# HUR SÄKRA ÄR VÅRA PERSONLIGA UPPGIFTER HOS E-TJÄNSTER?

— EN STUDIE OM FÖRSÄKRINGSKASSANS IMPLEMENTERING AV INFORMATIONSSÄKERHETSPOLICYN

Kandidatuppsats
Offentlig förvaltning

Elin Keskin
Alexandra Lampropoulou
Zainab Mohamud

**A-K2018:28**

HÖGSKOLAN I BORÅS

**Program:** **Offentlig förvaltning**

**Svensk titel:** **Hur säkra är våra personliga uppgifter hos e-tjänster?**
*En studie om Försäkringskassans implementering av informationssäkerhetspolicyn*

**Engelsk titel:** How secure are our private data through e-services?
*A study about Swedish social security agency's implementation of strategy concerning information safety*

**Utgivningsår:** 2018
**Författare:** Elin Keskin, Zainab Mohamud, Alexandra Lampropoulou
**Handledare:** Mikael Löfström
**Examinator:** Osvaldo Sala
**Nyckelord:** säkerhetspolicy, informationssäkerhet, säkerhetsmedvetenhet, chefers roll, implementering, offentlig sektor, Försäkringskassan

---

## Sammanfattning

Digitalisering av information inom offentlig förvaltning har väckt diskussionen kring informationssäkerhet, vilket har blivit mycket viktigt och nödvändigt för verksamheter under senaste tiden. På grund av digitaliseringen har organisationer infört ett utbyte av pappersrelaterat arbete till information och dokument via e-tjänster. För att kunna säkerställa att känsliga uppgifter skyddas implementerar offentliga organisationer policyn kring informationssäkerhet. Chefens roll och medvetenhet hos anställda kring informationssäkerhetspolicyns riktlinjer anses vara betydande för en lyckad implementering av förändringar. Syftet med studien är att analysera på vilket sätt Försäkringskassan i Göteborg har genomfört implementeringen av informationssäkerhetspolicyn hos sina e-tjänster, samt att upplysa om chefernas roll vid implementering av informationssäkerhetspolicyn och personalens medvetenhet kring policyns riktlinjer. Studier om informationssäkerhet har visat att det största hotet kommer inifrån, med andra ord kan en organisations anställda medvetet eller omedvetet utsätta en organisations informationssystem för risk genom att sprida eller dela känslig information med obehöriga. I denna studie har vi genomfört semistrukturerade intervjuer med både chefer och anställda inom Försäkringskassan i Göteborg för att kunna betrakta på vilket sätt implementeringen av informationssäkerhetspolicyn har påverkat verksamheten. Enligt resultatet har Försäkringskassan i Göteborg implementerat informationssäkerhetspolicyn under olika faser, men det som anses avgörande för att uppnå målet med policyn har varit att ha en tydlig plan, en förstudie och tydlig kommunikation om vad policyn innebär till alla inblandade vid implementeringen i ett tidigt stadie. Vidare har verksamheten använt olika strategier för att öka anställdas säkerhetsmedvetenhet genom broschyrer, skriftligt avtal och dokument, utbildningar samt workshops. Förutom detta har chefer följt en ledarstil som liknar transformellt ledarskap och på detta sätt ökat de anställdas motivation och prestation, samtidigt som det utförts kontroller och övervakning under hela implementeringsprocessen i syfte om att säkerställa att riktlinjer följs och att policyn efterlevs.

# Innehållsförteckning

# 1. Inledning

I detta kapitel beskrivs bakgrunden till uppsatsens ämne och en mer specifik beskrivning av problemområdet ges. Detta mynnar ut i uppsatsens frågeställning och vad syftet med att besvara denna är.

I dagens läge är det vanligt att offentliga organisationer använder digitaliserad information för att utföra sina vardagliga arbetsuppgifter inom verksamheten. Allt fler människor väljer att använda myndigheternas e-tjänster för att få hjälp med sina ärenden vilket leder till att en stor mängd information utbytes via myndigheters webbsidor och e-tjänster. Denna information berör ofta känsliga uppgifter och innehållet måste skyddas då myndigheter är ansvariga för att behandla denna information på ett säkert sätt. Förutom detta ställer en del lagar såsom personuppgiftslagen och offentlighets- och sekretesslagen större krav på att behandla känsliga uppgifter ansvarsfullt (Hagen, Albrechtsen, & Hovde, 2008). Dessutom har digitaliseringen av verksamheter samtidigt bidragit till en ökning av antalet hot mot säkerheten av den information som utbyts, vilket skapar en diskussion kring informationssäkerhet som är ett i synnerhet aktuellt ämne (Al-Hamdani & Dixie, 2009).

Med informationssäkerhet menas åtgärder som görs av en organisation för att säkerställa att all information som används inom organisationen hanteras korrekt, och att olaglig användning av denna information förhindras (Dhillon & Backhouse, 2000). När åtgärder som stödjer informationssäkerhet kring e-tjänster ses över är det i första hand tekniska åtgärder hos informationssystem som ligger i fokus (Hagen et al., 2008). Alla strategier som utvecklas för att skydda information inom e-tjänster formuleras som nya policyer och de måste implementeras i verksamheten så att myndigheter kan säkerställa att information skyddas. En policys implementering är en komplicerad process vilken utvecklas över tid, och det krävs att alla inblandade ständigt och försiktigt arbetar med olika handlingar så att policyn följs i praktiken (Hanberger, 2001).

Informationssäkerhetspolicy förklarar riktlinjer som skall tillämpas av personalen när de behandlar känsliga uppgifter som kommer in via e-tjänster. Däremot är det en utmaning att uppmuntra personalen för att följa policyns riktlinjer (Siponen & Vance, 2010). Det är viktigt att chefer och alla inblandade i implementeringen använder många olika sätt att förmedla och förklara till personalen kontinuerligt. På så sätt blir det lättare för personalen att förstå och se till att policyn stegvis blir en del av verksamhetens rutiner. Att uppnå medvetenhet kring informationssäkerhetspolicy är alltjämt essentiellt för policyns efterlevnad (Knapp & Ferrante, 2012). Säkerhetsmedvetenhet är ett begrepp som används för att förklara kunskapsnivån hos alla inblandade inom en verksamhet kring informationssäkerhet och säkerhetspolicys regler (Bulgurcu, 2010). Ökad medvetenhet bidrar till skapandet av en bra relation mellan anställda inom verksamheten och en känsla av att införandet av den nya policyn kommer till nytta för deras vardagliga arbetsrutiner. Detta bidrar till att minska sannolikheten för motstånd och ökar chansen att implementeringen av informationssäkerhetspolicyn uppnår sina mål (Alhogail, Mirza & Bakry, 2015).

En lyckad implementering av informationssäkerhetspolicy beror i hög grad på hur chefer kommer att hantera kommunikationen inom verksamheten för att skapa en bättre förståelse av policyns mål. Detta är betydande för verksamheten så att alla som medverkar är medvetna om informationssäkerhetspolicyns nytta och på så sätt engagerar de sig vid policyns implementering (Rokstad, Vatne,Engedal & Selbæk, 2015).

## 1.1 Syfte och problemformulering

Informationssäkerhetspolicy anses som ett verktyg som stödjer verksamheter i att vara förberedda inför potentiella risker och att skydda verksamheternas information (Whitman & Mattord, 2012). En stor del av den forskning som gjorts visar att upp till 70% av de incidenter som berör informationssäkerhet kring e-tjänster har sitt ursprung inom verksamheten, varför det anses som en verksamhets högsta prioritet att hantera denna risk, samt att utveckla strategier för att undvika ogynnsamma konsekvenser av sannolika hot mot informationssäkerheten (Hagen et al., 2008).

Studier har visat att de organisatoriska åtgärder som behövs för att uppnå informationssäkerhet varierar och att det inte finns endast en modell eller ett sätt som anses kunna vara underlag till att implementera informationssäkerhetspolicy inom alla verksamheter (Hagen et al., 2008; Dhillon & Backhouse, 2000). Däremot förekommer ett begränsat antal forskningar om hur offentliga organisationer i praktiken genomfört implementeringen av informationssäkerhetspolicyn inom organisationerna och på vilket sätt dessa organisationer lyckats uppnå informationssäkerhet hos sina e-tjänster (Flowerday & Tuyikeze, 2016; Hagen et al., 2008). I förhållande till detta är det tydligt från tidigare undersökningar inom informationssäkerhet att chefers roll i implementeringen av informationssäkerhetspolicy samt medvetenhet hos personal om säkerhetspolicyn är essentiella för att tillförsäkra informationssäkerhet inom verksamheter (Albrechtsen & Hovden, 2010). Däremot är det inte lika klart hur chefer i offentliga organisationer arbetar för att skapa förståelse kring säkerhetspolicyn hos personalen eller hur man når en högre grad av medvetenhet.

Denna studie inriktar sig till att täcka upp dessa luckor som förekommer från tidigare studier kring implementeringen av informationssäkerhetspolicy och skapa en tydligare bild av hur de offentliga organisationer genomför implementeringen av informationssäkerhetspolicy kring sina e-tjänster. Studien fokuserar på Försäkringskassans IT-avdelning, vilken är ansvarig för organisationens e-tjänster och implementeringen av informationssäkerhetspolicy.

Syftet med studien är att analysera på vilket sätt Försäkringskassan i Göteborg har genomfört implementeringen av informationssäkerhetspolicy om deras e-tjänster. Vi vill också upplysa chefernas roll vid implementering av informationssäkerhetspolicy och personalens medvetenhet kring policyns riktlinjer.

## 1.2 Frågeställningar

Syftet leder till följande frågeställningar:

På vilket sätt arbetar Försäkringskassan i Göteborg med att implementera säkerhetspolicyn kring sina e-tjänster?

a. Hur fungerar chefernas roller vid implementeringen av informationssäkerhetspolicy inom Försäkringskassan i Göteborg?

b. Hur väl medvetna är personalen hos Försäkringskassan i Göteborg om informationssäkerhetspolicyn?

# 2. Tidigare forskning

## 2.1 Vad innebär informationssäkerhetspolicy?

Vårt samhälle utvecklas ständigt, och detta har bidragit till att det har blivit enklare att hantera ärenden via datorer och Internet, vilket på så sätt har skapat en effektivare offentlig förvaltning. Informationssäkerhetspolicy är en policy som handlar om IT säkerhet och skydd av känsliga uppgifter som hanteras av olika organisationer (Bank, 1990). Enligt Bank (1990) är tillit mellan individer och organisationer betydande för att skapa en funktionell informationsteknik som är grunden till vad som utformar organisationen. Organisationer anses vara bundna till informationsteknik för att det gynnar deras ekonomiska hållbarhet och behovet av att hantera information. Det finns naturligtvis flera olika definitioner av informationssäkerhet. Bank (1990) påpekar att informationssäkerhetspolicy gör det möjligt att kunna tydliggöra olika riktlinjer för medarbetarna i organisationen gällande deras rättigheter och hur de bör behandla känslig information. Dessutom framkommer det i studien att om informationssystemet inte hanteras enligt organisationens policy kan detta bidra till framtida kostnader. För att motstå risker och problem som kan uppkomma bör man säkra informationssystemet och skydda informationen på bästa möjliga vis. Annars kan förlust av information uppstå, eller utnyttjande av känsliga uppgifter av obehöriga personer. Studiens resultat har visat att implementeringen av informationssäkerhetspolicyn måste vara en av organisationens prioriteter för att undvika besvärliga konsekvenser vilka kan leda till att organisationen förlorar sin integritet och medborgarnas tillit (Bank, 1990).

Enligt Zammani & Razali (2016) är informationssäkerhetspolicy (ISP) en uppsättning av regler som antas av en organisation för att säkerställa att alla användare samt IT-avdelningen inom organisationen (inklusive användare av e-tjänster) följer bestämmelserna om säkerheten för data som sparas digitalt inom gränserna vilka omfattas av organisationens utökade ansvarighet. Informationssäkerhetspolicy inriktar till att skydda tre huvudmål: 1. Sekretess - tillgången till data och information måste begränsas till personer som är behöriga och inte utlysas till obehöriga, 2. Integritet - hålla data intakta, fullständiga, korrekta, och IT-system operativa; 3. Tillgänglighet - ett syfte som anger att information eller system står till förfogande för behöriga användare vid behov (Zammani & Razali, 2016).

Deras studie upplyser om att organisationer skapar ISP av olika skäl, såsom att skapa en allmän inställning till informationssäkerhet, att upptäcka och förebygga kompromisser av informationssäkerhet som exempelvis missbruk av data, nätverk, datorsystem och e-tjänster. Andra anledningar kan vara att skydda organisationens rykte med hänsyn till dess etiska och juridiska ansvar, att tillvarata kundernas rättigheter och att tillhandahålla effektiva mekanismer för att svara på klagomål och frågor om verkliga eller uppfattade bristande överensstämmelse med policyn (Zammani & Razali, 2016).

Dessutom förklarar deras studie att en organisation som strävar efter att skapa en fungerande ISP behöver ha väldefinierade mål avseende informationssäkerhet samt en strategi för hur informationssäkerhet bör implementeras inom organisationen. Enligt studiens resultat är det avgörande att organisationen som vill implementera informationssäkerhet i sin verksamhet måste skapa ett dokument i form av en policy där alla riktlinjer kring informationssäkerhet presenteras tydligt och i detaljer. Språket som används i detta säkerhetspolicydokument måste vara enkelt för att förebygga missuppfattningar och garantera konsensus bland personal. Komplicerade uttryck måste undvikas och policyn bör formuleras kortfattat (Zammani & Razali, 2016).

## 2.2 Vikten av säkerhetsmedvetenhet

Bulgurcu (2010) hävdar att om organisationens anställda är mer medvetna om informationssäkerhet underlättar det processen för informationssäkerhetspolicyns implementering inom verksamheten. Författaren definierar informationssäkerhetsmedvetenhet som medarbetarnas övergripande kunskaper och förståelse av potentiella risker som relaterade till informationssäkerhet och dess konsekvenser. Förutom den allmänna säkerhetsmedvetenheten kring information som organisationen har finns det specifika förväntningar och krav på organisationens medarbetare. Organisationens medlemmar måste ha kunskap och förståelse för kraven som föreskrivs i organisationens informationssäkerhetspolicy och syftet med dessa. Säkerhetsmedvetenhet beskriver det tillstånd där medarbetarna är medvetna om informationssäkerhetspolicyn och om de är engagerade i sin organisations säkerhetsmål. Studien kommer fram till att organisationen möjliggör implementeringen av en säkerhetspolicy där det är oerhört viktigt att policyns innehåll är lättbegripligt och märkbart för användare i syfte om att skapa en ökad förståelse och säkerhetsmedvetenhet (Bulgurcu, 2010).

Knapp & Ferrante (2012) har visat att det också är viktigt att kontinuerligt vidta förebyggande åtgärder för att undvika motstånd som kan uppkomma bland anställda vilket kan bidra till att utsätta informationssäkerheten för risk. Författaren hävdar att de största säkerhetsproblemen kan uppstå vid omedvetenhet hos de anställda som inte förstår riskerna i samband med deras handlingar. Samtidigt påpekas i studiens resultat att organisationer behöver utveckla ett organisatoriskt träningsprogram för sina anställda med syfte att öka och stärka deras säkerhetsmedvetenhet för att övervinna detta problem (Knapp & Ferrante ,2012).

En annan studie analyserade effekterna av ett träningsprogram vars syfte är att öka säkerhetsmedvetenhet hos personalen inom en organisation, med fokus på de anställdas delaktighet, dialog och en kollektiv reflektion (Albrechtsen & Hovden, 2010). Träningsprogrammet består av olika aktiviteter där man med hjälp av experter fokuserar på att skapa förtroende i små grupper av deltagare, vilket ska leda till tydliga förändringar i deltagarnas beteende och medvetenhet kring informationssäkerhetsfrågor. Deras studie påpekar att medvetenhet och beteende bland personal är viktiga delar av en organisations informationssäkerhetsprestation. Därför är det viktigt att organisationen genomför utbildningar och använder olika sätt för att skapa och öka medvetenhet om säkerhetsfrågor hos de anställda. Enligt studiens resultat är delaktighet av personal vid organisationens utbildningar och träningsprogram betydande för att lyckas med att öka medvetenhet och efterlevnad av säkerhetspolicys implementering. Studien visade att utifrån statistiska analyser var träningsprograms påverkan kraftfullt och ledde till en ökning av deltagarnas medvetenhet kring informationssäkerhet (Albrechtsen & Hovden, 2010).

Författarna av studien förklarar vidare att det finns flera åtgärder som kan vidtas för att förbättra användarnas informationssäkerhetsprestation, såsom distribution av meddelanden via exempelvis broschyrer, e-postmeddelanden, intranät, affischer, formella presentationer, lunchmöten och kurser (Albrechtsen & Hovden, 2010). Det som de flesta av dessa åtgärder har gemensamt är att det här rör sig om envägskommunikation från myndighetens ledning till enskilda individer genom olika kanaler. Å andra sidan anses de anställdas engagemang och delaktighet vid detta försök att öka medvetenhet är både nödvändigt och effektivt för att uppnå alla slag av organisatoriska förändringar liksom informationssäkerhetspolicy. Studien påpekar att medarbetarnas motivation och intresse för interventionen har varit utmärkt och att detta var en av huvudorsakerna till framgångsrika förändringar av medvetenhet och beteende.

Den avslappnade och humoristiska atmosfären och det aktiva sättet deltagarna var involverade i interventionen bidrog till medarbetarnas motivation att vara med och följa riktlinjer under studiens gång (Albrechtsen & Hovden, 2010).

### 2.3 Chefens roll

En chef har den dominerande ställningen och är ansvarig för att skapa en välfungerande kommunikation och att kunna tillgodose organisationen med den nödvändiga strukturen för att möjliggöra detta. Chefers roll är att kunna ha inflytande hos medarbetarna och deras arbete och bevaka att arbetet följs enligt organisationens regler (Johansson & Miller, 2012). Enligt Johansson (2013) framgår det att bra kommunikation mellan chefer och medarbetare leder till positiva resultat vid implementeringen av en policy. Studien har visat att en chef måste kunna utforma, utveckla, engagera sig vid implementeringen av en policy medan det samtidigt är viktigt att kunna tydliggöra mål och planera, samt att uppmuntra och engagera medarbetarna. Chefens engagemang och inflytande inom organisationen blir omfattande när chefen är öppen och tillgänglig för medarbetarna (Johansson, 2013).

Enligt Fairholm (2004) finns det behov inom den offentliga förvaltningen för legitimitet hos chefer som utövar chefskap i sitt arbete för att komplettera de traditionella funktionerna i organisations hantering och policyimplementering. En annan studie upplyser att offentliga administratörer behöver inte bara praktiskt och intellektuellt tillstånd för att utöva chefskap, men också en praktisk och intellektuell förståelse för vad chefens roll innebär (Behn, 1998). Behn (1998) beskriver att chefers roll är betydande för att kunna hantera uppkommande problem inom offentliga verksamheter effektivt. Utifrån studiens resultat framkommer det att chefernas roll begränsas inte bara till att hantera problem som uppstår inom organisationen. För att organisationer och myndigheter ska fungera bör chefer skapa initiativ, motivation och inspiration mellan medarbetarna. Vikten ligger inte på hur chefer i den offentliga sektorn leder utan snarare vilken typ av ledarstil de utövar (Behn, 1998).

## 3. Teoretisk referensram

I detta avsnitt presenteras olika begrepp och teorier som kopplas ihop med studiens syfte för att skapa en bättre förståelse kring studiens ämne. För att underlätta läsaren är avsnittet uppdelat i olika rubriker.

### 3.1 Hur implementeras en policy?

Implementering avser en "*grupp av aktiviteter som inriktar sig för att genomföra en aktivitet eller ett program som har med kända dimensioner.*" (Durlak & DuPre, 2008). Implementeringsprocessen är målinriktad och aktiviteten eller programmet som implementeras beskrivs på så sätt att oberoende observatörer kan upptäcka aktivitetens eller programmets närvaro och styrka. Implementeringens kvalitet är avgörande för att uppnå resultat (Durlak & DuPre, 2008).

Ottoson och Green (1987) anser att "*implementering är en iterativ process där idéer uttrycktes som policy och omvandlas till beteende och betraktas som sociala åtgärder*" (p. 362). Den sociala åtgärden som omformas från policy riktar sig till en social förbättring och kommer i uttryck oftast som program, förfarande, regler eller praxis (Ottoson & Green, 1987). Policyimplementering innebär att samordna åtgärder mellan flera organisatoriska aktörer och

alla inblandade i implementeringen. Relationerna och samverkan mellan myndigheter och organisationer inom en implementeringskedja växer och blir mer komplicerade, eftersom de nya nätverken kommer fram inom policyimplementering. Nätverk kan variera i struktur, storlek och komplexitet och de omfattas bland annat av partnerskap, koalitioner och konsortier (O'Toole, 2000). De organisatoriska nätverksstrukturerna antas skapa fördelen av en ökad samverkan mellan organisationerna och ger organisationer potential att uppnå vad inget enskilt program eller organisation skulle kunna åstadkomma på egen hand. Samtidigt införs nya utmaningar kring nätverk under implementeringen, eftersom flera företrädare sammanträder med var och en om olika intressen och mål (O'Toole, 2000).

***Olika faser vid implementeringen***

Implementeringen har olika faser. I första fasen skall en förstudie förberedas. Det är i detta stadie som utvecklaren av implementeringen skall föra vidare processen till nästa stadie. Det är viktigt att ha rätt kvalifikation till införandet för att inte misslyckas med implementeringen samt att utnyttja alla resurser maximalt för att skapa en lyckad implementering av policy (Tonnquist, 2016: 308). Andra fasen består av planering och i denna fas skall varje detalj och villkor inom policyns implementering noggrant analyseras. Det tas hänsyn till om det förekommer ändringar som bör åtgärdas eller tilläggas i implementeringen. Att skapa en lyckad introduktion till anställda om vad implementeringen innebär och hur implementeringen kommer att utföras underlättar implementeringens process och minskar risker av potentiella konflikter från anställda (Tonnquist, 2016: 310). Tredje fasen blir ett genomförande av policy och resultatet utvärderas av styrgruppen om huruvida implementeringen har lyckats att uppnå målet (Tonnquist, 2016: 314).

***Uppkomande motstånd***

Det är möjligt att motstånd kan uppkomma vid genomförande av implementering. Att inte vara engagerad eller att inte uppvisa resultatet för medarbetarna kan vara problematisk då de kan vara väldigt skeptiska om hur resultatet påverkar deras arbete. Chefer brukar vara engagerade från början till slutet vid införandet av implementering medan anställda får chans att medverka när implementeringen har slutförts. När anställda inte är väl informerade om förändringar som uppkommer med implementeringen av ny policy är det möjligt att de blir oroliga och rädda inför den kommande förändringen. Motstånd kan förekomma och på så sätt förhindra implementeringen att uppnå sitt mål. Rädsla och oro påverkar negativt anställdas prestation medan det är möjligt att individer ur personalen bestämmer sig för att säga upp sig för att sedan hitta en enligt deras uppfattning bättre arbetsplats med en tryggare arbetsmiljö (Tonnquist, 2016 :298-299).

***Implementerings misslyckande***

Misslyckande av implementeringen inträffar när en aktivitet eller program finns som teori men inte fullgörs ordentligt i praktiken. Några orsaker till att en implementering misslyckas omfattar saker som brist på resurser, brist på utbildning samt otillräcklig erfarenhet hos personalen. Andra orsaker till misslyckande kan också relateras till i vilken utsträckning programmet eller aktiviteten implementeras med trovärdighet till den ursprungliga planen eller att man saknar kvalitetsanpassning (Durlak & DuPre 2008; Wandersman 2009). Implementering av en ny policy kräver stöd av systemet. Det är omöjligt att lyckas utan ett system som främjar kvalitet inom organisationen samt ett gynnsamt politiskt klimat. Det är heller inte möjligt att lyckas utan en tillräcklig kapacitet hos systemet att genomföra ett program, en aktivitet eller en strategi. Stöd kan ges i form av infrastrukturstöd (t.ex. ledarskap, kompetens, motivation) och kapacitet kan uppnås genom utbildning, teknisk assistans eller coaching (Wandersman, 2009).

***Uppifrån-ner modellen***
Vidare finns det enligt Hill (2012:183) ett perspektiv som heter uppifrån-ner modellen och det används vid genomförande av implementering. Detta perspektiv illustrerar en stadiemodell som förklarar utförandet från en policy till dess implementering. Organisationer använder ofta implementeringen av den nya policyn för att införa förändringar av den arbetsmetod som används i verksamheten. Målet med dessa förändringar är att förbättra organisationers effektivitet. Innan införandet av implementering är det viktigt att bestämma vem som formulerar policyn, vem som beslutar om implementeringen och vem som verkställer implementeringen (Hill, 2012:183). Formuleringen av policy och implementeringsprocess är ledningens ansvarighet medan alla andra inblandade i organisationen har som roll att verkställa implementeringen av policyn och följa ledningens riktlinjer. Det blir så kallad att "*implementeringen följer efter formulering och beslut",* menar Hill (2012: 183). När formuleringen av policyn är klar är det viktigt att planera på vilket sätt policyn förmedlas mellan olika medarbetare inom organisationen. För att slutföra implementeringen framgångsrikt är det grundläggande att alla inom organisationen är medvetna om de förändringar som ingår i policyn, och att de arbetar i linje med denna (Hill, 2012:184).

Däremot finns det kritik mot uppifrån-ner modellen som presenterats. Formulering av policy måste följa vissa regler för att vara tydlig och kunna medföra samma innebörd för alla som blir påverkade av policyn. Det finns två olika modeller som kan användas vid policyns formulering och det är antingen en generell hållning eller en påtaglig utformning. Policy i den allmänna hållningen kan betraktas som åtgärder med strikta riktlinjer. Å andra sidan i den konkreta utformningen av policyn förklaras policyn med enkla riktlinjer vilka är lättförståeliga för alla (Hill, 2012:186). Det beror på organisationens natur vilken modell som passar bäst för formuleringen av en ny policy. Det är inte alltid tydligt om implementeringen av en policy tillämpas i organisationens verksamhet eller om det är helt meningslöst. Vissa policyer blir bara symboliska då de inte bidrar till att önskade resultat uppnås (Hill, 2012:186).

Samtidigt kan utformningen av policy vara statligt ingripande vilket innebär att det är svårt att införa förändringar för att anpassa policyns riktlinjer till olika organisationers behov. Det statliga inflytandet brukar oftast inbegripa ökningar eller minskningar av resurser medan åtgärder redan är fastställda. Detta kan förhindra implementering och det blir komplicerat att skapa ett bra samband mellan förändringar och åtgärder som förekommer (Hill, 2012:187).

## 3.2 Att leda implementering effektivt

Ledarskap förklaras av litteraturen som ett svårdefinierat begrepp vilket oftast relateras till en del andra begrepp liksom makt, ledning, befogenhet, kontroll, administration och övervakning (Yukl, 2012:311). Det är svårt att formulera en tydlig och övergripande definition vilken på ett bra och fullständigt sätt beskriver vad ledaskap innebär (Maltén, 2000: 150). Maltén (2000:203) hävdar att ledarskap är nyckeln till att kunna skapa de nödvändiga förutsättningar som behövs för att uppnå uppsatta mål inom en organisation.

Dessutom finns det förutom ledarskap några andra begrepp vilka oftast kopplas samman och anses som närbesläktade. Chef, chefskap, ledare och ledarskap är fyra sammankopplade begrepp som ofta används i samma kontext. Begreppen chef och ledare är förknippade med positioner, roller och individer. En chef företräder en formell position i en organisation som

tilldelas denna av andra högre befattade chefer eller styrelse, och har oftast befogenhet att fatta beslut, samt ansvar att sätta mål som organisationens anställda ska arbeta mot (Yukl, 2012:147). Chefskap handlar om arbetsledning, styrning och kontroll (Yukl, 2012:176). Ledarskap definieras på olika sätt i forskning beroende på vilket perspektiv man utgår från, till exempel individuella egenskaper, ledarstilar eller beteenden. Däremot innebär detta inte att alla chefer anses vara ledare (Fairholm, 2004). Till skillnad från en chef kan en ledare beskrivas som en person som har förmågan att uppmuntra organisationens anställda till att sträva framåt för att uppnå ett uppsatt mål. En ledare styrs inte av någon instruktion eller ett regelverk, utan snarare av kunskap och personliga egenskaper som bidrar till att ledaren kan motivera sina anställda att engagera sig i uppfyllelsen av organisationens behov (Yukl, 2012:193).

Implementering av en policy betraktas inte som en del av ledarskaps utövande istället anses det som ledarkaps natur (Hrebiniak, 2006: 13). Det är emellertid viktigt att ledarkapet verkställas enligt vissa ramar och riktlinjer som bestäms innan implementeringens gång. Ledarskapet har en stor betydelse i implementeringsprocessen för att det är upp till ledaren att kunna sätta igång processen och utveckla en strategi för att lösa uppkommande problem på en effektivt och framgångsrikt sätt (Blomquist & Röding, 2010). Blomquist & Röding (2010) handlar om att ett lyckat ledarskap kan hindra motstånd och konflikter mellan personal genom att engagera alla inblandade till att samarbeta med varandra. Istället för att vara skeptisk mot uppkommande motstånd måste en ledare vara förberedd att minska motstånd för att främja implementeringen. Däremot anses inte alla konflikter och motstånd inom organisationen som ett hot mot arbetsmiljö. Vissa av dem kan leda till effektiva diskussioner mellan personal och ledningen och på så sätt uppmuntrar utvecklingen och förbättrar verksamhetens prestation. Förutom ledarens förmåga att undvika eller lösa konflikter och motstånd vid implementeringen av en ny policy är det också betydande att ledaren samordnar arbetet under implementeringen så att alla inblandande fokuserar sin arbetsinsats mot uppsatta mål (Tonnquist, 2016: 356).

### 3.2.1 Transformellt ledarskap och ledarbeteende i implementering

Implementeringen av en ny policy införs inom en organisations verksamhet förändringar i form av nya arbetsmetoder vilka påverkar medarbetarnas arbetssätt och dagliga arbetsrutiner (Gifford, Davies, Edwards, Griffin & Lybanon, 2007). Ledningens beteende vid förstudie stadium samt pågående under implementeringen, är av stor vikt för att tillförsäkra att implementeringen uppnår uppsatta mål med framgång. Aktiviteter som väljs från ledaren inom en organisation, för att underlätta implementeringen av en policy och uppmuntra personal engagerar sig aktivt vid implementeringens arbete, förklarar ledarens beteende och vilket ledarskapsstil ledaren väljer att följa. Det finns olika kategorier av ledarbeteende beroende på vilka aktiviteter inriktar ledaren till liksom att främja kommunikation mellan chefer och anställda, att stödja personal under implementeringsprocess, att skapa möjlighet till återkoppling vid alla steg av implementering, att kunna vara en förebild till medarbetarna, att inspirera personal till vidareutveckla sina förmågor och påverka positivt omgivningen (Gifford et al., 2007).

Enligt Backström, Granberg & Wilhelmson (2008) anses ledarskapsstil om transformellt ledarskap som ett slag av ledarskapsstil vilket relateras oftare till implementeringsarbete på grund av sin natur att stödja utvecklingen och förändringar inom organisationen. Ledaren som väljer att leda utifrån transformellt ledarskapsstil fokuserar på att väcka intresse hos medarbetaren angående uppkommande förändringar i deras arbetsrutiner och motivera de

utföra sina arbetsuppgifter effektivare i samband med införandet av dessa förändringar (Avolio, Walumbwa & Weber, 2009). En transformell ledare har förmågan att vägleda och påverka positivt medarbetaren till att uppnå uppsatta mål oberoende av organisationens kultur och kontext (Den Hartog, House, Hanges, Ruiz-Quintanilla & Dorfman, 1999). En ledare anses som transformell ledare när sitt arbete inriktar till att skapa motivation mellan medarbetarna, arbeta kreativt för att lösa konflikter, prioritera och underlätta diskussioner, vägleda medarbetaren och framförallt när ledaren försöker att vara en förebild för medarbetarna och inspirerar alla inom verksamheten (Bass, Avolio, Jung & Berson, 2003).

Chefer inom organisationen som vill följa transformell ledarskapsstil vid implementeringen av en ny policy måste först och främst vara tillgängliga till medarbetaren och öppna till diskutioner. På så sätt blir det lättare för chefen att informera och uppdatera medarbetaren kring implementeringens genomförande och mål medan samtidigt kan chefen förklara missuppfattningar kring nya policy på ett tidigt stadium innan dessa missuppfattningar väcker oro och konflikter. Förutom detta är det viktigt att chefen inspirerar personal att följa nya arbetsrutiner som implementeras genom att följa dessa rutiner sig själv och ge positiv återkoppling till medarbetare som anpassar stegvis deras arbetssätt till nya riktlinjer. Positiva återkopplingar möjliggör att fler medarbetaren kommer att motivera sig med att arbeta på samma sätt och eftersträva till att uppnå implementeringens mål. Enligt transformell ledarskapsstil är det en av chefens prioritet att uppmuntra medarbetaren uttrycka sina tankar och ideer om hur deras arbetsrutiner bör förändras för att förbättra verksamheten och öka effektivitet. På det sätt får chans medarbetaren att vara delaktiga i förändringsprocessen och komma fram med ideer vilka kan bidrar till utvecklingen av verksamheten (Bass et al., 2003).

Dessutom är det chefens ansvarighet att vara medarbetaren väl informerade kring implementeringen och uppkommande förändringar samt att chefen uppdaterar kontinuerligt alla inom organisationen om implementeringsprocess både muntligt i dagliga möten och skriftligt via mejl och annonser. Chefen som anses att de följer en transformell ledarskapsstil måste erbjuda utbildningar och träningsprogram till personal så att medarbetaren ska kunna utveckla vidare deras förmågor och skapa förståelse av vad nya arbetsrutiner innebär. Genom utbildningar ökar personal kunskapen som behövs för att utföra deras arbetsuppgifter enligt nya riktlinjer när implementeringen av förändringar slutförts (Bass et al., 2003).

Bass et al. (2003) hävdar att chefer som engagerar sig med att leda och införa implementeringen av nya policy inom en verksamhet, måste övervaka processen och anpassa alla aktiviteter för att informera, motivera, inspirera och utbilda personal i enlighet med nya policy för att öka chanser att implementeringen uppnås sitt mål och slutförs framgångsrikt. Ett effektivt ledaskap innebär ett aktivt ledarskap vilket motsvarar till en ledare som arbetar kontinuerligt under implementeringensgång och är positiv till att göra förändringar i sin strategi ifall återkopplingar från medarbetaren visar att implementeringen är svårt att genomföras (Bass et al., 2003).

Sist men inte minst förklarar teorin om transormellt ledarskap att en karismatisk chef måste alltid förbereda sig inför uppkommande konflikter och motstånd under implementeringens gång och särskilt i början av implementeringen (Backström et al., 2008). Förändringar i arbetsrutiner och dagliga uppgifter skapar oro, obekvämligheter och även rädsla till medarbetaren vilka är tveksamma om de kan utföra de nya rutiner som införts. Oron och rädsla kan leda till konflikter och motstånd inom verksamheten vilket kan förhindra implementeringen. Brist av tillräckligt kommunikation mellan ledningen och medarbetaren kring implementeringens syfte är en anledning som leder till motstånd. Förutom detta är det

möjligt att medarbetaren känner sig att de inte har tillräckligt kunskap eller förmågor för att utföra de nya arbetsrutiner eller att de inte har vilja att förändra deras rutiner för att de tycker att nya rutiner är meningslösa för deras arbete (Michie, van Stralen & West, 2011). Chefen måste planera i förväg att motivera medarbetaren vara delaktiga till utbildningar vilka kommer att fördereda dem inför implementeringen av nya rutiner. Det är också viktigt att chefen redan i början av implementeringen förmedla till medarbetaren alla information kring nya policy och tydliggöra vikten av införandet implementeringen för verksamhetens effektivitet (Michie et al., 2011).

### 3.3 Att skapa säkerhetsmedvetenhet

Enligt Flowerday & Tuyikeze (2016) har implementeringen av policyn tydliggjort att efterlevnad av en policy inom verksamheter i stor utsträckning beror på hur pass väl informerad personalen är om förändringar som införs, samt anställdas förståelse om nya rutiner och riktlinjer som måste följas. I samband med detta är det viktigt för organisationer att främja säkerhetsmedvetenhet mellan personal i en verksamhet för att kunna tillförsäkra att policyn om informationssäkerhet implementeras och följs långsiktigt. Grunden för att kunna lyckas med säkerhetsmedvetenhet är att uppmuntra förändringar av individers beteende när det gäller hantering av känslig information. Förändringar i beteende och attityder är en process som tar lång tid och kräver ständigt arbete från en organisations ledning, och genom utbildning och träningsprogram kan denna process underlättas och hjälpa organisationer att öka medvetenhet om informationssäkerhet mellan personal (Kruger & Kearney, 2006).

#### 3.3.1 Principer för informationssäkerhetsmedvetenhet

En organisation måste förbereda sig och skydda sin verksamhet från potentiella hot och risker mot informationssäkerhet, men det är också viktigt att erbjuda personalen utbildningar och träningsprogram som syftar till att hjälpa dem att förvärva ett lämpligt beteende när det gäller informationshantering, vilket bidrar till en lyckad implementering. Frye (2007:180) hävdar att det finns tre principer som måste tas hänsyn till för att skapa säkerhetsmedvetenhet inom en organisation. Först och främst används medvetenhet för att stimulera, motivera och påminna personal om vad som förväntas av dem. Den andra principen är träning, som anses vara en process som skapar lärande hos personal av en färdighet eller användningen av ett nödvändigt verktyg. Den tredje principen är utbildning, det specialiserade och djupgående lärande som krävs för att stödja verktygen eller förändringsprocessen. När en organisations ledning bestämmer sig för att utveckla en utbildning för att stödja informationssäkerhetsmedvetenhet bör organisationens personalavdelning samarbeta med IT-avdelningen för att säkerställa att utbildningen behandlar ämnesområdet tillräckligt, men också att den överensstämmer med relevanta lagar och förordningar (Frye, 2007:181).

Träningsprogram som genomförs inom organisationen betraktas inte som en process som alltid anpassas till alla anställda oavsett innehållet av träning. Detta för att det finns flera anställda med olika uppgifter och olika behov när det gäller IT-säkerhet. Ett tydligt exempel är att en högt uppsatt chef inte skall behöva lära sig den procedur man följer på en operativ nivå för att släppa information. Istället är det viktigt att lära sig att de aldrig bör handleda någon att släppa känslig information om de inte är 100 % säkra att kravet på informationen är legitim (Frye, 2007:182). Organisationen måste säkerställa att det finns ett spår av hur informationen utbytes och behandlas. Därför bör känslig information aldrig spridas efter endast efter en verbal begäran från någon medarbetare utan kontroll. Medarbetaren "behöver inte veta” vem som kommer att få del av informationen, eller hur informationen kommer att

användas, men de har rätt att veta att begäran är legitim samt vem som har behörighet att göra begäran om känslig information (Frye, 2007:182).

### 3.3.2 Metoder för att utbilda och träna personal

Frye (2007: 182) förklarar att det finns olika metoder för att träna och utbilda personal kring informationssäkerhet och hjälpa medarbetarna att skapa förståelse om vad som krävs för att skydda känslig information. Föreläsning är den mest traditionella träningsmetoden vilken ganska ofta används i organisationer. Föreläsning är idealisk för att få en "överblick" av begreppen och en förklaring av införandet ur ett teoretiskt perspektiv. En annan metod som ofta används är workshops. I en workshop är målet för deltagarna att aktivt delta i lärandet i motsats till föreläsningens passiva miljö. Workshops är korta i tid och hålls på deltagarnas arbetsplats medan deltagarna ofta delas in i mindre grupper, och de ämnen som omfattas kan då lättare anpassas till gruppens specifika krav. Möten är en annan metod att genomföra utbildning på. En mötesledare underlättar i det här fallet utbildningen och den kan också anpassas till ämnena som berör gruppens specifika behov (Frye, 2007:183). En annan metod är utbildning på arbetsplatsen vilket är ett sätt att snabbt lära en arbetare hur man utför en uppgift och denna metod har sju steg: 1. Visa arbetstagaren hur man utför uppgiften, 2. Förklara viktiga punkter av uppgiften, 3. Tillåt medarbetaren titta på när man utför uppgiften, 4. Tillåt medarbetaren utföra de enkla delarna av uppgiften under övervakning, 5. Hjälp medarbetaren att utföra hela uppgiften, 6. Övervaka arbetstagaren under tiden de utför hela uppgiften själv, 7. Tillåt medarbetaren att utföra uppgiften helt ensam. Förutom dessa metoder finns det också andra sätt att utföra utbildningar som träning med stöd av dator och webben. Dessa metoder är multimediaträning, träning via webben och diskussionsgrupper i nätverk. Dock används dessa metoder sällan i den offentliga sektorn (Frye, 2007:184).

Organisationer måste kontrollera verksamheten regelbundet för att kunna upptäcka om säkerhetspolicyn följs och i vilken grad de anställda följer regler och rutiner angående informationshantering. Ett viktigt underlag för att öka chansen att säkerhetspolicyn inte nonchaleras av personalen är att uppmärksamma dem om konsekvenser och risker för organisationen ifall informationen behandlas på ett oetiskt och olovligt sätt. Flera studier har föreslagit att organisationens ledning oftast måste påminna personalen om de riktlinjer som skall följas även om det anses att säkerhetspolicyns implementering har varit lyckad. Detta då det bidrar till en ständig ökning av säkerhetsmedvetenhet. Det finns några aktiviteter vilka anses vara effektiva när det gäller att regelbundet påminna personalen om säkerhetspolicyn. En av dessa aktiviteter som används allmänt av många verksamheter är instruktioner som gäller lösenord i datorer på arbetsplatsen som måste bytas ofta och som måste följa specifika riktlinjer för att vara starka så att informationssystemet skyddas från externa hot. Andra sätt att göra påminnelser om informationssäkerhet är att dela riktlinjer via mail eller genom broschyrer på arbetsplatsen, medan diskussionen om informationshantering under möten anses som vara ett i synnerhet effektivt och direkt sätt att fånga de anställdas intresse om informationssäkerhetsfrågor (Kruger & Kearney, 2006 :295).

# 4. Metod

Syftet med detta kapitel är att analysera och beskriva de forskningsmetoder som vi använder oss av för att utföra denna studie.

## 4.1 Val av strategi

I denna rapport har vi valt att använda en kvalitativ forskningsstrategi. Vi anser att det är mer lämpligt att undersöka människors reflektioner och betrakta deras åsikter kring valda ämnet istället för att samla siffror och genomföra mätningar för att kunna besvara studiens frågor. Genom en kvalitativ forskning ökar vi förståelsen om Försäkringskassans arbete kring implementering av informationssäkerhetspolicyn utifrån anställdas åsikter och chefers beskrivningar av hur implementeringens arbete genomförde inom verksamheten. Bryman (2018:61) förklarar att en kvalitativ forskning har en annan tolkning i jämförelse med en kvantitativ forskning. Den kvalitativa forskningen fokuserar mer på ord och reflektioner av människor och inte siffror eller mätningar av kvantitet.

## 4.2 Val av metod

I denna studie använder vi oss av kvalitativa intervjuer och mer specifik semistrukturerade intervjuer för att intervjua både chefer och anställda hos Försäkringskassan. Vi har valt semistrukturerade intervjuer för att intervjua både chefer och anställda hos Försäkringskassan. Anledningen till detta är att vi ville ha en flexibilitet vid intervjuer och hjälpa de intervjuade att uttrycka sig i en viss fråga på många olika sätt utan att behöva följa specifika regler eller strukturer i sina svar. Vi ville också uppmuntra respodenterna att vara öppna och utveckla sina svar på ett beskrivande sätt så att vi får bättre insyn i informationssäkerhetspolicyns implementerings process. Enligt Bryman (2018:561) är intervjuer den vanligaste metoden bland kvalitativa forskare. De två huvudtyperna av intervjuer som används i det kvalitativa tillvägagångssättet är de ostrukturerade intervjuerna och de semistrukturerade intervjuerna (Bryman 2018: 562-563). Enligt Bryman (2018: 563) kan respondenterna själva välja på vilket sätt de besvarar frågorna och beroende av vad de säger kan uppföljningsfrågor uppkomma.

Semistrukturerade intervjuer hjälpte oss att upptäcka olika problem som respondenterna märkte utifrån deras erfarenhet inom Försäkringskasssan samt deras upplevelser vid implementeringen av säkerhetspolicyn vilka skulle vara svåra att identifieras och komma fram via andra metoder. På samma sätt förklarar Bryman (2018: 564) att semistrukturerade intervjuer tillämpas vid undersökningar som behandlar ett specifikt ämne och respondenterna behöver diskutera vissa frågor med fokus på valda ämnet.

Genom semistrukturerade intervjuer fick vi också chans att analysera olika vinklar angående implementeringen av säkerhetspolicyn och hur arbetet genomförts i organisationen vilket i sin tur bidrar till att kunna besvara studiens frågeställningar. Vi valde att intervjua både chefer och anställda av olika avdelningar i Försäkringskassan och på så sätt kunna undersöka ämnet från olika aspekter. Olika synpunkter underlättat oss att dra mer tillförlitliga slutsatser och samtidigt identifiera på vilket sätt Försäkringskassan arbetat för att uppnå informationssäkerhet vid olika nivåer inom verksamheten. Enligt Bryman (2018: 564) beskrivs det som en annan fördel som semistrukturerade intervjun innehåller som metod. Semistrukturerade intervjuer möjliggör tillgång till många respondenter. I sin tur hjälper det till insamling av olika uppfattningar om fenomenet under diskussion som bidrar till undersökningens kvalitet och objektivitet (Bryman, 2018: 564).

Vi använde oss av två olika intervjuguiden en för cheferna och en för anställda för att vi ville ställa olika frågor till de kring implementeringen. Vi ville identifiera vad var chefenas roll vid implemeteringen av informationssäkerhetspolicyn medan samtidigt vi ville betrakta anställdas

medvetenhet om policyns riktlinjer. Därför var det viktigt att ställa olika frågor till intervjuade beroende av deras position i organisationen för att kunna besvara ordentligt våra frågeställningar och få en helhetsbild av hur implementeringen har genomförts. Däremot hade respondenterna frihet att besvara och diskutera frågor som de tyckte var viktiga även om dessa inte förekom i intervjuguiden. Detta möjliggjorde att författarna kunde fråga och diskutera mer i djup kring fler aspekter kring implementeringen av säkerhetspolicyn i Försäkringskassan, både från de anställdas och chefernas synpunkter. Enligt Bryman (2018:563) behöver semistrukturerade intervjuer en viss grad av struktur och förberedelse så att forskaren kan säkerställa att alla teman som har inverkan på undersökningen kommer att diskuteras under intervjun. Det är rekommenderat att använda sig av en intervjuguide och att följa flödet i denna, även om en sådan inte är obligatorisk.

Sist men inte minst hade vi chansen att kunna observera respondenternas reaktioner och känslor när de besvarade frågor och identifierade olika motiv som upprepades mellan respondenternas svar. Bryman (2018: 564) förklarar att semistrukturerade intervjuer anses lämpligare när fler författare involveras vid undersökningen eftersom denna form av intervju stödjer författaren att lättare identifiera och jämföra mönster som upprepas utifrån respondenternas svar vid olika intervjutillfällen.

### 4.2.1 Tillvägagångssätt av semistrukturerade intervjuer

Försäkringskassan är en offentlig myndighet med fokus på socialförsäkringen. Myndighetens uppdrag är att besluta om och betala ut en stor del av de förmåner som ingår i socialförsäkringen och har som vision att bidra till skapande av ett samhälle där människor känner trygghet oavsett hur livet förändras. Försäkringskassan har de senaste åren utvecklat sina e-tjänster och allt fler medborgare använder e-tjänster för sina ärenden. Anledningen till att vi valde att undersöka just denna myndighet var på grund av dess snabba utveckling av e-tjänster och den stora mängd känslig information som dagligen utbyts via dess webbsida.

Alla intervjuer genomfördes under december 2018 på Försäkringskassans huvudkontor i Göteborg vid två olika tillfällen medan transkribering av data gjordes i högskolans bibliotek dagen efter intervjuerna. Vi intervjuade 3 chefer och 7 anställda från 3 olika avdelningar (IT-avdelning, avdelningen för barn och familj samt avdelningen för gemensamma försäkringsfrågor) och intervjuerna gjordes individuellt med var och en av respondenterna. För att säkerställa respondenternas anonymitet bestämde sig vi för att använda koder istället för namn. På så sätt använder vi koderna Chef 1, Chef 2, Chef 3 för chefernas reflektioner, medan vi för de anställda använder R1 upp till R7 för deras insikter. Vid slutet av den 10:e intervjun bestämde sig vi för att avsluta datainsamlingen på grund av upprepning i respondenternas svar. Vi har samlat tillräckligt många data och var nöjda med resultatet av intervjuerna därför flera intervjuer ansåg att vara värdelösa. Enligt Bryman (2018: 561) möjliggör semistrukturerade intervjun tillgång till många respondenter. Detta hjälper i sin tur till en insamling av många olika uppfattningar om fenomenet under diskussion men den mängd data som kan insamlas från intervjuer anses ofta som en utmaning för författaren i och med att transkribering och analys av dessa data är en process som tar mycket tid i anspråk (Bryman, 2018: 561).

### 4.2.2 Urval

Huvudmålet för denna studie är att besvara forskningsfrågor och uppnå studiens syfte. Urval av respondenterna ansågs vara ett av de viktigaste stegen för att kunna uppnå detta mål. På

grund av detta valde vi att göra ett målstyrt urval. Målet med målstyrt urval är att vi inte valde deltagarna slumpmässigt, utan på ett sätt som hjälpte studien att utvecklas ordentligt. Bryman (2018:496) beskriver målstyrt urval som en process där urvalet görs för att svara på det mest effektiva sättet utifrån studiens frågeställning.

Urval av respondenterna har gjorts på så sätt att det uppfyller forskningsbehovet. Innan genomförandet av intervjuerna var det grundläggande att fastställa några viktiga kriterier innan vi valjer vilka respondenter som var lämpliga för studien. Ett kriterium för urvalet av respondenter var minst en chef samt en anställd på IT-avdelningen, detta på grund av att IT-avdelningen arbetar nära frågor som rör informationssäkerhet. Förutom detta har också anställda inom IT-avdelningen mer tekniska kunskaper som kan bidra till en bättre förklaring av säkerhetspolicyn och dess implementering inom verksamheten. Ett ytterligare kriterium var att respondenterna inte skulle vara nyanställda på Försäkringskassan. Detta så nyanställda inte har jobbat tillräckligt länge inom organisationen för att ha upplevt förändringar vid implementering av informationssäkerhetspolicyn och i och med detta saknar de kunskaper för att kunna besvara intervjuns frågor med. Enligt Bryman (2018:497) kan alla som har kunskap kring ämnet anses som lämpliga deltagare. Ibland kräver vissa ämnen deltagare med speciella kunskaper och därför finns det några begränsningar av vem som kan vara lämplig. Det finns emellertid alltid några begränsningar som forskaren sätter beroende på vad studien vill komma fram med.

### 4.2.3 Begränsningar av semistrukturerade intervjuer

Vi hade redan begränsningar i åtanke som denna metod innefattar, och det är viktigt att härmed hänvisa till dem. Först och främst hade vi liten kontroll över respondenterna eftersom det inte är alltid tydligt hur långt och rimligt det är att låta respondenterna utveckla sina tankar och prata om ämnet som diskuteras vid varje fråga. Det är heller inte klart i vilken grad det är lämpligt att överge kontrollen till respondenterna, särskilt inte när det finns många frågor som måste besvaras inom en viss tidsram. Vi valde att låta respondenterna prata hur mycket de ville om ett ämne och bara när respondenterna berörde något som inte var viktigt för studien avbröts diskussionen av oss genom att ställa en ny fråga till respondenterna.

Vidare är ett annat problem som kan uppstå att det ofta är svårt att analysera insamlade data. I denna studie valde vi att genomföra intervjuer så tidigt som möjligt samt att träffa alla respondenterna under samma vecka och på så sätt kunna ägna ännu mer tid åt transkribering. Enligt Bryman (2018: 578) är också den tid som behövs för att transkribera insamlade data en begränsning av semistrukturerade intervjuer. Transkribering innebär en betydande tidsinsats, och författarna behöver varsamt analysera allt som respondenterna diskuterar på ett effektivt sätt för att skapa nytta för studien.

I slutet av varje intervju läste vi igenom respondenternas svar och gjorde några anteckningar av insamlade data. På så sätt var det enklare att ha kontroll av hur mycket data som behövdes för att fullgöra undersökningen och kunna besvara studiens frågor. När de insamlade data ansågs vara tillräckliga för att kunna besvara studiens frågor bestämde oss vi för att upphöra med intervjuerna. För att minska risken för tekniska problem vid inspelning beslutade oss vi för att parallellt med inspelningen föra anteckningar över respondenternas svar. Bryman (2018: 578) handlar också att det är vanligt att mängden insamlade data efter varje intervju är stor. Det behövs en bra strategi för att identifiera mönster utifrån respondenternas reflektioner och analysera dessa på ett sätt som gör att de följer en röd tråd som underlättar för läsaren att förstå analysen och studiens resultat. Tekniska problem vid inspelning av respondenterna

under intervjuer kan leda till att vissa delar av intervju kan vara ohörbara vilket kan göra transkribering ännu svårare (Bryman,2018: 578).

### 4.3 Kvalitetskriterier

Många författare av samhällsvetenskapliga metoder hävdar att reliabilitet och validitet inte är relevanta för en kvalitativ studie. Dessutom föreslår Bryman (2018:467) att det finns fyra olika kriterier för att säkerställa att en kvalitativ studies resultat uppfyller kraven om validitet och reliabilitet. Kriterierna i fråga är trovärdighet, överförbarhet, pålitlighet, och möjligheten att styrka och konfirmera. Vi förklarar nedan hur arbetade vi under studiens gång för att öka studiens kvalitet och tillförlitlighet.

#### 4.3.1 Trovärdighet

För att kunna öka studiens trovärdighet genomförde vi semistrukturerade intervjuer både med chefer och anställda för att få fler synpunkter från olika aspekter och utröna på vilket sätt både ledningen och personalen anser att implementeringen av informationssäkerhetspolicyn har skett inom verksamheten. Utifrån respondenternas olika reflektioner och beskrivningar kunde vi dra mer objektiva slutsatser som återspeglade hur implementeringen genomfördes inom Försäkringskassan i praktiken. Ytterligare en faktor som hjälpte till att öka trovärdighet av studien är det urval av respondenterna där man följt speciella kriterier, och då särskilt kring respondenternas kunskap kring studiens ämne och deras relation till organisationen från olika nivåer (både ledning och personal) vilket bidragit till mångfalden bland resultaten. Bryman (2018:467) anser att trovärdighet är ett av de viktigaste kriterierna i en kvalitativ studie. Trovärdighet ger svar på frågan om i vilken grad resultatet överensstämmer med verkligheten (Bryman, 2018:467).

#### 4.3.2 Överförbarhet

I denna studie försöker vi att analysera alla processer som följts i detalj för att öka transparensen hos studien. Vi argumenterar kring varje val vi har gjort i metoden som använts för att utföra studien och läsaren bör få en bättre förståelse och bredare insyn i studiens resultat. Vi har valt Försäkringskassan på grund av att de flesta av deras ärenden nuförtiden hanteras via organisationens e-tjänster, detta i jämförelse med andra myndigheter som inte har utvecklat sina e-tjänster i samma utsträckning. Därför var det viktigt att kontrollera på vilket sätt organisationen arbetar med att implementera informationssäkerhetspolicyn. Vi tror att studien överförbarhet utgår i stor utsträckning ifrån faktum att resultatet beskriver hur implementeringen av policyn har uppnåts i Försäkringskassan utifrån reflektioner från individer som hade varit inblandade i policyns implementering. Respodenterna hade en tydlig bild av implementeringens process och studiens slutsatser i samband med teorin kan vara användbara också vid studier om implementeringen av olika policyn inom den offentliga förvaltning. Däremot är det svårt att påstå i vilken grad är studien överförbart när det gäller implementeringen av policyn inom den privata sektorn. Enligt Bryman (2018:468) handlar extern validitet om i vilken utsträckning resultaten av en studie kan tillämpas under andra omständigheter än de som studien beskriver. Kvalitativa studier undersöker ett begränsat antal människor och åsikter och därmed blir det svårt att uppnå extern validitet (Bryman ,2018:468).

### 4.3.3 Pålitlighet

Från urvalet av respondenterna vidare till alla steg av datainsamlingen beskriver vi allt som har gjorts för att öka transparens och möjliggöra för andra författare i framtiden att följa samma processer för att på så sätt upprepa studien. Förutom det faktum att vi klargör alla steg som följts för att genomföra denna studie, förklarar också vi alla begränsningar angående studiens metod. På samma sätt förklarar Bryman (2018:468) att målet med pålitlighet för en kvalitativ studie är att se till att liknande forskning kan vara genomförbar i framtiden, även om resultaten kan bli olika.

### 4.3.4 Möjlighet att styrka och konfirmera

I denna studie förklarar vi alla val vi har gort och diskuterar anledningen bakom dessa. Genom semistrukturerade intervjuer blev det möjligt för respondenterna att diskutera vad de verkligen tyckte om ämnet under diskussionen för varje fråga och uttrycka sig själva fritt utan någon kontroll från författarna. Dessutom argumenterar vi kring metodens val och förklarar begränsningar kring metoden där alla problem och svårigheter analyseras. Vidare beskriver vi på vilket sätt lyckades lösa och överkomma alla svårigheter som uppstod under studiens gång. Enligt Bryman (2018:470) kan objektivitet relateras till ‟confirmability” för de kvalitativa studierna. Att säkerställa ‟confirmability” i en kvalitativ studie är en utmaning då intervjufrågorna formuleras av författarna, och de inte kan vara helt och hållet objektiva. Däremot måste författarna vara medvetna och förstå varför de väljer en metod framför en annan, och varför de ställer de specifika frågor de valt ut till respondenterna. Huvudmålet för att öka ‟confirmability” är att man också presenterar alla svagheter vid användningen av en viss metod och få kunskap om dessa svagheter (Bryman, 2018:470).

## 4.4 Etiska aspekter

I denna studie var vi försiktiga i vårt beteende mot alla respondenter. Vi informerade alla respondenterna att deras identiteter kommer att skyddas och att man istället för deras namn använder koder som representerar dem i studien. Vi hade redan vid den första kontakten med respondenterna försäkrat att alla insamlade data som skulle presenteras i studien skulle vara anonyma. Dessutom blev alla respondenterna informerade innan sina intervjuer om att de kan svara på de frågor de känner sig bekväma att besvara, och ifall där var någon fråga de inte ville svara på hade de möjlighet att hoppa över denna. Vi klargjorde att det inte fanns ett rätt eller fel svar för att alla skulle kunna uttrycka sina åsikter utan stress. Sist men inte minst hade alla respondenterna möjlighet att svara på frågorna utan att vi ledde dem i en viss riktning och på så sätt borde detta resultera i att respondenternas reflektioner representerar objektivitet. Enligt Bryman (2018:170) representerar etiska frågor författarens beteende och roll under hela studien och först och främst på vilket sätt författaren behandlar respondenterna som vill delta i intervjuerna.

# 5. Resultat

Insamlade data från intervjuer sammanfattas och presenteras i detta kapitel. Svaren från intervjuerna kommer att presenteras under olika rubriker för att det ska vara lättare för läsaren att följa flöden. För att försäkra deltagarnas anonymitet har författaren valt att benämna dem som Chef 1, 2, 3 och R 1, 2, 3, 4, 5, 6, 7.

## 5.1 Implementeringen och chefers roll

Cheferna svarade samstämmigt att de hade en klar och tydlig strategi över vad de ville uppnå vid införandet av informationssäkerhetspolicy. Vidare förklarade de att deras mål var mätbara

vilket möjliggjort utvärderingar för att kontrollera om implementeringen av policyn var lyckad.

"*Det var hjälpsamt att vi visste från början varför implementeringen ska ske, vad förändringen innebär och hur den kommer att påverka alla som arbetar inom organisationen.*" (Chef 2)

Alla chefer hävdade att de anställda inte kunde sköta sina löpande arbetsuppgifter parallellt med implementeringen, och de insåg att det skulle ta mycket tid och kraft ifrån organisationen att implementera informationssäkerhetspolicyn. Verksamheten måste rulla på som vanligt och när den nya policyn införts fanns det en grupp från personalen för att stödja processen och introducera informationssäkerhetspolicyn stegvis för alla anställda.

*"Organisationen kan inte upphöra med sin normala verksamhet för att genomföra en implementering. Det måste ske parallellt med den ordinarie verksamheten, som heller inte får störas. Det var en utmaning."* (Chef 1)

*"Från början fanns det en styrgrupp på arbetsplatsen vilken fick mer en karaktär av statusrapportering och informering av personal."* (Chef 1)

Dessutom blev det enligt respondenterna avgörande att ledningen förankrat och förklarat hur och varför förändringarna skulle ske. Om detta inte sker så uppkommer problem såsom missnöje och motstånd längre fram i projektet. Det som alla chefer påpekade var att den största förändringen kom fram innan implementeringen av policyn. Det var viktigt att veta vad som skulle prioriteras, bli klar inom den uppsatta tidsramen, nå uppsatta mål, planera hur processen skulle gå till och skapa en plan för att informera löpande personalen.

"*Det var viktigt att kommunicera det stora målet; vad som ska bli enklare och vad som ska uppnås. För medarbetaren är det påfrestande att plötsligt behöva jobba på ett annat sätt och ändra sina rutiner. Vi hade en planering om att förbereda organisationen inför en förändring och vi la ner mer tid för att stödja anställda i olika former.*" (Chef 3)

Några av respondenterna märkte att det krävde en period för att verksamheten skulle anpassa sig i samband med införandet av den nya policyn. Det tog lång tid innan policyn började implementeras i praktiken och det var rimligt för personalen att få mer tid för att lära sig policyns riktlinjer, delta i utbildningar och möten samt vara väl informerade om det som krävdes vid nya rutiner. Enligt respondenterna finns det inom Försäkringskassan informationskanaler genom vilka man når ut till personalen med information. Informationsspridning sker i första hand via e-post till personalen och via möten där man introducerar den nya policyn. Under mötet blir personalen uppmärksammad om innehållet av policyn som skall implementeras och får möjligheten att träffa chefer och ställa frågor.

"*Viktigast av allt var att få personalen att se fördelarna, annars skulle motivationen saknas.*" (Chef 3)

Respondenterna förklarade att de hade och fortfarande har möjlighet att vända sig till ledningen med synpunkter angående arbetet med informationssäkerhet. Det hålls även veckomöten och månadsmöten där olika förändringar ses över. Dessa möten fungerar även som en viss kontroll och mätning av exempelvis huruvida information angående informationssäkerhet fått någon effekt bland de anställda. Kommer anställda med förslag tar

man hänsyn till detta och vidarebefordrar dessa vidare högre upp i ledningen genom enhetschefer eller styrgrupp ifall de anses relevanta. Samtidigt förklarar respondenterna att de fick vara delaktiga vid genomförandet av policyns implementering och att de i det stadiet bara fick komma med synpunkter men att de inte skulle kunna få igenom någon ändring.

*"Vi fick i första hand visa våra synpunkter angående policyn men det uppkom igen ändring. Riktlinjerna var fastställda och vi verkställer dem." (R5)*

Dessutom hävdade respondenterna att personalen i styrgruppen är ansvariga för att uppfylla vissa specifika uppgifter varje vecka. Dessa uppgifter fanns vid anslagstavlan i form av listor och innebar att styrgruppen måste övervaka servermiljö, backuper, kolla klienter, användarsupport och utföra slumpmässiga kontroller i anställdas utredningar med hjälp av enhetschefer för att se om riktlinjerna följdes.

"*Vi gjorde också kontroll ganska ofta under implementeringsprocessen för att ha koll på implementeringens framgång. Utifrån dessa kontroller kunde vi förstå om allt funkar som det måste eller om det behövdes förändringar för att underlätta policyns implementering.*" (Chef 2)

## 5.2 Efterlevnad av informationssäkerhetspolicy inom verksamheten

De riktlinjer som personalen måste följa är att sekretessbelagd information inte får spridas till andra medarbetare eller myndigheter utan godkännande av ansvariga chefer. Anställda har tillgång till styrdokument angående informationssäkerhetspolicyns riktlinjer varje gång ett arbete utförs för att vara bekanta med hur riktlinjerna ser ut och vad som bör tas hänsyn till. Dessutom blir handläggarna övervakade av enhetschefer angående de beslut de fattar och hur deras utredningar görs. Utredningar kontrolleras ofta slumpmässigt och på så sätt undviks felaktigheter och risker för missbruk av känslig information. Enligt respondenterna beaktas personuppgiftslagen samt offentlig- och sekretesslagen inom Försäkringskassan för att skydda känsliga uppgifter. Det finns regler om vilka uppgifter anställda kan ha tillgång till i de olika styrdokumenten vilka efterföljs av de anställda. Därmed hindrar detta att obehöriga får tillträde till uppgifterna. Därför finns regler om att anställda måste identifiera sig med personliga koder när uppgifterna vidarebefordras vid begäran.

"*De anställda har ansvar om att sekretess och informationen de tar del av inte sprids vidare.*" *(*Chef 1)

Respondent förklarar att användare har ett personligt ansvar att lägga in rätt information på rätt individ. Samtliga respondenter beskriver att användare har ett ansvar att inte ge ut sina inloggningsuppgifter. Användare får inte logga in och arbeta fritt i en kollegas användarprofil. Respondenterna insåg att det är organisationens prioritet att leverera bättre kvalitet till kunder via e-tjänster. IT-avdelningen har installerat övervakningssystem som larmar och skannar av nät, kollar farliga programvaror, samt för statistik över in- och uttrafik.

*"Vi tror inte att våra kunder drabbas av intrång för att om det finns någon som försöker hacka oss, då varnar systemet om hot som uppkommer och IT-avdelningen hanterar omständigheterna. Hotbilden ser ju olika ut för olika organisationer.*" *(*R2)

Respondenterna hävdade att det ofta sker uppdateringar av riktlinjer kring informationssäkerhetspolicy för att öka säkerhet av den information som behandlas, och några

av dem märkte att en rad uppdateringar påverkade deras arbetssätt vilket kan vara irriterande att såpass oftast anpassa sig till nya förändringar. Information angående nya hot eller annat inom informationssäkerheten skickas oftast ut över e-post eller genom andra kanaler som t.ex. anslagstavlan eller dokument.

"*Vid morgonmöte eller veckomöte tas det oftast upp påminnelser om policy och informationssäkerhet samt att det ges chans till en återkoppling från medarbetare. Det finns också många öppna e-postgrupper där man kan ställa frågor eller komma med synpunkter*." (R4)

Något som alla respondenterna upprepade mycket under intervjun var att skapa rätt förväntningar för policyns innebörd. Det var viktigt att i en tidig punkt av implementeringen av nya rutiner förmedla en förståelse för vilka processförändringar och andra förändringar som kommer att ske.

"*Det var nödvändigt att alla anställda var införstådda, involverade och motiverade eftersom vinsterna av informationssäkerhetspolicyimplementering realiseras först då alla är med på tåget*." (R7)

Enligt chefernas reflektioner hade tillräckligt antal möten för ändamålet med personalen, samt förmedlade all information som berörde informationssäkerhetspolicy via e-post, broschyrer och utbildningar som ägde rum under implementeringsprocessen. Chefernas planering började långt i förväg där de informerade de anställda, även om det fanns en viss oro för att de anställda skulle glömma bort informationen tills implementeringen slutförts. Trots detta ansågs det mer viktigt att alla var väl informerade innan införandet av förändringen än att fatta en rad beslut under implementeringens gång som inte kunde åtgärdas under processen.

"*Kommunikationsproblemet varierar även beroende på organisationens avdelning. Det är skillnad på att kommunicera ut information om informationssäkerhetspolicyn i en organisation där de anställda använder IT i sitt dagliga arbete liksom i vår organisation jämfört med en organisation där de anställda saknar direkt kontakt med IT*." (Chef 3)

Respondenterna hävdade att ett sätt att hantera kommunikationen är att satsa på träning och utbildning. Att utbilda anställda angående policyn är en viktig del av implementeringen. Däremot känner några av respondenterna att de inte har erhållit tillräcklig utbildning, då för lite resurser är tilldelade för detta ändamål.

"*Beroende på vilken grupp som åsyftas bör utbildningen genomföras såväl före, under och efter en implementering, däremot finns det en begränsning av hur mycket kunskaper anställda kan förvärva innan implementeringen av policyn sker i praktiken.*" (R4)

Dessutom är det oftast först en tid efteråt som anställda upptäcker hur policyn påverkar dem själva och då uppstår frågor som hur de ska agera och hantera detta. Vidare förklarade respondenter att det finns olika slags kontroller som genomförs för att upptäcka policyns efterlevnad i verksamheten.

"*Vi har olika möten med styrgruppen som utför kontroller vid anställdas utredningar och beslut regelbundet. Där kontrollerar de att all information behandlas enligt informationssäkerhetspolicyns riktlinjer. T.ex. det utförs kontroller på både gamla och nya backups för att säkerställa att all information finns bevarad.*" (Chef 1)

Enligt anställda sker kontroller om efterlevnaden av policyn mestadels på teknisk nivå med hjälp av vissa verktyg. All trafik in och ut från kontoret kontrolleras och övervakas för att se om det är något otillåtet som skickas eller hämtas. Utöver den tekniska kontrollen nämner de att de hela tiden jobbar på att bli bättre med att efterleva policyn, genom vidareutbildningar och diskussioner kring riktlinjer som tas upp på möten. Respondenterna beskriver att en informationsruta visas på användarens skärm vid inloggning i systemen.

"*All rapportering gällande fel vid hantering av information registreras i ärendehanteringssystemet. Alla anställda är också skyldiga att rapportera om de misstänker ett fel eller hot. Dessa ärenden som registreras delegeras sedan ut av supporten som har bra koll på vem som gör vad så att rätt person ska kunna lösa problemet effektivt och korrekt.*" (*R1*)

Anställda som inte följer uppsatta direktiv gällande publicering av information beskrivs som ett hot för verksamheten. R2 berättar att deras höga tillgång till information kan utgöra en risk mot informationssäkerheten eftersom det finns möjlighet för dem att ta del av information som inte behövs i arbetet. Respondenterna förklarar att det kan uppstå konsekvenser för en anställd som direkt bryter mot informationssäkerhetspolicyns riktlinjer.

"*Jag antar att min arbetsgivare skulle bli missnöjd med mitt agerande om jag inte följer informationssäkerhets riktlinjer. Det kommer säkert påverka min karriär. Vi är ansvariga för att behandla alla känsliga informationer med respekt till reglerna.*" (R5)

"*Konsekvenser bestäms utefter omständigheterna för varje specifik händelse. Vi gör i första hand en varning om brott mot riktlinjer inte är allvarligt och kan korrigeras, men om samma anställda fortsätter ignorera riktlinjer och hantera ärenden utan den ansvarighet som behövs då kan olika konsekvenser uppkomma. Liksom minskning av antal ärenden de anställda arbetar med eller även återkallelse av behörighet. Ett brott mot tystnadsplikten kan ge allvarliga konsekvenser och kan även leda till avsked för att alla ärenden är sekretessbelagda."* (Chef 2)

Respondenterna förklarar att risken kan minskas genom att motivera anställda till att vidareutbilda sig samtidigt som det höjer kompetensen och kvalitén på deras arbete. Denna ökade kompetens inom olika områden bidrar också till en ökad säkerhetsmedvetenhet. Möjligheterna till en ökad kunskap och kompetens kan leda till en mer positiv attityd bland de anställda.

"*Alla våra anställda måste vara väl medvetna och känna till alla procedurer och principer såväl tekniskt som juridiskt för att förebygga både potentiella och aktuella hot mot vår informationssäkerhet.*" (*Chef 3)*

R1 berättade också att det vid nyanställning hålls informationsdagar då nyanställda blir informerade om sekretess- och säkerhetspolicys.

### 5.3 Aktiviteter för att öka medvetenhet under implementeringen

Försäkringskassan i Göteborg har en policy om att inte skicka känsliga uppgifter via e-post, då det anses vara riskabelt att det utnyttjas av andra användare via nätet. Detta har man

upplyst alla anställda inom Försäkringskassan om utifrån informationssäkerhetspolicyns riktlinjer påpekar *R3,* och att om policyn inte efterföljs bryter de mot personuppgifts- och offentlig sekretesslagen. För att motverka brott mot lagen behöver de anställda få ett godkännande av en enhetschef för att kunna dela vidare informationen till andra anställda på arbetsplatsen.

"*Ja, vi har en e-post policy. Vi får inte föra vidare känsliga uppgifter via e-post för att inte riskera utnyttjande av informationen angående våra medborgare som har ärenden hos oss för att detta går mot personuppgifts- och offentlig sekretesslagen. Vi måste komma överens med våra enhetschefer om vi får lov att föra vidare informationen till andra kollegor om det så behövs.*" *(R5)*

Andra respondenter nämnde också några ytterligare riktlinjer såsom att ”Byta lösenord med jämna mellanrum och använda vissa tecken i detta, typ stora och små bokstäver”, ”Sätt ej in okända USB-stickor i datorn”, ”Att inte göra privata ärenden på organisationens datorer”, “Att inte tala om sitt lösenord för andra”, ”Att inte öppna bifogade filer om man är osäker på avsändaren”, ”Att inte öppna en specifik länk”, “Att inte ge ut sina inloggningsuppgifter”. R2 förklarade att informationssäkerhetspolicyns dokument finns på organisationens intranät så att alla kan gå in och läsa detta när som helst under arbetstid. Respondenterna förklarar att de är väl medvetna om detta då Försäkringskassan alltid informerar om nya riktlinjer som tillkommer eller om det sker ändringar i syfte om att få alla medarbetare att vara medvetna om hur arbetet bör utföras. Personalen blir kontaktad av enhetschefen när det sker uppdateringar och ändringar i policyn för att på så sätt öka deras medvetenhet, och att detta sker antingen via anslagstavlor, e-post eller möten. Samtliga respondenter beskriver också att aktiviteter som automatiska påminnelser i systemen regelbundet görs för att uppmana anställda till lösenordsbyte.

"*Det sker via e-post eller via våra anslagstavlor där vi blir informerade om det sker en uppdatering eller ändring som vid senare tillfälle tas fram vid möten.*" *(R2)*

Enligt respondenterna får personalen möjligheten att ta del av utbildningar för att öka medvetenheten kring informationssäkerhetspolicyn. De blir informerade och är väldigt aktiva vid de utbildningar som ges då de lär sig om hur policyn är utformad och om hur denna bör tillämpas. Utbildningarna sker under en viss period och i slutändan får man ett certifikat om att utbildningen har genomförts vilket registreras i styrdokumentet. Personalen får gå på en processutvecklingsutbildning. Processerna har olika stadier innan beslutsunderlaget går igenom, därför är det viktigt att ta del av policyn så att känsliga uppgifter inte läcker ut eller utnyttjas av andra, eftersom de har mycket information som säkras. Detta minskar risker för felaktigheter och det skapar en säkrare arbetsmiljö.

"*Utbildning är en aktivitet som bidrar till bättre medvetenhet kring säkerhetspolicy. Vi får gå på utbildningar som behövs vid en informationssäkerhetspolicy för att vara delaktiga och kunna tillämpa den på ett bra sätt. Jag tycker att detta är bra för att vi skall kunna utföra våra arbeten utan felaktigheter och att alla skall vara uppmärksamma om hur riktlinjerna fungerar hos Försäkringskassan.*" *(R7)*

# 6. Diskussion

I det här kapitlet presenterar författarna resultatet av studien och diskuterar det i samband med den utvalda teorin som beskrivits tidigare. För att underlätta för läsaren är avsnittet uppdelat i två huvudrubriker som diskuterar studiens ämne utifrån två perspektiv.

### 6.1 En framgångsrikt implementeringen av informationssäkerhetspolicyn

Enligt ovanstående reflektioner blir det klart att implementeringen av informationssäkerhetspolicy i Försäkringskassans e-tjänster skett vid olika steg och enligt en tydlig plan. En välplanerad strategi och klart mätbara mål ansågs från början som nödvändigt för att kunna införa policyn och värderas som viktiga faktorer vilka ledde till policyns implementerings framgång. Chefer och styrgruppen hade tydliggjort varför implementeringen skulle ske, vad förändringen innebar och hur den skulle komma att påverka alla som arbetar inom organisationen. Dessutom klargjorde resultatet att brist på tid och resurser var avgörande för genomförandet av implementeringen, och att det därför var det essentiellt att skapa en tidsplan och bestämma fördelning av resurser på bästa möjliga sätt redan vid förstudien. Tonnquist (2016:308) förklarar på samma sätt att förstudie är den första fasen vid implementering och att det i detta stadie är viktigt att ha rätt kvalifikation till införandet, samt att kunna utnyttja alla resurser maximalt för att skapa en lyckad implementering av policy.

Hos Försäkringskassan började förändringsarbetet vid ett tidigt stadie innan introduktionen av policyn till personalen. Alla som var ansvariga för policyns implementering, och först och främst chefer beslutade om vad som skulle prioriteras och i vilken ordning allt skulle ske för att uppfylla målet. En av de första prioriteringarna var att informera personalen löpande för att förbereda verksamheten på förändringar i god tid och stödja de anställda under hela förändringsprocessen. Det var viktigt att alla anställda hade en bra förståelse av policyn och att de var motiverade och engagerade vid förändringar. Därför arbetade styrgruppen och chefer intensivt för att förmedla policyn till alla på olika sätt. Vidare förklarar teorin att alla detaljer om processen måste analyseras och planeras försiktigt i nästa stadium av en implementering, och särskilt då introduktionen av förändringar om den nya policyn till de anställda. Vikten och målet av förändringarna måste tydliggöras för att minska risker av en implementerings misslyckande vilket kan inträffa vid ett senare stadie (Tonnquist, 2016:310–314).

Under möten blev personalen mer uppmärksammad om innehållet av policyn som skulle implementeras och de fick möjlighet att träffa chefer och ställa frågor. Cheferna ville uppmuntra personalen att se fördelarna med den nya policyn, då man fruktade att motivationen skulle saknas annars. Även Blomquist & Röding (2010) förklarar att ledarskap är vägen från konflikter till samverkan, samt att konflikter kan vara skrämmande men de kan också vara förlösande och utvecklande. Under genomförandet av policy är det möjligt att det uppkommer känslor av oro och rädsla hos personal angående införandet av policyn. Detta på grund av otillräckliga förklaringar och bristfällig kommunikation kring påverkan och förändringar i deras arbete. I sin tur kan oron leda till att implementeringen av policyn påträffar motstånd och konflikter, vilka kan öka risken att implementeringen aldrig fullgörs (Tonnquist, 2016:298). Enligt studiens resultat arbetade cheferna intensivt med att ha tillräckligt många möten med personalen, samt att man förmedlade all information som berör informationssäkerhetspolicy via e-post, broschyrer och utbildningar under implementeringsprocessen. Spridning av information angående policyns införande till de anställda började tidigt trots oron att anställda inte skulle minnas all information tills implementeringen slutförts. På så sätt var personalen förberedd när implementeringen var på gång, även om viss information behövde påminnas om för att få personalen att känna sig trygg inför den nya policyn. Styrgruppen gjorde ofta kontroller under implementeringsprocessen för att ha koll på implementeringens framgång och för att kunna

förstå om allt fungerade enligt planeringen, eller om det behövdes förändringar för att underlätta implementeringen.

Resultatet av studien visar att chefer hos Försäkringskassan på olika sätt följt en transformell ledarstil vid implementeringen av informationssäkerhetspolicyn. Chefer har ägnat mycket tid och resurser på träning och utbildning av personal, och beroende på vilken grupp som åsyftas bör utbildningen genomföras såväl före, under och efter en implementering. Vid olika möten togs det ofta upp påminnelser om policyn och informationssäkerhet, samt att ledningen fick möjlighet att åtnjuta återkoppling från medarbetare. Det finns också många öppna e-postgrupper på Försäkringskassans intranät där man kan ställa frågor eller komma med synpunkter. Förutom detta jobbar chefer kontinuerligt på att bli bättre på att efterleva policyn genom vidareutbildningar och diskussioner kring riktlinjer. Dessutom vidareutbildar sig personalen för att höja kompetensen och kvalitén på deras arbete kring informationssäkerhet. Enligt Gifford et al. (2007) behandlar fyra olika kunskapsöversikter när det gäller ledarskap vid implementering av en ny policy, vilka avspeglas hos ledarens beteende genom att stödja, återkoppla, kommunicera, vara en förebild, vidareutveckla medarbetare och påverka omgivningen. Alla dessa beteenden kopplas till transformell ledarstil vilket anses vara effektiv för att öka motivation och prestation hos medarbetare, samt att vara framgångsrik vid organisatoriska förändringar (Bass et al., 2003).

Studien visade att anställda har möjlighet att vända sig till ledningen med synpunkter angående arbetet med informationssäkerhetspolicyn under veckomöten och månadsmöten där olika förändringar ses över. Enligt teorin om transformellt ledarskap måste chefer inspirera medarbetarna och främja diskussioner och kreativa lösningar. En chef måste skapa möjligheter för medarbetarna att vara delaktiga och uttrycka sina åsikter för att kunna komma fram till nytänkande och innovativa processer i syfte om att förnya och förbättra befintliga rutiner (Bass et al., 2003).

Studiens resultat visar att om anställda har något förslag vidarebefordras detta högre upp i ledningen genom enhetschefer eller styrgrupp. De anställda var delaktiga vid genomförandet av policyns implementering, men inte senare för att riktlinjerna då redan var fastställda, och de då bara verkställde dem. Det kan härledas att riktlinjerna i en informationssäkerhetspolicy följer specifika regler och lagar som påverkar policyn i sin helhet. Det var även svårt för chefer att ändra innehållet av riktlinjerna. Detta kan förklaras i samband med vad Hill (2012:183) beskriver om uppifrån-ner modellen vilket används vid genomförande av implementering och förklarar att formuleringen av policyn ligger i topphierarkin, och de övriga anses bara verkställa policyn.

### 6.2 Medarbetare med en ökad informationssäkerhets medvetenhet

Respondenterna förklarar att det finns olika utbildningar och dokument för att säkra personalens medvetenhet kring informationssäkerhetspolicy. Olika dokument finns på organisationens intranät som de kan komma åt under arbetstid och läsa för att påminna sig om policyns innehåll. De blir mer medvetna när chefer kommer ut med information kring nya riktlinjer eller om det finns ändringar kring policyn. Detta bidrar till en ökad medvetenhet och att arbetet utförs med mindre felaktigheter. Samtidigt genomförde cheferna kontroller för att få återkoppling både under implementeringens gång samt när implementeringen slutförts. All trafik in och ut kontrolleras och övervakas för att kunna upptäcka om något otillåtet skickats eller mottagits. Det är viktigt att för personalen förklara konsekvenserna och vilka risker som kan uppkomma vid felaktigheter i deras arbete. Utredningar kontrolleras ofta

slumpmässigt och på så sätt undviks risken för felaktigheter och missbruk av känsliga informationer. Konsekvenser för en anställd som direkt bryter mot informationssäkerhetspolicyn kan uppstå. Enligt Knapp & Ferrante (2012) är ansvarsfördelningen viktig för verksamheten för att få personalen att inse hur viktigt det är med efterlevnad av policyn. Att övervaka och skapa bättre säkerhetsmedvetenhet hos personalen bidrar till att policyn efterföljs. Om de anställda inte är väl medvetna och delaktiga om den nya policyn finns det en stor risk att de anser att policyns nya riktlinjer är meningslösa att följa (Knapp & Ferrante, 2012).

Enligt respondenterna måste de byta lösenord med jämna mellanrum för att minska riskerna att informationen som finns på deras datorer hamnar i fel händer. De måste enligt verksamheten använda stora och små bokstäver samt olika icke alfanumeriska tecken vid val av nytt lösenord. Förutom detta får de som riktlinjer att de inte får hantera information som anses vara osäker för verksamheten och att inte ge ut sina inloggningsuppgifter till andra medarbetare inom verksamheten eller till någon utanför verksamheten. Om personalen inte följer riktlinjerna bryter de mot person- och offentlig sekretesslagen vilket innebär att detta är brottsligt. Knapp & Ferrante (2012) förklarar också att det är viktigt att några steg bör följas av personalen för att öka säkerheten i verksamheten som exempelvis att personalen måste ändra sina lösenord i datormiljön för att skydda informationssystemet från hackning eller virus.

Enligt respondenterna erbjuds det utbildningar för att öka personalens medvetenhet kring informationssäkerhetspolicyn. Huvudpunkten är att personalen blir aktiva och lär sig om hur policyn bör tillämpas vid användning av känsliga uppgifter. Försäkringskassan har utbildningar som hålls under olika perioder och personalen får ett certifikat efter sitt deltagande i utbildningen, vilket blir registrerat i Försäkringskassans databas. Det finns utbildningar som handlar om hur processer fungerar innan beslutet blir ålagt vid olika ärenden. Personalen bör vara medveten om hur detta genomförs enligt Försäkringskassan för att tillförsäkra att information inte blir borttappad, förklarar respondenterna. Kruger & Kearney (2006) hävdar också att det är viktigt att uppmuntra personalen att ha ett korrekt beteende när det gäller att hantera känsliga uppgifter. Att skapa förändringar i personalens beteende och attityder kräver en hel del tid för att denna förändring skall ske. Dessutom skapar enligt Frye (2007) utbildningar en förmåga till att kunna hantera förändringar i arbetsrutiner snabbt och effektivt och ökar medvetenhet om hur man kan lösa framtida problem och felaktigheter

# 7. Slutsats

I detta kapitel redovisar vi våra slutsatser som i stor utsträckning utgår från vårt resultat. I detta avsnitt redovisar vi också vilka svar vi har kommit fram till angående våra frågeställningar.

Syfte med studiens genomförandet var att visa hur Försäkringskassan i Göteborg implementerar informationssäkerhetspolicy angående deras e-tjänster. Förutom ville vi också upplysa vad chefers roll är vid implementering av informationssäkerhetspolicy liksom hur medvetna personalen är när det gäller policyns riktlinjer. Resultat av studien har visat att Försäkringskassan i Göteborg har implementerat informationssäkerhethetspolicyn i olika stadier och har lyckats med att förändra verksamhetens arbetsrutiner så att känsliga informationer behandlas enligt riktlinjerna och är säkra hos myndigheten. Dessutom visar studien att chefer har en viktig roll när det gäller implementeringen av policyn och att de

aktivt har bidragit till att säkerställa att de anställdas säkerhetsmetvetenhet ligger på en hög nivå, samt att implementeringen fullgjorts enligt uppsatta mål.

I studien visar det sig att Försäkringskassan i Göteborg genomförde delmoment av implementeringen av informationssäkerhetspolicyn kring organisationens e-tjänster vid olika faser. De har följt en tydlig plan som beskriver processen på ett detaljerat sätt. Styrgruppen inom Försäkringskassan har varit ansvariga för implementeringen och har fokuserat på att få med och inkludera organisationens anställda vid implementeringen, framför allt i genomförandefasen. Författarna kom fram till att organisationen har lyckats med policyimplementeringen, och att de faktorer som ansågs ha möjliggjort framgången var ett tydlig och välformulerat syfte av policyn samt att implementeringens mål var mätbart. Samtliga chefer har vidhållit att de från början av implementeringsprocessen informerade varför implementeringen av informationspolicy var nödvändig, vad förändringen skulle innebära, samt hur förändringen skulle påverka de olika anställdas arbetssätt inom organisationen.

Studien visar hur ansvariga av policyimplementeringen hade beslutat på vilket sätt implementeringen skulle ske och att det funnits vissa steg som prioriterades för att uppnå målen inom den förbestämda tidsramen. Resultatet visar att cheferna främst hade prioriterat att i god tid förmedla syftet med informationssäkerhetspolicyn samt hur implementeringen av policyn skulle genomföras. Chefer och styrgruppen hos Försäkringskassan hade ansvaret att övervaka huruvida implementeringen av policyn utförts enligt policyns syfte. Dessutom var de tillgängliga för de anställda för att stödja och vägleda dem vid behov under förändringsprocessen.

Utifrån studiens resultat har det tydliggjorts att cheferna aktivt arbetade för att motivera och engagera personalen vid genomförandet av implementeringen. Genom utbildningar och workshoppar blev personalen uppmärksammad om policyns innehåll och olika procedurer och riktlinjer kring informationssäkerhetspolicyn. Styrgruppen och cheferna uppmuntrade de anställda att se den nya policyns fördelar för deras arbete och på så sätt har de lyckats med att minska motståndet för implementeringen. Det har visat sig i undersökningen att cheferna gett de anställda möjlighet att kunna framföra sina tankar kring policyn och dess implementering och att de alltid hade möjligheten till att ställa frågor när de uppstod.

I studien visas att cheferna hos Försäkringskassan använde en ledarstil som liknar transformellt ledarskap, vilket bidrog till att öka de anställdas motivation och prestation. Cheferna använde mycket tid och resurser för att utveckla de anställdas kompetens och kunskap för att kunna underlätta implementeringen av informationssäkerhetspolicyn. Försäkringskassan erbjöd de anställda träning och utbildning löpande under hela processens gång. Dessutom har ledningen övervakat implementeringsprocessen och ständigt gjort utvärderingar för att kunna utröna om implementeringen av policyn var på väg i rätt riktning.

I studien har författarna funnit att cheferna hade kontroll över den information som skickas ut eller delas med andra, samt vilken information som obehöriga inte får ha tillgång till i organisationens IT-system. Studien har upplyst om att det finns konsekvenser för de som inte följer informationssäkerhetspolicyns riktlinjer. För att undvika att organisationens medarbetare medvetet eller omedvetet bryter mot informationssäkerhetspolicyn har organisationen erbjudit utbildningar till medlemmar för att de bättre ska kunna efterleva informationssäkerhetspolicyn.

Utifrån de intervjuades synpunkter står det klart att det råder en hög nivå av säkerhetsmedvetenhet inom Försäkringskassan. Studien visar att organisationens informationssäkerhetspolicy informeras redan vid anställning, där nyanställda kan ta del av lagreglerade föreskrifter som tydligt beskriver hanteringen av känslig och sekretessbelagd information. Anställda har alltid möjlighet att fråga chefer om råd utifall där skulle förekomma oklarheter kring policyns riktlinjer när som helst under arbetstid via organisationens intranät. Automatiska varningar och påminnelsemeddelanden där personalen uppmanas om att till exempel byta inloggningslösenord periodiskt för att minska många av de förutsägbara riskerna mot e-tjänsterna är implementerade.

### 7.1 Framtida forskningar

Från ovanstående tydliggörs att det finns ett behov av ytterligare forskning i framtiden kring informationssäkerhetsimplementering inom offentliga organisationer. Utvecklingen av e-tjänster hos offentliga organisationer i Sverige är ständigt pågående, varför det blir alltmer aktuellt att ta i beaktande hur information som utbyts mellan medborgaren och myndigheter bör skyddas. Antalet undersökningar kring detta ämne är begränsat och därför finns det ett behov av att utföra fler, för att på så sätt stödja organisationer vid utvecklingen av effektivare strategier inom informationssäkerhetspolicyimplementering för att förbättra sina verksamheter. Författarna har genomfört studien med användningen av en kvalitativ metod, vilket innebär att det skulle det vara intressant att också se en studie som genomförts utifrån ett kvantitativt tillvägagångssätt för att sedan kunna jämföra resultaten.

Ett annat förslag är att studien upprepas i andra offentliga organisationer i framtiden för att kunna betrakta i vilken utsträckning offentliga organisationer arbetar på samma sätt vid implementeringen av sin informationssäkerhetspolicy. Sist men inte minst skulle det vara intressant att genomföra samma studie vid andra kontor runt om i landet inom Försäkringskassan, och inte bara Göteborg, för att kunna observera om Försäkringskassan arbetar på samma sätt kring implementering av informationssäkerhetspolicyn i hela Sverige.

## Käll- och litteraturförteckning


Albrechtsen E., Hovden J.(2010). "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study". *Computers & security* 29 (2010) 432–445

Al-Hamdani, W.A. & Dixie, W.D. (2009) "Information Security Policy in Small Education Organization." *Information Security Curriculum Development Conference* (S. 72-78).

Alhogail, Mirza, Bakry (2015). "A comprehensive human factor framework for Information Security in organizations". *Journal of Theoretic and Applied Information Technology*. (Volym 78, No. 2), 201-211

Avolio, B. J., Walumbwa, F. O. & Weber, T. J. (2009). "Leadership: current theories, research, and future directions." *Annual review of psychology*, 60: 421-449.

Backström, T., Granberg, O,. &, Wilhelmson, L. (2008). *Alternativa former för chefers ledarskap – en kunskapsöversikt om sätt att förstå hur ledarskap kan utövas mellan chefer och medarbetare i svenskt arbetsliv*. Enheten för arbetslivsutveckling - Vinnova.

Bank S. (1990). "Security policy". *The Royal London Mutual Insurance Society, Middlesborough, Colchester, Essex, U.K.* Volume 9, Issue 7, November 1990, Pages 605-610

Bass, B. M., Avolio, B. J., Jung, D. I. & Berson, Y. (2003). *Predicting unit performance by assessing transformational and transactional leadership.* Journal of Applied Psychology, 88: 207-18.

Behn, R.(1998). "What Right Do Public Managers Have to Lead*?"*. *Public Administration Review* 58(3):209-25

Blomquist, C. & Röding, P. (2010). *Ledarskap – personen, reflektionen, samtalet*. Sweden: Studentlitteratur AB, Lund

Bulgurcu B., (2010). "Information security policy compliance: An empirical study of rationality- Based beliefs and information security awareness". *MIS Quarterly* Vol. 34 No. 3 pp. 523-548/september 2010

Bryman A. (2018). *Samhällsvetenskapliga metoder*. Liber 2018, Upplaga 3

Den Hartog, D. N., House, R. J., Hanges, P. J., Ruiz-Quintanilla, S. A. & Dorfman, P. W. (1999). "Culture specific and cross-culturally generalizable implicit leadership theories: Are attributes of charismatic/transformational leadership universally endorsed*?"*. *The Leadership Quarterly*, 10: 219-256.

Dhillon G. & Backhouse J. (2000). "Information system security management in the new millennium*." In: Technical Opinion*, volym. 43 nr. 7 sid. 126-128 .

Durlak, J. A., & DuPre, E. P. (2008). "Implementation matters: A review of research on the influence of implementation on program outcomes and the factors affecting implementation." *American Journal of Community Psychology*, 41, 689–708.

Fairholm, R.M. (2004). “Different Perspectives on the Practice of Leadership”. Public *Administration Review*; Sep/Oct 2004; 64, 5; ProQuest Central pg. 577

Flowerday T. S. & Tuyikeze T. (2016) “Information security policy development and implementation: The what, how and who.” *Department of Information Systems, University of Fort Hare, South Africa*. June 2016, 169–183

Frye, W., D. (2007). *Network Security Policies and Procedures*. Springer Science & Business Media, LLC 2007. (179-185).

Gifford, W., Davies, B., Edwards, N., Griffin, P. & Lybanon, V. (2007). “Managerial leadership for nurses' use of research evidence: an integrative review of the literature.” *Worldviews of Evidence Based Nursing*, 4: 126-45.

Hagen, J., Albrechtsen, E., & Hovden, J. (2008). “Implementation and effectiveness of organizational information security measures.” *Information Management & Computer Security*, 16. (4), 377-397.

Hanberger, A. (2001). *“*What is the policy problem? Methodological challenges in policy evaluation*”. Evaluation,* vol. 7, no. 1, pp. 4562.

Hill, M. (2012) *Policyprocessen.* 1 uppl. Liber AB

Hrebiniak, L. G. (2006). “Obstacles to effective strategy implementation*”. Organizational Dynamics*, 25(1) 12-31

Johansson, C. (2013) ”Kommunikativt ledarskap som påverkar organisationens resultat”. *Mitt universitet. Avdelningen för medie och kommunikationsvetenskap*, 2-10

Johansson, C,. Miller V. (2012) ”Kommunikativt ledarskap. Metod och processer för utvärdering.” *Mitt universitet*

Knapp, K. J. & Ferrante, C. J. (2012). *”*Policy awareness, enforcement and maintenance: critical to information security effectiveness in organizations”. *Journal of Management Policy and Practice*. 13(5), 66-80.

Kruger, H. A. & W. D. Kearney. (2006). “A prototype for assessing information security awareness*.” Computers & security*. vol. 25, nr. 4, ss. 289-296.

Maltén, A. (2000). *Det pedagogiska ledarskapet*. Lund: Studentlitteratur.

Michie, S., van Stralen, M.M. & West, R. (2011). ”The behaviour change wheel: a new method for characterising and designing behaviour change interventions.” *Implementation Science*, 6:42.

O’Toole, L. J. (2000). “Research on policy implementation: Assessment and prospects.” *Journal of Public Administration Research and Theory*, 10(2), 263–288.

Ottoson, J. M., & Green, L. W. (1987). “Reconciling concept and context: Theory ofimplementation.*” Health Education and Promotion,* 2,353–382.

Rokstad, A, Vatne, S, Engedal, K, & Selbæk, G (2015). “The role of leadership in the implementation of person-centred care using Dementia Care Mapping: a study in three nursing homes*”, Journal of Nursing Management, 23, 1, pp. 15-26*

Siponen, M. & Vance, A. (2010).” Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations”. *MIS Quarterly*, 34(3), 487-502.

Tonnquist, B. (2016). *Projektledning*. 2 uppl. Stockholm: Sanoma utbildning.

Yukl, G. (2012). *Ledarskap i organisationer*. London: Pearson Education Limited

Wandersman, A.(2009). *Four Keys to Success (Theory, Implementation, Evaluation, and Resource/System Support): High Hopes and Challenges in Participation*. Springer Science+Business Media, LLC 2009

Whitman, M.E. & Mattord, H. J. (2012). *Principles of Informations Security*. Boston. Nelson Education Ltd.

Zammani M.; Razali R. (2016). “An Empirical Study of Information Security Management Success Factors.” *International Journal on Advanced Science*, 01 December 2016, Vol.6 (6), pp.904-913

# Bilagor

Bilaga 1

(Intervjufrågor till anställda)

-Vilka informationskanaler har ni för att sprida intern information? Vilka riktlinjer måste följas när anställda delar information inom organisationen?

-Känner du till om det finns några informationssäkerhetspolicyn på din arbetsplats?

-Är ni medvetna om vad säkerhetspolicy (riktlinjer) innehåller och på vilket sätt fick ni känna till dessa riktlinjer i första hand?

- Hur fick ni ta del av säkerhetspolicyns riktlinjer i första hand?

-På vilket sätt har anställda i verksamheten tillgång till säkerhetspolicyn för att utföra sina vardagliga uppgifter?

-Hur ser era rutiner ut efter säkerhetspolicyns införandet?

-På vilket sätt integreras personuppgiftslagen och offentlighets- och sekretesslagen i säkerhetspolicyn?

- På vilket sätt blir ni informerade om förändringar och uppdateringar av säkerhetspolicyn?

-Vilka aktiviteter finns det inom organisationen för att hjälpa er som anställda att ha en ökat medvetenhet kring säkerhetspolicyn? På vilket sätt anser du att de bidrar till medarbetarnas medvetenhet?

-Kan du beskriva någon form av utbildningar som du fick göra inom organisationen för att öka ditt lärande kring säkerhetspolicyns riktlinjer?

-Hur löser ni missuppfattningar och misförståelser kring säkerhetspolicyn inom organisationen?

- På vilket sätt anser du att anställda engagerar sig till säkerhetspolicyns efterlevnad?

-På vilket sätt anser du att din chef har arbetat med säkerhetspolicy för att säkerställa att ni som anställda ska följa policyns riktlinjer?

-Upplever ni att det finns en bra kommunikation mellan chefer och anställda angående säkerhetspolicyns riktlinjer och på vilket sätt föregår kommunikationen?

- Vilka konsekvenser finns det för anställda som bryter mot säkerhetspolicyns riktlinjer?

Bilaga 2

(Intervjufrågor till chefer)

1. Kan ni ge en beskrivning om hur ni har arbetat med att implementera säkerhetspolicyn i verksamheten?

2. Har ni en säkerhetsnål och isa fall hur arbetar ni för att säkerställa att säkerhetspolicyn mål uppnås?

3. På vilket sätt informerar ni era anställda om vikten att följa säkerhetspolicyn riktlinjer?

4. Hur arbetar ni för att förmedla säkerhetspolicyn ut till era anställda?

5. Vilka aktiviteter utförs för att öka era anställdas medvetenhet kring säkerhetspolicyns riktlinjer?

6. Finns det någon eller några utbildningsform/er och upplärning av säkerhetspolicyn som sker inom organisationen?

7. Vilka metoder brukar ni använda för att upprätthålla en kontinuerlig säkerhets tanke bland era anställda? T.ex. genom veckobrev, notiser, eventuellt olika sammankomster?

8. Hur informerar ni de anställda om de aktuella och eventuella interna eller externa säkerhetshoten?

9. Hur arbetar ni för att skapa ett bra arbetsklimat mellan anställda för att minska motstånd säkerhetspolicyn implementering?

10. På vilket sätt arbetar ni för att förändra eller att påverka anställdas beteende/attityd mot säkerhetspolicyn?

11. Har de anställda möjlighet att utrycka sina tankar eller ge feedback kring arbetet med säkerhetspolicyn och på vilket sätt sker detta?

12. Hur arbetar ni för att säkerställa att anställda efterlever säkerhetspolicyns uppsatta riktlinjer?

13. Vad blir det för konsekvenser ifall en anställd bryter mot era säkerhetsregler, oavsiktliga som avsiktliga?

HÖGSKOLAN
I BORÅS

Besöksadress: Allégatan 1 · Postadress: 501 90 Borås · Tfn: 033-435 40 00 · E-post: registrator@hb.se · Webb: www.hb.se