Revisionsrapport

Granskning av generell behörighetshantering

Botkyrka kommun

Göran Persson Lingman

Sept 2012

Innehåll

1 Sammanfattning

Vår övergripande revisionsfråga var följande:

- Finns det en ändamålsenlig generell behörighetshantering för åtkomst till information i kommunens IT-system/IT-miljö?

Revisionsfrågan avgränsades till ett antal kontrollmål.

Efter genomförd granskning är vår sammanfattande bedömning att behörighetshanteringen inte i alla delar är ändamålsenlig. Vi har identifierat flera utvecklingsområden, men kan samtidigt konstaterat att det pågår ett positivt förbättringsarbete. Det är givetvis viktigt att styrelse och nämnder följer upp att förbättringsarbetet genomförs i enlighet med de planer som finns.

De olika utvecklingsområden och förslag till förbättringar som finns intagna i rapporten sammanfattas nedan:

- Det viktigt att det sker en kontinuerlig uppföljning kring att policys, riktlinjer och anvisningar tillämpas. Förslagsvis bör det tas fram dokumenterade processer kring hur uppföljningsarbetet ska bedrivas samt hur status ska rapporteras till styrelse och nämnder. Informationssäkerhetschef och informationssäkerhetssamordnaren har en viktig roll i detta arbete. Detta är även omnämnt i kommunens riktlinjer kring informationssäkerhet.

- Vi föreslår att kommunen överväger att införa ett s.k. ledningssystem[1] för informationssäkerhet.

- Avseende beställning av nya konton till det gemensamma nätverket konstaterar vi att det finns en enhetlig process mellan behörig beställare och IT-enheten. Dock varierar hanteringen inom förvaltningarna avseende hanteringen till och från behörig och chef och nyanställd. Vi föreslår här att det sker en översyn kring hanteringen mellan behörig beställare och den nyanställde. Den hantering som sker vid vård- och omsorgsförvaltningen kan utgöra ett gott exempel.

- Den hantering som sker då ett nytt lösenord behöver meddelas den anställde är bristfällig. Det är viktigt att det sker en översyn och förbättringar för att säkerställa att lösenordet tilldelas rätt och hålls skyddad så det inte kommer obehörig till del.

- Det är viktigt att det säkerställs att chefer meddelar när anställda ska sluta i enlighet med de rutiner som finns och att hanteringen vid tjänstledighet fungerar som avsett.

- Vi har noterat att det pågår ett utvecklingsarbete med att knyta ett ID-kort till behörighetssystemet. Detta kommer sannolikt att underlätta för användare och förbättra behörighetsskyddet.

[1] Begreppet LIS – Ledningssystem för informationssäkerhet – är den sammanfattande benämningen på verksamhetsprocessen för löpande säkerhetsarbete med rutiner, regler, åtgärder och funktioner i en organisation. ISO 27000-serien är en standard för informationssäkerhet

- Vi vill betona vikten av att den pågående informationssäkerhetsklassningen genomförs som planerat. Informationsklassningen stödjer anpassning av olika typer av skydd och behörighetshantering.

- Vi föreslår att det sker en översyn kring hanteringen av skärmsläckare. Samtliga datorer bör ha skärmsläckare som går på med automatik.

- En kontroll av att användarens behörigheter överensstämmer med deras uppgifter bör genomföras regelbundet (förslagsvis bör detta ske varje år).

- Hanteringen kring att följa upp loggar bör ses över. Detta är extra viktigt avseende anställda med hög behörighet.

- Svaren på webbenkäten indikerar[2] ett behov av utbildningsaktiviteter på olika sätt. I avsnitt 3.2 har vi noterat att det planeras att genomföra olika typer av utbildningsaktiviteter inom området. Vi rekommenderar att utbildningsbehovet inom området analyseras inom förvaltningarna. Därefter fattas beslut om hur olika utbildningsaktiviteter ska genomföras.

- Vi föreslår att det sker en översyn av rutiner och tekniken vid utskrifter. Detta för att säkerställa att känsliga utskrifter inte kan nås av obehöriga.

- Vi ser behov av att det sker en översyn kring hur uttjänta band som används för backuptagning kasseras

- Avseende brandväggen är det viktigt att det sker s.k. penetrationstester med regelbundenhet. Vi har noterat att detta är något som planeras.

- Det viktigt att säkerställa tillförlitligheten kring utrusning och inloggning till olika system. Här kan vi konstatera att det pågår ett förbättringsarbete. Detta har omnämnts i avsnitt 3.2.

[2] Vi noterar att i gruppen övriga ej pedagoger anger många av de svarande att de inte fått tillräcklig utbildning. Dock anger ett betydligt färre antal att de har otillräckliga kunskaper i användningen av datorn.

2 Inledning

2.1 Bakgrund

Kommunens IT-stöd är av stor betydelse på olika sätt. Den moderna informationsteknologin ger möjlighet till att höja kvalité, säkerhet och effektivitet i verksamheten, sprida och öka tillgängligheten till information m m. Inom många områden är det idag självklart att IT är en förutsättning för att aktiviteter och processer ska fungera. IT blir därigenom en viktig del av verksamheten och ska bedrivas med en tillräcklig säkerhetsnivå, bl a hantera behörighet till information.

En risk- och väsenlighetsanalys har genomförts. Resultatet visade bl a på behovet av att genomföra en granskning av informationssäkerhet och främst behörighetshantering.

Kommunens revisorer har därför beslutat att PwC ska genomföra en övergripande granskning inom området.

Revisionsfråga

Finns det en ändamålsenlig generell behörighetshantering för åtkomst till information i kommunens IT-system/IT-miljö?

2.2 Metod och avgränsning

Granskningen berör nedanstående kontroll-/granskningsmål

- Tydlighet kring roller och ansvar kring behörighetstilldelning
- Rutiner vid anställning, förnyelse och borttag av behörighet
- Styrande dokument och beskrivningar kring processer och rutiner kring behörighetstilldelning
- Rutiner och kontroll för att säkerställa autentisering (lösenordets utformning, tvingande byte, hantering av loggar etc)
- Användarnas medvetenhet och kunskap kring hantering av lösenord och olika skydd för obehörig åtkomst säkerställs
- Regler och rutiner kring hantering av leverantörer och konsulter
- Säkerställande av att utskrifter och säkerhetskopior inte hamnar hos obehöriga
- Hemarbete, skydd mot intrång och trådlösa nät.

I bilaga visas grafik från enkäten samt ett urval av fritextkommentarer. Vi har främst efterfrågat kommentarer då användare inte instämt i påståendet [3] (svarat inte alls eller till viss del). Färgerna ska tolkas enligt följande. Värden till vänster innebär att användare besvarat frågan med instämmer inte alls eller till viss del . Värden till höger

[3] Efter att användare haft svarsalternativen helt, i huvudsak, till viss del, inte alls fanns texten *"Om du svarar till viss del eller inte alls. Kommentera om du upplever problem med detta och/eller vilka konsekvenser detta ger"*

innebär att användare besvarat med i huvudsak ■ eller helt ■. Siffror i liggande staplar visar antalet svarande. Gråvit färg innebär att användare besvarat med vet ej.

Vidare har intervjuer genomförts inom ramen för granskningen.

Granskningsobjekt är i första hand kommunstyrelsen, dock berörs samtliga nämnder. Granskningen är generell och berör hanteringen i separata system i ringa omfattning.

3 Resultat

3.1 Övergripande styrande dokument inom informationssäkerhetsområdet Iakttagelser

Det finns en informationssäkerhetspolicy som behandlar informationssäkerhet. Policyn är fastställd av kommunstyrelsen 2007.

I dokumentet *Riktlinjer för informationssäkerhet* från 2010-09-29 konkretiseras informationssäkerhetspolicyn. Riktlinjerna har reviderats under året.

Riktlinjer behandlar bl a:

- Organisation och ansvar för informationssäkerheten (systemägarens ansvar, medarbetarens ansvar under och efter anställning, konsulters ansvar, ansvarsförbindelser)
- Riskbedömning och riskhantering
- Klassificering och hantering av information, t ex sekretess
- Fysisk säkerhet kring informationsbehandling
- Driftrutiner och ansvar för kommunens informationssystem
- Åtkomst till information och system (användarens ansvar, kryptering, åtkomst till nätverk, m.m.)
- Rapportering av säkerhetshändelser och svagheter

Det pågår ett omfattande förbättringsarbete avseende generella stödjande dokument (anvisningar m.m). Arbetet leds av informationssäkerhetschefen med hjälp av informationssäkerhetssamordnare och IT-chef.

Exempel på dokument där ett arbete pågår är:

- Anvisningar kring informationssäkerhet som riktas till chefer
- Sammanställning kring lagar och regler inom den kommunala verksamheten
- Stöd för riskbedömning, riskhantering. säkerhetsklassning
- Fysisk säkerhet kring informationsbehandling
- Anvisningar för medarbetare
- Botkyrka kommuns policy om skyddade personuppgifter med riktlinjer till nämnder

- Hantering av incidenter
- Säkerhet vid hemarbete
- Hantering av telefoner, surfplattor och datorer då de används både privat och i tjänsten. Kring detta pågår även en utredning[4] kring vad som bör gälla inom kommunen
- Stöd för att informationssäkerhetsklassa information inom verksamheterna.

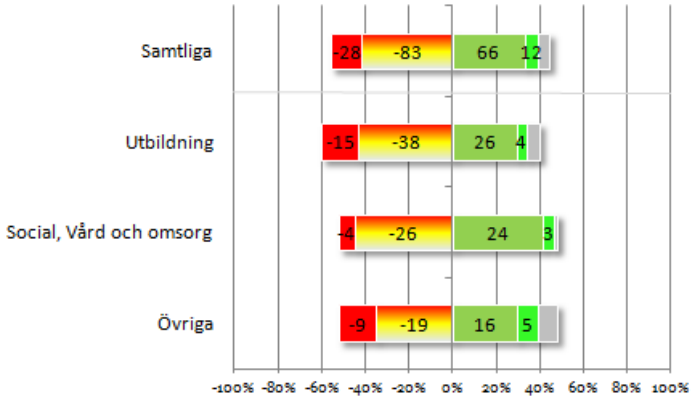
Det finns enligt uppgifter anvisningar och rutiner som kan variera från förvaltning till förvaltning. Vi har i vår granskning inte kunnat identifiera vad som finns och inte finns.

Vid intervjuer och i användarenkäten (se nedan) har det framkommit behov av att implementera policy och riktlinjer på ett bättre sätt inom nämnderna.

Enkäten

Nedan visas svar från enkäten. Flera av de svarande utrycker en osäkerhet kring dokument avseende informationssäkerhet. På fråga om var dokumenten finns anger även flera att de är osäkra. Se bilaga 1.

Fråga i enkäten "Jag känner till kommunens informationssäkerhetspolicy och/eller riktlinjer och/eller anvisningar för informationssäkerhet?"



[4] Det förkommer att privat information lagras på arbetsgivarens mobila enhet. Utrustningen blir en korsreferens av information. Problemet uppstår den dagen medarbetaren byter arbetsgivare eller lämnar arbetet av annan orsak. Kommunen äger information, tjänstemannen äger information, utrustningen ägs av kommunen eller tjänstemannen.

Våra kommentarer

- Vi har tagit del av övergripande policy och riktlinjer. Enligt vår bedömning är dessa dokument är tillfredsställande som underlag för informationssäkerhetsarbetet.

- Avseende anvisningar och rutiner som ska konkretisera policy och riktlinjer har vi upplevt att det är svårt att få en överblick av vilka aktuella dokument som finns och inte finns. Vi kan dock konstatera att det pågår ett positivt förbättringsarbete avseende framtagande av underliggande dokument (anvisningar, rutiner m.m.) till policy och riktlinjer.

- Avseende svar från användare varierar svaren men flera av de svarande är osäkra på vilka dokument som finns och var de återfinns. Efter att arbetet med framtagande av olika dokument slutförts är det därför viktigt att styrelse och nämnder säkerställer att det planerade arbetet med att implementera[5] dokumenten till olika målgrupper genomförs. Se mer i avsnitt 3.2 nedan.

3.2 Aktiviteter med att implementera styrande dokument samt uppföljning

Iakttagelser

Det har framkommit att ett implementeringsarbete avseende generella dokument[6] kring informationssäkerhet inte bedrivits i tillräcklig omfattning tidigare. Ett förbättringsarbete kring detta har påbörjats under året.

Utifrån de uppgifter vi fått finns behov av att tydliggöra hur information ska hanteras. Det som framkommit är t ex:

- Behov av att tydliggöra hur privat utrustning får användas inom tjänsten.
- Tydliggöra vad som får/inte får lagras på kommunens servrar.
- Vad innebär det att informationsklassa den information som hanteras inom nämnderna.
- Vad måste beaktas avseende offentlighetsprincip, personuppgiftslag m.m.
- Vad ska kommuniceras via e-post och vad ska inte kommuniceras.

5 Ett mål är att olika dokument ska nå rätt målgrupp och att det är tydligt hur förändringar och nyheter kommuniceras (t ex hur används intranätet som kommunikationsväg).

6 informationssäkerhetspolicy m.m.

Enkäten

Flera användare som besvarat enkäten utrycker t ex en osäkerhet kring hur känslig skyddsvärd information ska sparas och hanteras. Flera användare anger ett behov av mer utbildning inom området. Se mer kring svar från enkäten i bilaga 1.

Pågående förbättringar

Det har planerats att genomföra olika förbättringsaktiveter kring att utveckla informationshanteringen. Exempel på aktiviteter som har påbörjats under året eller kommer att påbörjas under hösten 2012 sammanfattas nedan:

- Det är planerat att genomföra utbildningar vid varje förvaltning under hösten 2012. Utbildningen kommer att behandla informationssäkerhet och ligga till grund för förvaltningarnas egen klassning av information och risk- och sårbarhetsanalyser.

- All personal kommer att ges möjlighet att genomgå en utbildning via internet (DISA7).

- Det planeras att genomföra en föreläsningsserie med förläsare från MSB, Länsstyrelsen, Datainspektionen, m fl för alla som arbetar i kommunen. Några tidpunkter finns inte bestämda.

- Ett arbete med att införa en generell systemförvaltningsmodell (PM38) pågår. Enligt ansvariga vi intervjuat kommer modellen att leda till ett tydliggörande av ansvar och uppgifter för varje system.

- Ett arbete med att informationsklassa uppgifter i olika system kommer att påbörjas. (Enligt uppgifter är endast ett system informationsklassat9 idag). Informationssäkerhetschefen ansvarar för att följa upp förvaltningarnas arbete medan respektive verksamhetschef också har ett ansvar för att arbetet blir genomfört. Dokumenten kommer att ge ett viktigt underlag för att säkerställa att det skydd som finns matchar klassningen av informationen.

- Det planeras att förbättra tillsynen av de riktlinjer som finns framtagna följs. Avseende detta är det tänkt att informationssäkerhetssamordnaren ska ha en viktig roll.

7 DISA, står för datorstödd informationssäkerhetsutbildning för användare, är en kostnadsfri utbildning som funnits sedan tidigare. Utbildningen sker via Myndigheten för Samhällsskydd och Beredskap.
8 PM3 (På maintenance management model) beskriver ansvar och hur olika roller samverkar kring ett system,
9 I riktlinjer anges att detta ska genomföras. Ansvariga anges.

Våra kommentarer

- Enligt vår bedömning är policys och riktlinjer otillräckligt införda inom nämnderna. Vi kan dock konstatera att det pågår ett förbättringsarbete.

- Det är viktigt att kommunstyrelsen och övriga nämnder följer det framtida arbetet via uppföljning och tydliga realistiska tidplaner samt ansvar för olika aktiviteter[10].

- Vi föreslår att kommunen överväger att införa ett s.k. ledningssystem[11] för informationssäkerhet.

3.3 Tydlighet kring roller och ansvar för att arbeta förebyggande och uppföljande inom informationssäkerhetsområdet

Iakttagelser

Sedan cirka ett år tillbaka finns en informationssäkerhetssamordnare som arbetar på uppdrag från säkerhetschefen (säkerhetschefen har även ett övergripande ansvar för stöd och uppföljning kring informationssäkerhet - informationssäkerhetschef).

Exempel på uppgifter avseende rollen informationssäkerhetssamordnare är:

- Att tolka befintligt regelverk och sammanställa detta på ett pedagogiskt sätt så att det blir användarvänligt och lätt att förstå för den genomsnittlige användaren
- Informera och utbilda i och om regelverk och anvisningar
- Upprätta kontrollplan för informationssäkerheten
- Omvärldsbevakning
- Analysera externa händelser för att se hur det kan komma att påverka kommunens verksamhet
- Följa upp och presentera nyheter inom informationssäkerhetsområdet
- Ta fram förslag på åtgärder för att tillgodose kravet från verksamheten vad avser kravet på säkerhetsnivå och smidigt arbetssätt
- Utbilda medarbetare inom informationssäkerhetsområdet vad avser analyser, metoder, metodstöd etc

En samverkan sker med IT-driftledare, kommunjurist, IT- och E-utvecklingsenheten.

10 T ex samtliga IT-system skall ha informationssäkerhetsklass klart senast 2014-07-01. Plan för detta skall vara upprättad senast åå mm dd. Arbetet påbörjas senast åå mm dd . Ansvarig är xx.

11 Begreppet LIS – Ledningssystem för informationssäkerhet – är den sammanfattande benämningen på verksamhetsprocessen för löpande säkerhetsarbete med rutiner, regler, åtgärder och funktioner i en organisation. ISO 27000-serien är en standard för informationssäkerhet.

Det finns ingen aktuell förteckning kring vilka som är systemägare. Det anges att ansvaret kring systemen inte är tillräckligt tydlig tydliggjort. Avsaknaden av utpekade ansvariga gör det otydligt för olika intressenter att veta vem som ansvarar för systemen, drift och underhåll m.m. En konsekvens kan bli att det uppfattas som att IT-enheten ska ha ett ansvar för uppgifter som de inte har[12].

Systemägaren[13] har enligt riktlinjer ett ansvar att klassificera den information [14] som används inom verksamheten. De har även ett ansvar att riskvärdera och säkerställa att erforderligt behörighetsskydd finns. Klassificering och riskvärderingar är enligt uppgifter eftersatt i dagsläget.

Som omnämnts pågår ett arbete med en ny systemförvaltningsmodell där ett av målen är att tydliggöra vilka som är systemägare, systemansvariga och ansvariga för drift och underhåll samt vilka uppgifter som ska utföras och fördelas mellan olika roller. (I tidigare riktlinjer har respektive nämnd pekats ut som systemägare. Detta kommer att ändras i samband med att den nya systemförvaltarmodellen införs).

Enligt riktlinjer har respektive chef ett ansvarar för att medarbetaren får information[15] om kommunens informationssäkerhetspolicy, riktlinjer och de anvisningar som är aktuella för respektive arbetsuppgift.

Enligt riktlinjer ska det även utses informationsägare. Detta är inget som genomförts.

I riktlinjer anges att den anställde ska informeras om gällande lagar och andra föreskrifter som ska följas. Det anges även att anställda ska underteckna en ansvars- och sekretessförbindelse.

Det finns en upprättad blankett för sekretess- och ansvarsförbindelse och det pågår arbete med att implementera hanteringen kring förbindelsen (rutiner, ansvar, etc).

I enkäten ställdes fråga kring om den anställde skrivit under någon förbindelse. De flesta av de svarande anger vet ej eller nej (130 av de svarande anger vet ej eller nej).

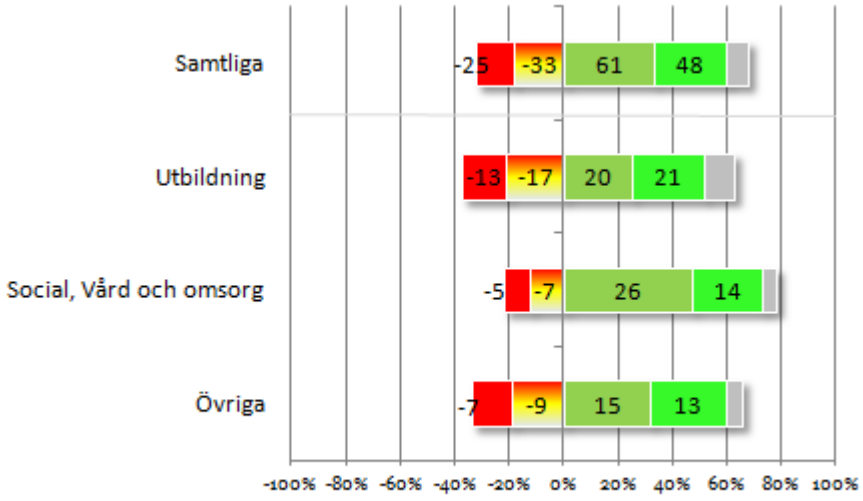
Enkäten

I riktlinjer finns inskrivet till vem användarna ska vända sig till om de ser brister (t ex risker) som berör informationssäkerhet.

I enkäten ställdes en fråga kring tydlighet avseende vart man vänder sig. Svaren varierar men flera anger att detta inte är tillräckligt tydligt (55 av de svarande anger inte alls eller till viss del tydligt).

[12] Leverantören kanske har ett större ansvar.
[13] Som vanligtvis är förvaltningchef avseende verksamhetskritiska system.
[14] Bl a den information som finns i verksamhetens system.
[15] Om en medarbetare får ändrade anställningsförhållanden ska behörigheter anpassas enligt de nya förhållanden som ska gälla. Chefen på den nya arbetsplatsen ska avgöra vad som ska gälla. Chefen på den gamla arbetsplatsen avgör vilken information som medarbetaren får ta med sig till den nya arbetsplatsen.

Det är tydligt vart jag ska vända mig om jag misstänker brister kring vår behörighetshantering



Våra kommentarer

- Vi kan konstatera att det pågår olika förbättringsaktiviteter, vilka vi bedömer vara positiva.

- Det är viktigt att styrelse och nämnder följer upp att det förbättringsarbetet som pågår genomförs som avsett. Därefter är det givetvis viktigt att det ser en kontinuerlig uppföljning kring att policys, riktlinjer och anvisningar tillämpas. Förslagsvis bör det tas fram dokumenterade processer kring hur uppföljningsarbetet ska bedrivas samt hur status ska rapporteras till styrelse och nämnder. Informationssäkerhetssamordnaren har en viktig roll i detta arbete. Detta är även omnämnt i riktlinjer. Se även kommentarer i avsnitt 3.2.

3.4 Tillfredställande rutiner vid anställning, förnyelse och bortag av behörighet till det gemensamma nätet

Att observera är att tilldelning av behörighet i separata system inte berörs i granskningen.

Iakttagelser

Vid varje förvaltning finns behöriga beställare. Detta innebär att endast ”behörig beställare” har rätt att beställa konto från IT-enheten då det skett nyanställningar.

Ansvarig chef ska meddela behörig beställare att ett nytt konto krävs.

Via den s.k. beställningsportalen meddelar behörig beställare att det finns behov av ett nytt konto. (Servicedesk skapar ett nytt id för användaren).

Via mail erhåller behörig beställare ett id och lösenord. Det krävs att lösenordet byts första gången.

Processer och rutiner kring hur kommunikationen sker mellan behörig beställare, ansvarig chef och den nyanställde varierar. Inom vård- och omsorgsförvaltningen har man t ex tagit fram en datorstödd process kring hanteringen mellan ansvarig beställare, chef och den anställde.

När en anställning upphör ska ansvarig chef meddela ansvarig beställare att behörighet till informationssystemen ska tas bort[16]. Ansvarig beställare ska sedan meddela servicedesk. Vid intervjuer har det framkommit att det finns behov av att förbättra rapporteringen då anställningen upphör.

Enligt riktlinjer ska anställande chef vid varje tjänstledighet och föräldraledighet längre än en månad skriva ett avtal där det framgår vilka konton medarbetaren har tillgång till under sin frånvaro. Dokumentet ska delges dem som är berörda, t ex driftorganisationen. Enligt uppgifter är denna hantering otillräckligt implementerad.

Det har även framkommit att det finns förbättringsbehov kring hanteringen då ett nytt lösenord behöver meddelas den anställde, t ex vid förlust av lösenordet.

<u>Planerade förbättringar</u>

Det har initierats ett arbete med att införa ett id-kort[17] för alla anställda. Kommunen har genomfört en förstudie och tagit fram en plan för arbetet. Ett genomförandeprojekt är startat. Målet är att samordna och så långt möjligt automatisera behörighetshanteringen

[16] I riktliner anges att ansvarig chef har ett ansvar för att säkerställa att behörigheter till informationssystemen tas bort då tjänsten avslutas.

[17] Mål/Funktion: Ett kort för alla tillfällen och behov med foto och personuppgifter. "Nyckeln" för anställda och andra av kommunen i anspråkstagna, ett passerkort med ID-uppgifter och foto. Kortet har chip och används för inloggning i kommunens IT-miljö.

mellan de viktigaste systemen. Syftet är bland annat att på sikt möjliggöra en sammankoppling med ett kommande kommun id-kort som både skulle kunna vara id-handling, inpasseringskort och utrustas med certifikat för stark inloggning. Det senare kräver dock noggranna rutiner och regelverk och behöver utredas ytterligare. Kommunen samverkar kommunen i ett arbete som pågår inom området i Stockholms län (KSL/IT-forum).

Våra kommentarer

- Vi konstaterar att det finns en enhetlig process mellan behörig beställare och IT-enheten. Dock varierar hanteringen inom förvaltningarna avseende hanteringen till och från behörig chef och nyanställd. Vi föreslår här att det sker en översyn kring hanteringen mellan behörig beställare och den nyanställde. Den hantering som sker inom vård- och omsorgsförvaltningen kan utgöra ett gott exempel.

- Den hantering som sker då ett nytt lösenord behöver meddelas den anställde är bristfällig. Det är viktigt att det sker en översyn och förbättringar för att säkerställa att lösenordet tilldelas rätt och hålls skyddad så det inte kommer obehörig till del.

- Det är viktigt att det säkerställs att chefer meddelar när anställda ska sluta i enlighet med de rutiner som finns samt att hanteringen vid tjänstledighet fungerar som avsett.

- Vi har noterat att det pågår ett utvecklingsarbete med att knyta ett ID-kort till behörighetssystemet. Detta kommer sannolikt att underlätta för användare och förbättra behörighetsskyddet.

- Vi vill betona vikten av att den pågående informationssäkerhetsklassningen genomförs som planerat. Informationsklassningen stödjer anpassning av olika typer av skydd och behörighetshantering.

3.5 Skärmsläckare och en god utformning av lösenord m.m.

Iakttagelser

Avseende skärmsläckare anges att detta varierar inom kommunen. De flesta användarna har skärmsläckare som går på med automatik, men det finns även många användare som saknar skärmsläckare. Många skärmsläckare kan enligt uppgifter avaktiveras av användaren.

Det finns ingen policy som anger krav kring skärmsläckare.

Avseende lösenord krävs ett byte första gången man erhåller lösenordet. Byten måste ske kontinuerligt. Intervall för detta finns styrt via behörighetssystemet. Längden på lösenordet samt vissa andra krav är reglerade. Det finns upprättade instruktioner till användare kring vad de ska tänka på avseende utformningen. Tilldelning av lösenord har berörts i avsnitt 3.4.

Kontroll av att behörighetsstrukturen i behörighetssystemet överensstämmer med verkligheten[18] sker ej regelbundet. De ansvariga vi intervjuat ser ett förbättringsbehov kring detta.

Det saknas skriftliga rutiner kring hur loggar ska kontrolleras. Kontroller sker ibland då något uppmärksammats. Dock sker ingen systematisk kontroll.

Våra kommentarer

- Vi föreslår att det sker en översyn kring hanteringen av skärmsläckare. Samtliga datorer bör ha skärmsläckare som går på med automatik.
- En kontroll av att användarens behörigheter överensstämmer med deras uppgifter bör genomföras regelbundet (förslagsvis bör detta ske varje år).
- Hanteringen kring att följa upp loggar bör ses över. Detta är extra viktigt avseende anställda med hög behörighet.

3.6 Tillräcklig utbildning och kompetens t ex kring hantering av lösenord och olika skydd för obehörig åtkomst

Iakttagelser

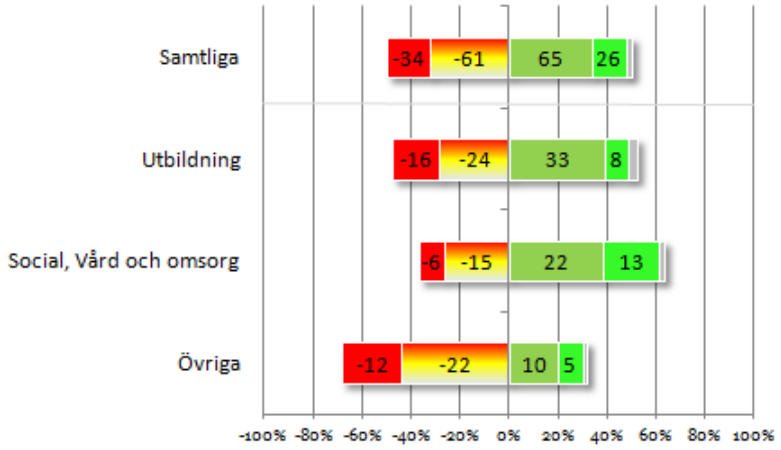
I vår enkät har de flesta angett att de har kännedom kring vad man ska tänka på[19] kring hantering av lösenordet. Se mer i bilaga 1.

I enkäten ställdes fråga om användare fått tillräcklig utbildning kring hur känslig information ska hanteras. Svaren varierar men många av de svarande anger at det finns behov av utbildning.

Vi har även inom andra frågeområden i enkäten uppmärksammat behov av ökad information och utbildning, t ex vilka dokument som är viktiga för olika roller.

Fråga i enkäten: *Jag har fått en tillräcklig utbildning och/eller information kring hur känslig information ska hanteras. (t ex information där personuppgiftslagen ska beaktas)?*

[18] T ex att det beaktas att en anställd byter befattning eller slutar.
[19] Många användare har även exemplifierat hur ett bra lösenord kan se ut.



- *Ja men detta är saker som behöver upprepas och utbildas i hela tiden, då frågorna i sig skapar osäkerhet. Vad får man göra, vad får man inte göra m.m., Serviceförvaltningen*

- *Jag började min anställning här för många år sedan. Vi uppdateras inte, Utbildningsförvaltningen*

- *behöver återerövras med jämna mellanrum, kan var i forma av en digital påminnelse i ett enkelt bildspel via epost 1 ggr/år, Arbetsmarknads- och vuxenutbildningsförvaltningen.*

- *Frågan är så viktig att den aldrig får tappas bort. Regelbundna informationsinsatser krävs för att hålla den vid liv, Vård- och omsorgsförvaltningen.*

Våra kommentarer

- Svaren indikerar ett behov av utbildningsaktiviteter på olika sätt. I avsnitt 3.2 har vi noterat att det planeras att genomföra olika typer av utbildningsaktiviteter inom området.

- Vi rekommenderar att utbildningsbehovet inom området analyseras inom förvaltningarna. Därefter fattas beslut om hur olika utbildningsaktiviteter ska genomföras.

3.7 Regler och rutiner kring hantering av leverantörer och konsulter

Iakttagelser

Riktlinjerna kring informationssäkerhet behandlar hur leverantörer ska hanteras.

I riktlinjer sägs bl a att säkerhetskontrollen av konsulter och leverantörer ska göras utifrån vilken information (känslig eller mycket känslig) som hanteras. Respektive chef är ansvarig för att sådana kontroller görs. Hur leverantörer och konsulter ska hanteras efter att arbetet avslutas finns beskrivet. Ytterligare anvisningar håller på att upprättas. Vidare anges att samtliga konsulter och leverantörer som hanterar kommunens informationstillgångar eller informationssystem ska underteckna en ansvars- och sekretessförbindelse. Vi har tagit del av en upprättad blankett som ska användas mot leverantörer.

Det anges att hanteringen av detta kommer att säkerställas via information och en förbättrad uppföljning.

Kommentarer

- Vi konstaterar att det sker ett förbättringsarbete kring att implementera styrande och stödjande dokument. Se avsnitt 3.2 Sker aktiviteter med att implementera styrande dokument samt sker uppföljning.

3.8 Säkerställande av att utskrifter och säkerhetskopior inte hamnar hos obehöriga

Iakttagelser

Vissa användare har möjlighet att skydda sina utskrifter via en utmatningskod (lösenordsskyddad utskrift). Dock anges att majoriteten av användare inte har denna möjlighet.

<u>Enkäten</u>

I enkäten ställdes frågor kring om användare lösenordsskyddar sina utskrifter och/eller anger att det är säkerställt att känsliga uppgifter inte når obehöriga vid utskrift. En stor andel av de svarande anger att de aldrig lösenordsskyddar sina utskrifter. Flera användare anger i kommentarer att det inte går eller att de inte känner till möjligheter att skydda sina utskrifter.

Nedan visas några exempel på kommentarer avseende lösenordsskyddad utskrift.

- *”Det går ej att lösenordsskydda”, Socialförvaltningen*
- *”Jag brukar vara extra försiktig när jag skriver ut dokumentation men det är flera som har lånat mitt lösenord, det kan bero på att de inte fått sitt lösenord ännu”, Vård- och omsorgsförvaltningen.*

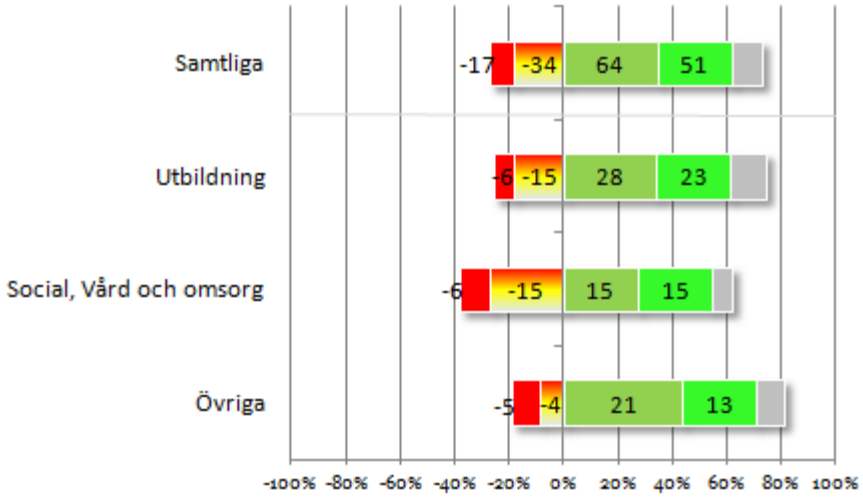
- *”Vet inte hur man gör”, Vård- och omsorgsförvaltningen.*
- *Vet inte hur man gör så jag skriver inte ut känsliga dokument på arbetsplatsen, Annan.*
- *”Vet inte ens vad detta är”, Socialförvaltningen.*
- *”Jag visste inte att man kunde lösenordskydda utskriften”, Arbetsmarknads- och vuxenutbildningsförvaltningen.*
- *”Behörigheten till privat utskrift är inte tillgänlig efter inköp av ny skrivare”, Socialförvaltningen.*
- *Funktionen finns inte på skrivaren, Utbildningsförvaltningen.*

Se grafik och kommentarer från användare i bilaga 1.

Fråga ställdes även till användare kring om de ser risker att obehöriga tar del av känsliga uppgifter vid utskrifter (t ex att skrivare står i en oskyddad miljö och eller kod för utmatning saknas). Svaren varierar där de flesta anger att det inte finns risker. Dock anger även flera att det finns risker.

Grafik och exempel på kommentarer då användare angett att de ser risker[20] visas nedan.

Då jag skriver ut känsliga dokument på vår/min skrivare så medför detta inga risker att obehöriga tar del av dokumenten



- *”I bland ändrar sig skrivaren sig själv o kan då hamna någon annanstans i komunen eller på huset”, Vård- och omsorgsförvaltningen.*
- *”Tidigare så råkade utskrifterna skrivas ut på andra enheter i stället för på vår.vet dock inte om det är åtgärdat idag”, Vård- och omsorgsförvaltningen.*

[20] besvarat frågan med inte alls eller till viss del.

- *”Det händer att datorn "själv" andrar vald skrivare och att man då inte vet var det hamnar. Skrivare är placerad i en allmän korridor som dock inte används av så många”, Vård- och omsorgsförvaltninge*

- *”Skrivaren finns i lättillgänglig korridor”, Utbildningsförvaltningen*

- *skrivaren ligger i ett rum som alla anställda i huset har tillgång till, Arbets-marknads- och vuxenutbildningsförvaltningen*

- *En liten feltryckning kan gå till vilken som helst enhet inom förvaltningen och läsas av vem som helst, Vård- och omsorgsförvaltningen*

Se mer kommentarer i bilaga 1.

Säkerhetskopior (band finns i bandrobot) som är placerat i särskild utrymme. Utrymmet är enligt uppgifter motståndskraftigt med en låst dörr. Endast personal från IT-enheten har tillträde till detta utrymme. Band som inte ska används kan kasseras på olika sätt.

Våra kommentarer

- Det är viktigt att det sker en översyn av rutiner och tekniken vid utskrifter. Detta för att säkerställa att känsliga utskrifter inte kan nås av obehöriga.

- Vi ser behov av att det sker en översyn kring hur uttjänta band kasseras.

3.9 Hantering avseende hemarbete, skydd mot obehörigt intrång och åtkomst till trådlösa nät

Iakttagelser

Säkerheten kring hemarbete, de trådlösa näten och brandväggen har kommunicerats med ansvariga.

Det sker s.k. intrångstest för att säkerställa tillförlitligheten i brandväggen. Dock görs inte detta med någon regelbundenhet. Detta är dock något som planeras.

Hantering av mobil datoranvändning och distansarbet finns intaget i riktlinjer avseende informationssäkerhet. Det anges att det finns behov av att utreda vilken typ av utrust-ning som får användas. Det anges även att det finns behov av att se över olika inlogg-ningsförfarande till systemen. Information kring och uppföljning av riktlinjer kommer att förbättras. Se avsnitt 3.2 (Aktiviteter med att implementera styrande dokument samt sker uppföljning).

Våra kommentarer

- Avseende brandväggen är det viktigt att det sker s.k. penetrationstester med regelbundenhet. Vi har noterat att detta är något som planeras.

- Det viktigt att säkerställa tillförlitligheten kring utrusning och inloggning till olika system. Här kan vi konstatera att det pågår ett förbättringsarbete. Detta har omnämnts i avsnitt 3.2.

2012-09-25

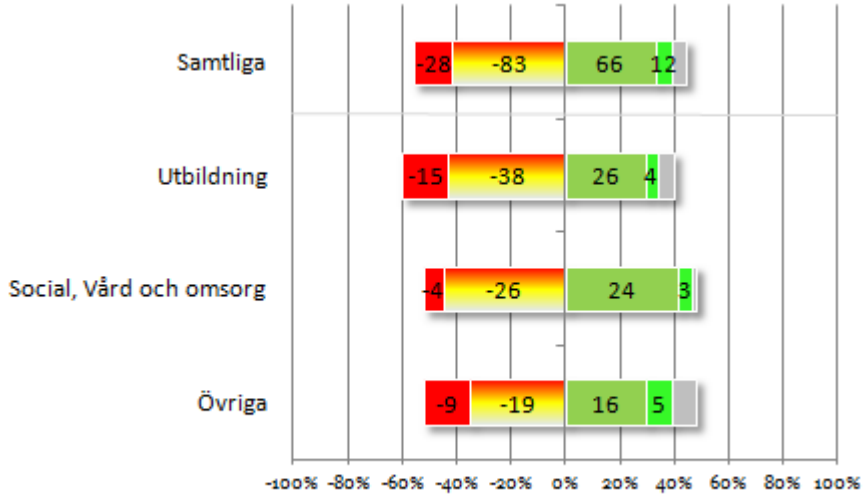
Göran Persson Lingman — Projektledare

Jan Nilsson — Uppdragsansvarig

Bilaga 1: Användarsvar

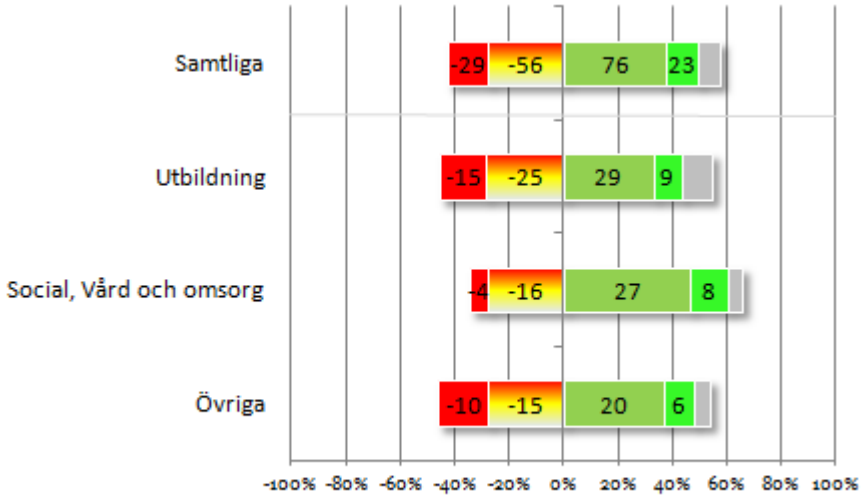
Nedan visas grafik från användarsvar. Exempel på kommenterar visas under grafiken. Vi har önskat kommentarer då användare inte instämt i påstående

01. Jag känner till kommunens informationssäkerhetspolicy och/eller riktlinjer och/eller anvisningar för informationssäkerhet?



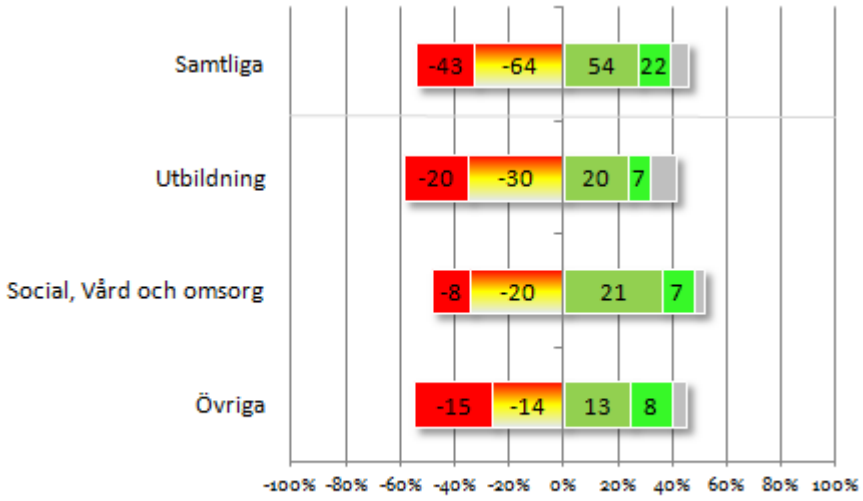
- *Men jag försöker vara diskret med känslig information i alla lägen., Utbildningsförvaltningen.*
- *Jag känner till policyn och riktlinjerna som finns på nätet men anvisningar för informationssäkerheten har jag inte vetat de finns, Vård- och omsorgsförvaltningen.*
- *Jag vet inte vad ni menar med informationssäkerhet. Vi använder inte det begreppet, Utbildningsförvaltningen.*
- *Jag är osäker på vad som menas, Utbildningsförvaltningen.*
- *Jag vet att man ska ta hänsyn till säkerhetsfråga när man jobbar på kommunen men jag fick inte riktad information om det från ngn som ansvarig för detta område. Samhällsbyggnadsförvaltningen.*

02. Jag bedömer att jag är tillräckligt insatt i det som behandlas i informationssäkerhetspolicys och riktlinjer och anvisningar (det som berör dig i din roll)



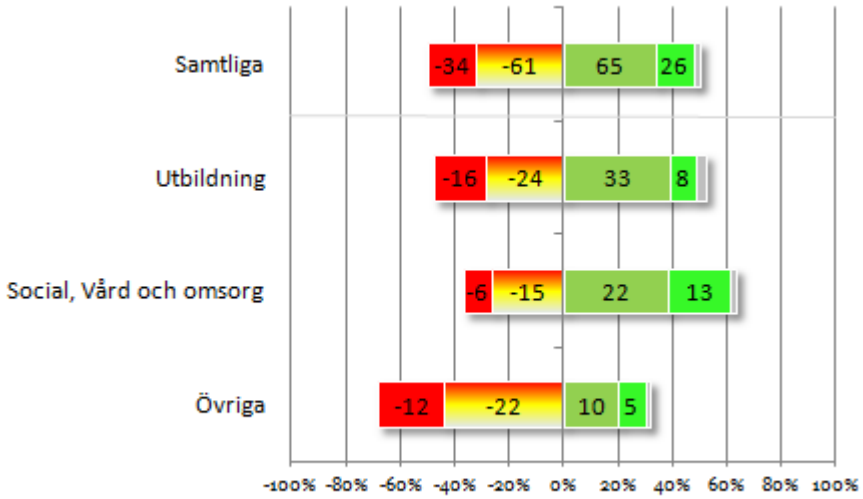
- *Skulle vara bra med bättre information så att jag känner mig tryggare kring vad jag får och inte får göra, Utbildningsförvaltningen.*
- *Jag vet vilket material som är sekretessbelagt, men inte hur jag ska hantera det och i vilka fall man får göra undantag, Samhällsbyggnadsförvaltningen.*
- *Känner jag mig osäker tar jag kontakt med överordnad chef, Utbildningsförvaltningen.*
- *Skulle behöva en uppgradering och information kring detta, Utbildningsförvaltningen.*
- *Jag har inte tillräkligt kunskap, Utbildningsförvaltningen.*
- *Det är färskvara och lätt att glömma bland allt man ska ha i huvudet. Jag har läst om det för ett tag sedan när jag fick papper. Att regelbundet få muntlig info på ett möte skulle vara bra tycker jag. Lättare än att komma ihåg att sitta själv och läsa regelbundet, Socialförvaltningen.*
- *Har dock hamnat i kontakt med informationssäkerhetssamordnaren via ett IT-projekt. Börjar därför blir insatt i policyn, Samhällsbyggnadsförvaltningen.*
- *Är ny på jobbet och är inte insatt i detta ännu, Utbildningsförvaltningen.*
- *Jag har aldrig sett något papper om policy, riktlinjer eller anvisningar, Utbildningsförvaltningen.*

03. Jag känner till var dokument som behandlar informationssäkerhet och behörighet till information återfinns?



- *Antar att de finns på Helgonet. Har aldrig letat efter dem, Samhällsbyggnadsförvaltningen.*
- *Det är svårt att hitta dom på Helgonet, Kultur- och fritidsförvaltningen.*
- *Det saknas Policys, Riktlinjer på användarnivå och som är "läsvänliga", Utbildningsförvaltningen.*
- *Men det tog lång tid att hitta. Dåliga uppdateringar och aldrig information när revideringar eller uppdateringar sker, Utbildningsförvaltningen.*
- *Jag tycker att vårt intranät är svårt att hitta i om man letar efter specifika dokument, Utbildningsförvaltningen.*

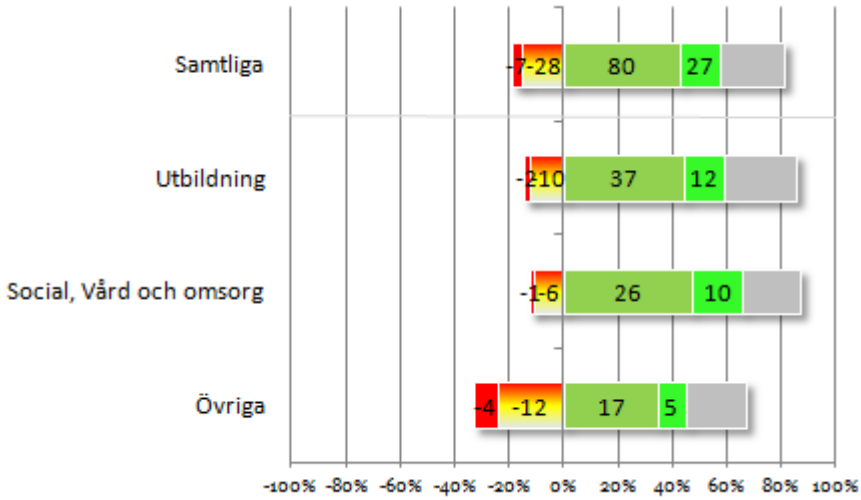
04. Jag har fått en tillräcklig utbildning och/eller information kring hur känslig information ska hanteras. (t ex information där person-uppgiftslagen ska beaktas)?



- *Förvärvat kunskap i frågan på annat sätt än utbildning/information på förvaltningen, Kommunledningsförvaltningen.*
- *Dem flesta vet att man ska bevara en viss information oåtkomligt för personal utanför verksamheten, t ex pärmar och allt sånt som berör brukaren ska vara inlåst. Men vi har lite brist på annat som t ex att en del inte riktigt vet vad man får och hur man dokumenterar, Vård- och omsorgsförvaltningen.*
- *Ja men detta är saker som behöver upprepas och utbildas i hela tiden, då frågorna i sig skapar osäkerhet. Vad får man göra, vad får man inte göra m.m, Serviceförvaltningen.*
- *Den information jag fått har jag fått av elevhälsoteamet här på skolan och jag följer deras instruktioner, Utbildningsförvaltningen.*
- *På andra arbetsplatser och genom "självstudier", Vård- och omsorgsförvaltningen.*
- *Har själv läst policyn och tagit reda på hur vida sekretess på min arbetsplats skall hanteras, Annan.*
- *Jag är osäkert vilka information ska jag lämna när man jobba offentlig, Utbildningsförvaltningen.*
- *Frågan är så viktig att den aldrig får tappas bort. Regelbundna informationsinsatser krävs för att hålla den vid liv, Vård- och omsorgsförvaltningen.*

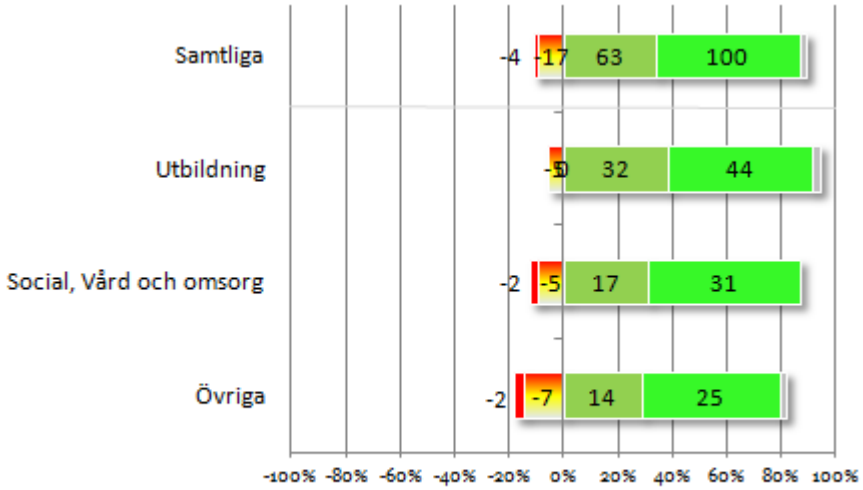
- *Dock inte i denna kommun, Vård- och omsorgsförvaltningen.*
- *Jag har agerat efter att jag vet att det rör sig om känsliga uppgifter. Någon utbildning har jag inte fått utan det handlar mer om sunt förnuft, Arbetsmarknads- och vuxenutbildningsförvaltningen.*
- *Det har inte förekommit info eller utbildning kring detta, Samhällsbyggnadsförvaltningen.*
- *Har inget minne av någon utbildning då det handlar om säkerhet, Annan.*

05. De rutiner vi har kring behörighetshantering känns trygga och säkra

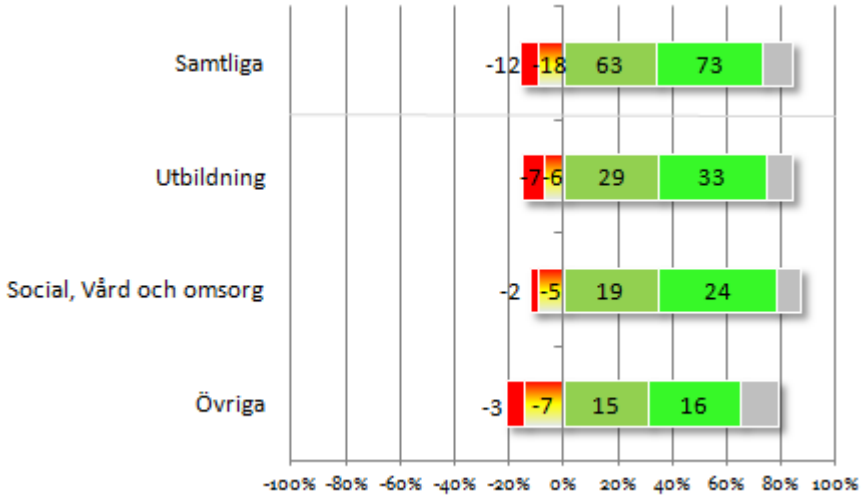


- *Svarar för de system jag känner till. Överlag i kommunen vet jag inte hur det ser ut med alla system. Dock - det pågående införandet av modellen för förvaltningsstyrning med strukturer, ordning och reda, vem ansvarar för vad o.sv. gagnar detta.*
- *Jag känner mig inte säker på att samma vikt vid t ex PUL läggs när barnen är på fritids eller på andra aktiviteter. Man hoppas att det efterlevs även då.*
- *Det saknas rutiner när användare slutar i kommunen. Användarkonton kan bli kvar i systemen.*
- *Dålig info generellt sett. Vilken info får de nyanställda? De som jobbat många år, innan datorerna gjorde sitt intåg, vilken info ha de fått? Vem ansvarar för att info om detta ska ges?*
- *VA-enheten har på eget initiativ styrt upp regler etc. kring detta. Inget förvaltnings- eller kommunövergripande har kommunicerats.*

06. Jag har tillräcklig kunskap kring vad jag ska tänka på kring utformning och hantering av mitt lösenord.



07.Jag bedömer att det är säkerställt att ingen kommer åt känslig information via min dator



- *Jag loggar oftast själv ut mig när jag lämnar datorn. Samt att jag låser rummet när jag lämnar det. Däremot har jag lappar med lösenord på rummet som nog lätt hittas om man letar. I det fallet är säkerheten noll, Utbildningsförvaltningen*

- *Skärmsläckare som slås på automatiskt finns och lösen krävs för att komma in i datorn. Kan väl inte påstå att jag alltid tar cntr/alt/delete när jag lämnar rummet, men försöker tänka på det, Kommunledningsförvaltningen*

- *Jag låser alltid när jag lämnar datorn. "dubbel" inloggning. Jag sparar allt i smart, Vård- och omsorgsförvaltningen.*

- *Skrämsläckare sätts på efter kort tid och då krävs kod, Utbildningsförvaltningen.*

- *Besökare kan lätt råka se andras personuppgifter på skärmen, Kultur- och fritidsförvaltningen.*

- *Jag har ingen kunskap i hur man lägger in t ex skärmsläckare med kod osv. Vi behöver låsbara skåp för våra datorer i närheten av klassrummet, Utbildningsförvaltningen.*

- *Skärmsläckare finns som kräver kod för åtkomst, Arbetsmarknads- och vuxenutbildningsförvaltningen.*

- *Måste logga in igen efter 10 min. Vet inte om det gäller andra datorer Utbildningsförvaltningen.*

- *Skärmsläckare som kräver kod finns aktiv, Vård- och omsorgsförvaltningen.*

- *Vet att eleverna lätt tar sig in i arken/first class. Elev har visat - frågade vems användare han skulle ta. Visade på två olika lärares användare. Informerade då skolledning om detta. Detta skedde för drygt två år sedan, Utbildningsförvaltningen.*

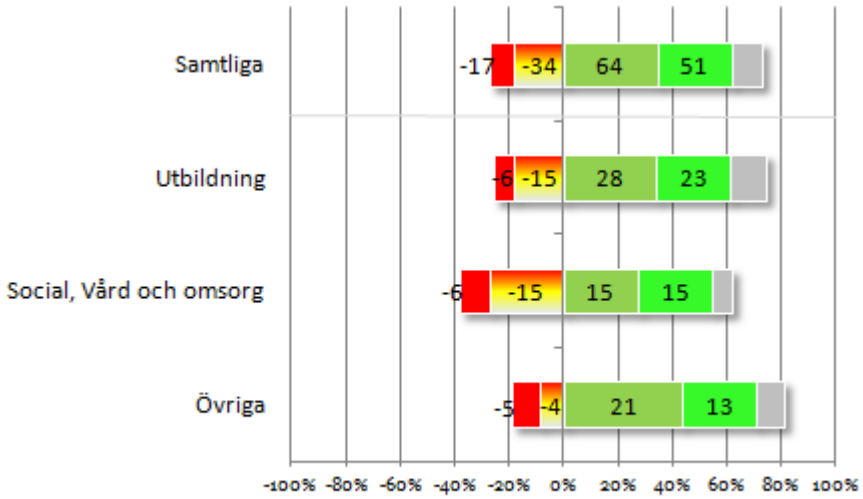
- *Skärmsläckaren kräver kod för åtkomst är den säkerhetsåtgärd jag känner till, Arbetsmarknads- och vuxenutbildningsförvaltningen.*

- *Tex kan it-personal antagligen komma åt samtliga filer på G: H: och tom C: via admininloggning. Är denna personal säkerhetsklassad? Hur administreras rättigheter etc. på gemensamma mappar?, Samhällsbyggnadsförvaltningen.*

- *Min kollega använder också min dator till och från, Annan.*

- *Skärmsläckare efter bara 2min som sen kräver lösen för att öppnas, Utbildningsförvaltningen.*

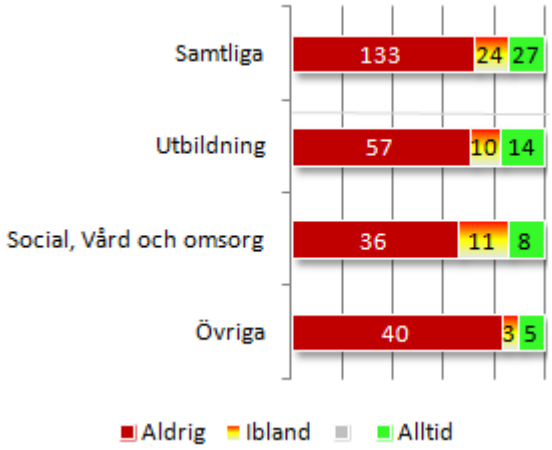
08. Då jag skriver ut känsliga dokument på vår/min skrivare så medför detta inga risker att obehöriga tar del av dokumenten



- *Hanterar inte den typen av dokument, men är det något jag inte vill ska bli läst av andra, ställer jag mig vid skrivaren och väntar på att utskriften är klar, Kommunledningsförvaltningen.*
- *Behörigheten till privat utskrift är inte tillgänlig efter inköp av ny skrivare, Socialförvaltningen.*
- *Det händer att när man skriver ut något så är det jätte viktigt att man kollar att rätt skrivare är inställd. De brukar vara rätt inställning men det har hänt ett antal gånger att den ändras och är man inte uppmärksam när kan skriver ut så kan en annan verksamhet få dina papper. Vet att verksamheten bredvid oss har samma adress och det har hänt att man skrivit ut papper som dem har fått. Sen om det just har varit sekretess info det har jag ingen aning om, Vård- och omsorgsförvaltningen.*
- *I bland ändrar sig skrivaren sig själv o kan då hamna någon annanstans i kommunen eller på huset, Vård- och omsorgsförvaltningen.*
- *Tidigare så RÅKADE utskrifterna skrivas ut på andra enheter i stället för på vår..vet dock inte om det är åtgärdat idag, Vård- och omsorgsförvaltningen.*
- *Skrivaren finns i lättillgänglig korridor, Utbildningsförvaltningen.*
- *Det händer sällan men utskrifter har skrivits ut på fel skrivare fast jag inte ändrade inställningar, Arbetsmarknads- och vuxenutbildningsförvaltningen.*
- *Skrivaren ligger i ett rum som alla anställda i huset har tillgång till, Arbetsmarknads- och vuxenutbildningsförvaltningen.*

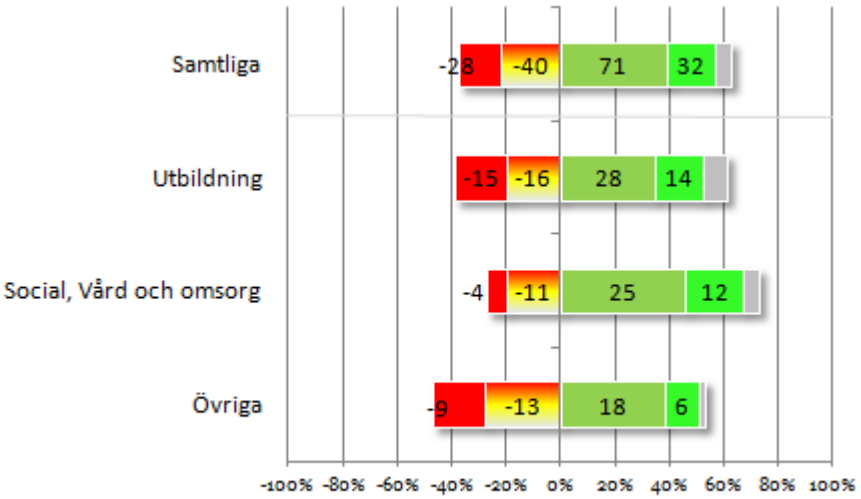
- *En liten feltryckning kan gå till vilken som helst enhet inom förvaltningen och läsas av vem som helst, Vård- och omsorgsförvaltningen.*

09. Jag lösenordskyddar mitt dokument vid utskrift.

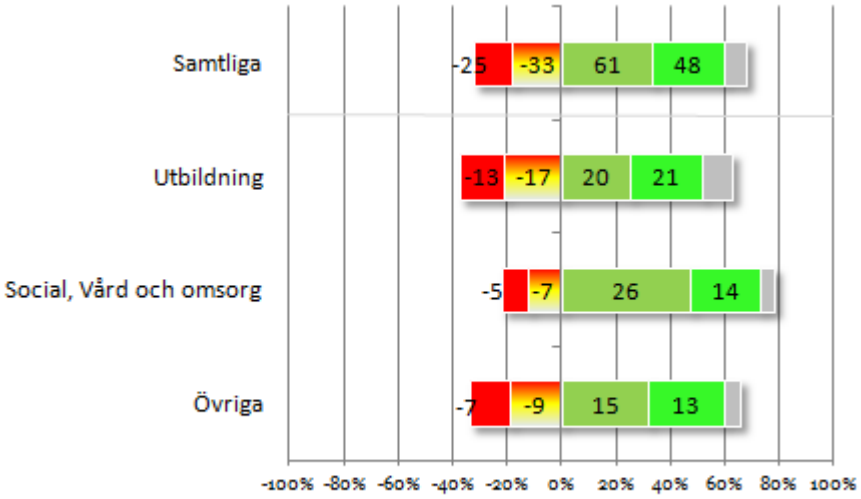


- *Det går ej, Socialförvaltningen.*
- *Jag brukar vara extra försiktig när jag skriver ut dokumentation men det är flera som har lånat mitt lösenord, det kan bero på att dem inte fått sitt lösenord ännu, Vård- och omsorgsförvaltningen.*
- *Vet inte hur man gör, Utbildningsförvaltningen.*
- *Vet inte hur man gör så jag skriver inte ut känsliga dokument på arbetsplatsen, Annan.*
- *Har inte den möjligheten, Kultur- och fritidsförvaltningen.*
- *Skriver ingen patient uppgift, Vård- och omsorgsförvaltningen.*
- *Jag själv måste alltid bevaka utskrift genom att DIREKT gå ut i korridoren och hämta det utskrivna dokumentet, Utbildningsförvaltningen.*
- *Har inte det behovet, Vård- och omsorgsförvaltningen.*
- *Vad är det?? och hur gör man, Kultur- och fritidsförvaltningen.*
- *Vet ej vad detta innebär, Utbildningsförvaltningen.*
- *Hur gör man det? Utbildning behövs!, Utbildningsförvaltningen.*

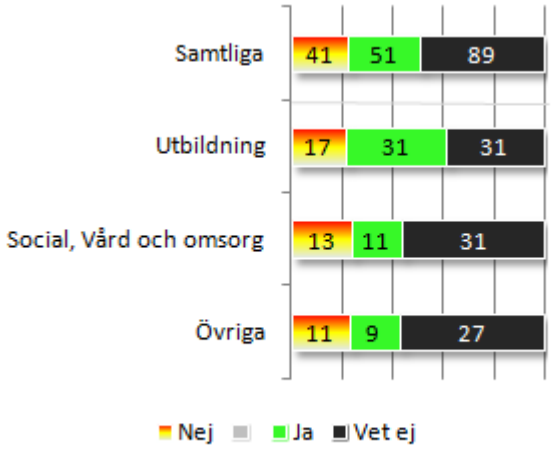
10. Det är tydligt för mig hur känslig skyddsvärd information ska sparas och hanteras?



11. Det är tydligt vart jag ska vända mig om jag misstänker brister kring vår behörighetshantering



12. Har du skrivit på ansvarsförbindelse för medarbetare i Botkyrka kommun?



13. Ge gärna förslag på hur behörighet till känslig information skulle kunna förbättras

Flera av de svarande anger utbildning och information.