



Handläggare:
Marie Broberg, telefon: 508 14 050

Till
Enskede-Årsta-Vantörs stadsdelsnämnd

Informationssäkerhetsgranskning av paraplysystemets applikation ParaSol – remissvar

Förslag till beslut

Förvaltningens tjänsteutlåtande åberopas som yttrande till stadsrevisionen.

Gillis Hammar
Stadsdelsdirektör

Leif Fransson
Avdelningschef

Kristina Goldring
Avdelningschef

Thomas Björnstad
Avdelningschef

Sammanfattning

Revisionskontoret har genomfört en informationssäkerhetsgranskning av ParaSol, med fokus på behörighetsadministration och spårbarhet i systemet. ParaSol är en applikation till paraplysystemet, som tillhandahåller IT-stödet för stadens verksamheter inom socialtjänsten. Syftet med granskningen har varit att se om ParaSol uppfyller de krav som ställs i kommunfullmäktiges informationssäkerhetsregler med särskilt fokus på behörighetsadministration och spårbarhet i systemet.

Granskningen visar att det finns ett antal brister av såväl generell som förvaltningsspecifik karaktär. Vid samtliga stadsdelsförvaltningar fungerar rutinerna för tilldelning av behörighet på ett tillfredsställande sätt. Granskningen visar att ParaSol uppfyller de krav som kan ställas på god spårbarhet. Användare har unika användar-id som inte går att återanvända och det går att följa vad som

gjorts i systemet. För stadsdelsförvaltningarna pekar rapporten ut granskning av utdelade behörigheter, rutiner/ansvar vid borttagande av användare samt uppföljning av gjorda journalanteckningar som förbättringsområden.

Vad gäller granskning av utdelade behörigheter är det viktigt att såväl IT-verksamheten och enhetscheferna på de berörda avdelningarna har rutiner för detta. IT-enheten ska därför innan årsskiftet anordna ett par utbildningstillfällen kring detta. Förvaltningen medger att rutiner kring nya användare och borttag av användare behöver styras upp. Utbildningen kommer därför även att innehålla information och instruktioner om detta.

Inom äldreomsorgen är det enhetschefernas ansvar att genomföra stickprov för att följa upp journalanteckningar. Det sker inom ramen för enheternas internkontroll, men det finns behov av förbättrade rutiner för bättre granskning av hur användarna skriver i ParaSol.

Inom avdelningen för stöd och service till personer med funktionsnedsättning finns idag brister i rutiner för uppföljning och kontroll av journalanteckningar i systemet. För samtliga enheter ska nu rutinerna stärkas genom att stickprov genomförs på samma sätt som inom äldreomsorgen.

Ärendets beredning

Detta ärende har utarbetats inom avdelningen förskola och fritid som ansvarar för IT-frågor, i samarbete med avdelningen för äldreomsorg och avdelningen för stöd och service till personer med funktionsnedsättning. Remisstiden sträcker sig till den 30 november 2008.

Bakgrund

Revisionskontoret har genomfört en informationssäkerhetsgranskning av ParaSol, med fokus på behörighetsadministration och spårbarhet i systemet. Fem stadsdelsförvaltningar har granskats; Spånga-Tensta, Östermalm, Skarpnäck, Hägersten-Liljeholmen och Enskede-Årsta-Vantör.

ParaSol är en applikation till paraplysystemet för dokumentation enligt socialtjänstlagen, som tillhandahåller IT-stödet för stadens verksamheter inom socialtjänsten. Användare är utförare inom äldreomsorgen, stöd och service till personer med funktionsnedsättning och socialpsykiatri.

Syftet med granskningen har varit att se om ParaSol uppfyller de krav som ställs i kommunfullmäktiges informationssäkerhetsregler med särskilt fokus på

behörighetsadministration och spårbarhet i systemet. Granskningen har genomförts genom intervjuer med tjänstemän vid stadsledningskontorets IT-avdelning och de fem stadsdelsförvaltningarna, samt genom granskning av styrdokument och verksamhetssystemets arkitektur.

Granskningen har bestått av två aktiviteter:

1. Applikationsgranskning utifrån åtkomstbegränsning och spårbarhet, med särskilt fokus på behörighetsstyrning och möjligheter att införa lämplig uppdelning av behörigheter
2. Test av applikationen vid stadsdelsnämnderna i form av genomgång och kontroll av rutiner för styrning av behörigheter

Rapporten i korthet

Granskningen visar att det finns ett antal brister av såväl generell som förvaltningsspecifik karaktär. Det saknas centralt fastställda anvisningar och rutiner som reglerar och beskriver ansvar och tillvägagångssätt för ändring och borttag av utdelade behörigheter. Det saknas också tydliga direktiv för hur ofta och av vem utdelade behörigheter ska granskas och följas upp, samt rutiner för hur en användares identitet ska verifieras innan ett konto låses upp.

Granskningen visar att en tydlig och heltäckande rutin för behörighetsadministration bör innehålla instruktioner för:

- Upplägg av ny behörighet
- Ändring av behörighet
- Borttag av behörighet
- Rutiner beskrivande ansvar och frekvens för granskning av utdelade behörigheter

Vid samtliga stadsdelsförvaltningar fungerar rutinerna för tilldelning av behörighet på ett tillfredsställande sätt. Endast vid Skarpnäcks stadsdelsförvaltning genomförs behörighetsuppföljningar på ett ändamålsenligt sätt. Granskningen visar att ParaSol uppfyller de krav som kan ställas på god spårbarhet. Användare har unika användar-id som inte går att återanvända och det går att följa vad som gjorts i systemet.

För stadsdelsförvaltningarna pekar granskningen ut följande förbättringsområden:

Granskning av utdelade behörigheter

Om rutiner för granskning av utdelade behörigheter saknas ökar risken att obehöriga personer eller personer som har slutat sin anställning har kvar sin

behörighet. Granskningen föreslås ske 3-4 gånger per år genom att en lokal IT-/paraplysamordnare skriver listor över utdelade behörigheter per enhet som skickas till respektive enhetschef för åtgärd.

Förbättringsområdet har riskklassificerats som mycket kritiskt för Stockholms stads uppfyllande av verksamhetsmål på kort och lång sikt och föreslås åtgärdas omgående.

Rutiner/ansvar vid borttagande av användare

Om det saknas rutiner för borttagning och inaktivering av användare - samt om rutinerna för granskning av utdelade behörigheter uppvisar brister – ökar risken för olovlig åtkomst till ParaSol. Stadsdelsförvaltningarna rekommenderas att formalisera ansvaret för de rutiner som finns för borttagande och inaktivering av användare. Förvaltningarna rekommenderas att inte avvakta de gemensamma riktlinjerna för Stockholms stad.

Förbättringsområdet har riskklassificerats som kritiskt för en god intern kontroll, effektivitet och tillförlitlighet avseende Stockholms stad och föreslås åtgärdas omgående.

Uppföljning av gjorda journalanteckningar

Om ingen uppföljning görs av gjorda anteckningar, ökar risken för att dessa inte håller tillfredsställande kvalitet eller är felaktiga. Förvaltningarna rekommenderas att formalisera ansvaret för de rutiner som finns för kontroll och genomgång av journalanteckningar med syfte att kvalitetssäkra dessa.

Förbättringsområdet har riskklassificerats som väsentligt för en god intern kontroll, effektivitet och tillförlitlighet avseende Stockholms stad och föreslås åtgärdas inom 6 månader.

Förvaltningens yttrande

Förvaltningen har valt att i första hand svara på de synpunkter och rekommendationer som berör stadsdelsförvaltningarna.

Vad gäller granskning av utdelade behörigheter är det viktigt att såväl IT-verksamheten och enhetscheferna på de berörda avdelningarna har rutiner för detta. Rekommendationerna att genomföra granskning av behörigheter 3-4 gånger per år bedömer förvaltningen vara ett genomförbart antal.



Dagens rutin är att förvaltningens IT-enhet skickar ut listor som enhetscheferna fyller i och skickar tillbaka för uppdatering av systemet. Det är viktigt att hanteringen av dessa listor mellan enhetscheferna och IT-enhetens behörighetsadministratörer fungerar, och att de är korrekt ifyllda, för att systemet ska uppdateras och vara säkert.

Ett stort flöde av blanketter hanteras inom förvaltningen och det finns kunskapsbrister för hur dessa ska fyllas i. Det har bidragit till ett växande behov av en översyn av blanketthantering och information om hur de fylls i. IT-enheten ska därför innan årsskiftet anordna ett par utbildningstillfällen kring detta för avdelningschefer, enhetschefer, biträdande enhetschefer och utredare. Utbildningstillfället ska vara obligatoriskt, då kunskapen är väsentlig för att riskerna i behörighetssystemet ska minimeras. Personal från stadsledningskontorets IT-avdelning ska också bjudas in till utbildningstillfällena, som ansvariga för blanketter rörande ParaSol.

Det är i första hand enhetscheferna som ansvarar för att korrekt ifyllda blanketter skickas till IT-enhetens behörighetsadministratörer. Förvaltningen medger att rutiner kring borttag av användare samt för nya användare behöver styras upp. Ovan nämnda utbildning kommer därför även att innehålla information och instruktioner om detta.

Inom äldreomsorgen är det enhetschefernas ansvar att genomföra stickprov för att följa upp gjorda journalanteckningar. Vid avdelningens enheter ges idag individuell handledning och stickprov görs vid specifika behov. Stickproven genomförs inom ramen för enheternas internkontroll, men det finns behov av förbättrade rutiner för bättre granskning av hur användarna skriver i ParaSol. Avdelningen har både ett granskningsdokument med checklista för användarna på enheterna, samt en handbok för vägledning i dokumentation enligt socialtjänstlagen. Handboken har tagits fram i en arbetsgrupp av handledare och boken är förankrad hos enhetscheferna och handledarna på varje enhet. Just nu pågår, efter synpunkter från bland annat Länsstyrelsen, revidering och komplettering av handboken.

Inom avdelningen för stöd och service till personer med funktionsnedsättning finns idag brister i rutiner för uppföljning och kontroll av journalanteckningar i systemet. Många utförare har dessutom nyligen fått riktiga uppkopplingar, vilket bidragit till att det i många fall gått en längre tid från utbildningstillfälle till dess att man kunnat använda systemet. Flera utförare behöver stöd för och uppdatering av dokumentationen i ParaSol. Vid avdelningens samtliga enheter ska nu rutinerna



för uppföljning av gjorda journalanteckningar stärkas genom att stickprov genomförs på samma sätt som inom äldreomsorgen.

Förvaltningen vill påpeka att det vore meningsfullt med en handbok för dokumentation i ParaSol som riktar sig till alla verksamheter och för alla stadsdelsförvaltningar. En sådan handbok kan med fördel tas fram från centralt håll i staden, så att information och riktlinjer samordnas för hela staden och med syfte att den används systematiskt inom stadens berörda enheter.

Till sist vill förvaltningen även uppmärksamma om vad som kommer att hända med hanteringen av behörigheter då IT-verksamheten försvinner från stadsdelsförvaltningarna under 2009.

Bilaga

Informationssäkerhetsgranskning av paraplysystemets applikation ParaSol, 2008-09-18, dnr 420-117/08