



Svedala kommun

**IT-granskning
Generella IT kontroller
Revisionsrapport**

Offentlig sektor/IT Advisory
KPMG AB
2010-12-16
Antal sidor: 18

Innehåll

1.	Sammanfattning och rekommendationer	1
2.	Inledning	3
2.1	Uppdrag	3
2.2	Genomförande	3
3.	Struktur och IT-organisation	4
3.1	Framväxt	4
3.2	Ansvarsområden	4
3.3	IT-enheten	4
3.3.1	Organisation	4
3.3.2	Finansiering	5
3.3.3	Verksamhet och support	5
3.4	Mål och strategier	5
4.	IT-stödet	6
4.1	Väsentliga stödsystem	6
4.1.1	Klassificering av system	6
4.2	Verksamhetens beroende av systemstödet	7
5.	Systemförvaltningen	7
5.1	Inledning	7
5.2	Personal (Heroma)	7
5.3	Socialförvaltningen (<i>Procapita</i>)	8
6.	IT generella kontroller	10
6.1	Styrning av IS/IT-verksamheten	10
6.1.1	Styrande dokument	10
6.1.2	Organisation	10
6.1.3	Individuella Systemsäkerhetsanalyser	11
6.1.4	Kontinuitetsplanering	12
6.1.5	Användarstyrning	12
6.2	Fysisk säkerhet	12
6.3	Logiska accesskontroller	13
6.3.1	Användarkonton i nätverket	13
6.4	Backup och Restore	15
6.5	End-User Computing	16

1. Sammanfattning och rekommendationer

På uppdrag av kommunens revisorer har KPMG genomfört en granskning av IT-verksamheten med inriktning på den centrala IT-funktionen och IT-säkerheten.

Vår bedömning är att det är en väl fungerande verksamhet, men det finns också förbättringsområden.

När det gäller den övergripande styrningen finns dokument som täcker IT-policy allmänt liksom särskilt vad avser informationssäkerhet. Det finns emellertid ett behov av att IT-policy/IT-strategi uppdateras och synkroniserat till övriga styrdokument.

Ansvar för och utformningen av IT-verksamheten inom Svedala kommun regleras genom de för IT verksamheten styrande dokumenten (*Informationssäkerhetspolicyn och därtill kopplade Informationssäkerhetsinstruktioner*), som fastställdes av kommunstyrelsen under 2007. Genom dessa dokument har kommunen bland annat fastställt ansvarsfördelning och grundläggande informationssäkerhetsrutiner.

Ansvar för kommunens olika verksamhetssystem, såväl funktionellt som säkerhetsmässigt, har fördelats till respektive verksamhetsledning. De styrande dokumenten fastställer dessutom att respektive verksamhetsledning ska genomföra *systemsäkerhetsanalyser* för varje (kritiskt) verksamhetssystem. Avsikten med detta är att uppnå en effektiv informationssäkerhet anpassad till varje system individuellt och där utgångspunkten är varje systems betydelse för verksamheten samt känsligheten i den av systemet hanterade informationen.

Hittills har dock endast informationssäkerhetsanalyser genomförts för de system som IT support ansvarar för. För de system som kommunens olika verksamheter använder (Heroma, Procapita med flera), *har inga sådana systemsäkerhetsanalyser genomförts*. Detta medför att det för dessa system inte fastställts några individuellt anpassade informationssäkerhetskrav. Detta är en brist som bör åtgärdas. Det är lämpligt att följa upp anledningen till att systemsäkerhetsanalyser inte genomförts.

Förutom avsaknaden av informationssäkerhetsanalyser visar vår granskning att den interna kontrollen inom IT-verksamheten kan förstärkas i ett antal avseenden. Dessa framgår i punktform nedan. För en bättre förståelse av de olika punkterna rekommenderas genomläsning av rapportens olika avsnitt.

Vi rekommenderar kommunen att

- Utveckla regler för "Segregation of Duty", d v s ett regelverk av vilket det framgår vilka kombinationer av arbetsansvar/systemrättigheter som är olämpliga att kombinera. Dessa regler bör användas av behörighetsadministrationen för de olika systemen
- Vi rekommenderar kommunen att komplettera avstämningsarbetet inom Heroma så att det även inkluderar en avstämning mellan rapporterad (attesterad) kostnad enligt Heroma och utbetalningsfilen, innan denna skickas till banken

- Utveckla rutiner för att regelbundet granska aktualiteten i samtliga systembehörigheter i alla kritiska system. Avseende Heroma var det inte möjligt att granska aktuella behörigheter eftersom det inte gick att ta ut en sådan rapport
- Utveckla rutiner varigenom undantag från fastställd, implementerad säkerhetspolicy avseende inaktivitet, byteskrav för lösenord mm, kan undvikas. Detta avser bland annat systemet Procapita men även övriga system
- Förtydliga kravet på sekretess avseende Procapita i supportavtalet med Tieto. Innevarande supportavtal hänvisar endast till interna sekretessbestämmelser inom Tieto, vilket innebär att kommunen inte haft möjlighet att ta ställning till vilka konkreta regler som skall tillämpas
- Vi rekommenderar kommunen att vidta åtgärder för att IT kontinuitetsplanering, inklusive avbrottsplaner, skall utvecklas och regelbundet testas för kritiska system
- Eftersom systemsäkerhetsanalyser inte genomförts, har systemindividuella krav avseende fysisk - och miljömässig säkerhet - inte fastställts. Däremot är det vår rekommendation att de mest känsliga och betydelsefulla systemen bör driftas i kommunhusets serverrum mot bakgrund av ett bättre skalskydd (gjutna väggar) och mer tillförlitlig kontinuitet (med avseende på reservkraft i form av ett dieselvek)
- Förstärka aktuella inställningar i den säkerhetspolicy som implementerats i Windows AD i nätverksmiljön, enligt rekommendationer från Sekchek analysen. I samband med remisshanteringen av innevarande rapport framkom att man beslutat genomföra följande förstärkande åtgärder:
 - "Minimum Password Length" kommer att ändras till 8 tecken,
 - "Maximum password Age in Days" kommer att ändras till 60,
 - "Password History Size" kommer att ändras till 13,
 - "Password Complexity" kommer att införas,
 - "Force Logoff when Logon Times Expires" kommer att införas och
 - "Prevent Transfer of Password in Clear Text" kommer att införas.
- Vi rekommenderar dessutom kommunen att analysera noterade iakttagelser utifrån Sekchek analysen avseende inaktiva nätverkskonton och nätverkskonton som undantagits från byteskrav avseende lösenord
- Eftersom nuvarande metod för backup och restore (ingen planmässig restore) inte utvecklats utifrån av verksamheterna analyserade och dokumenterade behov (lagenliga såväl som verksamhetsmässiga), är det vår rekommendation att dessa rutiner omprövas
- Utveckla en rutin där egenutvecklade (Excelkalkyler eller liknande) applikationer identifieras och dokumenteras för att skapa möjlighet att inkludera dessa i informationssäkerhetsarbetet (åtkomst, ändringar mm).

2. Inledning

2.1 Uppdrag

KPMG har av Svedala kommuns revisorer fått i uppdrag att övergripande granska hur kommunen samordnar IT-verksamheten i kommunen samt hur IT-säkerheten i detta sammanhang upprätthålls och kontrolleras.

Dataverksamheten är omfattande och av stor betydelse för att kärnverksamheten ska kunna bedrivas ändamålsenligt och effektivt. Samtidigt kan konstateras att verksamheternas beroende av ett fullgott IT-stöd är kritiskt ur säkerhetssynpunkt.

Granskningens inriktning mot Generella IT kontroller i användningen av verksamhetskritisk IT-verksamhet, omfattar såväl IT-system som infrastruktur (t ex nätverk och drift) inom Svedala kommun.

2.2 Genomförande

Granskningen har inriktats dels mot den centrala IT-enhetens verksamhet som omfattar kommunens nätverk, systemdrift och användarsupport (IT-infrastruktur) och dels mot ett urval av den decentraliserade systemförvaltningen.

För att bland annat verifiera hanteringen av användarkonton i operativsystemet (Windows AD) för nätverket, har vi använt ett verktyg (Sekchek), för att ”läsa av” vissa inställningar och aktiviteter. Ett detaljerat resultat av denna analys avrapporteras separat, samtidigt som de väsentligaste noteringarna från analysen dessutom framgår under respektive avsnitt i denna rapport.

Ansvar för den operativa *förvaltningen av de olika verksamhetssystemen* är decentraliserat till ledningen för respektive verksamhet som utnyttjar de aktuella systemen. Vi har valt att granska vissa rutiner vid systemförvaltningarna av två system, dels vid Personal (*Heroma*) och dels vid Socialförvaltningen (*Procapita*).

Granskningen är baserad på intervjuer med IT chef Pekka Kalliomäki, enhetschef IT Support Hans-Åke Olsson, Systemförvaltare Personal Robert Aradszky (*Heroma*) och Systemförvaltare Vård och omsorg Annika Persson (*Procapita*) samt IT-ansvarig vid verksamhetsområde utbildning. Vi har också Dessutom har vi tagit del av för granskningen erforderliga dokument, instruktioner, rutinbeskrivningar mm, liksom att vi beställt och tagit del av extraerad information från vissa system.

Granskningen har genomförts av Jan-Inge Hedin med biträde av Olof Eriksson, hösten 2010.

3. Struktur och IT-organisation

3.1 Framväxt

En mycket stor del av verksamheten i kommunen bedrivs och kopplas till någon form av datoriserat stöd som med tiden utvecklats till att bli en förutsättning för att kunna bedriva verksamheten på ett effektivt och ändamålsenligt sätt. Antalet datorer, tillhörande utrustning och utbyggnad av nät för kommunikation har under senare år ökat i snabb takt.

3.2 Ansvarsområden

För att hantera alla system och samordna dem på olika sätt är det viktigt att klara ut vem som ansvarar för vad i sammanhanget. Några nyckelbegrepp som beskriver ansvarsfördelningen kan beskrivas som följer.

Systemägare är den myndighet (t ex nämnd) i kommunen vars verksamhetsområde är användare av ett system t ex ett verksamhetssystem. I det fall ett system används av flera nämnder kan en nämnd, t ex kommunstyrelsen vara systemägare. Systemägaransvaret kan delegeras till exempelvis förvaltningschefen. Nämnden är registeransvarig enligt datalagen även om nämnden inte är systemägare.

Systemförvaltning är det planeringsarbete som systemägaren själv eller genom delegation till annan skall ansvara för, till exempel att följa verksamhetens behov av nya och förändrade arbetssätt samt tillse att användare får den utbildning och information som behövs.

Systemförvaltaren eller systemansvarig är den som **genom delegation från systemägaren** fått i uppdrag att bereda systemärenden för förvaltningsledningen samt att svara för administration, förvaltning och användning. Systemförvaltaren fastställer krav på behörighet och kompetens för systemets användare, initierar utbildning av systemets användare, bevakar och bereder frågor kring systemsäkerhet, ansvarar för information till användarna om förändringar och nyheter i systemet och IT-stödet.

IT-avdelningen har det tekniska kunnandet och finns som stöd till de ansvariga och verksamheterna som använder IT-systemen. IT-avdelningens huvuduppgift kan sägas vara drift av systemen men enheten har också en viktig roll när det gäller att bereda ärenden gällande IT-verksamheten samt när det gäller bevakning av att riktlinjer och regler följs till exempel i samband med upphandling av datorer och IT-system.

3.3 IT-enheten

3.3.1 Organisation

Kommunen samordnar IT-stödet till verksamheterna i en gemensam IT-enhet. Denna organisation bildades för fyra år sedan. IT-enheten i Svedala är organiserad i den centrala administrationen och redovisningschefen är övergripande chef för avdelningen som operativt leds av IT-chefen. Det finns en IT-grupp som består av representanter för verksamheterna som under

arbetsledaren för IT-support hanterar och utreder IT-frågor. Vid viktigare beslut deltar IT-chefen (Informationssäkerhetsinstruktionen 2007-06-18).

Av kommunstyrelsens reglemente framgår att kommunstyrelsen har ett ansvar för att yttra sig eller fatta beslut i utvecklingen av informationssystem och IT.

Enheten omfattar 9,75 tjänster. Tre av dessa undervisar som en del av sin tjänst också vid gymnasieskolans KY-utbildning (kvalificerad yrkesutbildning). Enheten har jour dygnet runt.

3.3.2 Finansiering

IT-enhetens verksamhet är anslagsfinansierad och interndebering förekommer inte. Verksamheterna behöver bara betala datorer om det är fråga om utökning av beståndet.

För år 2010 omsluter driftbudgeten 10,3 Mkr.

3.3.3 Verksamhet och support

Vid IT-enhetens start för fyra år sedan fanns 300 datorer administrerade i den egna verksamheten. Nu ligger antalet datorarbetsplatser på 2 600 (varav ca 1 500 är elevdatorer).

Enligt de uppgifter vi erhållit fungerar IT-supporten bra. För två år sedan har en intern kundnöjdhetsenkät genomförts med 87 procents svarsfrekvens från användarna och de administrativa användarna gav IT-avdelningen ett högt betyg. Från skolans användare har dock funnits en besvikelse grundad på att IT-ansvariga vid skolenheterna togs bort. Enligt intervjukommentar har det inneburit att närheten tappats och trögheten blivit högre, men samtidigt att en jämnare servicenivå och mindre sårbarhet i verksamheten.

Drift

IT-enheten sköter all drift själva. Man bygger egna system, exempelvis har man tagit fram systemet för Medborgardialogen.

3.4 Mål och strategier

Det finns flera övergripande styrdokument. En **IT-policy** finns upprättad 1999 och den har i en skrivning till kommunstyrelsen reviderats 2004-05-03, **Förslag till förändringar i IT-strategin**. Kommunstyrelsen har (2007-10-24) fastställt dels en **Informationssäkerhetspolicy** och en **Informationssäkerhetsinstruktion** har tagits fram och beslutats i kommunledningsgruppen (2007-06-18). Policydokumenten avseende informationssäkerhet kommenteras vidare i avsnitt 9.

Det finns utöver dessa dokument inte någon ytterligare beslutad övergripande strategi för den nuvarande och framtida IT-utvecklingen som vi tagit del av.

Vår notering:

Det finns ett behov av att styrdokumentet vad avser IT-policy/strategi lyfts fram och uppdateras med hänsyn till exempel till utvecklingen av sociala media. Det finns också behov av att de renodlas/synkroniseras. Exempelvis definieras "IT-grupp" helt olika i IT-strategin jämfört med

Informationssäkerhetspolicyn. Ett par av styrdokument har angivna tidpunkter för revidering, men vi kan inte se att det ännu effektuerats.

4. IT-stödet

4.1 Väsentliga stödsystem

4.1.1 Klassificering av system

Under 2008 beslutade Kommunstyrelsen om ”Programförteckning för Svedala kommun, 2008-12-02”, med uppgift om kommunens Program, Avdelningstillhörighet, Systemägare, Systemförvaltare, Systemadministratör, Notering om respektive program är samhällsviktigt samt Klassning utifrån ”Sekretess”, ”Riktighet” och ”Tillgänglighet”.

Förteckningen omfattar 108 program, varav 22 bedömdes vara samhällskritiska. Sammantaget klassades 76 av 108 program. Man valde tre klassningsnivåer, ”Mkt hög”, ”Hög” och ”Normal”. Samtliga klassade program har bedömts vara lika känsliga utifrån alla tre bedömningsvariablerna. Nivån ”Mkt hög” blev bedömningen för 10 program, ”Hög” 20 program, ”normal” 46 program medan 32 program inte klassats. I tabellen nedan framgår de program som bedöms vara känsligast för kommunens verksamhet.

Program	Systemägare	Anm.	Sekretess	Riktighet	Tillgänglighet
Raindance	Pekka Kalliomäki	SV	Mkt hög	Mkt hög	Mkt hög
Active Directory	Pekka Kalliomäki		Mkt hög	Mkt hög	Mkt hög
Heroma	Jonas Jönsson	SV	Mkt hög	Mkt hög	Mkt hög
LPS	Jonas Jönsson	SV	Mkt hög	Mkt hög	Mkt hög
PA direkt	Jonas Jönsson		Mkt hög	Mkt hög	Mkt hög
Alarmos	Örjan Thorné	SV	Mkt hög	Mkt hög	Mkt hög
Procapita	Thomas Persson	SV	Mkt hög	Mkt hög	Mkt hög
Synergi	Thomas Persson		Mkt hög	Mkt hög	Mkt hög
ProfDok	Karin Jense		Mkt hög	Mkt hög	Mkt hög
Bewator 2010	Fredrik Löfqvist	SV	Mkt hög	Mkt hög	Mkt hög

SV = Systemet anses vara samhällskritiskt

Klassificering av IT system kan inte ske utan koppling till den verksamhet som ett system stödjer. Respektive kärnverksamhets betydelse för kommunen, känsligheten i den information som behandlas i systemen och en bedömning av konsekvenserna vid ett systemavbrott är underlag vid bedömningen.

Fördelen med att klassificera de olika systemen är att det ger möjlighet att anpassa säkerhet och skydd systemindividuellt (exempelvis avseende drift, support, logisk och fysisk säkerhet). Säkerhetsarbetet kan då anpassas på ett ändamålsenligt och kostnadseffektivt sätt för kommunen.

4.2 Verksamhetens beroende av systemstödet

Klassificeringen enligt föregående avsnitt visar att flera av kommunens verksamheter har ett stort beroende av systemstödet.

Detta ställer höga krav på ett antal av de rutiner/processer/kontroller som tillämpas inom IT-verksamheten (systemförvaltningen och verksamheten inom den centrala IT-enheten).

5. Systemförvaltningen

5.1 Inledning

Som nämnts ovan har vi valt att granska vissa rutiner vid två av systemförvaltningarna inom Svedala Kommun, nämligen dels Personal (*Heroma*) och dels Socialförvaltningen (*Procapita*).

Resultatet av dessa systemförvaltningar har vi valt att avrapportera separat, huvudsakligen för att förtydliga att de rutiner systemförvaltningarna tillämpar handläggningssmässigt är åtskilda från IT-enhetens verksamhet.

5.2 Personal (*Heroma*)

De löneadministrativa rutinerna inom personalförvaltningen stöds av systemet *Heroma*. Systemägare är Personalchef Jonas Jönsson och systemförvaltare är Robert Aradszky.

Robert är behörighetsadministratör, en systemrättighet att registrera nya, ändra befintliga och att ta bort inaktuella användarkonton. Robert har också administrationsrättigheter i *Heroma*, som ger rätt att påverka alla inställningar och uppgifter i systemet. Även andra medarbetare på personalavdelningen har administrativa rättigheter i systemet.

Via systemet administreras löner åt ca 1 800 anställda vid kommunen.

Chefer attesterar avvikelser från normaltids i *Heroma*. Reseersättningar och traktamenten kommer också att hanteras via attester i systemet från hösten 2010. Löneadministratören registrerar avdelningar och enheter i systemet samt vem som är chef för respektive verksamhetsdel. Chefer registrerar själva vem man är chef över. Detta ger attesträtt för de olika anställdas rapporter via *Heroma*.

Alla ändringar loggas i systemet, men inga loggar utgör underlag för regelbundna kontroller.

Varje månads lönebearbetning hanteras av Robert Aradszky genom att köra ”Lön 1”, med fellistor som rättas innan nästa körning. Efter körning av ”Lön klar” erhålls ett antal slutlistor som bland annat visar månadens löneutbetalning. Detta kontrolleras och attesteras av ekonomichef.

Det kan finnas oattesterade rapporter i systemet då inte ingår i aktuell månads utbetalning. Kontroll av oattesterade rapporter i *Heroma* vid granskningstillfället visade att de äldsta

oattesterade rapporterna var per april 2010 (2 st). Robert försöker påminna för att undvika för långa eftersläpningar.

Efter attest skickas en fil till banken för utbetalning. Fyra tjänstemän, inklusive Robert Aradszky på personalavdelningen har behörighet (kort och kod) att ”släppa” filen på banken för utbetalning. Innan filen ”släpps” sker ingen kontroll av att utbetalning enligt filen stämmer överens med det belopp som ekonomichefen attesterat. Däremot kontrolleras i efterhand att det belopp som dras från kontot stämmer överens med av ekonomichefen attesterat belopp.

Vi efterfrågade en fil för att kontrollera aktuella behörigheter i systemet, men detta var inte möjligt att extrahera på kort sikt. Sådana rapporter extraheras inte i den löpande verksamheten.

Systemsäkerhetsanalys, i enlighet med Informationssäkerhetsinstruktionerna saknas. Betydelsen av Heroma har erhållit högsta skyddsklass (”Mkt hög”), se avsnitt 4.1.1, ovan. Dessutom har systemet ansetts vara samhällskritiskt.

Vår notering:

Vi rekommenderar systemägaren att genomföra en Systemsäkerhetsanalys enligt kommunens beslutade Informationssäkerhetsinstruktioner.

Vi rekommenderar dessutom kommunen att generellt överväga att utveckla regler för ”Segregation of Duty”, d v s ett regelverk av vilket det framgår vilka kombinationer av arbetsansvar/systemrättigheter som är olämpliga att kombinera. Exempel på sådana olämpliga kombinationer är starka rättigheter i ett system (administrativa rättigheter) samtidigt med verksamhetsmässiga arbetsuppgifter som utförs via systemet.

Vi rekommenderar kommunen att komplettera avstämningsarbetet så att det även inkluderar en avstämning mellan rapporterad kostnad enligt Heroma och utbetalningsfilen innan den skickas till banken.

Vi rekommenderar dessutom kommunen att utveckla rutiner för att regelbundet granska att systembehörigheterna är aktuella i systemet. Vi lyckades inte få ut en lista där de aktuella behörigheterna framgår och kommunen tillämpar inte heller någon rutin varigenom detta granskas löpande.

5.3 Socialförvaltningen (*Procapita*)

Socialförvaltningen består av flera enheter (IFO, Hälso- och Sjukvård, Äldreomsorg, LSS-verksamhet och avgifter inom Vård och omsorg), vars verksamheter stöds av systemet Procapita. Systemet innehåller känslig information och har klassificerats med högsta skyddsklass (”Mkt hög”) och anses dessutom vara samhällskritiskt.

Systemsäkerhetsanalys (se avsnitt 6.1.3), i enlighet med kommunens Systemsäkerhetsinstruktioner, har inte genomförts. Man har således inte bedömt behovet av förstärkta skyddsåtgärder med avseende på informationssäkerheten.

Utifrån en extraherad lista över aktiva användare vid granskningstillfället fanns 361 aktiva användarkonton i systemet. 25 av dessa konton är undantagna från kravet att byta lösenord (för övriga konton krävs byte efter 30 dagar). I stort motsvarande konton har dessutom undantagits från automatisk inaktivering om kontot inte används under 50 dagar. Dessa undantag, på enskild kontonivå, är motstridiga mot bestämmelser enligt kommunens Systemsäkerhetsinstruktioner.

Alla aktiviteter i systemet loggas. Dessa loggar granskas enligt särskild rutin och från innevarande år kommer detta att utföras av respektive enhetschefer.

Rutinerna kring behörighetsadministrationen för Procapita har inte dokumenterats. Annika Persson är behörighetsadministratör. Uppdrag att ändra användarkonto (ny, ändring, avslut) behöver inte alltid vara skriftligt. Uppdragen kommer dock alltid från enhetschef. Man tillämpar en rutin där listor över användare regelbundet tillställs enhetschefer för kontroll. Enhetscheferna återlämnar listorna efter genomgång av aktuella användare och undertecknande. Dessa förteckningar kommer i framtiden att kompletteras med användarkontonas rättigheter.

Användare av Procapita får särskilda Användaranvisningar med regler att följa när man arbetar i systemet. Dessa anvisningar innehåller särskilda sekretessanvisningar, men kommer att kompletteras med ett förtydligande om att man endast får ta del av sådana uppgifter i systemet som behövs för att fullfölja tilldelade arbetsuppgifter vid varje tillfälle. Detta saknas i nuvarande anvisningar.

Tieto supportar systemet och har av denna anledning ett användarkonto (TElfoSUP) till systemet. Kontot har undantagits från såväl lösenord som automatisk inaktivering. Vi rekommenderar kommunen att överväga att inte tillåta liknande undantag, för något användarkonto, för att undvika att detta kan underlätta obehörig åtkomst och därmed sammanhängande risker.

Kommunen bör vidare överväga att förstärka sekretessförbindelsen i supportavtalet med Tieto. Denna hänvisar endast till interna sekretessbestämmelser inom Tieto.

Särskilda regler kring roller och tilldelning av rättigheter har utvecklats av Systemförvaltningen för Procapita. Syftet är att förstärka sekretesskyddet i systemet.

Vår notering:

Vi rekommenderar systemägaren till Procapita att genomföra Systemsäkerhetsanalys enligt kommunens beslutade Informationssäkerhetsinstruktioner för Procapita.

Vi rekommenderar också systemägaren att (undantaget servicekonton där lösenord inte kan förekomma) inte tillåta undantag från fastställda regler kring lösenord (bytesfrekvens) och inaktivering av användarkonton. Dessa regler syftar till att förhindra obehörig åtkomst och bör därför tillämpas utan undantag. Vid granskningen fanns 25 användarkonton med undantag från byteskrav för lösenord.

Kommunen bör vidare överväga att förstärka sekretessförbindelsen i supportavtalet med Tieto. Denna hänvisar endast till interna sekretessbestämmelser inom Tieto.

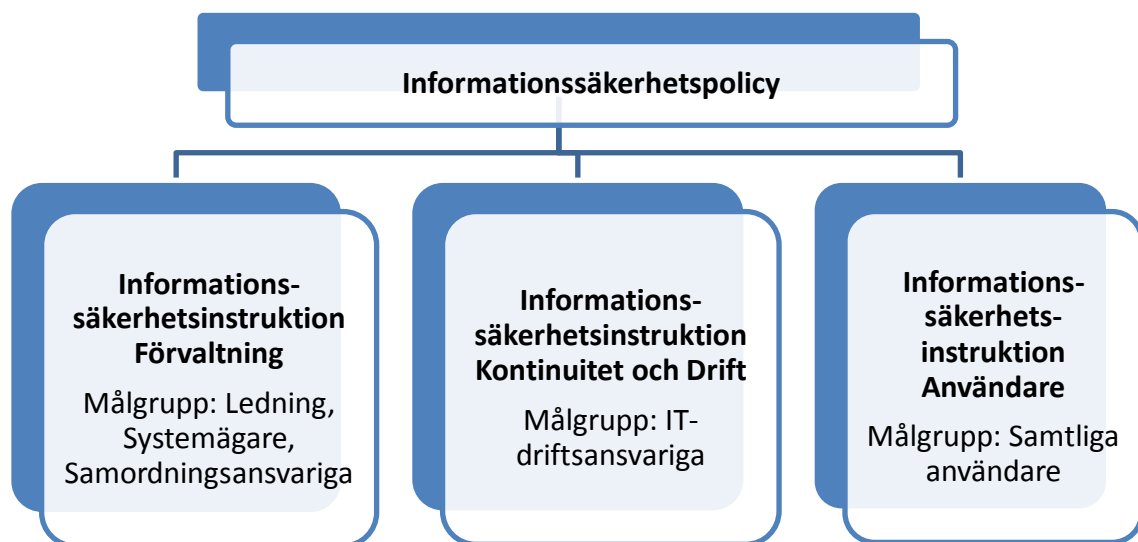
Vi rekommenderar dessutom kommunen att tillämpa rutiner för behörighetsadministrationen där uppdrag att ändra användarkonto (ny, ändring, borttag) alltid är skriftliga.

6. IT generella kontroller

6.1 Styrning av IS/IT-verksamheten

6.1.1 Styrande dokument

Fastställda styrande dokument för kommunens informationssäkerhet framgår av nedanstående bild



Genom Informationssäkerhetspolicyn har kommunen beslutat att Krisberedskapsmyndighetens (KBM:s) rekommendationer om basnivå för informationssäkerhet (BITS) ska gälla som ramverk för informationssäkerhetsarbetet. Kommunstyrelsen fastställde de ovan beskrivna dokumenten under 2007.

Dokumenterna skapar en robust utgångspunkt för kommunens arbete med informationssäkerhet, där **Informationssäkerhetspolicyn** fastställer de övergripande kraven medan de övriga tre instruktionerna konkretiserar och förtydligar såväl det löpande arbetet som de mer detaljerade kraven. Bland annat beskrivs den basnivå för informationssäkerhet som är kravet för samtliga system som kommunens olika verksamheter använder.

6.1.2 Organisation

Det sätt som informationssäkerhetsarbetet är organiserat framgår på ett tydligt sätt av de styrande dokumenten. Bland annat visar "Informationssäkerhetsinstruktion, Förvaltning" en detaljerad bild av arbets-, och ansvarsfördelningen för informationssäkerhetsarbetet.

Bland annat framgår att kommunstyrelsen fastställer de styrande dokumenten medan systemägaren för respektive system har ansvar för att genomföra en *systemsäkerhetsanalys* individuellt för de olika systemen.

Av avsnitt ”4.2.1, Klassificering av system”, ovan framgår att kommunstyrelsen under 2008 fastställde en ”Programförteckning för Svedala kommun”. Av förteckningen framgår bland annat systemägare och klassificering för samtliga väsentliga system.

6.1.3 Individuella Systemsäkerhetsanalyser

De styrande dokumenten (se avsnitt 6.1.1) reglerar att säkerhetsarbetet skall bedrivas/utformas individuellt för de olika systemen, beroende på systemens betydelse för kommunen och dess kärnverksamheter. Detta innebär att samtliga system skall klassificeras (se avsnitt 2.1.1) och att respektive systemägare har ansvar för att en *systemsäkerhetsanalys* genomförs med utgångspunkt från systemets klassificering.

Av ”Informationssäkerhetsinstruktion Förvaltning” framgår att systemsäkerhetsanalysen skall fastställa eventuella tilläggskrav, utöver basnivån, som framgår av de styrande dokumenten. Därutöver skall systemägarna genomföra en analys utifrån

- den information systemet hanterar
- lagar, förordningar och författningar
- verksamhetens krav på säkerhet vad avser sekretess, riktighet och tillgänglighet
- hotbilden mot informationen
- vilka olika behörighetsprofiler som ska gälla
- att i samverkan med IT-support fastställa avbrottsplan för informationssystemet
- omfattning av loggning (trans- och säkerhetsloggar)
- hur loggar ska följas upp, arkiveras, förvaras och sparas
- längsta acceptabla tid för driftavbrott och/eller informationsbortfall
- tid för hur snabbt återläsning av säkerhetskopierat material ska kunna ske

Genom individuella analyser kan kommunen anpassa säkerhetsarbetet så att väsentliga värden skyddas på ett säkrare sätt medan skyddet för mindre betydelsefulla system kan ske mer kostnadseffektivt.

Våra intervjuer visar dock att det inom kommunen inte genomförts några systemsäkerhetsanalyser och då inte heller för de system som bedömts vara mycket känsligt och betydelsefullt för kommunens verksamhet (se avsnitt 4.1.1).

Vår notering:

Vi rekommenderar kommunen att vidta åtgärder för att individuella systemsäkerhetsanalyser, enligt kraven i Informationssäkerhetsinstruktionerna, skall genomföras för de system (108 system) som används inom kommunen. Kravet på att sådana analyser skall genomföras, beslutades av kommunstyrelsen under 2007, men hittills har inga analyser av verksamhetssystem genomförts. Systemsäkerhetsanalyser har endast genomförts för system där IT support är systemägare. Arbetet bör i första hand genomföras för de system som erhållit högsta nivå (”Mkt hög”)

vid systemklassificeringen (22 system), samt även för de system som bedömts vara "sällsamt viktiga program".

6.1.4 Kontinuitetsplanering

Av "Informationssäkerhetspolicyn" framgår att kontinuitetsplaneringen är ett av ett antal områden som är av särskild vikt inom kommunen. Dessutom framgår av "Informationssäkerhetsinstruktion, Förvaltning" att systemägaren, i samverkan med IT-support, skall "fastställa en avbrottsplan för informationssystemet". Särskilda avbrottsplaner för de olika systemen inom kommunen saknas.

Vår notering:

Vi rekommenderar kommunen att vidta åtgärder för att IT kontinuitetsplanering, inklusive avbrottsplaner, skall utvecklas och regelbundet testas för de olika system som används inom kommunen. Detta arbete bör i första hand utvecklas för de system som bedömts ha störst betydelse för kommunens verksamhet.

6.1.5 Användarstyrning

De, under avsnitt 6.1.1 beskrivna styrande dokumenten för arbetet med informationssäkerheten inom kommunen, inkluderar även så kallade Användarbeskrivningar. Här framgår, på ett konkret och tydligt sätt, de regler som gäller vid användningen av kommunens IT resurser. Här framgår dessutom vad som inte är tillåtet, exempelvis vid användningen av internet och kommunens email.

6.2 Fysisk säkerhet

Fysiskt skydd och skyddsmiljö skall i första hand skydda installationer och information mot obehörig fysisk access vilket kan leda till skada eller stöld. Kontroll av skyddsmiljön säkerställer att serverna finns i en datoranpassad miljö och säkerställer fortsatt drift och minimerar effekterna av en katastrof, naturlig eller inte. Områden som berörs är framförallt IT-utrustning i datahallar. Kommunens krav avseende fysisk säkerhet framgår av "Informationssäkerhetsinstruktion, Kontinuitet och Drift".

Kommunen har två serverrum, ett i kommunhusets källare och ett i en av kommunens skolbyggnader. Serverrummet i skolbyggnaden har svagare skalskydd, eftersom väggarna är av gips. Båda utrymmena har särskilda skåp med brandlarm, automatisk släckning vid brand, UPS med tillräcklig kraft att avsluta systemverksamheten på ett ordentligt sätt vid strömavbrott, kylning, fuktalarm och rörelsedetektorer installerade. Dessutom finns ett dieselvek som automatiskt övertar driften av kommunhusets serverar vid ett längre strömavbrott. Åtkomsten till serverrummen skyddas genom personliga taggar med individuella koder. Åtkomst loggas.

Back up banden förvaras i låst utrymme på IT support.

Vår notering:

Eftersom individuella systemsäkerhetsanalyser inte genomförts inom kommunen, framgår inte vilka speciella krav avseende fysisk - och miljömässig säkerhet som de mest betydelsefulla systemen ställer krav på. Däremot är det vår rekommendation att de mest känsliga och betydelsefulla systemen, bör drifas i kommunhusets serverrum mot bakgrund av ett bättre skalskydd (gjutna väggar) och mer tillförlitlig kontinuitet (med avseende på reservkraft i form av ett dieselverk).

6.3 Logiska accesskontroller

Även avseende Logiska accesskontroller framgår baskraven enligt de av kommunen fastställda "Styrande dokumenten" (se avsnitt 6.1.1) för informationssäkerhet.

Här framgår exempelvis att systemanvändningen skall utgå ifrån att varje användares systemrättigheter skall vara anpassade utifrån arbets- och ansvarsfördelningen ("Vad man måste veta" respektive "Vad man måste göra").

Genom att tilldela respektive användare individuella användarnamn och personliga lösenord skapas en bra grund för en säker och ändamålsenlig systemanvändning. Integritet, sekretess och kontinuitet i driften är några aspekter som gynnas genom att förhindra obehörig åtkomst till system och information.

Logiskt åtkomstskydd innebär dessutom att samtliga användarkonton är personliga (med undantag för servicekonton) och att kontonas lösenord har krav på teckenlängd, bytesfrekvens, historik och komplexitet.

För att undvika obehörig access är det vidare viktigt att tillämpa rutiner varigenom inaktiva konton kan identifieras och spärras.

6.3.1 Användarkonton i nätverket

Behörighetsadministrationen kring användarkonton i nätverket (nya, ändrade och borttagna) sker utifrån uppdrag via e-post till IT-enhetens Helpdesk. Uppdragen från användarnas chefer är därmed alltid skriftliga. Helpdesk använder ett egenbyggt SQL Server ärendebaserat system.

Utifrån Sekchek har de aktuella inställningarna inhämtats från Windows AD för användarkonton i nätverket. Dessa framgår av tabellen nedan!

<u>Policy</u>	<u>Policy Value</u>	<u>Leading Practice</u>
<i>Minimum Password Length</i>	6	7 or greater
<i>Effective Minimum Password Length</i>	6	7 or greater
<i>Maximum Password Age in Days</i>	90	30 to 60
<i>Minimum Password Age in Days</i>	0	0
<i>Password History Size</i>	6	13 or greater
<i>Password Complexity</i>	Disabled	Enabled
<i>Reversible Password Encryption</i>	Disabled	Disabled
<i>Lockout Threshold</i>	5	3
<i>Lockout Duration</i>	30	0
<i>Reset Lockout Counter in Minutes</i>	30	1440
<i>Force Logoff When Logon Time Expires</i>	Disabled	Enabled
<i>Rename Administrator Account</i>	Not Defined	New Name
<i>Rename Guest Account</i>	Not Defined	New Name
<i>Allow Lockout of Local Administrator Account</i>	Disabled	Enabled
<i>Prevent Transfer of Passwords in Clear Text</i>	Disabled	Enabled
<i>Disable Password Changes for Machine Accounts</i>	Disabled	Disabled

”Policy Value” enligt tabellen är Svedala Kommuns aktuella inställningar medan ”Leading Practice” är den rekommendation som Sekchek lämnar. Enligt kommunens ”Styrande dokument” för informationssäkerhet framgår vad som beslutats gälla för en del av dessa områden. Här framgår att bytesfrekvensen har beslutats vara 90 dagar samt att nuvarande teckenlängd är 6 tecken men att detta kommer att ändras till 8 tecken i enlighet med rekommendationer från BITS+. Det framgår också att användarna inte behöver använda lösenord med viss komplexitet (bokstäver, siffror och specialtecken) enligt nuvarande inställning. Detta rekommenderas dock enligt ”Informationssäkerhetsinstruktion, Användare”.

Sammanställningen visar också att kommunen inte namnändrat ”Administrator Account” och ”Guest Account”, vilket rekommenderas eftersom detta är default konton som många känner till.

Ytterligare information om de olika inställningarna och dess betydelse samt risker som detta kan förknippas med, framgår av en separat överlämnad rapport från analysen med hjälp av Sekchek.

Enligt Sekchek analysen framgår att det finns 2 305 aktiva användarkonton (som inte disablats eller där kontots giltighetstid passerats) i kommunens nätverk (exklusive skolnätet). Enligt Bilaga 1 till denna rapport framgår exempelvis att

- 895 av kontona inte använts de senaste 90 dagarna. Det är viktigt att kommunen implementerar en rutin varigenom inaktiva konton löpande identifieras och disablas, för att undvika att oanvända konton kan användas för obehörig åtkomst
- 413 användarkonton behöver inte ändra lösenord genom inställningar på kontonivå. Detta innebär avsteg från kommunens generella säkerhetsinstruktion
- 1 517 användarkonton kan logga in med ett lösenord med 0 (noll) tecken genom inställningar på kontonivå. Detta innebär avsteg från kommunens generella säkerhetsinstruktion. Detta avser datorkonton och inte personliga konton

- 27 konton har administrativa rättigheter. Det är viktigt att antalet konton med starka rättigheter begränsas varför vi rekommenderar kommunen att analysera om samtliga dessa konton erfordras

Vår notering:

Vi rekommenderar Svedala kommun att överväga att förstärka vissa inställningar i säkerhetspolycyn i Windows AD, i enlighet med rekommendationerna från Sekchek analysen.

Kontakter med IT Support i samband med remisshanteringen av denna rapport visar att man redan beslutat genomföra följande förstärkande åtgärder:

- "Minimum Password Length" kommer att ändras till 8 tecken,
- "Maximum password Age in Days" kommer att ändras till 60,
- "Password History Size" kommer att ändras till 13,
- "Password Complexity" kommer att införas,
- "Force Logoff when Logon Times Expires" kommer att införas och
- "Prevent Transfer of Password in Clear Text" kommer att införas.

Vi rekommenderar dessutom kommunen att analysera de enligt Bilaga 1 noterade iakttagelser utifrån Sekchek analysen avseende inaktiva konton och konton som inte behöver ändra lösenord.

Även avseende dessa noteringar har IT Support beslutat införa förändringar för undvika inaktiva användarkonton och konton med undantag från byteskrav av password.

6.4 Backup och Restore

Den vanligaste kontinuitetsåtgärden för systemverksamhet är backup kopiering av kritisk information i systemen.

Dessutom är det viktigt att säkerställa att det kopierade materialet fungerar om verksamheten råkar ut för ett avbrott, som dessutom innebär att information förloras. Funktionen bör säkerställas genom att testa att återställa det kopierade materialet utifrån planerad (dokumenterad) frekvens och metod (restore).

Nuvarande rutiner innebär att man med hjälp av Tivoli Storage Manager, TSM, dagligen tar backup kopior till disk för att därefter kopiera materialet (enbart inkrementellt) till band. Borttagna filer finns kvar i ca 60 dagar. Planer finns på att ersätta band med diskpool med placering off-site. Speciella månads- och årsband sparas inte därutöver.

Restore sker inte enligt planerad metod utan enbart om någon användare anmäler att förlorat någon fil. Eftersom kopieringen innebär att förändringar uppdateras, innebär metoden att om någon användare oavsiktligt raderar information och inte upptäcker misstaget förrän efter en månad kan informationen eventuellt inte återställas. Verksamhetscheferna har inte analyserat om detta medför några risker för deras verksamhet.

”Informationssäkerhetsinstruktion, Kontinuitet och Drift” beskriver att respektive systemägare skall bestämma metod för backup och restore. Detta har man dock inte gjort.

Vår notering:

Eftersom nuvarande metod för backup och restore (ingen planmässig restore) inte utvecklats utifrån av verksamheterna analyserade och dokumenterade behov (lagenliga såväl som verksamhetsmässiga), är det vår rekommendation att rutinerna ses över.

För att ha möjlighet att tillämpa rutiner utifrån verksamheternas behov, förutsätts att respektive systemägare dokumenterar behovet individuellt för varje system. Detta i sin tur kommer att utgöra en systemindividuell kravspecifikation för IT support att anpassa rutinerna utifrån.

6.5 End-User Computing

End-User Computing syftar på användares egenutvecklade applikationer (exempelvis i Excel eller Access) och som har stor betydelse för verksamheten. Oftast är det komplexa kalkyler och sammanställningar som inte kan utföras med hjälp av det ordinarie systemstödet, och där flexibla hjälpmedel som Excel då kommer till användning.

Det är då viktigt att inkludera dessa applikationer vid implementeringen av säkerhetslösningar som exempelvis backup och krav på åtkomstskyddande lösenord.

Vår notering:

Intervjuer visar att man inte tillämpar någon rutin för att identifiera egenutvecklade applikationer, som bedöms vara kritiska för kommunens verksamhet. Vår rekommendation är att en rutin där sådana applikationer identifieras för att man skall ha möjlighet att inkludera dem i säkerhetsarbetet.

KPMG

Olof Eriksson
Certifierad kommunal revisor

Jan-Inge Hedin
IT/Advisory