Revisionsrapport 2016:5

Genomförd på uppdrag av
Västerås stads revisorer

18 oktober 2016

Uppföljande granskning av IT-säkerheten inom Sociala nämndernas förvaltning

Västerås stad

Building a better working world

Innehållsförteckning

1 Sammanfattning

1.1 Bakgrund

På uppdrag av de förtroendevalda revisorerna i Västerås stad genomförde EY under 2014 en granskning inriktad mot stadens IT-säkerhet. Granskningens övergripande syfte var att granska om IT-säkerheten inom Sociala nämndernas förvaltning (forts. SNF) var ändamålsenlig beträffande dess väsentliga verksamhetssystem; ProCapita HSL, ProCapita IFO, och Pulsen Combine. Denna granskning mynnade ut i tio rekommendationer syftande till att stärka IT-säkerheten i verksamheten.

Västerås stads förtroendevalda revisorer har gett EY i uppdrag att följa upp och bedöma i vilken grad iakttagelserna från 2014 har åtgärdats, samt i relevanta fall lämna vidare rekommendationer för fortsatt arbete med verksamhetens IT-säkerhet.

1.2 Slutsats

Av de tio iakttagelser med tillhörande rekommendationer som gavs i granskningen 2014 bedöms sex iakttagelser vara åtgärdade, tre iakttagelser vara delvis åtgärdade, och en iakttagelse bedöms inte vara åtgärdad.

#	Iakttagelser 2014	Status 2016
1.	Avsaknad av dokumenterade rutiner för hantering av behörigheter	Delvis åtgärdad
2.	Användare som slutat har kvar behörigheter i verksamhetssystem	Åtgärdad
3.	Avsaknad av regelverk för hantering av programförändringar	Delvis åtgärdad
4.	Logguppföljning genomförs inte i samtliga system	Åtgärdad
5.	Testning och godkännande av programändringar saknar spårbarhet	Delvis åtgärdad
6.	Ofullständig modell för systemsäkerhetsanalys	Åtgärdad
7.	Inaktuell systemsäkerhetsanalys för *Vård och omsorg*	Åtgärdad
8.	Avsaknad av regler kring distansarbete	Åtgärdad
9.	Ofullständig kontinuitets- och avbrottsplanering	Åtgärdad
10.	Leverantörers åtaganden följs inte upp	Ej åtgärdad

SNF har vidtagit åtgärder för att säkerställa att hantering av behörigheter sker rutinmässigt liksom att periodvis uppföljning av behörigheter genomförs (p1-2), vilket bedömdes vara av hög prioritet i granskningen 2014. Staden har dock inte uppdaterat riktlinjer för åtkomst varvid (p 1) bedöms som delvis åtgärdad.

Rekommendationen att genomföra systematisk och återkommande logguppföljning (p 4) bedömdes vara av hög prioritet i granskningen 2014, och vår bedömning är att övergripande riktlinjer avseende logguppföljning införts och att logguppföljning nu utförs regelbundet för berörda verksamhetssystem.

Västerås stad har uppdaterat modellen för systemsäkerhetsanalyser i enlighet med rekommendationen från 2014, och systemsäkerhetsanalysen för berörda system har uppdaterats (p 6-7). Regelverk för mobilt arbete och distansarbete har införts (p 8), och en mer omfattande kontinuitets- och avbrottsplan har utarbetats (p 9).

Iakttagelsen avseende avsaknad av regelverk för hantering av programändringar (p 3), bedömdes vara av hög prioritet i granskningen 2014. Rutinbeskrivning för hur beställning, testning, godkännande, och övervakning skall ske för samtliga ändringar har etablerats. Följsamheten gentemot denna är dock inte enhetlig och förbises ibland för mindre förändringar, varför iakttagelsen bedöms som delvis åtgärdad. Detta relaterar även till iakttagelsen om dokumentation av testning och godkännande av programändringar (p 5). Godkännande av mindre programändringar dokumenteras inte alltid enligt rutin.

Uppföljning av leverantörers åtaganden (p 10) bedöms inte utföras i enlighet med rekommendationen från 2014, och den möjlighet till granskning av leverantörerna som finns avtalad praktiseras inte.

1.3 Rekommendationer

För de iakttagelser som bedöms som delvis eller inte åtgärdade ges följande rekommendationer för fortsatt arbete med att stärka IT-säkerheten:

- Avsaknad av dokumenterade rutiner för hantering av behörigheter
  - Västerås stad rekommenderas att uppdatera riktlinjerna för informationssäkerhet avseende styrning av åtkomst till system och nätverk. Detta för att tydliggöra vilka rutiner som bör finnas dokumenterade per verksamhetssystem och vilka kontroller som skall utföras avseende styrning av åtkomst. Om skillnad görs mellan olika verksamhetssystem bör detta framgå i riktlinjerna.
- Avsaknad av regelverk för hantering av programändringar
  - SNF rekommenderas att vidare se över rutiner för programändringshantering. Dokumenterade rutiner beskriver att programändringshantering skall ske enhetligt för alla typer av programändringar, men vid mindre ändringar följs inte alltid denna instruktion. Om skillnad skall göras mellan olika typer av programändringar bör det tydligt framgå i instruktionen på vilket sätt ändringar skall klassificeras och därefter hanteras.
- Testning och godkännande av programändringar saknar spårbarhet
  - Relaterat till föregående punkt rekommenderas SNF att vidare se över rutiner för dokumentation och testning av programändringar. Enligt dokumenterade rutiner skall testning och godkännande utföras och dokumenteras för alla programändringar, vilket inte alltid sker vid mindre programändringar. Vi rekommenderar att godkännande att införa programändringar, oavsett komplexitet, alltid dokumenteras.
- Leverantörers åtaganden följs inte alltid upp
  - SNF rekommenderas att stärka uppföljningen av leverantörernas åtaganden gällande deras ansvar och hantering avseende avbrottsplanering, behörighetshantering, samt programändringshantering. SNF bör praktisera den möjlighet till granskning av leverantörerna som finns avtalad för att säkerställa en korrekt och ändamålsenlig hantering i enlighet med etablerade avtal.

2 Bakgrund

2.1 Inledning

Idag bedrivs så gott som all verksamhet i en stad med någon form av datoriserat stöd. Stödet har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet och antalet olika programvaror är stort. För att uppnå målen för stadernas verksamheter krävs att informationen i verksamhetsstödet är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

Under 2014 genomförde EY på uppdrag av Västerås stads förtroendevalda revisorer en granskning av IT-säkerheten inom Sociala nämndernas förvaltning (SNF), vilken mynnade ut i 10 rekommendationer i syfte att stärka IT-säkerheten.

På uppdrag av de förtroendevalda revisorerna har EY genomfört en uppföljning av rekommendationerna från 2014.

2.2 Syfte

Granskningens syfte har varit att följa upp och bedöma om rekommendationerna från granskningen 2014 har åtgärdats.

För verksamhetssystemen ProCapita HSL, ProCapita IFO och Pulsen Combine har lokala rutiners överensstämmelse, berörande iakttagelserna från 2014, med stadövergripande styrande dokument inom IT-säkerhetsområdet verifierats.

Granskningen besvarar följande revisionsfrågor:

- Vilka åtgärder har genomförts för att hantera iakttagelserna från granskningen 2014?
- Har iakttagelserna från granskningen 2014 åtgärdats?

2.3 Avgränsningar

Granskningen har fokuserat på brister identifierade i granskningen av SNF som rapporterades 2014-10-21. Det har således inte verifierats att kontroller som fungerade 2014 fortfarande fungerar.

2.4 Metod

Granskningen har genomförts i följande steg:

1. Insamling av bakgrundsinformation inför intervjuer.
2. Bokning och genomförande av intervjuer för identifiering av övergripande rutiner och kontroller, liksom rutiner och kontroller avseende berörda system. Stickprovstestning har använts för att verifiera genomförda åtgärder.
3. Utformning av rapport som underlag för revisorernas bedömning av hur iakttagelserna från granskningen 2014 har hanterats. Rapporten beskriver en bedömning av hur väl iakttagelserna har hanterats, inkluderat iakttagelser och rekommendationer.

I källförteckning framgår vilka som intervjuats samt vilka dokument som granskningen baseras på.

Joa Silver har varit kontaktrevisor.

2.5 Kvalitetssäkring

Utöver vår interna kvalitetssäkring har intervjuade givits möjlighet att komma med synpunkter på rapportutkastet för att säkerställa att revisionsrapporten bygger på korrekta fakta och uttalanden. Skriftliga bekräftelser på att de intervjuade mottagit rapporten och givits denna möjlighet, har inhämtats. All korrespondens kring faktakontrollen har arkiverats.

3 Status på iakttagelser från 2014

Nedan följer iakttagelser och rekommendationer från 2014 samt en beskrivning av åtgärd och status på åtgärder. Status är definierat enligt följande:

Åtgärdad	Iakttagelserna bedöms vara åtgärdade
Delvis åtgärdad	Iakttagelserna bedöms delvis vara åtgärdade
Ej åtgärdad	Iakttagelserna bedöms inte vara åtgärdade

#	Iakttagelse, rekommendation, och status	Status

1.	**Iakttagelse 2014: Avsaknad av dokumenterade rutiner för hantering av behörigheter**
	I stadens riktlinjer för informationssäkerhet regleras styrning av åtkomst till system och nätverk. Riktlinjerna beskriver att det ska finnas rutiner för att säkerställa de behörigas åtkomst och för att förhindra obehörigas åtkomst till stadens information.
	Vi har noterat att Västerås stad saknar dokumenterade systemspecifika rutiner för hantering av behörigheter i verksamhetssystemen ProCapita HSL och Pulsen Combine samt att rutinerna relaterat till ProCapita IFO saknar kontroll avseende periodisk genomgång av tilldelade behörigheter.
	Rekommendation 2014:
	Vi rekommenderar Västerås stad att tydliggöra riktlinjerna för informationssäkerhet avseende styrning av åtkomst till system och nätverk. Det bör tydligt framgå vilka rutiner som bör finnas dokumenterade per verksamhetssystem och vilka kontroller som förväntas utföras avseende styrning av åtkomst. Riktlinjerna kan med fördel beskriva skillnader mellan verksamhetssystem av olika klassificeringar.
	Vidare rekommenderar vi SNF att dokumentera rutiner för att skapa nya/ta bort/förändra behörigheter i verksamhetssystemen, samt för att periodiskt granska behörigheter. Rutinerna bör minst omfatta följande kontroller och aktiviteter:
	• Det bör framgå vem som får beställa nya/ändrade behörigheter och på vilket sätt detta skall göras
	• Det bör framgå vem som får beställa borttag av behörigheter och på vilket sätt detta skall göras
	• Behörighetsadministratörer bör kontrollera att beställaren har befogenheter att göra beställning
	• Det bör vara klarlagt vem som ansvarar för att en person som slutar eller byter arbetsuppgifter inte längre har behörigheter till systemen
	• Det bör vara klarlagt vem som ansvarar för att initiera periodiska kontroller av behörigheter och på vilket sätt detta skall göras
	  • Behörighetsadministratörer bör förse verksamheten med listor över behörigheter periodvis
	  • Verksamheten bör gå igenom listorna, markera felaktigheter, signera samt sända tillbaka listorna till behörighetsadministratörerna
	• Behörighetsadministratörerna tar bort eller förändrar behörigheter enligt underlag
		Delvis åtgärdad

#	Iakttagelse, rekommendation, och status	Status
	Status 2016: SNF har under 2015 upprättat dokumenterade rutiner för hantering av behörigheter i berörda verksamhetssystem ProCapita HSL, Pulsen Combine, och ProCapita IFO. Dessa innefattar även fastlagda rutiner för periodisk granskning av behörigheter. SNFs följsamhet gentemot fastställda rutiner bedöms som god. För borttag av behörigheter kan viss förbättringspotential identifieras där behörighetsadministratörer upplever att verksamheten inte alltid meddelar dem då anställda byter tjänst alternativt slutar. Risken bedöms dock som lägre då rutiner för periodisk granskning av behörigheter etablerats (se vidare rekommendation #2). Staden har inte uppdaterat riktlinjerna för informationssäkerhet avseende styrning av åtkomst till system och nätverk, vilket kan medföra en risk att verksamhetssystem inom andra delar av staden har undermåliga rutiner för hantering av behörigheter. **Rekommendation 2016:** Västerås stad rekommenderas att uppdatera riktlinjerna för informationssäkerhet avseende styrning av åtkomst till system och nätverk. Detta för att tydliggöra vilka rutiner som bör finnas dokumenterade per verksamhetssystem och vilka kontroller som skall utföras avseende styrning av åtkomst. Om skillnad görs mellan olika verksamhetssystem bör detta framgå i riktlinjerna.	
2.	**Iakttagelse 2014: Användare som slutat har kvar behörigheter i verksamhetssystem** Via testning har vi konstaterat att 12 användare som slutat under de senaste sex månaderna fortfarande har behörighet i något av systemen, vidare har periodisk genomgång inte genomförts sedan augusti 2013 trots att stadens egna rutiner föreskriver att detta skall genomföras kvartalsvis. **Rekommendation 2014:** Vi rekommenderar Västerås stad att snarast ta bort de identifierade användarna samt se över det praktiska utförandet relaterat till borttag av användare. Dels bör det säkerställas att ansvarig person meddelas när en medarbetare slutar och dels bör periodisk genomgång av samtliga tilldelade behörigheter ske kvartalsvis in enlighet med stadens egna rutiner. Genomgångarna bör dokumenteras och vara spårbara.	**Åtgärdad**
	Status 2016: Identifierade obehöriga användare från granskningen 2014 har enligt uppgifts fått sina behörigheter borttagna/inaktiverade. Vidare har praktiska rutiner och ansvarsfördelning vid borttag av behörigheter dokumenterats. Respektive enhetschef är vid avslut av anställning ansvarig för att meddela behörighetsadministratörer för borttag av behörighet. Ytterligare kontroll sker genom inaktivering av användarkonton efter ett års inaktivitet, samt periodisk genomgång (kvartalsvis) i vilken respektive enhetschef kontrollerar behörigheterna. Via stickprovstestning har vi verifierat att rutinen för periodisk genomgång följs. Det pågår ett initiativ för att skapa en integration mellan stadens personaladministrativa system och berörda verksamhetssystem för att säkerställa automatisk borttagning/inaktivering av behörigheter då anställda med behörigheter slutar inom staden.	

#	Iakttagelse, rekommendation, och status	Status
3.	**Iakttagelse 2014: Avsaknad av regelverk för hantering av programändringar** Vi har noterat att Västerås stad saknar övergripande regelverk för hantering av programändringar och dokumenterade systemspecifika rutiner för hantering av programändringar i verksamhetssystemen. **Rekommendation 2014:** Vi rekommenderar Västerås stad att tydliggöra riktlinjerna för informationssäkerhet avseende anskaffning, utveckling och underhåll av programvaror. Riktlinjerna bör tydliggöra stadens regelverk för styrning av programförändringar. Detta regelverk kan med fördel beskriva skillnader mellan system av olika klassificeringar och bör omfatta regler för att förhindra obehörig förändring av information och funktionalitet. Vidare rekommenderar vi SNF att dokumentera rutiner för att beställa, testa, godkänna och övervaka programändringar. Rutinerna bör minst omfatta följande kontroller och aktiviteter: • Om skillnad skall göras mellan rutinerna för olika typer av programändringar bör det tydligt definieras vad olika typer av programändring innebär • Det bör framgå vem som får beställa programändringar och hur detta skall göras och dokumenteras • Det bör framgå vem som är ansvarig för att acceptanstesta programändringar och hur detta skall göras och dokumenteras • Acceptanstest av förändring bör göras i miljö separerad från produktionsmiljö. Testfall i testprotokoll bör vara länkade till innehåll i programförändringen • Det bör framgå vem som får godkänna driftsättning av programändringar och hur detta skall göras och dokumenteras • Det bör framgå vem som är ansvarig för att övervaka driftmiljön för att säkerställa att inga programändringar införs som inte är godkända, och hur detta skall göras och dokumenteras	**Delvis åtgärdad**
	Status 2016: Stadsövergripande instruktioner för beställning, testning, godkännande, och övervakning gällande programändringar har etablerats. SNF har under 2016 etablerat rutiner för ändringshantering i de för verksamheten berörda systemen. De beskrivna rutinerna följer väl både givna rekommendationer från granskningen 2014 samt stadsövergripande instruktioner. Noterbart är att SNF inte alltid i praktiken följer dessa rutiner för ändringshantering. Mindre förändringar sker frekvent och dessa hanteras ofta genom muntliga överenskommelser med leverantörerna, utan dokumenterat godkännande innan produktionssättning som beskrivet enligt rutinerna. Under våren 2016 inträffade en incident efter att en produktionssättning genomförts trots att SNF inte godkänt utfallet i testmiljö. **Rekommendation 2016:** Relaterat till föregående punkt rekommenderas SNF att vidare se över rutiner för dokumentation och testning av programändringar. Enligt dokumenterad rutin skall testning och godkännande utföras och dokumenteras för alla programändringar, vilket inte alltid sker vid mindre programändringar. Vi rekommenderar att godkännande att införa programändringar, oavsett komplexitet, alltid dokumenteras.	

#	Iakttagelse, rekommendation, och status	Status
4.	**Iakttagelse 2014: Logguppföljning genomförs inte i samtliga system** Vi har noterat att dokumenterad rutin för logguppföljning inte finns för samtliga system samt att uppföljning i ProCapita HSL och Pulsen Combine inte görs regelbundet. Enligt respondenterna har framtagandet av en gemensam rutin för logguppföljning påbörjats under 2010, dokumentet finns dock endast i utkast. **Rekommendation 2014:** Vi rekommenderar staden att ta fram en gemensam rutin för logguppföljning för att säkerställa hantering i enlighet med patientdatalagen. Vårdgivaren ska enligt densamma systematiskt och återkommande kontrollera åtkomsten till patientuppgifter.	**Åtgärdad**
	Status 2016: SNF har upprättat dokumentation om att logguppföljning skall ske av respektive verksamhet på regelbunden basis. Dokumentation innefattar även beskrivning om att granskning skall ske reaktivt, vid misstanke om felaktig hantering från användares sida. Granskning av tillhandahållna protokoll från SNF påvisar att systematisk stickprovskontroll har genomförts på regelbunden basis för systemen ProCapita HSL, Pulsen Combine, och ProCapita IFO.	
5.	**Iakttagelse 2014: Testning och godkännande av programändringar saknar spårbarhet** Vi har noterat att Västerås stad saknar spårbarhet från test och godkännanden av programändringar. **Rekommendation 2014:** Vi rekommenderar staden att se över de praktiska rutinerna relaterat till test och godkännande av programändringar. All testning bör dokumenteras och vara spårbar, vidare bör godkännanden inför driftsättning kommuniceras skriftligt till leverantören och sparas.	**Delvis åtgärdad**
	Status 2016: Upprättad rutinbeskrivning för programändringar beskriver att testning skall genomföras och dokumenteras för alla typer av programändringar. Granskning av testningsförfarandet visar att dokumentation av testning sker vid större förändringar. Vid mindre förändringar, som hanteras frekvent, dokumenteras inte alltid testningsförfarandet. **Rekommendation 2016:** SNF rekommenderas att se över rutiner för dokumentation och testning av programförändringar. Om skillnad görs bör det framgå i rutinbeskrivning hur man hanterar olika typer av programändringar. Vi rekommenderar alltid att godkännande att införa programändringar, oavsett komplexitet, dokumenteras.	
6.	**Iakttagelse 2014: Ofullständig modell för systemsäkerhetsanalys** Vi har noterat att stadens modell för systemsäkerhetsanalys inte inkluderar praktiska konsekvenser respektive klassificering innebär för informationshanteringen. Vidare finns ingen rutin för att uppdatera sårbarhetsanalysen samt följa upp de åtgärder som beslutas. Vi har noterat att det parallellt med granskningen pågår ett arbete med att uppdatera modellen. **Rekommendation 2014:** Vi rekommenderar Västerås stad att slutföra uppdateringen av modellen för systemsäkerhetsanalys och inkludera praktiska konsekvenser respektive klassificering skall ha på informationsbehandlingen samt rutin för att periodisk uppdatera och följa upp åtgärder inom sårbarhetsanalysen.	**Åtgärdad**
	Status 2016: Modellen för systemsäkerhetsanalys är uppdaterad i enlighet med rekommendationen från 2014. Modellen inkluderar hot- och riskbedömning samt åtgärdsplan för att hantera de praktiska konsekvenserna av informationsklassificeringen. Åtgärder hanteras efterhand baserat på hur kritiska de har bedömts.	

#	Iakttagelse, rekommendation, och status	Status
7.	**Iakttagelse 2014: Inaktuell systemsäkerhetsanalys för *Vård och omsorg*** Vi har noterat att systemsäkerhetsanalysen för *Vård och omsorg* inte uppdaterats sedan verksamhetssystemet Pulsen Combine inkluderades i förvaltningsobjektet. **Rekommendation 2014:** Vi rekommenderar staden att uppdatera systemsäkerhetsanalysen och den tillhörande sårbarhetsanalysen för förvaltningsobjektet *Vård och omsorg* för att säkerställa att verksamhetens krav återspeglas i förvaltningen.	**Åtgärdad**
	Status 2016: Systemsäkerhetsanalysen, med tillhörande riskbedömning och åtgärdsplan, har uppdaterats för *Vård och omsorg* under 2015 och att uppdateras på nytt under hösten 2016.	
8.	**Iakttagelse 2014: Avsaknad av regler kring distansarbete** Vi har noterat att staden saknar regler kring distansarbete. **Rekommendation 2014:** Vi rekommenderar staden att upprätta dokumentation med regler för distansarbete. Reglerna bör bland annat täcka in fysisk säkerhet och regler rörande utförande av informationsbehandlingsresurser från organisationens lokaler.	**Åtgärdad**
	Status 2016: Staden har under 2015 tagit fram övergripande dokumentation med instruktioner att varje lokal verksamhet skall upprätta rutiner gällande distansarbete. Vi har tagit del av för SNF upprättade regler kring distansarbete och mobilt arbete vilka är i enlighet med rekommendationerna från 2014.	
9.	**Iakttagelse 2014: Ofullständig kontinuitets- och avbrottsplanering** Vi har inte identifierat några existerande avbrottsplaner hos driftleverantörerna och verksamheten saknar dokumenterade reservrutiner för Pulsen Combine. Vidare har test för att säkerställa att systemen kan återstartas från säkerhetskopiorna inte genomförts. **Rekommendation 2014:** Vi rekommenderar Västerås stad att se över rutinerna för kontinuitetsplanering. Rutinerna bör adressera reservrutiner vid avbrott och rutiner för inmatning av data från reservrutiner. Vidare rekommenderar vi Västerås stad att genomföra en granskning av leverantörernas avbrottsplanering för att säkerställa att det finns ändamålsenliga rutiner för återställning av system, säkerhetskopiering av information, återskapande av förlorad information, och periodisk testning av rutiner.	**Åtgärdad**
	Status 2016: Staden har övergripande riktlinjer som uttrycker att respektive verksamhet ansvarar för relevant avbrotts- och kontinuitetsplanering. SNF har upprättade kontinuitetsplaner och avbrottsplan för verksamhetssystemen ProCapita HSL, Pulsen Combine, samt ProCapita IFO med god följsamhet gentemot rekommendationerna från 2014. Leverantörernas avbrottsplanering följs upp genom kontinuerlig dialog samt genom kontinuerlig återläsning av data från produktionsmiljön (säkerhetskopior) till testmiljön.	
	Iakttagelse 2014: Leverantörers åtaganden följs inte upp Vi har noterat att Västerås stad inte följer upp system- och driftleverantörernas avtalade åtaganden. Enligt stadens riktlinjer för informationssäkerhet skall det finnas rutiner för hur uppföljning och granskning ska göras på utomstående leverantörers tjänster. **Rekommendation 2014:** Vi rekommenderar Västerås stad att kontinuerligt följa upp de åtaganden som avtalats för att säkerställa att stadens system och data hanteras på ett ändamålsenligt sätt samt att verksamhetens krav tillgodoses. Vi har noterat att staden har inkluderat rätten att granska leverantörerna i avtalen, vilket bör praktiseras. Förslag på områden att inkludera i en sådan granskning är exempelvis avbrottsplanering, hantering av behörigheter samt hantering av programförändringar.	**Ej åtgärdad**

#	Iakttagelse, rekommendation, och status	Status
	Status 2016: Uppföljning av leverantörers åtaganden sker inte fullt ut i enlighet med rekommendationen. Regelbundna uppföljningsmöten hålls med systemleverantörer på månatlig basis, men man har fortsatt inte utnyttjat de revisionsklausuler som finns i avtalen med leverantörerna. **Rekommendation 2016:** SNF rekommenderas att stärka uppföljningen av leverantörernas åtaganden gällande deras ansvar och hantering avseende avbrottsplanering, behörighetshantering, samt programändringshantering. SNF bör praktisera den möjlighet till granskning av leverantörerna som finns avtalad för att säkerställa en korrekt och ändamålsenlig hantering i enlighet med etablerade avtal.	

Västerås, 18 oktober 2016

Tobias Hermansson

Oscar Rydén

4 Källförteckning

Intervjuade

IKT-strateg, SNF

Förvaltningsledare Vård & Omsorg och Individ & Familj, SNF

Granskad dokumentation

Loggkontroll HSL, 2016-08-30

Riktlinjer för informationssäkerhet, 2012-01-18

Protokoll för förvaltingsrådsmöte, 2016-08-23

Statusrapport ersättningshanteringen (Pulsen), 2016-08-25

Testfall 1, Skultuna

Testfall 2, Attendo 4

Information inför kommande uppdatering av Pulsen Combine i TEST, 2016-02-03

Rutin för att beställa programförändringar

Gemensam avbrottsplan, 2011-12-22

Social dokumentation i Pulsen, 2016-09-05

Basrutin Biståndsenheten äldreomsorg, 2016-06-21

Arbeta mobilt SNF, 2016-05-13

SSA Objekt VoO, 2015-03-06

Instruktion Systemsäkerhetsanalys i Västerås stad, 2016-06-09

Instruktion Basnivå IT-säkerhet, 2015-05-18

Leveransprotokoll Pulsen Combine, 2013-09-18

Kundtester användare och behörigheter checklistor, 2016-01-28

Rutin behörighet systemadministration,

Rutin behörighet utförare, 2016-02-08

Rutin behörighetshantering Vård och omsorg, 2015-03-15

Rutin för registervård i Procapita HSL, Synergi, Prator, 2016-02-09

Avslutade behörigheter 2016

Reg. HSA kontroll Västerås

HSA-SITHS kontroll IFO Mars 2016

HSA-SITHS kontroll IFO Juni 2016

Reg. HSA kontroll Västerås Procapita HSL och Pulsen

Instruktion avsteg från korrekt informationshantering, 2015-01-29

Loggkontroll rutin, 2015-03-26

Instruktion loggning i Procapita IFO

Instruktion loggning i Vård o omsorg HSL system

Instruktion loggning i Pulsen Combine

Loggkontrollprotokoll, SocialkontorBoUSamhällsvård, 2015-12-07

Loggkontrollprotokoll, Samhällsvårdsenheten, 2016-04-11

Loggkontrollprotokoll, ÖVFamiljUngoVux, 2016-04-05

Loggkontrollprotokoll, Sysselsättning psykiatri, 2016-01-19

Loggkontrollprotokoll, MissbrukBoenden, 2016-04-11

Loggkontroll slumpmässigt urval

Loggkontrollprotokoll, Ankaret, 2015-06-22

Loggkontrollprotokoll, Mottagningen och på Familjehemsenheten, 2015-10-23