om Informationssäkerhet till Revisionskontoret.

## Sammanfattning

Stadsrevisionen har 2017-10-09 översänt en revisionsrapport angående ”Informationssäkerhet” till Kommunstyrelsen.

Kommunstyrelsen instämmer i stort i de påpekanden som finns i revisionsrapporten, men pekar också på att en rad åtgärder vidtagits och kommer att vidtas.

Kommunstyrelsen har i budget för 2018, äskat medel för att anställa en Informationssäkerhetsansvarig som skall arbeta med de frågor som beskrivs i rapporten.

Utbildningar i informationssäkerhet både har genomförts och planeras, t.ex. i SKLs metod KLASSA.

Efterfrågade rutiner och styrdokument i informationssäkerhet kommer att tas fram.

## Ärendet i sin helhet

Stadsrevisionen har 2017-10-09 översänt en revisionsrapport angående ”Informationssäkerhet” till Kommunstyrelsen, Servicenamnden samt Vård- och äldrenämnden, där man granskat in-formationssäkerheten i Borås Stad. Då såväl Servicenamnden som Vård- och äldrenämnden tillskrivits avser detta svar endast de punkter som rör Kommunstyrelsen.

Kommunstyrelsen instämmer i stort i de påpekanden som finns i revisionsrapporten, men pekar också på att en rad åtgärder vidtagits och kommer att vidtas, vilket redovisas nedan.

Revisionskontoret skriver ”De brister som har identifierats i granskningen bedöms främst bero på att Borås Stad till stor del saknar uppdaterade policys och rutiner för informationssäkerhet. De dokument som finns har i flertalet fall inte beslutats i enlighet med delegationsordningen.”. Man påpekar vidare att ”det inte finns någon särskilt utsedd person som arbetar med övergripande informationssäkerhetsfrågor.”.



Postadress
501 80 Borås

Besöksadress
Kungsgatan 55

Hemsida
boras.se

E-post
boras.stad@boras.se

Telefon
033-35 70 00 vxl

Kommunstyrelsen har i budget för 2018, äskat medel för att anställa en Informationssäkerhetsansvarig. Dennes primära uppgift blir att ta fram ett koncernövergripande LIS (Ledningsinformationssystem) för Informationssäkerhet. Själva Informationssäkerhetspolicyn avses ta fram till politiskt beslut, medan de underliggande dokumenten beslutas på tjänstemannanivå, då de rör verkställighet. Därmed åtgärdas de brister som idag finns vad gäller styrdokument för Informationssäkerhet. Den uppdaterade versionen av ”Informationssäkerhetsinstruktion användare”, kommer att spridas till samtliga medarbetare.

Revisionen pekar på att ”Inga utbildningar inom Informationssäkerhet genomförs”, men att sådana planeras. Under hösten har samtliga förvaltnings- och bolagschefer fått en kortare genomgång av Dataskyddsförordningen. Ett antal styr- och ledningsgrupper på förvaltningarna samt samtliga IT-ansvariga, har fått en längre genomgång. Samtliga systemansvariga för våra verksamhetssystem och snarlika kompetenser (ca 90 personer), har fått en heldagsgenomgång av ISO 27000 och KLASSA. För att snabbt sätta fokus på och höja kunskapen om informationssäkerhetsfrågorna bland anställda, beslutade IT-styrgruppen den 30 oktober 2017 att samt-liga anställda ska genomgå MSBs informationssäkerhetsutbildning DISA (Datorstödd Informat-ionssäkerhetsutbildning för Användare).

Kommunstyrelsen kommer att följa upp hur bolagen arbetar med den nya Dataskyddsförordningen som träder i kraft den 25/5 2018, t.ex. vid planerings- och uppföljningssamtalen.

Kommunstyrelsen anser det dock varken nödvändigt eller lämpligt att skriva in i bolagens ägar-direktiv, vilka policys som gäller för bolagen. Detta framgår när besluten tas i Kommunfullmäktige.

De två dokument som uppges ej ha beslutats enligt delegationsordningen är ”Informationssäkerhetsinstruktion användare” och ”Riktlinjer för informationssäkerhet - Brandväggfunktion”.

Det förstnämnda dokumentet ingick i BITS-konceptet (Basnivå för IT-säkerhet) framtaget av Krisberedskapsmyndigheten. Dokumentet ansågs när det togs fram ligga inom verkställighet och underställdes därför inte för politiskt beslut. Dock var avsikten att ta fram en överordnad Informationssäkerhetspolicy till politiskt beslut, i vilken underliggande dokument, bl.a. detta, skulle pekas ut.

Vad gäller dokumentet ”Riktlinjer för informationssäkerhet - Brandväggfunktion”, så är det inte avsett att ingå bland Borås Stads styrdokument, även om ordet ”brandväggspolicy” förekommer i själva dokumentet. Uttrycket ”brandväggspolicy” är vedertagen branschstandard och avser den uppsättning regler som läggs in i brandväggen, så att den ger det skydd och de funktioner som organisationen är i behov av. Dokumentet benämns istället ”Standardiserad IT - Brand-väggsfunktion”. Det kommer inte, i sin nuvarande form, att tas upp till politiskt beslut, då dokumentet rör teknisk konfiguration av brandväggens funktion.

Borås Stads IT-styrgrupp fattade den 30 november 2017 beslut om att använda SKL's metod KLASSA för klassning av personuppgiftsbehandlingar. I detta sammanhang hanteras såväl frå-gan om klassning av information och personuppgiftsbiträdesavtal samt med vilket lagstöd registreringen görs.

Stadsrevisionen framhåller att ”Det finns inga dokumenterade säkerhetsrutiner för Heroma” och att ”Kommunstyrelsen bör i samarbete med övriga nämnder ta fram säkerhetsrutiner…”.

Tjänsteförvaltaren kommer att få i uppdrag att tillsammans med informationssäkerhetsansvarig ta fram säkerhetsrutiner.

Stadsrevisionen menar att ”Kommunstyrelsen bör säkerställa att behörighetskontroller sker löpande…” samt att ”kontinuitetsplaner prövas löpande”. Detta är uppgifter som ingår i ordinarie systemförvaltning för respektive verksamhetssystem. Kommande LIS för informationssäker-het, kommer att täcka in och ställa krav på att dessa aspekter beaktas och följs upp.

## Samverkan

Ej aktuellt.

## Beslutet expedieras till

1. Revisionskontoret, Borås Stad

Ulf Olsson
Kommunstyrelsens ordförande

Magnus Widén
Ekonomichef