STADSREVISIONEN
REVISORSGRUPP 1

Bilaga

DNR 420-117/08
SID 1 (1)
2008-09-18

Kommunstyrelsen
Samtliga stadsdelsnämnder

Informationssäkerhetsgranskning av paraplysystemets applikation ParaSoL

Revisorsgrupp 1 har den 18 september 2008 behandlat bifogade revisionsrapport (nr 6 2008).

Revisorerna överlämnar rapporten till kommunstyrelsen och till stadsdelsnämnderna Spånga-Tensta, Östermalm, Skarpnäck, Hägersten-Liljeholmen och Enskede-Årsta-Vantör för yttrande till revisorsgrupp 1.

Yttrandet ska ha inkommit till revisorsgruppen senast 2008-11-30.

Till övriga stadsdelsnämnder överlämnas rapporten för kännedom.

På revisorernas vägnar

Bengt Akalla
ordförande

Stefan Rydberg
sekreterare

105 35 Stockholm. Telefon 08-508 29 000. Fax 08-508 29 399
revision@rvk.stockholm.se
Besöksadress Hantverkargatan 3 A 1 tr
www.stockholm.se/revision

STADSREVISIONEN
www.stockholm.se/revision

Nr 6
September 2008
DNR 420-117/08

Rapportsammandrag

INFORMATIONSSÄKERHETSGRANSKNING AV PARAPLYSYSTEMETS APPLIKATION PARASOL

Revisionskontoret har med stöd av konsult genomfört en informationssäkerhetsgranskning av ParaSoL. 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.

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 socialpsykiatrin.

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.

STADSREVISIONENS REKOMMENDATIONER

- Kommunstyrelsen bör 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.

FRÅGOR OM RAPPORTEN BESVARAS AV

- Förtroendevald revisor:
  Amanj Mala-Ali
  073-776 48 26
- Förtroendevald revisor:
  Bo Dahlström
  08-690 43 68, 0708-90 43 68
- Stadsrevisor Staffan Moberg
  08-508 29 414

Rapporten finns på www.stockholm.se/revision

STADSREVISIONEN
www.stockholm.se/revision

Nr 6
September 2008
DNR 420-117/2008

Revisionsrapport

INFORMATIONSSÄKERHETSGRANSKNING AV PARAPLYSYSTEMETS APPLIKATION PARASOL

Stadsdelsnämndernas tilldelning av behörigheter till ParaSoL sker enligt kommunfullmäktiges informationssäkerhetsregler

Det finns brister i rutinerna för uppföljning och avslut av behörigheter

ParaSoL uppfyller kraven på god spårbarhet, dvs det går att följa vad användarna har gjort i systemet

Den kommunala revisionen är fullmäktiges kontrollinstrument för att granska den verksamhet som bedrivs i nämnder och bolagsstyrelser. Stadsrevisionen i Stockholm granskar nämnders och styrelsers ansvarstagande för att genomföra verksamheten enligt fullmäktiges uppdrag. Stadsrevisionen omfattar både de förtroendevalda revisorerna och revisionskontoret.

I "årsrapporter" för nämnder och "granskningspromemorior" för styrelser sammanfattar Stadsrevisionen det gångna årets synpunkter på verksamheten. Särskilda granskningar som sker under året publiceras löpande som "revisionsrapporter" och i vissa fall som "promemorior".

Publikationerna finns på Stadsrevisionens hemsida. De kan också beställas från revisionskontoret.

STADSREVISIONEN
Revisionskontoret
www.stockholm.se/revision

Besöksadress: Hantverkargatan 3 A, 1 tr
Postadress: 105 35 Stockholm
Telefon: 08-508 29 000
Fax: 08-508 29 399

STADSREVISIONEN
REVISORSGRUPP 1

Kommunstyrelsen
Samtliga stadsdelsnämnder

Informationssäkerhetsgranskning av paraplysystemets applikation ParaSoL

Revisorsgrupp 1 har den 18 september 2008 behandlat bifogade revisionsrapport (nr 6 2008).

Revisorerna överlämnar rapporten till kommunstyrelsen och till stadsdelsnämnderna Spånga-Tensta, Östermalm, Skarpnäck, Hägersten-Liljeholmen och Enskede-Årsta-Vantör för yttrande till revisorsgrupp 1.

Yttrandet ska ha inkommit till revisorsgruppen senast 2008-11-30.

Till övriga stadsdelsnämnder överlämnas rapporten för kännedom.

På revisorernas vägnar

Bengt Akalla
ordförande

Stefan Rydberg
sekreterare

105 35 Stockholm. Telefon 08-508 29 000. Fax 08-508 29 399
revision@rvk.stockholm.se
Besöksadress Hantverkargatan 3 A 1 tr
www.stockholm.se/revision

Informationssäkerhetsgranskning av paraplysystemets applikation ParaSoL

Revisionskontoret har med stöd av konsult genomfört en informationssäkerhetsgranskning av ParaSoL. 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.

ParaSoL är en applikation till paraplysystemet, som tillhandahåller IT-stödet för stadens verksamheter inom socialtjänsten, och används av äldreomsorgen, omsorgen om personer med funktionsnedsättning och socialpsykiatrin.

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.

Genomförd informationssäkerhetsgranskning visar att stadsdelsnämndernas rutiner för tilldelning av behörigheter till ParaSoL sker i enlighet med kommunfullmäktiges policy och riktlinjer för informationssäkerhet. Däremot finns det brister i rutinerna för behörighetsuppföljning och borttag/inaktivering av behörigheter.

Granskningen visar också att ParaSoL uppfyller de krav som kan ställas på god spårbarhet, dvs det går att följa vad användarna har gjort i systemet.

I egenskap av systemägare till paraplysystemet och dess applikationer bör kommunstyrelsen upprätta gemensamma riktlinjer för behörighetsadministrationen. Vidare rekommenderas stadsdelsnämnderna att följa upp tilldelade behörigheter kontinuerligt, förslagsvis 3-4 gånger per år.

En redovisning av granskningsresultatet framgår av konsultens rapport. Sammantaget har sju avvikelser identifierats. Fyra av dessa har bedömts vara kritiska.

En mer utförlig redovisning av gjorda iakttagelser samt konsultens lämnade rekommendationer framgår av bilaga 1.

Lars-Erik Örsing
Enhetschef

Mats Bergqvist
Projektledare

Stockholms Stad

Granskning av Paraplysystemets applikation ParaSol

8 september, 2008

transcendent group

SAMMANFATTNING

Vi har på uppdrag från Stockholms stads revisionskontor genomfört en IT-revision avseende styrningen av tillgång och åtkomst till applikationen ParaSoL som är en del av verksamhetssystemet Paraplyet. Syftet med granskningen har varit att bedöma hur den administrativa hanteringen av systemet lever upp till de krav som ställs i stadens informationssäkerhetsregler "Policy och riktlinjer för Informationssäkerhet, Stockholms stad"

Den sammanfattande bedömningen är att det finns ett antal brister, vissa av generell karaktär som återfinns vid samtliga granskade förvaltningar. Andra brister är i huvudsak förvaltningsspecifika. Vid granskningen identifierades 7 avvikelser. Av dessa har 4 bedömts som kritiska. Våra rekommendationer redovisas i bilaga 1.

Flertalet av de brister vi har identifierat 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 skall följas upp. Därutöver saknas fastslagna rutiner för hur en användares identitet skall verifieras innan ett konto låses upp.

Vid de fem stadsdelsnämnder som har ingått i granskningen fungerar rutinerna för tilldelning av behörigheter på ett tillfredsställande sätt.

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.

Martin Malm
CIA CISA CISSP

Gustav Alm
CISA CISSP

INNEHÅLLSFÖRTECKNING

1 INLEDNING

Vi har på uppdrag från Stockholms stads revisionskontor genomfört en IT-revision avseende styrningen av tillgång och åtkomst till applikationen ParaSoL, hädanefter kallat ParaSoL, som är en del av verksamhetssystemet Paraplyet, hädanefter kallat paraplysystemet.

Syftet med granskningen har varit att bedöma om ParaSoL uppfyller de krav som ställs i kommunfullmäktiges informationssäkerhetsregler med särskilt fokus på behörighetsadministration och spårbarhet i systemet.

1.1 Bakgrund

ParaSoL används för dokumentation av planerade och genomförda insatser inom omsorgen i staden. Största användargruppen återfinns inom hemtjänsten och på gruppboenden för personer med funktionsnedsättning. ParaSoL har varit i drift sedan våren 2007.

1.2 Omfattning

Granskningen har bestått av två aktiviteter:

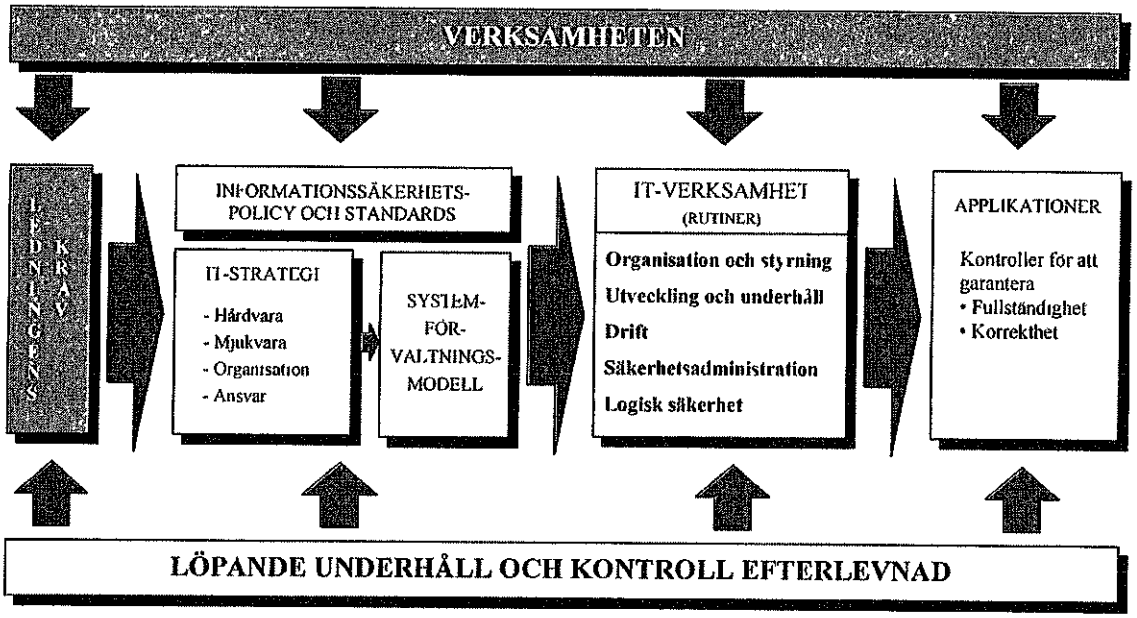
- Applikationsgranskning där ParaSol bedöms utifrån åtkomstbegränsning samt spårbarhet. Särskilt fokus läggs på behörighetsstyrning och möjligheter att införa lämplig uppdelning av behörigheter.
- Test av ParaSoL vid fem stadsdelsnämnder i form av genomgång och kontroll av rutiner för styrning av behörigheter. De fem stadsdelsnämnderna är Spånga-Tensta, Östermalm, Skarpnäck, Hägersten-Liljeholmen och Enskede-Årsta-Vantör.

1.3 Granskningsmetod och avgränsningar

Granskningen har genomförts genom intervjuer med tjänstemän vid stadsledningskontorets IT-avdelning samt med tjänstemän på de granskade stadsdelsförvaltningarna. Vidare har vi tagit del av gällande styrdokument samt verksamhetssystemets arkitektur. Det har inte genomförts några tekniska tester av systemet. Ej heller har risker hos driftoperatören Tieto Enator bedömts.

2 Generellt avseende tillförlitlighet i informationssystem

För att erhålla tillförlitlighet i ett företags informationssystem erfordras ett antal policys och rutiner. Dessa policys och dess samverkan kan beskrivas med nedanstående figur.



För att försäkra sig om tillförlitlighet i en organisations informationssystem erfordras tillfredsställande policys och rutiner inom följande områden:

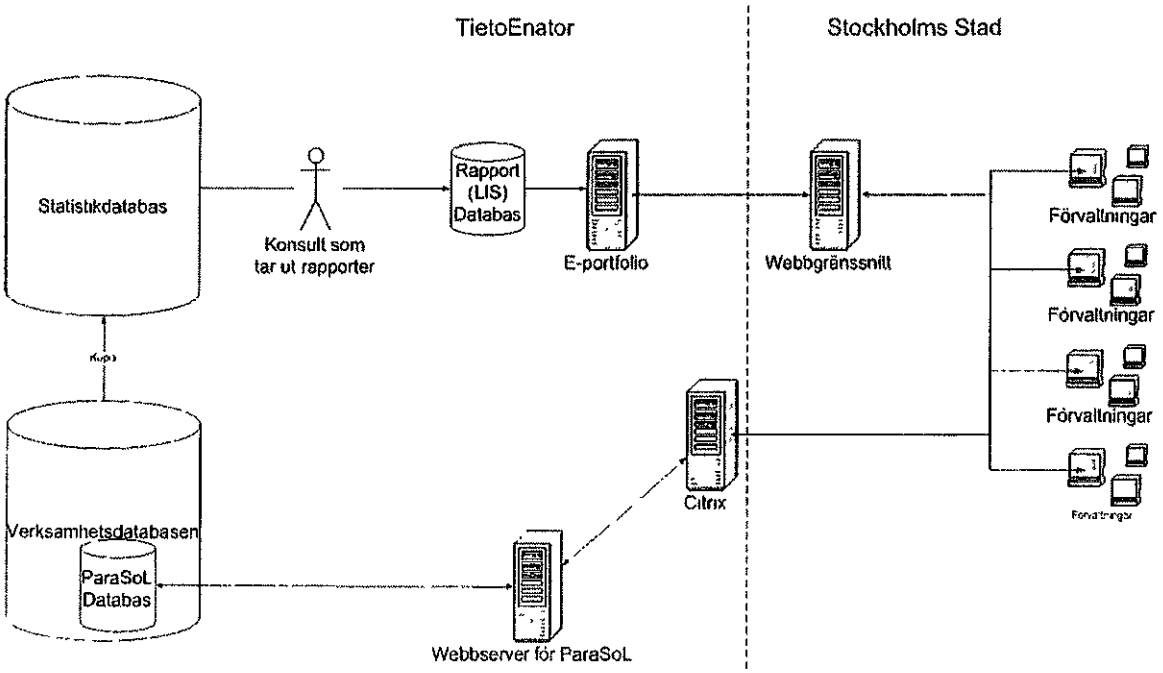
- IT-strategi
- Informationssäkerhetspolicy och standards
- Systemförvaltningsmodell
- Rutiner i IT-verksamheten
- Applikationer.

Behovet av policys och rutiner inom vart och ett av dessa områden styrs av organisationens verksamhet och ledningens krav på tillförlitlighet i informationen. Brister inom något av ovan nämnda områden minskar tillförlitligheten i information, genererad eller lagrad, i informationssystemet. Vidare bör rutiner upprättas för löpande underhåll av policys och riktlinjer samt kontroll för efterlevnad av dessa.

3 RESULTAT FRÅN GRANSKNINGEN

Resultatet från granskningen presenteras i 3 delar, en del som beskriver systemarkitekturen på ett övergripande plan, en del som beskriver behörighetssystemet för ParaSoL samt en del som beskriver de iakttagelser som har gjorts efter intervjuer på utvalda stadsdelsförvaltningar.

3.1 Grafisk beskrivning av ParaSoL



Figur 1. Schema över ParaSoL

ParaSoL består av en Webbserver och en databas. Webbservern nås via den, för staden, gemensamma Citrix-lösningen. ParaSoLs databas är en del av Paraplysystemets verksamhetsdatabas.

Rapportuttagen sker genom att staden har anlitat en konsult som på uppdrag av förvaltningarna genererar rapporter från statistikdatabasen som sedan läggs i en rapportdatabas. Rapporterna nås av förvaltningarna genom ett separat webbgränsnitt.

Beskrivning av behörighetssystemet för ParaSol

ParaInn är ett stödsystem för Paraplysystemets användarhantering, behörighetshantering och inloggning. För administration av behörigheterna till ParaSoL används applikationen ParaInn Admin.

När en användare skall ges tillgång till ParaSoL registreras denne i ParaInn Admin av en lokal IT administratör hos resp. förvaltning.

Följande ParaSoL-roller finns:

- **Personal** är den roll som normalt ges till personal som inte har chefsbefattning
    - **Kontaktman** är egentligen inte en roll utan ett tillägg till rollen personal med något utökad behörighet att kunna, för de kunder han eller hon är kontaktman för, upprätta, följa, uppdatera genomförandeplan, dokumentera välkomstsamtal och levnadsberättelse samt ändra kundens personuppgifter
- **Enhetschef utförare** tilldelas den som har ansvar för att ta emot och behandla beställningar och göra enhetens utförarrapportering
- **Verksamhetschef utförare** har tillgång till samma applikationer och funktioner som Enhetschef utförare men kan se information om kunder och beställningar för alla sina utförarenheter.

3.2 Våra iakttagelser och gjorda bedömningar

Den sammanfattande bedömningen är att det finns ett antal brister både av generell som förvaltningsspecifik karaktär.

En förklaring till bristerna är bl a 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 skall granskas och följas upp. Utöver detta saknas rutiner för hur en användares identitet skall verifieras innan ett konto låses upp.

En tydlig och heltäckande rutin för behörighetsadministration bör innehålla rutiner/instruktioner för:

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

Vi har noterat att under våren 2008 genomfördes en överföring centralt av de Vodokanvändare[1] som inte redan hade tillgång till ParaSoL. Detta rörde sig om ca 20 % av Vodokanvändarna. Vid de granskade stadsdelsförvaltningarna hade inte informationen om att en överföring skulle ske nått berörda tjänstemän. Med anledning av att behörighetstilldelningen genomfördes centralt skulle beslut i form av underskrivna behörighetsblanketter ha upprättats i efterhand vid respektive stadsdelsnämnd. Inte heller denna information nådde berörda tjänstemän. Detta innebär att underskrivna behörighetsblanketter saknas för denna grupp Vodokanvändare.

Vid de fem stadsdelsnämnder som har ingått i granskningen fungerar rutinerna för tilldelning av behörigheter på ett tillfredsställande sätt. Däremot är det endast vid Skarpnäcks stadsdelsförvaltning det genomförs behörighetsuppföljningar på ett ändamålsenligt sätt. Uppföljningsrutinen är dock inte formell fastställd.

ParaSoL uppfyller enligt vår uppfattning de krav som kan ställas på god spårbarhet. Varje användare har unika användar-id som inte går att återanvända. Det går att följa vad användarna har gjort i systemet. Dock har vi noterat att det går att radera/ändra i gjorda journal/dagboksanteckningar om det görs under samma dag som den ursprungliga anteckningen gjordes. Denna möjlighet finns för att kunna rätta till eventuella felaktigheter i dokumentationen i anslutning till att den upprättas.

Vid granskningen identifierades 7 avvikelser. Av dessa har 4 bedömts som kritiska. Dessa är:

Formell rutin för behörighetsgranskning	[rekommendation 2]
Vodok användare	[rekommendation 4]
Granskning av utdelade behörigheter	[rekommendation 5]
Rutiner/ansvar vid borttag av användare	[rekommendation 6]

Detaljer avseende samtliga iakttagelser återfinns i bilaga 1.

[1] Vodok är stadens system för dokumentation i enlighet med hälso- och sjukvårdslagen (HSL). Dokumentationssystemet vänder sig till legitimerad personal såsom sjuksköterska, arbetsterapeut och sjukgymnast, vilka arbetar med hälso- och sjukvårdsuppdrag inom stadens särskilda boendeformer och dagverksamheter inom äldreomsorgen.

3.3 *Identifierade förbättringsområden*

Nedan redovisas identifierade förbättringsområden. Detaljer avseende varje iakttagelse återfinns i bilaga 1.

Risk- och ansvarsklassificering av förbättringsområden						
Förbättringsområden	**Risk**			**Ansvarig**	**Investering**	**Prioritet**
	1	**2**	**3**			
Förbättringsområden – Gemensamt för samtliga förvaltningar inom Stockholms Stad						
1. Frekvens för byte av lösenord		2		A	**	III
2. Formell rutin för behörighetsadministration	1			A	**	I
3. Upplåsning av konton		2		A	**	II
4. Vodok-användare	1			A	**	I
Förbättringsområden – Enskilda förvaltningar						
5. Granskning av utdelade behörigheter	1			B	*	I
6. Rutiner/ansvar vid borttag av användare	1			B	*	I
7. Uppföljning av gjorda journalanteckningar		2		B	*	II

Riskklassificering
Respektive område har riskklassificerats enligt följande skala:

1. Mycket kritiskt för Stockholms stads uppfyllande av verksamhetsmål på kort och lång sikt
2. Kritiskt för en god intern kontroll, effektivitet och tillförlitlighet avseende Stockholms stad
3. Väsentligt för en god intern kontroll, effektivitet och tillförlitlighet avseende Stockholms stad

Ansvarig
Respektive ansvarig har definierats för varje förbättringsområde enligt nedan. Ansvarsklassificeringen baseras på Stockholms stads nuvarande organisation.

A. Kommunstyrelsen
B. Stadsdelsnämnderna

Investering
Vi har uppskattat den totala investeringen för att åtgärda förbättringsförslagen enligt nedan:

* 10-50 tkr
** 51-100 tkr
*** 101---500 tkr

Kostnaden är baserad på en internkostnad per timme om 600 kr.

Prioritet
För respektive åtgärd har vi gjort en prioritering som stöd för upprättandet av en handlingsplan. Prioriteringen baseras på risken, investeringskostnaden, samt rekommenderad tidplan för att vidta åtgärder. Följande kategorier har använts:

I Åtgärdas omgående
II Projekt initieras eller åtgärdas inom 6 månader
III Åtgärdas inom 18 månader

Gemensamt för samtliga förvaltningar inom Stockholms Stad

1. Frekvens för byte av lösenord

OMRÅDE: GEMENSAMT FÖR SAMTLIGA FÖRVALTNINGAR INOM STOCKHOLMS STAD	
NOTERAT Vi har på ett flertal av de granskade stadsdelsförvaltningarna noterat att användarna upplever att frekvensen för byte av lösenord (var 30:e dag) är för hög. Detta har lett till många ärenden rörande upplåsning av låsta konton samt till att användare skriver ner sina lösenord på post-it lappar. Denna frekvens finns beskriven i kommunfullmäktiges informationssäkerhetsregler "Policy och riktlinjer för Informationssäkerhet, Stockholms stad".	**GRAD AV RISK 2** **RISK** Med frekvensen för byte av lösenord satt till var 30:e dag ökar risken att användare får svårt att komma ihåg sitt lösenord. Detta kan leda till att användaren hittar något enkelt system som är enkelt att både gissa och forcera, eller helt enkelt skriver ned sitt lösenord som förvaras i anslutning till datorn. **REKOMMENDATION** Vi rekommenderar att frekvensen för lösenordsbyte ses över för att finna en nivå som är en god avvägning mellan säkerhet och funktion. En ofta använd frekvens är var 90:e dag.

2. Formell rutin för behörighetsadminstration

OMRÅDE: GEMENSAMT FÖR SAMTLIGA FÖRVALTNINGAR INOM STOCKHOLMS STAD	
NOTERAT Vi har noterat att det endast finns en formell rutin som beskriver upplägg av nya behörigheter och ändring av utdelade behörigheter. Det saknas dock formella och gemensamma rutiner som beskriver behörighetsadministrationen gällande borttag och granskning av utdelade behörigheter. I dokumentet "Policy och riktlinjer för Informationssäkerhet, Stockholms stad" finns följande skrivet om behörighetsadministration (sektion 9.2.1 Behörighetsadministration): *"Hantering av behörigheter skall ske enligt gällande anvisningar"* samt en referens till sektion 9.2.1.1 i Appendix A. Denna sektion beskriver dock endast hur ett upplägg av ny användare skall gå till och ingenting om vad som gäller vid ändring och borttagning. Vidare så sägs endast att " Med lämpligt tidsintervall skall listor på samtliga behörigheter ta ut och kontrolleras. Intervallet avgörs av omfattningen på förändringar" utan någon definition av tidsintervallet.	**GRAD AV RISK 1** **RISK** Då det saknas klara direktiv/instruktioner för hur behörighetsadministration skall gå till i sin helhet ökar risken att en god och ändamålsenlig kontroll över utdelade behörigheter ej kan upprätthållas. Detta kan i sin tur leda till att obehöriga eller personal som slutat har tillgång till system och information. **REKOMMENDATION** Vi rekommenderar att det tas fram gemensamma riktlinjer/instruktioner som beskriver följande delar av behörighetsadministrationen: • Upplägg av nya användare • Ändring av utdelad behörighet • Borttag av användare • Granskning av utdelade behörigheter

3. Upplåsning av konton

OMRÅDE: GEMENSAMT FÖR SAMTLIGA FÖRVALTNINGAR INOM STOCKHOLMS STAD	
NOTERAT Vi har noterat att det inte finns några dokumenterade rutiner för hur verifiering av en användares identitet skall göras innan en upplåsning av konton genomförs. Detta gäller framförallt då användare ringer in till lokala IT-avdelningen eller Paraply-samordnaren. Vid vissa förvaltningar används motringning eller att verifierande information från användaren begärs in, detta är dock individuellt och är inte fastslaget i någon dokumenterad rutin. Det finns lokala lösenordsadminstratörer ute på utförarenheterna som kan verifiera en identitet och genomföra en upplåsning, dock kan de bara göra detta för personer med den lägsta behörighetsnivån "Personal".	**GRAD AV RISK 2** **RISK** Avsaknad av, eller bristande, rutin för verifiering av en användares identitet, föregående en upplåsning, ökar risken att obehöriga personer får tillgång till ParaSoL. Detta är särskilt allvarligt då de lokala lösenordsadminstratörerna, som kan verifiera identitet direkt på plats, endast kan låsa upp "Personal"-konton och inte de konton som finns med högre behörigheter såsom verksamhets- och enhetschef. **REKOMMENDATION** Vi rekommenderar att Staden tar fram gemensamma instruktioner för hur verifiering av en användares identitet skall göras då de tar kontakt via telefon eller e-post för att få sitt konto upplåst.

4. Vodok-användare

OMRÅDE: GEMENSAMT FÖR SAMTLIGA FÖRVALTNINGAR INOM STOCKHOLMS STAD	
NOTERAT Vi har noterat att under våren 2008 genomfördes en överföring av de Vodok-användare som inte redan hade tillgång till ParaSoL (ca 20 % av de befintliga Vodok-användarna). Vid de granskade stadsdelsförvaltningarna hade inte informationen om att en överföring skulle ske nått fram till berörda tjänstemän. Ej heller att respektive förvaltning i efterhand skulle upprätta beslutsunderlag i form av behörighetsblanketter. Under våren 2008 hölls ett möte med lokala IT administratörer från förvaltningarna där detta togs upp, men endast 5 av 60 st. kallade närvarade vid mötet. Härigenom har tillgång till ParaSoL givits utan att beslutsunderlag (behörighetsblanketter) har upprättats, vilket strider mot stadens informationssäkerhetsregler. Vodok är stadens system för dokumentation i enlighet med hälso- och sjukvårdslagen (HSL). Dokumentationssystemet vänder sig till legitimerad personal såsom sjuksköterska, arbetsterapeut och sjukgymnast, vilka arbetar med hälso- och sjukvårdsuppdrag inom stadens särskilda boendeformer och dagverksamheter inom äldreomsorgen.	**GRAD AV RISK 1** **RISK** Brister i behörighetshanteringen innebär risk för att obehöriga användare får tillgång till känslig information. Vidare har inte kommunfullmäktiges informationssäkerhetsregler följts "Policy och riktlinjer för Informationssäkerhet, Stockholms stad" som stipulerar att nya behörigheter skall föregås av en skriftlig ansökan. **REKOMMENDATION** Vi rekommenderar att rutinerna ses över i syfte att säkerställa, så långt det är möjligt, att väsentlig information når berörda tjänstemän i framtiden. Vi rekommenderar även att arbetet med att ta fram beslutsunderlag (behörighetsblanketter) inleds omgående samt att stadsdelsförvaltningarna informeras om varför Vodok-användare har tillkommit.

Enskilda Förvaltningar

5. Granskning av utdelade behörigheter

OMRÅDE: ENSKILDA FÖRVALTNINGAR	
NOTERAT Vi har noterat att endast en av de granskade stadsdelsförvaltningarna (Skarpnäck) genomför behörighetsuppföljningar på ett ändamålsenligt sätt. Dock är inte rutinerna för detta formellt fastställda.	**GRAD AV RISK 1**
	RISK Då rutinerna för granskning av utdelade behörigheter saknas/är informella ökar risken att uppföljande granskningar inte genomförs om de personer som ansvarat för dem slutar eller ej hinner med. Detta kan medföra att obehöriga personer eller personer som har slutat har kvar sin behörighet till ParaSoL , vilket i sin tur kan innebära att kraven i kommunfullmäktiges informationssäkerhetsregler "Policy och riktlinjer för Informationssäkerhet, Stockholms stad" inte följs.
	REKOMMENDATION Vi rekommenderar att förvaltningarna dokumenterar de rutiner som finns för granskning av utdelade behörigheter och ej avvaktar de gemensamma riktlinjerna för Stockholms Stad angående granskning av utdelade behörigheter som bör utvecklas [se rekommendation 2]. Granskning av utdelade behörigheter bör genomföras 3-4 gånger per år och lämpligen genom att lokal IT-/Paraplysamordnare skriver ut listor över utdelade behörigheter per enhet och skickar dem till resp. enhetschef eller motsvarande för kontroll.

6. Rutiner/ansvar vid borttag av användare

OMRÅDE: ENSKILDA FÖRVALTNINGAR	
NOTERAT Vi har noterat att det inte på någon av de granskade förvaltningarna finns någon skriftlig rutin för borttagning av användare. I behörighetssystemet ParaInn så innebär detta en användare inaktiveras då ett användar-ID aldrig kan återanvändas. Ansvaret för att tillse att behörigheter avslutas är delegerat till enhetschef eller motsvarande (behörighetsbeställaren). Rutinerna för borttag av behörigheter fungerar dock inte tillfredsställande. Det är vidare oklart i vilken mån enhetscheferna är medvetna om deras ansvar. Endast på Skarpnäcks Stadsdelsförvaltning sker kontroll av en användares samtliga behörigheter när en ansökan om borttag från nätverket kommer in. Denna rutin är informell och personberoende. Vi har även noterat att det på Spånga-Tensta stadsdelsförvaltning finns en lokal IT-säkerhetsinstruktion som beskriver rutinerna för behörighetsadministration. Denna är dock inte känd av verksamheten ej heller har den uppdaterats sedan den antogs 2003.	**GRAD AV RISK 1** **RISK** Då det saknas rutiner för borttag/inaktivering av användare, tillsammans med att rutinerna för granskning av utdelade behörigheter uppvisar brister, ökar risken för olovlig åtkomst till ParaSoL. Detta kan i sin tur innebära att de föreskrifter som finns i kommunfullmäktiges informationssäkerhetsregler "Policy och riktlinjer för Informationssäkerhet, Stockholms stad" ej följs. **REKOMMENDATION** Vi rekommenderar att Stadsdelsförvaltningarna formaliserar ansvaret gällande de rutiner som finns för borttag/inaktivering av användare. Förvaltningarna bör ej avvakta de gemensamma riktlinjerna för Stockholms Stad angående behörighetsadministration som bör utvecklas [se rekommendation 2].

7. Uppföljning av gjorda anteckningar

<table>
<tr><th colspan="2">OMRÅDE: GEMENSAMT FÖR SAMTLIGA FÖRVALTNINGAR INOM STOCKHOLMS STAD</th></tr>
<tr><td rowspan="3">NOTERAT
Vi har noterat att det inte finns några rutiner gällande granskning/kontroll av införda journalanteckningar i ParaSoL. Denna kontroll skulle ha som mål att kvalitetssäkra texterna avseende hur man gör en anteckning, omfattning och språk.

Då det finns en osäkerhet om vad journal- resp. arbetsanteckningar är, ökar betydelsen att följa upp gjorda anteckningar, i kombination med utbildning, för att tillse att dokumentation görs på ett likartat sätt oavsett vem som gör den.</td><td>GRAD AV RISK 2</td></tr>
<tr><td>RISK
Då ingen uppföljning av gjorde anteckningar görs ökar risken att de inte är tillräckligt omfattande, har språkliga brister eller, i värsta fall, kan vara direkt felaktiga.</td></tr>
<tr><td>REKOMMENDATION
Vi rekommenderar att det vid respektive förvaltning utarbetas rutiner för kontroll och genomgång av gjorde journalanteckningar för att kvalitetetssäkra dessa. Detta bör göras genom stickprov på gjorda journaler.</td></tr>
</table>