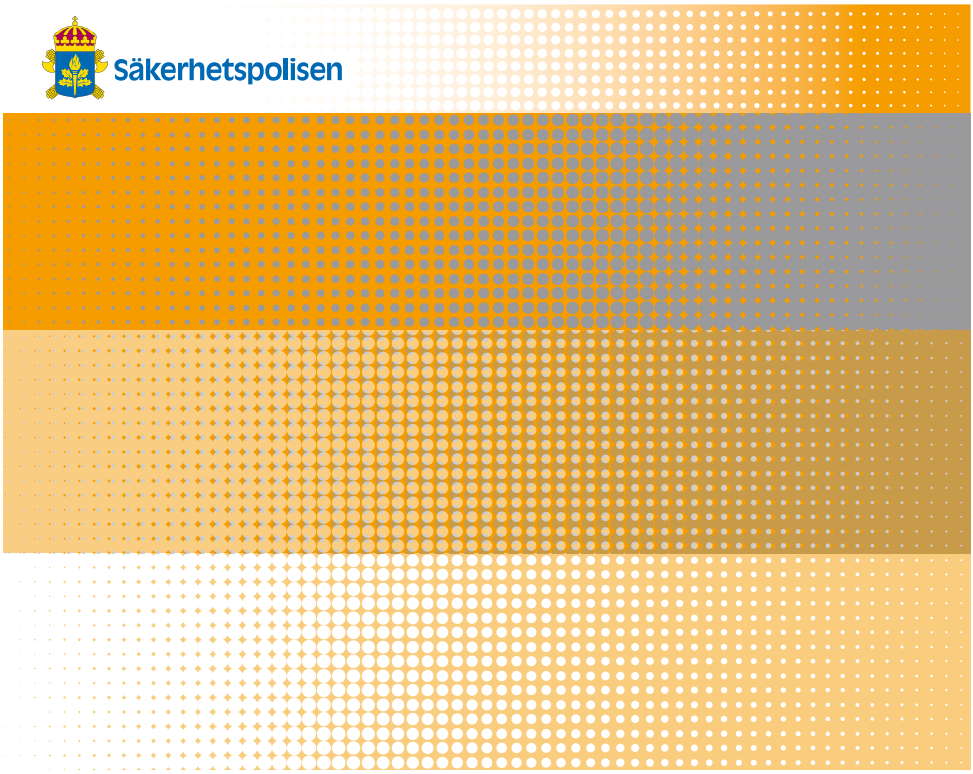
10 tips för säkrare outsourcing



Inledning – outsourcing

Myndigheter och andra organ inom den offentliga sektorn väljer i dag att i allt större utsträckning anlita externa parter för att utföra sådan verksamhet som inte utgör myndighetens kärnverksamhet. Upplägg att utkontraktera tjänster kallas i denna lathund för outsourcing. Outsourcing av it-tjänster innefattande informationshantering är särskilt vanligt.

En av de största utmaningarna med outscourcing är att kontrollen över den outsourcade verksamheten starkt begränsas, vilket utgör en särskild komplikation när det gäller säkerhetskänslig verksamhet.

Idag kan vi se en koncentration av it-uppdrag till ett fåtal leverantörer. Denna koncentration till ett fåtal företag som därmed får tillgång till en stor mängd samlad information medför en ökad sårbarhet för samhället.

Tendensen i samhället är att outsourcing av it kommer att fortsätta att öka. Molntjänster blir en allt vanligare leveransform samtidigt som säkerhetsaspekterna blir allt viktigare. Särskilda säkerhetsrelaterade aspekter gör sig

gällande när outsourcingen sker till en utländsk leverantör, s.k. offshoring.

Beroendet av externa aktörer kräver en kompetent kravställning, då ansvaret för bl.a. säkerhetsskyddskrav aldrig kan flyttas ut ur organisationen utan förblir detsamma som om myndigheten tillhandahållit tjänsten i egen regi.

I denna lathund beskrivs kortfattade rekommendationer inför upphandling och outsourcing. I lathunden används genomgående termen ”myndighet” vilket i detta fall avses omfatta även kommuner och landsting.

Med ”hemlig uppgift” avses i denna lathund detsamma som anges i 4 § säkerhetsskyddsförordningen (1996:633).

1. Kartlägg verksamhetens skyddsvärden i en säkerhetsanalys

Den mest grundläggande uppgiften en myndighet har inom säkerhetsskyddsarbetet är att kartlägga sin verksamhet i en säkerhetsanalys. En säkerhetsanalys ska svara på frågorna; *vad ska skyddas*, *mot vad* och *hur*.

- ✓ Börja med att identifiera myndighetens skyddsvärda resurser såsom lokaler, anläggningar, befattningar, information, system och rutiner.

- ✓ I säkerhetsanalysen ska en urskiljning göras avseende vilka delar av verksamheten som rör:
  - rikets säkerhet eller behöver skyddas mot terrorism och därför faller inom ramen för säkerhetsskyddsregleringen, och
  - andra skyddsvärden, t.ex. uppgifter som kan skada enskilda eller verksamhetens intressen, och därför kan behöva skyddas på annat sätt.

- ✓ Definiera vilka områden i verksamheten som kan bli föremål för outsourcing och vilka områden som av säkerhetsskyddsskäl bör hanteras internt.

- ✓ Omfattas viss mängd information av sekretess måste en sekretessprövning enligt offentlighets- och sekretesslagen (2009:400) (OSL) göras för att se om uppgifterna får lämnas ut till en privat leverantör.

- ✓ Bestäm och dokumentera vilken nivå av skydd som ska uppnås utifrån en dimensionerande hotanalys.

2. Placera in funktioner och tjänster i säkerhetsklass utifrån tillgång till hemlig information

Genom en säkerhetsanalys innehållande en process-orienterad informationskartläggning kan de funktioner och tjänster som hanterar hemliga uppgifter identifieras.

- ✓ Placera in de befattningar som hanterar hemliga uppgifter i säkerhetsklass (1-3).

- ✓ För de funktioner som placerats in i säkerhetsklass ska säkerhetsprövning och registerkontroll göras. För att göra en registerkontroll krävs samtycke från den enskilde. Tänk på att registerkontroll endast är en del av säkerhetsprövningen.

- ✓ Om en tjänst inplacerad i säkerhetsklass ska tillsättas av en konsult ska ett säkerhetsskyddsavtal (SUA) tecknas med konsultföretaget. Innan en konsult tillsätts på en säkerhetsklassificerad tjänst bör dock först utredas om tillgången till hemliga handlingar kan begränsas eller undvikas.

- ✓ Ett tecknat säkerhetsskyddsavtal är en förutsättning för att registerkontrollera extern personal. Personer som anlitas för säkerhetsklassade tjänster ska utbildas i säkerhetsskydd.

- ✓ Se över skrivningar i myndighetens allmänna villkor. Många myndigheter tillämpar allmänna villkor där förbehåll görs för att kräva registerkontroll av extern personal. Sådana förbehåll måste dock korrelera med krav på att teckna säkerhetsskyddsavtal och framgå redan av upphandlingsdokumenten.

3. Gör en säkerhetsanalys inför ditt upphandlings- eller outsourcingprojekt

Även om myndigheten har en generell säkerhetsanalys så behövs en specifik säkerhetsanalys som avgränsas för upphandlings- eller outsourcingprojektet, vilken med fördel kan tas fram under förstudiefasen.

- ✓ Bedöm om den specifika upphandlingen eller outsourcingprojektet behöver omges av säkerhetsskydd. Identifiera de säkerhetsskyddsåtgärder som ska vidtas av myndigheten själv och de krav som ska ställas på externa aktörer.

- ✓ Ställ säkerhetsskyddskrav i ett säkerhetsskyddsavtal *innan* hemliga uppgifter lämnas till en extern part. Bedöm vilken nivå säkerhetsskyddsavtalet ska vara på (1-3). På nivå 1 tillåts den externa parten ta med de hemliga uppgifterna till sina egna lokaler.

- ✓ Ett säkerhetsskyddsavtal på nivå 1 är inte säkrare än ett avtal på nivå 3. Försök istället så långt möjligt

att styra projektet så att de skyddsvärda uppgifterna behålls inom den egna verksamhetens kontroll.

- ✓ Vad gäller it-system så kan dessa ofta brytas ned i komponenter för att isolera områden som är särskilt skyddsvärda. Dessa områden kan sedan hanteras inom myndigheten med mindre eller obefintlig exponering för extern part.

- ✓ Var särskilt uppmärksam på aggregerade mängder uppgifter samt konsekvenserna av ett realiserat hot och uppgifternas betydelse, även för verksamheter som bedrivs av andra aktörer i samhället.

4. Samla de kompetenser som behövs

Att genomföra ett säkerhetsskyddat projekt inom upphandling eller outsourcing kräver kompetenser från olika delar av organisationen, såsom t.ex. verksamhetsföreträdare, upphandlare, informationssäkerhetsspecialist, it-säkerhetsspecialist, jurist, arkivarie, it-arkitekt, ev. SUA-handläggare m.fl.

- ✓ Om upphandlingen ska göras som en säkerhetsskyddad upphandling med säkerhetsskyddsavtal bör kompetens från säkerhetsorganisationen anlitas redan i inledningsskedet av upphandlingen så att kravställning på säkerhetsskydd görs redan i upphandlingsdokumenten.

- ✓ För att få med aspekter som t.ex. driftsäkerhet och tillgänglighet kan det vara bra att involvera handläggare för kontinuitetshantering.

- ✓ Ta hjälp av it-avdelningen för att kravställa på lagringslösningar, back-up-rutiner, säkerhetskopiering, loggning m.m.

- ✓ Säkerhetsskyddschefen, eller en person som denne utser, ska närvara vid förhandling och undertecknande av säkerhetsskyddsavtalet.

- ✓ Planera redan vid framtagandet av säkerhetsskyddsavtalet vem i myndigheten som ansvarar för avtalet och som ska sköta avtalsförvaltning, kontroll och uppföljning.

5. Anpassa ditt säkerhets-skyddsavtal utifrån situation

Säkerhetsskyddsbedömningar ska ske löpande så det är viktigt att både affärsavtalet och säkerhetsskyddsavtalet är skrivet med handlingsutrymme och möjlighet till justeringar.

- ✓ Använd gärna Säkerhetspolisens mallar för säkerhetsskyddsavtal men anpassa dem efter situation och behov. Säkerhetsskyddsavtal ska träffas med både huvudleverantör och eventuella underleverantörer.

- ✓ Undvik standardavtal för affärsavtalet då dessa sällan är anpassade för säkerhetsskyddad upphandling.

- ✓ Glöm inte att reglera säkerhetsskyddsaspekter även för sido- och tilläggsavtal såsom supportavtal.

- ✓ Ta hjälp av en jurist även för arbetet med säkerhetsskyddsavtalet för att säkerställa tydlighet i avtalet. Oklara avtalsvillkor tolkas till nackdel för den som tillhandahåller avtalet.

- ✓ Var noga med att reglera vad som händer vid avslut av affärsförbindelsen, särskilt vad gäller

återlämnande eller förstöring av hemliga uppgifter samt räckvidden av tystnadsplikten.

- ✓ Underteckna aldrig affärsavtalet innan säkerhetsskyddsavtalet är undertecknat och leverantören blivit godkänd.

6. Skriv bara säkerhetsskyddskrav som kan kontrolleras och följas upp

Även om verksamhet outsourcas krävs kompetenta kravställare internt. Säkerställ intern kompetens bl.a. avseende informations- och it-säkerhet. Utse vem i den egna organisationen som är ansvarig för den outsourcade verksamheten.

- ✓ Ställ endast sådana krav som är relevanta, tydliga och mätbara.

- ✓ Internt kontinuitetshanteringsarbete kan utgöra en bra grund för kravställningen på leverantören.

- ✓ Se till att ha en så nära dialog som möjligt med leverantören och en bra samverkansmodell, också vad gäller säkerhetsskyddsfrågor. Ha gärna en tidig dialog med leverantörerna för att säkerställa att de har en mognad och erfarenhet av att bemöta och hantera säkerhetsskyddskrav.

- ✓ Ställ krav på leverantören att dokumentera säkerhetsprövningssamtal, registerkontroller och genomförd utbildning. Sådan dokumentation underlättar myndighetens kontroll.

- ✓ Krav på säkerhetsskydd kan förenas med vite. Säkerställ att nivån för vitets takbelopp inte sätts för lågt.

7. Tänk efter extra vid utländska leverantörer

Långa leverantörskedjor minskar möjligheterna till insyn i den outsourcade verksamheten vilket särskilt gäller när leverantören utför arbetet utanför Sveriges gränser. Ställ krav att som myndighet få godkänna vilka underleverantörer som huvudleverantören använder under uppdraget.

- ✓ Ta reda på om Sverige har tecknat ett generellt säkerhetsskyddsavtal (GSA) med det aktuella landet. I ett GSA regleras bl.a. hur parterna ska agera vid ett eventuellt röjande av hemlig information.

- ✓ Det är särskilt viktigt att de krav som ställs är konkreta och möjliga att kontrollera. Se till att inga nyanser i språkbruk försvinner i avtalsöversättningen.

- ✓ Notera att Säkerhetspolisens registerkontroll inte alltid ger ett relevant resultat avseende utländska medborgare. Det är därför av ännu större vikt att omfattande arbete görs avseende säkerhetsprövningen i övrigt.

- ✓ Ta kontroll över säkerhetsprövningen. Om möjligt genomför säkerhetsprövningen själv eller begär in noggrann dokumentation.

- ✓ Bedöm särskilt den utländska personalens lojalitet mot svenska intressen och andra eventuella intressekonflikter.

- ✓ Att ha en representant från myndigheten på plats, s.k. on-site liaison officer, kan vara ett bra sätt att förbättra kontrollen över den outsourcade verksamheten och kan användas även avseende säkerhetsskyddsarbetet.

8. Kan man använda molntjänster?

Det finns inga generella förbud mot att i vissa fall använda molntjänster, däremot behövs en noggrann analys göras då det inte alltid är lämpligt att använda en sådan leverantör eller tjänst. Särskild försiktighet bör iakttas då den information som molntjänstleverantören ska hantera innehåller allmänna handlingar, sekretessbelagda uppgifter eller personuppgifter.

Det är vanligt att outsourcingleverantören tillhandahåller molntjänster från en tredje part vilket gör det svårare för den verksamhetsansvarige att kontrollera säkerhetsskyddsaspekter.

- ✓ En informationsklassificering underlättar en bedömning av vilken information som kan läggas ut i molnet. Om klassificeringen visar på hög känslighet och stora risker bör myndigheten avstå från en molnlösning. Information som rör rikets säkerhet får inte hanteras i molnet om inte tillfredsställande säkerhetsskydd kan garanteras.

- ✓ Även om informationen får lämnas ut enligt offentlighets- och sekretesslagen kan det finnas

omständigheter som ändå gör det olämpligt att anlita en molntjänstleverantör. Omständigheter att beakta kan t.ex. vara vilket lands rättsordning som blir tillämplig på lagrad information, om leverantören regelbundet byter ut sina underleverantörer och vem som ansvarar för informationsförlust m.m.

- ✓ System och information som upprättas i molnet kan bli låst till leverantören och vara mycket svår att flytta därifrån. Information som upprättas i molnet kan också vara svår att gallra och radera. Att ta bort information från molnet är inte att jämställa med att radera.

9. Integrera säkerhetsskyddsarbetet i verksamhetens ordinarie processer

En framgångsfaktor för att få med säkerhetsskyddsaspekter vid upphandling och outsourcing är att göra säkerhetsskyddsarbetet till en ordinarie process i verksamheten. Det är viktigt att säkerhetsskyddsfrågor inte bara blir en angelägenhet för säkerhetsorganisationen inom myndigheten utan även för verksamhetsföreträdare, ledningen och inköpsorganisationen.

- ✓ Säkerhetsskyddad upphandling blir ofta en fråga som faller utanför ordinarie ansvarsfördelning. Utnyttja de styrande dokument som finns inom organisationen och lägg fast ansvar för de olika rollerna inom ramen för upphandlings- och SUA-processen.

- ✓ Inköpsorganisationen bör arbeta med anskaffningsplaner som delges säkerhetsorganisationen för att i god tid identifiera projekt som kräver säkerhetsskydd.

- ✓ Glöm inte att efter avtalsslut utvärdera affärsrelationen och säkerhetsskyddsarbetet; vad har

fungerat bra och vad har fungerat mindre bra? Utnyttja de uppföljningsmekanismer som finns på plats i organisationen. Utvärdera särskilt hur kravställningen på säkerhetsskydd har tagits emot och implementerats; kanske finns det krav som bör förtydligas.

10. Anmäl och avanmäl säkerhets-skyddsavtal och registerkontroller hos Säkerhetspolisen

- ✓ Alla ingångna säkerhetsskyddsavtal ska anmälas till Säkerhetspolisen enligt särskild blankett. Det är viktigt att de ansökningar om registerkontroll som görs kopplas till relevant säkerhetsskyddsavtal samt affärsavtal och/eller upphandlingsprojekt.

- ✓ Vad gäller löpande registerkontroller ska förändringar i civilstånd anmälas till Säkerhets-polisen för klass 1 och 2.

- ✓ När ett säkerhetsskyddsavtal upphör ska det avanmälas hos Säkerhetspolisen. Avanmäl också de registerkontroller som inte längre är relevanta. Observera att ett gällande säkerhetsskyddsavtal är en förutsättning för att registerkontrollera extern personal. Om säkerhetsskyddsavtalet inte längre är gällande så finns inte längre grund för att utföra registerkontroll.

- ✓ Observera också att den skyldighet som finns för myndigheter att anmäla it-incidenter i enlighet med 10 a § säkerhetsskyddsförordningen också gäller sådan verksamhet som outsourcas. Det är därför viktigt att i avtal tillse att sådan information lämnas till myndigheten från leverantören.

För mer information om hur du kan tänka kring säkerhetsskydd och outsourcing – läs mer på www.sakerhetspolisen.se.

Säkerhetspolisen