Granskning av Informationssäkerhetspolicy

Av Andreas Wallén, Arash Dowlatyar, Eric Frånlund, Erik Gustafsson, Pontus Sundberg och Viktor Springe (grupp 12)

Inledning

I denna uppsats presenterar vi resultaten från tre verksamhetsanalyser. Analyserna utgår från ISO 27000-serien och undersöker hur väl verksamheterna lyckats implementera standarderna i den egna verksamhetens styrdokument. Således är det frågan om i huvudsak granskningar av

informationssäkerhetspolicies, där närliggande styrdokument utgör stöd och goda komplement. Dokumentstudierna fördjupas tack vare relevanta intervjuer med verksamheternas nyckelpersoner (beträffande informationssäkerhet).

De tre verksamheterna, vars informationssäkerhetspolicies granskas, är Uppsala kommun, Sollentuna kommun, samt Läkemedelsverket. Vad gäller kommunerna så kan likheter och skillnader vara intressanta att notera; i viss mån är det alltså en studie med komparativa inslag. Läkemedelsverket kompletterar på ett relevant sätt kommunerna då de troligen har större behov av utarbetade säkerhetsrutiner.

Uppsala kommun

Inledning

Då Uppsala kommun saknar en renodlad informationssäkerhetspolicy tar vår dokumentstudie avstamp i andra styrdokument. Två policydokument: *Säkerhetspolicy* och *IT-policy*. Säkerhetspolicyn är att betrakta som den mest fullgoda ersättaren i frånvaron av informationssäkerhetspolicy, något som även stöds av vårt intervjuobjekt. Värt att nämna är att en informationssäkerhetspolicy för några år sedan höll på att arbetas fram, men den gick i stöpet bl. a. på grund av att kommunen vid tidpunkten saknade en säkerhetschef. När detta skrivs så är även en (ny) informationssäkerhetspolicy på gång, men eftersom den inte finns färdigställd ännu så får vi följaktligen arbeta med nu tillgängligt material. Vi har också under intervjun fått tillgång till två anvisningar: *Anvisningar för säkerhetsarbetet i Uppsala kommun* och *Anvisning för informationsklassificering*. Dessa fungerar som konkretiserande stöddokument vars syfte är att underlätta den praktiska tillämpningen av policy för anställda inom verksamheten. Till dokumenten tillkommer en intervju med informationssäkerhetssamordnare Peter Lidholm. Intervjun syftar till att få djupare kännedom om dokumentens utformning och vilka tankegångar som ligger bakom dem.

Översikt över styrdokument

De fyra dokumenten som nämndes ovan redovisas enligt följande.

Säkerhetspolicy

Säkerhetspolicyn är antagen av kommunfullmäktige den 25 oktober 1999, medan anvisningarna för säkerhetsarbetet, efter beslut av kommunstyrelsen, reviderades 2012. Tillämpningen av policyn gäller för nämnder, bolag och stiftelser inom kommunen. Anvisningarna skall betraktas som ett led i att omsätta riktlinjerna i praktisk handling; ett slags manual med konkreta exempel i syfte att underlätta och stödja.

Själva säkerhetspolicyn är mycket kortfattad och i sedvanlig ordning uttryckt i generella ordalag. Policyn berör inte direkt informationssäkerhetsaspekter, men kan med fördel ses som en indirekt fingervisning eftersom begreppet säkerhet inrymmer informationssäkerhet.

Säkerhetspolicyn har tre kärnor, och lyder som följer.

”*HÖG SÄKERHET i kommunen skall medverka till att skapa trygghet och goda livsbetingelser för människor samt skydda och säkerställa kommunens egendom och miljö. ”*

Även om hela säkerhetspolicyn kan läsas som ett strategiskt dokument vilket påtalar *att* säkerhet läggs vikt vid, så är det denna den första kärna som tydligast proklamerar vad policyn syftar till: hög säkerhet. En viss betoning på skydd och säkerställande av kommunens egendom och miljö exkluderar i viss mån fokus på skyddande av information. Det är inte svårt att se att en särskild policy tillägnad informationssäkerhet skulle vara önskvärd. Vi har som nämndes ovan förstått att en sådan arbetades fram för några år sedan, men till syvende och sist inte fastställdes. Detta illustrerar även vikten av tydlig uppdelning av ansvarsområden (frånvaron av säkerhetschef vid tillfället är givetvis att betrakta som en olycklig omständighet). Om den första kärnan ovan beträffande hög säkerhet tydligast tar formen av en policy, så kan de två formuleringarna nedan närmast läsas som riktlinjer, vilka syftar till att förstärka den första kärnan, eller - annorlunda uttryckt: de syftar till att beskriva hur den höga säkerheten nås.

”*KOMMUNEN SKALL bedriva ett aktivt och förebyggande säkerhetsarbete som skapar en robust, flexibel och uthållig kommunal verksamhet med hög säkerhet. ”*

Detta är egentligen en upprepning av mantrat 'hög säkerhet', men vi kan se ett fokusskifte från *varför* säkerhetsfrågan är viktig, till *hur* säkerhet skall åstadkommas. Förvisso beskrivet så kortfattat och med så breda penseldrag att det kan verka intetsägande, men upprepningen är inte utan förtjänster. En gång är ingen gång, två gånger är en vana; hög säkerhet tillskrivs undantagslöst värde. Detta i samband med säkerhetspolicyns mycket korta och koncisa anslag bäddar för principer som går att tillämpa på många olika områden. Detaljerna för hur det ska fungera i exempelvis informationsklassning är lämnad åt mer detaljerade dokument som anvisningar, där det står exakt hur man ska gå tillväga när man klassar information inom Uppsala kommun. Återigen vill vi dock poängtera att riktlinjer (och en policy) dedikerad till specifikt informationssäkerhet hade varit att föredra.

”*SÄKERHETSFRÅGORNA SKALL ingå som naturlig och integrerad del i ledning och samordning av verksamheterna.”*

Slutligen betonas kort behovet av att integrera frågor som rör säkerhet i själva styrningen av verksamheten. Låt oss gå vidare och ägna anvisningarna för säkerhetsarbetet närmare studium.

Anvisningar för säkerhetsarbetet i Uppsala

Det påtalas att säkerhet (samt trygghet) ständigt kräver aktivt säkerhetsarbete. Detta implicerar att ett säkerhetstänk skall genomsyra verksamhet och inte ligga där vid sidan om som något som går att separera från den övriga verksamheten. Kopplingar kan göras till den sistnämnda

delen av säkerhetspolicyn, där det poängterades att säkerhetsfrågor skall integreras i styrningen av verksamheterna.

Vidare betraktas säkerhetsarbete ur fyra perspektiv: *allmän intern säkerhet, skydd mot olyckor, verksamhet vid extraordinära händelser*, samt *säkerhetsskydd*. Informationssäkerhet ryms under det första perspektivet – *allmän intern säkerhet.* Där kategoriseras informationssäkerhet in under begreppet allmän säkerhet. Graden av informationssäkerhet ska vara behovsanpassat, där kommun samt verksamhet och allmänheten ska beaktas. Detta oavsett om kommunen själv hanterar information (eller informationssystem) eller om det hanteras av extern part. (Med avseende på det sistnämnda finns många framtidsutmaningar (molntjänster etc.). Uppsala kommun definierar informationssäkerhet i termer av bevarande av konfidentialitet, riktighet och tillgänglighet. De använder här samma begrepp som ISO 27000. Detta innebär att informationsklassning är ett av de områden där Uppsala kommun följer ISO-standarden.

Vad beträffar ansvar och ledning är det informationssäkerhetssamordnaren – Peter Lidholm, som vi intervjuade – som har kommunstyrelsens uppdrag att koordinera informationssäkerhetsarbetet.

IT-policy
Bortsett från att säkerhetspolicyn bifogas i även IT-policyn så står det inget i IT-policyn om informationssäkerhet inom verksamheten. Det står dock att medborgarna ska kunna känna sig trygga med att kommunens säkerhetslösningar skyddar medborgarnas personliga integritet. Det står också en mening om att kommunens system ska vara tillförlitliga och ha hög tillgänglighet. Utöver det handlar policyn mest om kostnadseffektivitet och medborgarnyttan som kommer med e-tjänster.

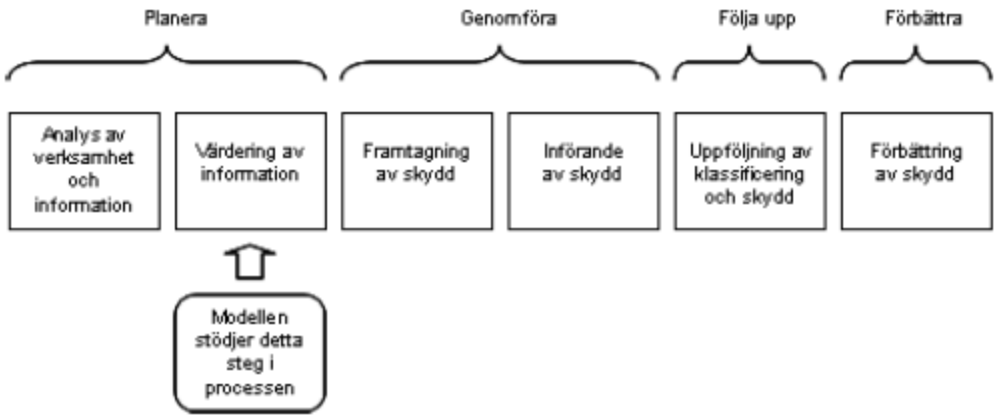
Anvisning – Informationsklassificering
Informationen är för verksamheten ett viktigt skyddsobjekt. Klassificering sker utifrån två principer. Den första är hur stor betydelse för verksamhet，alltså hur stor potentiell konsekvens som skulle kunna uppstå vid felhantering. Den andra är sannolikheten att detta inträffar. Dessa två faktorer vägs samman för att avgöra hur stor den totala risken är. Modellen är till för att bedöma lämplig säkerhetsnivå för en viss information, så att den, oavsett var i organisationen informationen hanteras, ska kunna ge ett konsistent skydd. Klassificering utgår i mångt och mycket från de kriterier som ställs upp i LIS i ISO 27000-serien.

Modellen utgår från tre säkerhetsaspekter när informationen klassificeras:
Konfidentialitet - Egenskapen att information inte tillgängliggörs eller avslöjas till obehöriga individer, enheter, eller processer .
Riktighet - Egenskapen att skydda exaktheten och fullständigheten i informationstillgångar .
Tillgänglighet - Egenskapen att vara åtkomlig och användbar vid begäran av behörig enhet .

Hanteringsregler:
Informationen är allmän eller icke allmän. Allmän information kan i sin tur delas upp i att vara offentlig eller sekretessbelagd. Information som klassas som nivå 3 eller högre ska hanteringsklassas och märkas.
Uppsala kommun har definierat nivåer som information kan klassificeras efter. Nivåerna representeras av siffrorna ett till fyra.
1 - Försumbar - Skadan är så liten att den går att bortse från
2 - Måttlig - Skadan är måttligt negativ men ej kan bortses från.
3 - Betydande - När det kommer upp till när skadan är betydande, exempelvis lagbrott.
4 - Allvarlig - Denna nivå handlar det om när det är en fara för liv och hälsa.
Nivåerna definieras och förklaras ännu mer på djupet i kommunens anvisningsdokument. Även konsekvenser som uppstår externt tas med i bedömningen.

Klassificering och hantering är förmodligen det som Uppsala kommun uttryckligen, i sina styrdokument, ligger närmast formulerat innehållet i ISO 27000-standarderna. Här kan man tänka sig att kommunen i egenskap av att vara en myndighet med tjänstemän har bred erfarenhet av dokumenthantering (offentliga dokument kontra sekretessbelagda är som bekant inget nytt för offentlig förvaltning att förhålla sig till).

Del i ledningssystem
Uppsala kommuns anvisningar för informationsklassning har en kort hänvisning till PDCA modellen från ISO 27000. Det finns dock inte så mycket information i Uppsala kommuns material förutom en hänvisning till modellen.



PDCA modellen från ISO 27000 som hänvisas till i Uppsala kommuns informationsklassningsanvisningar.

Intervjumaterial

Hej! Hur ser en dag på jobbet ut för dig i egenskap av att vara informationssäkerhetsamordnare?

Arbetet sker både på en strategisk nivå (som riskanalyser och klassificering av information), och operativa frågor, som exempelvis att något system inte fungerar som det ska och måste felsökas.

Har det gjorts någon riskanalys som kommit fram till vilka risker Uppsala kommun har? Görs kontinuerliga risk- och säkerhetsanalyser?
Ja, det görs. Varje gång något nytt införs, och förutom det ytterligare ca en gång per år. Detta är idealet, sedan genomförs det inte alltid fullt ut i praktiken.

Vi har från er hemsida tagit del av IT-policy samt säkerhetspolicy. Vad finns det mer för styrande dokument?
Det finns fyra nivåer av styrande dokument, som går mellan väldigt översiktligt till detaljnivå:
1 Policies. Dessa är principer och de fattas politiker.
2 Riktlinjer. Dessa fattas på kommunstyrelsenivå, och säger vad som ska göras.
3 Anvisningar. Dessa skrivs på förvaltningsnivå, och säger på vilket sätt saker ska göras.
4 Instruktioner. Dessa skrivs på förvaltningsnivå, dessa är mer detaljerade om vem ska ska göra vad.

Ni har en IT-policy och ni har en säkerhetspolicy, men ni har ingen informationssäkerhetspolicy?
Vår IT-policy och informationssäkerhetspolicy täcker in även vår informationssäkerhet. Vi hade tidigare diskussioner om att skapa en ren informationssäkerhetspolicy men vi kom fram till att vi inte skulle uppföra en i dagsläget, detta kan nog förklaras av att vi vid tidpunkten inte hade någon säkerhetschef. En informationssäkerhetspolicy är i skrivandes stund under utveckling.

Hur informeras era anställda om er säkerhet och säkerhetspolicys?
Säkerhetspolicyn ska visas upp för de anställda när de blir anställda. Det finns också tillgängligt att hämta på kommunens intranät. Vid nyanställning använder vi en introduktionsvideo i informationssäkherhet baserat på material från MSB. I praktiken används säkerhetspolicyn mest när någonting har hänt, då folk till vardags är upptagna med sina vanliga arbetsuppgifter.

Hur förhåller ni er till ISO-27000 serien?
Uppsala kommun kollar på ISO 27000 men följer den inte strikt. Vi använder MSB:s rekommendationer som vårt främsta stöd när det gäller informationssäkerhet, och MSB bygger i sin tur rekommendationerna på ISO 27000.

Klassificerar ni er information efter säkerhetsnivå på något sätt?
Uppsala kommun använder en informatoinsklassifisering som bygger på nivåerna ett till fyra. Där ett är ingen konsekvens och fyra är högsta konsekvensen. Detta är den informationsklassningsmodell som rekommenderas av myndigheten för samhällsskydd och beredskap. Även systemen informationsklassas. Detta är dock mest av praktiska skäl, eftersom information i ett visst system då kan få en automatisk klassning, utan att behöva klassa varje dokument på detaljnivå.

Har ni anvisningar för medarbetare vad gäller sociala medier etc?
Ja, det finns det. Vad man får ge ut, och allmänt uppträdande. Man får säga mer på kommunen än på ett privat företag, utan att bli av med jobbet. Det är dock problematiskt att använda sociala medier i kommunsammanhang, för det material man producerar på facebook exempelvs i en chatt under kontorstid blir automatiskt offentlig handling som måste sparas och kunna lämnas ut. Här är det tydligt att det finns framtidsutmaningar och att styrdokumenten inte riktigt hängt med i den digitala utvecklingen.

Om olyckan väl är framme, har ni någon krishanteringsplan?
Inte specifikt faktiskt, det mesta löser vi efter att olyckan är framme och vi har analyserat situationen. Man kan väl säga att det finns plats för förbättringsarbete här.

Har ni haft någon incident vad ni känner till?
Inga riktigt stora, men vi har haft några mindre i form av DDoS attacker (överbelastningsattacker) som vi lyckats hantera och stoppa.

Vad är på gång just nu i Uppsala kommun när det gäller informationssäkerhet?
Vi har sagt att “digitalt ska vara norm”. Det innebär att allt så långt det går ska hanteras på datorer, webb, surfplattor m.m istället för papper. Att få fungerande rutiner för säkerheten på bland annat surfplattor är en av utmaningarna vi arbetar med just nu.

Jämförelse med checklista

Ger policyn ledningens viljeinriktning och stöd för informationssäkerhetsarbetet?
Ja, detta står ganska väl uttryckt i säkerhetspolicyn. Exempelvis “KOMMUNEN SKALL bedriva ett aktivt och förebyggande säkerhetsarbete som skapar en robust, flexibel och uthållig kommunal verksamhet med hög säkerhet.”

Har ledningen fastställt policyn?
Ja, kommunfullmäktige har fastställt policyn och denna kan man se som kommunens ledning.

Är det beskrivet hur policyn ska underhållas och på vilket sätt?
Nej, däremot står det att handlingsplaner ska upprättas kontinuerligt, i *Säkerhetspolicyn.*

Är policyn spridd i verksamheten och finns det ett system för detta?
Delvis. Det finns i kommunens intranät som alla inom verksamheten kan nå. När någon är nyanställd så får de ta del av policyn, vidare ansvarar envar för att hålla sig uppdaterad. Däremot används det inte lika mycket i praktiken som man skulle kunna önska.

Finns det en definition av informationssäkerhetsbegreppet?
Ja, det finns och definitionen från säkerhetspolicyn lyder: “Med informationssäkerhet menas bevarande av konfidentialitet, riktighet och tillgänglighet hos information. “

Tar policyn hänsyn till hoten från anställda och utomstående?
Nej. Detta saknas i policyn. Det kommer sig troligen av att det (i synnerhet interna hot) är en känslig fråga eftersom personalen kan ta illa upp.

Visar policyn mål och omfattning samt vikten av informationssäkerhet?
Delvis. Det står att omfattningen ska vara i princip behovsanpassad. I säkerhetspolicyn står det "Kommunen ska upprätthålla en väl avvägd informationssäkerhet med hänsyn till behoven hos kommunen, verksamheterna i kommunen och allmänheten.".

Är ansvaret definierat?
Ja, det får man påstå. Ansvarsfrågan är väldokumenterad och olika roller har olika ansvarsområden, ex. har kommunstyrelsen det övergripande ansvaret för arbetet med säkerhet i kommunen. Och informationssäkerhetssamordnare har det övergripande ansvaret att koordinera informationssäkerheten i kommunens olika verksamheter

Finns det reglerat hur rapportering av incidenter ska gå till?
Nej, det finns det inte. Kommunen hanterar istället incidenter när de väl dyker upp, vilket får ses som en stor brist.

Hänvisar policyn till andra styrande dokument inom organisationen?
Nej, inte policyn i sig. Däremot finns det en praxis inom kommunen att åtgärder konkretiseras via anvisningar.

Är det klart och tydligt beskrivet vem som är ägare till policyn?
Ja. Det står att kommunfullmäktige står bakom dokumentet, och att det gäller för kommunen vilket får tolkas som att kommunen äger policyn. Dock är det inte så tydligt definierat som man skulle kunna önska.

Sammafattning

Överlag följer Uppsala kommun något som kan liknas vid ISO 27000, i synnerhet beträffande informationsklassificering. Dock följs standarden inte på alla punkter. De största avvikelserna från 27000 är incidenthantering, underhåll samt interna hot. Eftersom framförallt underhåll och incidenthantering är väldigt väsentliga delar av 27000 kan inte Uppsala Kommun sägas följa standarden fullt ut. Man kan dock se att mycket av deras säkerhetsarbete är inspirerat av ISO 27000 standarden.

Sollentuna kommun

Inledning

Sollentuna kommun arbetar främst mot två dokument gällande informationssäkerhet, utöver detta finns även kommunens IT-policy som berör delar av informationssäkerhet. De två huvudsakliga dokumenten vi har gått igenom är *Informationssäkerhetspolicy* och *Regler för informationssäkerhet.* Vi har även intervjuat Christer Sävensjö, *tillfällig informationssäkerhetssamordnare.* Då vi kommer att jämföra Sollentuna kommun med Uppsala kommun är intervjufrågorna någorlunda lika utformade, för att underlätta en jämförelse.

Översikt över styrdokument

De tre dokumenten som nämndes ovan redovisas enligt följande.

Policy för informationssäkerhet

Utgör en grundprincip inom informationssäkerhet för Sollentuna kommun, policyn gäller för nämnder och förvaltningar dvs i princip hela kommunen. I policyn definierar man information som vilken typ av information som helst, både elektroniskt lagrad information och manuellt hanterad information. Policyn utgör grunden för arbetet för en säkrare informationshantering, detta med hjälp av diverse regler, anvisningar och metoder.

I dokumentet berör man syftet med policyn – att säkerställa konfidentialitet, tillgänglighet, riktighet samt sårbarhet. Samtliga nämnder är ansvariga för att upprätthålla sin egen informationssäkerhet, dock är det kommunstyrelsen som leder, samordnar och granskar hela kommunens arbete med informationssäkerhet.

De krav som ställs på nämnderna är:

” - Genom verksamhetsrutiner, granskningar, riskhantering och kontinuitetsplanering minimera och förebygga störningar i verksamheten

- Tillförsäkra att all informationsbehandling följer organisationens regelverk för informationssäkerhet och standarder och att erforderliga skyddåtgärder implementeras

- Minimera risken för avsiktlig eller oavsiktlig överträdelse av lagregler, avtalsförpliktelser m.m.

- Se till att informationssäkerhetsaspekter beaktas vid utveckling, anskaffning, förvaltning och avveckling av informationsbärare “.

Enligt policyn skall kommunens informationssäkerhetsarbete bedrivas enligt tillämplig svensk standard för förvaltning och revision, det är dock ej specificerat vilken standard de syftar på.

IT-policy
Sollentuna kommuns IT-policy berör knappt området informationssäkerhet. Policyn beskriver kortfattat att det finns en infromationssäkerhetspolicy och ett dokument för regler inom informationssäkerhet samt att kommunens information är en nyckelresurs för samtliga verksamheter inom kommunen. Då det är inom IT-policyn så syftar de på elektronisk information. Enligt policyn skall ansvar för att rätt information upprätthålls skall vara fastställt och organiserat i organisationen enligt sex kriterier.

”Grundsynen är att information är tillgänglig för alla berörda och anpassad till målgruppernas behov. Behörighet ska där så är tillämpligt tilldelas formellt enligt dokumenterade rutiner Informationsägare ska utses. Lagring och arkivering ska följa gällande lagar och standarder Upphovsrättliga aspekter och etiska regler ska beaktas. Verksamhetskritisk information ska finnas i digital form och lätt åtkomlig för behöriga användare”.

Sollentuna kommuns IT-policy revideras varje mandatperiod, kommunfullmäkte beslutar om kommunens gemensamm e-vision och it-policy.

Regler för informationssäkerhet I Sollentuna kommun
Antagna av kommunstyrelsen 2014-02-19 § 26, dnr 2014/0041

All information som hanteras inom kommunen skall ha rätt skyddsnivå, med utgångspunkt i informationens värde. Hela styrdokumenten är baserat på ISO/IEC 2007:2006 samt LIS, dessa anges I detalj I tillämpningsanvisningarna.

Kommunen har en säkerhetschef som har huvudansvaret över informationssäkerheten, samt samordnar arbetet mot en säkrare informationssäkerhetsmiljö. Dock är det upp till respektive nämnd att upprätthålla sin egen informationssäkerhet. Säkerhetschefen följer dessutom upp samtliga nämnders arbete för att uppnå en hög informationssäkerhet, samt förvaltar och följer upp policys.

Innan nya it-system tas i bruk skall en risk- och sårbarhetsanalys göras, för att få en överblick över hur pass säker informationen är i det nya systemet. En riskanalys görs även när it-system uppdateras och avvecklas, samt när särskilda behov uppstår. All information i kommunen klassas i olika säkerhetsklasser, beroende på hur viktig informationen är. Installation av program eller liknande får icke göras via mail, internet eller via någon annan flyttbar media, utan informationssäkerhetsansvarigs godkännande.

Hantering av incidenter

En rutin för händelseförloppet när en incident har inträffat skall finnas inom nämnden, ansvarig ser till att samtliga anställda känner till rutinen. Även brister och potentiella säkerhetsrisker skall rapporteras in. En funktion inom kommunen skall finnas som hanterar it-säkerhetsincidenter.

Sollentuna kommuns regler för informationssäkerhet följer märkbart en röd tråd genom hela dokumentet. Innehållande en definitionslista för både termer och olika befattningar anser vi att man värnar om att samtliga anställda skall förstå innebörden i reglerna.

Intervjumaterial

Har det gjorts någon riskanalys som kommit fram till vilka risker Sollentuna kommun har?

När det gäller informationssäkerhet så gör varje förvaltning en riskanalys och den får inte jag ta del av. Där går man in och tittar specifikt på ett system som finns på förvaltningen. Vad händer till exempel om inte detta system fungerar av en eller annan orsak.

Vad finns det för risker för Sollentuna kommun med avseende på informationssäkerhet?

Varje förvaltning gör en riskanalys och vi är snart färdiga med det arbetet. Tyvärr som jag sade tidigare får jag inte ta del av de resultaten utan det är endast för respektive förvaltning. Men naturligtvis finns det många risker. En del som alltid innebär risker är stora elavbrott som i sin tur påverkar datorer och servrar.

Klassificerar ni er information efter säkerhetsnivå på något sätt?

Ja, vi klassificerar information hos samtliga förvaltningar.

Ges nyanställda en säkerhetsutbildning som en del av introduktionsutbildningen? Hur högt är deltagandet på de säkerhetsrelaterade utbildningarna som ges?

Sollentuna kommun har också tagit fram en interaktiv säkerhetsutbildning som omfattar områdena brand, utrymning, säkerhet och olycksfall. Utbildningen syftar till all alla som arbetar i kommunen ska ha en gemensam plattform när det gäller säkerhetskunskap och ska öka vårt säkerhetsmedvetande. Utbildningen avslutas med ett prov. Denna utbildning är obligatorisk för samtliga som jobbar inom Sollentuna kommun.

Görs uppföljningar på genomförda åtgärder?

Uppföljning görs på genomförda åtgärder och när det gäller utbildningen vet vi vilka som genomfört den eller inte. Vi håller på att förnya utbildningen så att den ständigt ska vara aktuell.

Görs kontinuerliga risk- och säkerhetsanalyser?

Det görs kontinuerliga risk- och sårbarhetsanalyser varje år som Länsstyrelsen kräver in.

Har ni anvisningar för medarbetare vad gäller sociala medier etc?

Det finns anvisningar för medarbetare vad gäller sociala medier och framför allt mobiltelefoner. Vad får jag göra och vad får jag framför allt inte göra.

Har ni haft någon större incident inom informationssäkerhet som vi får tag del av?

Vi har haft en större incident inom informationssäkerheten men som ni tyvärr inte kan ta del av på grund av olika orsaker.

Jämförelse med checklista

Ger policyn ledningens viljeinriktning (motivation) och stöd för informationssäkerhetsarbetet?
Ja. Det står klart och tydligt att:
“Syftet med kommunens informationssäkerhetsarbete är att säkerställa informationens
- konfidentialitet/sekretess
- tillgänglighet
- riktighet
- spårbarhet”

Har ledningen fastställt policyn?
Ja. Kommunstyrelsen har tagit fram alla policys, kommunfullmäktige har i sin tur antagit samtliga policys.

Är det beskrivet hur policyn ska underhållas och på vilket sätt?
Ja. Säkerhetschefen ansvarar för att samtliga policys inom informationssäkerhet revideras i början på varje mandatperiod.

Är policyn spridd i verksamheten och finns det ett system för detta?
Ja, varje anställd går en kurs inom informationssäkerhet, samt att varje ny anställd är tvungen att gå kurs inom informationssäkerhet.

Finns det en definition av informationssäkerhetsbegreppet?
Ja, men inte i policyn. I dokumentet *Regler för informationssäkerhet* definierar man olika uttryck samt vad informationssäkerhet är.

Tar policyn hänsyn till hoten från anställda och utomstående?
Delvis. Bara det som är kopplat till arbetet får de anställda söka efter. Samt att arbetsgivaren får göra kontroller när som helst.

Visar policyn mål och omfattning samt vikten av informationssäkerhet?
Delvis, IT-policyn beskriver vikten av informationssäkerhet, samt vad informationssäkerhet innebär.

Är ansvaret definierat?
Ja, det finns skrivet att “Respektive nämnd ska upprätthålla informationssäkerheten inom sin verksamhet”. Samt ansvarsområden och olika roller.

Finns det reglerat hur rapportering av incidenter ska gå till?
Ja, det finns det. Rapportering omedelbart och det ska ske enligt den rutinen som finns. Den policyn skall alla anställda inom kommunen känna till.

Hänvisar policyn till andra styrande dokument inom organisationen?
Ja, IT-policyn hänvisar till dokumentet “regler för informationssäkerhet”

Är det klart och tydligt beskrivet vem som är ägare till policyn?
Nej.

Sammanfattning
Sollentuna kommun följer inte standarden för 27001 och 27002 som vi förväntat oss De kan förbättra sin informationssäkerhet på flera aspekter, eftersom att de har haft en större incident inom verksamheten. Sollentuna kommun hanterar utbildning och informering av personal på ett bra sätt då en informationssäkerhetsutbildning är en obligatorisk del av introduktionsutbildningen. I policyn refererar man sällan till externa dokument, vilket man med fördel bör göra. Kommunens incidenthantering är till synes väl planerad, då även detta ingår i introduktionsutbildningen vet samtliga anställda vad som gäller vid en incident. Kommunen kan bli bättre på att sätta upp tydliga mål inom informationssäkerhet för att kunna mäta framgångar och utveckling.

Läkemedelsverket

Inledning
Läkemedelsverket har som myndighet en väldigt utarbetad och välstrukturerad informationssäkerhetspolicy samt många andra styrande dokument. Läkemedelsverket följer standarderna 27001/27002 till en så stor utsträckning som möjligt. Fler standarder följs också, exempelvis 27005. Vi fick tillgång till Läkemedelsverkets säkerhetspolicy samt andra styrande dokument:

- Läkemedelsverkets Säkerhetsskydd(Policy)
- Arbetsordning för Läkemedelsverket

- Informationssäkerhet för Chefer(Instruktion)
- Informationssäkerhet - utveckling och förvaltning(Instruktion)
- Informationssäkerhet för IT-drift och IT-support(Instruktion)
- Informationssäkerhet för medarbetare(Instruktion)

Efter det att vi tagit del av och behandlat dokumenten utfördes även en intervju med säkerhetsansvarig Robert Reineck. Vi fick då svar på frågor som uppstått när vi arbetat med dokumenten, samt andra funderingar. Han är även den som har ett uttalat ledningsansvar över utveckling, granskning och utvärdering av säkerhetspolicyn.

Översikt över styrdokument

Läkemedelsverkets Säkerhetsskydd (Policy)
Policyn började gälla 2012-07-06, den är skriven av Robert Reineck. Policyn är väldigt generell, den är också väldigt kortfattad och lyder:
“Den höga tilltron till Läkemedelsverket och vår roll i samhället ska inte skadas. Läkemedelsverket ska upplevas som en trygg och säker arbetsplats.” Hela dokumentet är märkt policy men det är just den meningen som är rubricerad “POLICY FÖR LÄKEMEDELSVERKETS SÄKERHETSSKYDD”. Policyn efterföljs sedan av “PRINCIPER FÖR SÄKERHETSARBETET PÅ LÄKEMEDELSVERKET” Där flera generella riktlinjer för säkerhetsarbetet tas upp.

I och med att den inte går in på speciella fall eller scenarion så känns det som att den är designad för att täcka upp så mycket som möjligt och lämnar de mer ingående fallen och de specifika reglerna för verksamheten till de andra styrande dokumenten . Policyn refererar dock inte till de andra styrande dokumenten utan man har låtit dem referera till policyn istället. Policyn går inte in direkt på informationssäkerhet men pratar om säkerhet där informationssäkerheten ingår, vissa av de andra styrande dokumenten är dock inriktade på informationssäkerheten.

Informationssäkerhet för medarbetare är en instruktion som är bindande för medarbetare och konsulter vid läkemedelsverket just inom säkerhetsområdet. Dokumentet beskriver den enskildes ansvar utifrån ett informationssäkerhetsperspektiv, alltså hur man ska handskas och behandla viss information och vilka påföljder det kan få om man inte följer dessa instruktioner. Dokumentet är välskrivet och strukturerat, det beskriver väldigt väl hur man ska gå tillväga med specifik hård och mjukvara, samt hur man ska hantera information.

Informationssäkerhet för IT-drift och och IT-support är en instruktion som beskriver vilka krav som gäller för att upprätthålla just informationssäkerheten inom detta område. Instruktionen fungerar som ett tillägg till instruktionen för medarbetare.

Slutligen har vi instruktionerna Informationssäkerhet för chefer och Informationssäkerhet – Utveckling och förvaltning. Dessa fungerar också som komplement till instruktionen för medarbetare och innehåller krav och riktlinjer inom de specifika områdena. Instruktionen för

chefer beskriver vilket ansvar en sådan medarbetare har med avseende på informationssäkerhet.

Dessa instruktioner är alla väldigt viktiga för verksamheten då de i detalj går igenom instruktioner, riktlinjer, krav och ansvar för informationssäkerheten på Läkemedelsverket.

Intervjumaterial

I vilken mån och omfattning tillämpar ni standarderna 27001/27002?
Läkemedelsverket mål är att följa standarderna så långt som möjligt. I några fall så har det uttryckts att de ska vara så gott som certifierade men det har aldrig tagits ett officiellt beslut i frågan. Det har inte bestämts hur långt standarderna ska följas men som sagt är målsättningen att följa dem så långt som möjligt.

Har du(Robert Reineck) ett uttalat ledningsansvar för utveckling, granskning och utvärdering av er säkerhetspolicy?
Ja.

Er säkerhetspolicy är väldigt "starkt" formulerad, alltså att ni ska "ha skydd mot alla identifierade risker och hot som kan orsaka skada", anser du(Robert Reineck) att ni uppfyller det?
Ja, men det man inte vet någonting om kan man inte skydda sig mot. Alla upptäckta hot och sårbarheter har tagits ställning till. Alltså har det antingen vidtagits åtgärder mot riskerna, eller så har risken bedömts som accepterbar jämfört med skadan som risken skulle orsaka.

----------Informationssäkerhet för medarbetare----------

I policyn står det att alla medarbetare ska ha förståelse och känna delaktighet i Läkemedelsverkets säkerhetsarbete, vad gör ni för att uppfylla det?
Alla nya anställda går ett introduktionsprogram, vilket finns för att bland annat ge kunskap om "LIS". Annars finns det inget systematiskt utbildningsprogram för anställda, det finns tankar om att införa ett. Men de tankarna har inte kommit så långt, det är verksamhetsområdet HR bedriver den frågan. Själva säkerhetsbiten kommer ligga som ett paket i det planerade utbildningsprogrammet. Utbildningen just nu baseras mer på efterfrågan och Roberts förslag än något annat.

I paragraf 1.7 står det att det måste göras en säkerhetsprövning innan man lämnar ut information, både internt och externt. Gör medarbetarna denna prövning eller vem/vilka är det som har hand om det?
Den som hanterar utlämningen gör en prövning med eventuellt stöd från till exempel rättsenheten. Det finns instruktioner för hur det ska skötas.

Under "anmäla avvikelser" (informationssäkerhet för medarbetare) säger ni att det är varje medarbetares ansvar att anmäla misstänkta eller upptäckta avvikelser. Sker det tillräckligt många sådana anmälningar?
Ja, inom vissa områden, men det finns även ett stort mörkertal inom andra områden. Just inom IT-säkerheten så är det väldigt bra, men även där så går det upp och ner. Det beror också på område och gruppering, till exempel ett laboratorium som är autentiserade har väldigt

välutvecklade processer för att hantera sådant.

- Om en medarbetare blir misstänkt för otillåtet användande av internet/dator/epost/mobiltelefon ska det enligt “Uppföljning, kontroll och påföljder (Informationssäkerhet för medarbetare) ske en intern utredning. Om en sådan situation skulle uppstå, vad händer med medarbetaren under tiden utredningen sker?
Det beror på karaktären av det specifika fallet. Det finns olika vägar, är det till exempel något dataintrång eller brottsligt så ska det polisanmälas. Annars är det personalsanvarsnämden som ansvarar för uppföljning, kontroll och påföljd. Har det uppstått någonting brukar dock jag (Robert Reineck) först säkerställa händelsen så att vi har fakta, till exempel loggar, och naturligtvis prata med personen i fråga.

I paragraf 1.13.1 står det att “läkemedelsverket vill uppmuntra sina anställda att utnyttja internets möjligheter” Vad innebär det?
Då skrivningarna från början är 10-15 år gamla så kan det finns det lite sådant som har följt med och kanske inte riktigt passar in i tiden. Det kommer ifrån då tankeställningen till Internet var lite negativ.

Enligt 01004 (Informationssäkerhet för medarbetare) står det att en person med högre behörighet än vad som krävs ska meddela det till sin chef. Varför gör ni så?
Det är chefen som har ansvar för att medarbetaren har rätt behörighet. Det är mer som en “backup” för att behörigheten ska stämma med den aktuella arbetsuppgiften.

Har ni någon policy för sociala medier?
När det kommer till social media finns det tyvärr ett gap idag. Det borde finnas en policy för det och ansvaret för det ligger det på kommunikationsenheten. Till exempel så tillåter Läkemedelsverket inte Facebook för medarbetarna. Det är blockerat för att vi just nu inte har någon policy för att hantera det på rätt sätt, problemet är alltså att skilja på den privata personen och den offentliga personen.

----------Informationssäkerhet för chefer----------

Enligt vår uppfattning av “01137 Informationssäkerhet för chefer” Så har chefen stort ansvar över att sköta medarbetares behörighet och rättigheter. Enligt dokumentet ska behörigheten för medarbetare kontrolleras varje år och för särskild behörighet var tredje månad. Tycker du att detta uppfylls? Har det uppstått några problem med denna arbetsinstans?
Nej, inte alls. Det finns många faktorer som spelar in i det, det är en dels en utbildnings och medvetande fråga för cheferna. Det hänger också ihop med flera frågor som har med chefernas arbetsmiljö och ansvar att göra. Det finns en otydlighet av vad det innebär att vara chef. Idag är det väldigt jobbigt att efterleva detta och det är inte alltid så effektivt. Vissa problem kan uppstå när det av en händelse råkar ligga kvar behörigheter på medarbetare som har slutat etc.

Vet medarbetarna om att dem inte har rätt till sin egen e-post? Eftersom detta inte nämns i 01004?
Nej, det vet de inte. Det är nog tyvärr så att det inte är helt medvetet att det är organisationen som äger e-posten. Det är dock tydligt är att den inte ska användas i privat bruk och oftast uppstår det inga problem kring det.

Skriver IT-support och drift under instruktionen för informationssäkerhet för medarbetare?
Alla som arbetar på läkemedelsverket skriver under det, de flesta konsulter som arbetar här skriver också under.

----------Informationssäkerhet för IT-drift och support----------

Har drift och IT-support någon utbildning eller liknande i standarderna 27001/27002/27005, då dessa ska följas i samband med riskbedömning och riskhantering?
Nej, de har ingen särskild utbildning. Men de ska ha koll på vissa saker med anknytning till standarderna.

Vi reagerade lite på paragraf 1.5 i dokumentet. Punkten säger att det ska finnas en brandvägg med så “restriktiva regler” som möjligt. Vad innebär det för er?
Det finns ett behov att blockera en viss information från utsidan. Det säger egentligen bara att man ska ha ett restriktivt sätt mot utsidan.

Enligt dokumentet är trådlösa tangentbord tillåtna om dem är krypterade med en algoritm godkända av läkemedelsverket, men i medarbetarinstruktionen är det specificerat att trådlösa tangentbord endast får användas i konferensrummet. Gäller båda eller står IT-drift och support instruktionen över det?
Det är bara en motsägelse som ska hanteras.

Känner du att det finns några brister du skulle vilja åtgärda i er säkerhetspolicy och andra styrande dokument?
Ja, det finns en del saker som behövs arbetas med. Det som fungerar bra nu är policyn, den tydlig och rent skriven. Instruktionen för medarbetare fungerar också bra, den har en lagom nivå och en bra acceptans. Instruktionen för chefer behövs göras om vid implementation och skrivning. Vad gäller drift och support behövs den också omarbetas, den är ojämn i nivån och är inte så tydlig. Vissa regler kan tas ut och göras om på ett tydligare sätt. Det viktiga är dock att hitta processerna som effektiviserar dessa regler, alltså att dem vävs in i det sammanhang där dem behövs.

Hur fungerar ditt arbete gentemot ledningen?
Ibland så sitter jag lite långt ifrån ledningen men då jag har deras förtroende att driva dem här frågorna så uppstår det inga problem.

Har det skett någon incident?
Ja, många men det beror lite på vad man menar med incident.

Hanterades den enligt ert skydd eller var det en oidentifierad risk?
Det har skett incidenter där risken varit både oförutsedd och behandlad, dem behandlade riskerna har hanterats utifrån vårt skydd. Det kan bero på brister i det befintliga skyddet eller att risken är oidentifierade. Det kan också vara så att skyddet inte är infört på en identifierad risk.

Ändrades något p.g.a den incidenten? (skydd e.t.c)
Ja, tyvärr är det oftast det som gör att det blir aktuellt att ändra eller utöka någonting. Utmaningen är att täppa till det innan incidenten inträffar.

Görs uppföljningar på genomförda åtgärder? Hur ofta/varför inte?
Ja, det görs. Men mer stickprov än någon systematisk uppföljning. Det finns inget system i stickproven utan det är mera vid behov.

Gör ledningen en genomgång av informationssäkerhetspolicyn varje år?
Inte policyn, varje styrande dokument ses över var tredje år. Säkerhetsarbetet följs däremot upp på en årscykel. Min uppgift i det sammanhanget är att förklara oklarheter eller funderingar kring reglerna för ledningen. Så att de med min vägledning kan fatta ett beslut.

Jämförelse med checklista

Ger policyn ledningens viljeinriktning och stöd för informationssäkerhetsarbetet?
Nej, det är inte enligt vår uppfattning klart att det är ledningens viljeinriktning och stöd som beskrivs i policyn.

Har ledningen fastställt policyn?
Ja, den ställföreträdande generaldirektören har fastställt policyn.

Är det beskrivet hur policyn ska underhållas och på vilket sätt?
Nej, det finns inte med i policyn.

Är policyn spridd i verksamheten och finns det ett system för detta?
Ja, policyn och andra styrande dokument gås igenom vid varje ny anställning i form av ett introduktionsprogram.

Finns det en definition av informationssäkerhetsbegreppet?
Ja, men det finns men inte i policyn utan i instruktionen; informationssäkerhet för medarbetare.

Tar policyn hänsyn till hoten från anställda och utomstående?
Ja, enligt policyn ska verksamheten, tillgångar och värden i alla dess former skyddas mot alla identifierade risker och hot – avsiktliga eller oavsiktliga, interna eller externa – som kan orsaka skada.

Visar policyn mål och omfattning samt vikten av informationssäkerhet?
Ja.
Målet är att “Den höga tilltron till Läkemedelsverket och vår roll i samhället ska inte skadas. Läkemedelsverket ska upplevas som en trygg och säker arbetsplats”.
Omfattningen är “Läkemedelsverkets verksamhet, tillgångar och värden i form av medarbetare,

information, anseende och egendom ska skyddas mot alla identifierade risker och hot – avsiktliga eller oavsiktliga, interna eller externa – som kan orsaka skada”
Vikten beskrivs också kortfattat, “Läkemedelsverket ska ordna sin verksamhet kring området för behandling av personuppgifter på ett sådant sätt att integritetskänslig information inte av misstag lämnas ut”.
Men även i de styrande dokumenten så beskrivs dessa mer.

Är ansvaret definierat?
Ja, dock inte i policyn men det finns dokumenterat i de övriga styrande dokumenten.

Finns det reglerat hur rapportering av incidenter ska gå till?
Ja, men bara inom vissa områden. Men inom informationssäkerheten så finns det färdiga mallar för rapportering.

Hänvisar policyn till andra styrande dokument inom organisationen?
Nej, däremot så hänvisar de styrande dokumenten till policyn.

Är det klart och tydligt beskrivet vem som är ägare till policyn?
Ja, under titeln fastställare.

Sammanfattning

Läkemedelsverket med sin policy och sina andra styrande dokument följer innehållsmässigt standarderna 27001/27002 väldigt bra. Dem har en välutarbetad och väl införd policy, tillsammans med dem andra styrande dokumenten. Med sina instruktioner beträffande informationssäkerhet har de i detalj beskrivit hur informationssäkerhetsarbetet ska utföras och hur information ska behandlas.

Även om det i stor utsträckning finns fungerade dokument som styr och kontrollerar arbetet med informationssäkerhet så råder det även inom denna verksamhet brister. Till exempel att det inte finns någon information i policyn om hur denna ska underhållas. Vissa av dokumenten skulle också behövas skrivas om och på vissa punkter så saknas vissa grundläggande krav från standarderna.

Om vi skulle ge ett slutgiltigt betyg till Läkemedelsverket så vill vi säga att vi tycker att dagens implementation är på en lämplig nivå och de är väl medvetna om vad som de behöver arbeta med och vad de har uppfyllt ifall de skulle vilja bli certifierade. Vår generella uppfattning är att dem har väldigt bra implementationer och rutiner för informationssäkerheten och versamhetens säkerhet i helhet.

Sammanfattning på checklistan

UK = Uppsala kommun
SK = Sollentuna kommun
LV = Läkemedelsverket

	UK	SK	LV
Ger policyn ledningens viljeinriktning och stöd för informationssäkerhetsarbetet?	**Ja**	**Ja**	**Nej**
Har ledningen fastställt policyn?	**Ja**	**Ja**	**Ja**
Är det beskrivet hur policyn ska underhållas och på vilket sätt?	**Nej**	**Ja**	**Nej**
Är policyn spridd i verksamheten och finns det ett system för detta?	**Delvis**	**Ja**	**Ja**
Finns det en definition av informationssäkerhetsbegreppet?	**Ja**	**Ja**	**Ja**
Tar policyn hänsyn till hoten från anställda och utomstående?	**Nej**	**Delvis**	**Ja**
Visar policyn mål och omfattning samt vikten av informationssäkerhet?	**Delvis**	**Nej**	**Ja**
Är ansvaret definierat?	**Ja**	**Ja**	**Ja**
Finns det reglerat hur rapportering av incidenter ska gå till?	**Nej**	**Ja**	**Delvis**
Hänvisar policyn till andra styrande dokument inom organisationen?	**Nej**	**Nej**	**Nej**
Är det klart och tydligt beskrivet vem som är ägare till policyn?	**Ja**	**Nej**	**Ja**

Sammanfattning

Vi har besökt två kommuner samt läkemedelsverket. Läkemedelsverket var bättre än de två kommunerna på informationssäkerhet. Detta kan eventuellt komma sig av att läkemedelsverket har större vana att hantera sekretessbelagd information samt att läkemedelsverket behandlar en betydligt större mängd sådan information i olika former. Kommuner har inte så mycket sekretessklassad information. Det mesta hos kommuner är offentliga handlingar som går att lämna ut. Den känsligaste informationen en kommun har är personuppgifter som måste censureras, eftersom de oftast inte får lämnas ut enligt personuppgiftslagen. Att kommunen får lämna ut informationen gör att behovet av konfidentialitet minskar. Behovet av tillgänglighet och riktighet påverkas dock inte av detta.

Uppsala kommun har uppenbara brister när det kommer till policy. Inte minst mot bakgrund av att de helt saknar en policy dedikerad till informationssäkerhet. Istället täcks säkerhetsfrågan avseende information in i det bredare säkerhetsbegreppet; således är vi i egenskap av granskare hänvisade till främst säkerhetspolicyn. Då denna är kort och primärt uttryckt i generella ordalag (”säkerheten ska vara hög”) är det kanske främst i anvisningarna vi hittar fundamentet i Uppsala kommuns säkerhetsarbete. I synnerhet är kommun väl förtrogen med ISO 27000-standarderna när det kommer till informationsklassificering och hantering. Sämre ställt är det med underhåll, samt inte minst incidenthantering där styrdokumenten inte ägnar frågan utrymme (vilket leder till en praxis där man tar saker när de dyker upp). Intentionen är ofta god från kommunens sida, som att alla medarbetare ska genomgå utbildning och ständigt ha ett säkerhetstänk integrerar i de andra arbetsuppgifterna. Men i praktiken fungerar inte detta fullt ut: medarbetare betraktar säkerhetsfrågan som väsensskild från arbetsuppgifterna och det är de senare som ständigt prioriteras till följd av tidsbegränsningar. Bättre uppföljning skulle åtminstone i viss mån kunna råda bot på detta.
På detta område är Sollentuna kommun bättre; personal utbildas och informeras om informationssäkerhet. Vidare har de goda rutiner för rapportering av incidenter. Jämför man översiktligt kommunerna komparativt så får man nog säga att Sollentuna bättre implementerar standarderna i sina styrdokument än vad Uppsala kommun gör, detta kan illustreras av en sådan sak som att Sollentuna har en dedikerad informationssäkerhetspolicy medan Uppsala helt saknar en sådan. Emellertid saknar inte heller Sollentuna brister och områden där det finns potential för förbättringsarbete. Tydligare mål för informationssäkerhet vore önskvärt, så man får referenspunkter att förhålla uppföljning till. Bäst i test är föga förvånande Läkemedelsverket som har en välutarbetad policy och genomarbetade styrdokument som understöd och för konkretiserade ändamål. Informationssäkerhetsarbetet är jämfört med kommunernas mer genomtänkt och uttryckt på en detaljerad nivå. Det rotar sig troligtvis i att de har ett större behov av att på ett säkert och rutinmässigt sätt hantera sekretessbelagd information, möjligen inte när det kommer till personuppgifter men när det handlar om journaler och affärshemligheter. Läkemedelsverket måste också enligt MSB följa standarderna efter bästa förmåga. Läkemedelsverket har likt kommunerna inte heller något system för att följa upp införda åtgärder, de utför istället stickprov vid behov. Checklistan visar på att skillnaden mellan organisationerna

inte är så stora men vår slutsats är att läkemedelsverket skiljer sig från de andra då vi kommit fram till uppfattningen att de har en högre medvetenhet när det kommer till informatonssäkerhetsarbetet.

Källförteckning

Swedish Standards Institute (2007). *SSISO/IEC 27001 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav*. 2. Uppl. Stockholm: SIS.

Swedish Standards Institute (2007). *SSISO/IEC 27002 Informationsteknik - Säkerhetstekniker - Riktlinjer för styrning av informationssäkerhet*. 1. Uppl. Stockholm: SIS.

Källor Uppsala kommun

Uppsala kommun (1999). *Säkerhetspolicy för Uppsala kommun antagen av kommunfullmäktige 25 oktober 1999.*
Uppsala kommun (2012). *Anvisningar för säkerhetsarbetet i Uppsala kommun.*
Uppsala kommun (2012). *IT-policy, riktlinjer för styrning av IT i Uppsala kommun samt revidering av anvisningar för säkerhetsarbetet i Uppsala kommun.*
Uppsala kommun (2014). *Anvisning - Informationsklassificering.*
Lidholm, Peter (2014). Informationssäkerhetssamordnare vid Uppsala kommun. [Intervju] 7:e mars.

Källor Solentuna kommun

Sollentuna Kommun (2011) *Policy för informationssäkerhet för Sollentuna kommun.*
Sollentuna Kommun(2011) *It-policy för Sollentuna kommun*
Sollentuna kommun(2014) *LIS Sollentuna Genomgång*
Sollentuna kommun(2014) *Regler för informationssäkerhet*
Sollentuna kommun: *Årsplan för informationssäkerhet*
Sävensjö, Christer(2014). *T.f. informationssäkerhetssamordnare*

Källor Läkemedelsverket

Läkemedelsverkets Säkerhetsskydd
Arbetsordning för Läkemedelsverket
Informationssäkerhet för Chefer
Informationssäkerhet - utveckling och förvaltning
Informationssäkerhet för IT-drift och IT-support
Informationssäkerhet för medarbetare
Reineck, Robert (2014). Säkerhetsansvarig vid Läkemedelsverket. [Intervju] 14:e mars.

Bilagorna finnes bifogade i mappen *Bilagor.*