



Handläggare: Anna Ambjörn
Telefon: 08-508 22 048

Till
Hägersten-Liljeholmens
stadsdelsnämnd

Stadsrevisionens Granskning av informationssäkerheten av paraplysystemets applikation ParaSoL

Förslag till beslut

1. Stadsdelsnämnden godkänner och översänder tjänsteutlåtandet som svar på remissen till stadsrevisionen.

Maria Mannerholm
Stadsdelsdirektör

Gunnar Ohlsén
Avdelningschef

Sammanfattning

Stadsrevisionen har genomfört en informationssäkerhetsgranskning av applikationen ParaSoL. Resultatet av granskningen presenteras i en rapport (nr 6 2008). ParaSoL är en applikation till paraplysystemet, som tillhandahåller IT-stödet för stadens verksamheter inom socialtjänsten.

Syftet med granskningen har varit att bedöma om den administrativa hanteringen uppfyller de krav som ställs i kommunfullmäktiges policy och riktlinjer för informationssäkerhet. Särskilt fokus har lagts på behörighetsadministration och spårbarhet i systemet.

I rapporten presenteras stadsrevisionens iakttagelser och rekommendationer. Iakttagelserna rör rutiner för tilldelning av behörigheter till ParaSoL, rutinerna för behörighetsuppföljning och borttag/inaktivering av behörigheter samt spårbarhet i systemet.



Stadsrevisionen rekommenderar att kommunstyrelsen tillser att gemensamma riktlinjer utarbetas för hur behörigheterna till verksamhetssystemet paraplyet och dess applikationer ska administreras. Vidare att stadsdelsnämnderna följer upp tilldelade behörigheter kontinuerligt, förslagsvis 3-4 gånger per år.

Förvaltningen ser över rutinerna för borttag av behörigheter i systemet, uppföljning av gjorda journalanteckningar samt genomföra uppföljningar av behörigheter. Förvaltningen anser att byte av lösenord var 30:e dag är acceptabelt.

Ärendets beredning

Ärendet har beretts inom Avdelningen för samhällsplanering.

Bakgrund

Stadsrevisionen, revisorsgrupp 1, har med stöd av konsult genomfört en informationssäkerhetsgranskning av applikationen ParaSoL. Resultatet av granskningen presenteras i en rapport (nr 6 2008). Rapporten har överlämnats till kommunstyrelsen och stadsdelsnämnderna Spånga- Tensta, Östermalm, Skarpnäck, Hägersten- Liljeholmen och Enskede- Årsta- Vantör för yttrande. Yttrandet ska ha inkommit till revisorsgruppen senast 2008-11-30. Till övriga stadsdelsnämnder överlämnas rapporten för kännedom. Rapporten finns på www.stockholm.se/revision

ParaSoL

ParaSoL är en applikation till paraplysystemet, som tillhandahåller IT-stödet för stadens verksamheter inom socialtjänsten. ParaSoL används inom äldreomsorgen, omsorgen om personer med funktionsnedsättning och socialpsykiatri. Med stöd av ParaSoL ska utförarna upprätta en genomförandeplan, dokumentera viktiga händelser som är av betydelse för insatserna samt avvikelser och förändringar. Denna dokumentation ska arkiveras.

Granskningen

Syftet med granskningen har varit att bedöma om den administrativa hanteringen uppfyller de krav som ställs i kommunfullmäktiges policy och riktlinjer för informationssäkerhet. Särskilt fokus har lagts på behörighetsadministration och spårbarhet i systemet.

Granskningen har bestått av två aktiviteter:

En applikationsgranskning där ParaSoL bedömts utifrån åtkomstbegränsning samt spårbarhet. Särskilt fokus har lagts på behörighetsstyrning och möjligheter att införa lämplig uppdelning av behörigheter.

Vid fem stadsdelsförvaltningar, Spånga- Tensta, Östermalm, Skarpnäck, Hägersten- Liljeholmen och Enskede- Årsta- Vantör, har test av ParaSoL



genomförts i form av genomgång och kontroll av rutiner för styrning av behörigheter.

Stadsrevisionens iakttagelser

- Stadsdelsnämndernas rutiner för tilldelning av behörigheter till ParaSoL sker i enlighet med kommunfullmäktiges policy och riktlinjer för informationssäkerhet.
- Det brister i rutinerna för behörighetsuppföljning och borttag/inaktivering av behörigheter.
- ParaSoL uppfyller de krav som kan ställas på god spårbarhet. Varje användare har unika användar-id som inte går att återanvända och det går att följa vad användarna har gjort i systemet.

Flertalet av de brister som identifierats förklaras av att det saknas centralt fastställda anvisningar och rutiner som reglerar och beskriver ansvar och tillvägagångssätt för ändring och borttag av utdelade behörigheter. Vidare saknas tydliga direktiv för hur ofta och av vem utdelade behörigheter ska följas upp. Därutöver saknas fastslagna rutiner för hur en användares identitet ska verifieras innan ett konto låses upp.

Stadsrevisionens rekommendationer

- Kommunstyrelsen bör, i egenskap av systemägare, tillse att gemensamma riktlinjer utarbetas för hur behörigheterna till verksamhetssystemet paraplyet och dess applikationer ska administreras.
- Stadsdelsnämnderna rekommenderas att följa upp tilldelade behörigheter kontinuerligt, förslagsvis 3-4 gånger per år.

Förvaltningens synpunkter

Förvaltningen har inlett ett arbete med att se över rutinerna för borttag av behörigheter i systemet. En hjälp i det arbetet skulle vara tillgång till listor över personer som inte loggat in på en viss tid. Förvaltningen föreslår att en sådan funktion läggs in i behörighetssystemet (Parainn).

Förvaltningen kommer också att se över rutinerna för uppföljning av gjorda journalanteckningar samt genomföra uppföljningar av behörigheter. I rapporten föreslås uppföljning av behörigheter ske 3-4 gånger per år. Förvaltningen anser att detta är ett rimligt intervall.



När det gäller byte av lösenord anser förvaltningen att byte var 30:e dag, enligt stadens riktlinjer, är acceptabelt.

Bilagor

Bilaga 1. Sammandrag av revisionsrapport nr 6 2008