Säkerhetspolisen

SÄKERHETSSKYDDAD UPPHANDLING

– en vägledning

PRODUKTION: Säkerhetspolisen, april 2009. Reviderad januari 2010
GRAFISK FORMGIVNING: Jerhammar & Co Reklambyrå AB
TYPOGRAFI: Eurostile och Swift

Förord

Detta är Säkerhetspolisens vägledning till handläggning av säkerhetsskyddad upphandling. Syftet med vägledningen är att stödja den enskilda handläggaren i upphandlingsarbetet. Den ska också kunna användas i utbildningssammanhang.

Vägledningen vänder sig i första hand till de myndigheter över vilka Säkerhetspolisen har ett tillsynsansvar. Den är en omarbetning av publikationen Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (H SÄK SUA), utarbetad i samverkan mellan Säkerhetspolisen och Försvarsmakten och utgiven 2000 av Försvarsmakten.

Grunden till denna vägledning har utarbetats genom ett nära och omfattande samarbete med Försvarsmakten. Förhoppningen är att vägledningen ska tydliggöra och förenkla processen för dem som arbetar med säkerhetsskyddad upphandling i den civila sektorn.

Ett säkerhetsskyddsavtal innebär att säkerhetsskyddsåtgärder vidtas hos en leverantör för att säkerställa att uppgifter som omfattas av sekretess med hänsyn till rikets säkerhet hanteras på ett säkert sätt. Därför är det av största vikt att processen med säkerhetsskyddad upphandling går rätt till.

PÄR KIHLSTRÖM
Chef säkerhetsskyddsenheten, Säkerhetspolisen

Innehållsförteckning

1 Inledning

1.1 SYFTE, MÅLGRUPP OCH AVGRÄNSNINGAR

När en myndighet (staten, kommun eller landsting) avser att begära in ett anbud eller träffa avtal om upphandling där det förekommer hemliga uppgifter, ska myndigheten enligt 8 § säkerhetsskyddslagen träffa ett skriftligt säkerhetsskyddsavtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet. Syftet med denna vägledning är att beskriva handläggningen av säkerhetsskyddsarbetet vid en säkerhetsskyddad upphandling. Den vänder sig i första hand till de myndigheter över vilka Säkerhetspolisen har ett tillsynsansvar.

Bestämmelserna om säkerhetsskyddad upphandling gäller inte för bolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt inflytande. Bestämmelserna gäller inte heller för enskilda som omfattas av säkerhetsskyddslagen, eller för sådana kommittéer eller särskilda utredare som avses i kommittéförordningen (1976:119).

För riksdagen och dess myndigheter finns likalydande bestämmelser om säkerhetsskyddad upphandling i 8 § lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter.

Vägledningen beskriver främst upphandlingar där uppdraget genomförs i Sverige.

1.2 VÄGLEDNINGENS DISPOSITION OCH INNEHÅLL

Vägledningen innehåller fyra kapitel samt bilagor:

- *Kapitel 1 (Inledning)* innehåller allmän information kring säkerhetsskyddad upphandling samt vägledningens målgrupp, avgränsningar, upplägg och innehåll.
- *Kapitel 2 (Säkerhetsskydd)* förklarar vad som ingår i begreppet säkerhetsskydd.
- *Kapitel 3 (Processen säkerhetsskyddad upphandling)* beskriver utifrån ett flödesschema hur arbetet med en säkerhetsskyddad upphandling kan genomföras.
- *Kapitel 4 (Säkerhetsskyddad upphandling med utländskt företag m.m.)* beskriver översiktligt säkerhetsskyddad upphandling med utländska företag.
- *Bilagorna A–C* innehåller mallar för säkerhetsskyddsavtal. Mallarna ska ses som vägledande, och ska justeras efter behov.
- *Bilaga D* innehåller ett exempel på sekretessförbindelse.
- *Bilaga E* innehåller begreppsförklaringar över ord och termer som används i denna vägledning.
- *Bilaga F* innehåller en lista över de bestämmelser och publikationer som hänvisas till i texten och, i förekommande fall, i inledningen till kapitlen. I bilagan listas även andra publikationer som är relevanta för ämnet.

Med begreppet MYNDIGHET avses stat, kommun och landsting. Fortsättningsvis kommer begreppet att användas med denna heltäckande innebörd, utan att detta preciseras varje gång det förekommer i vägledningen.

Med begreppet HEMLIG UPPGIFT avses en uppgift som omfattas av sekretess och som rör rikets säkerhet.

1.3 VAD ÄR SÄKERHETSSKYDDAD UPPHANDLING?

Verksamhet som omfattas av säkerhetsskyddslagen ska ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Ansvaret för säkerhetsskyddet ligger hos den som är verksamhetsansvarig. När det i en upphandling förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess (hemliga uppgifter) har staten, kommuner och landsting ansvaret för att det finns ett fullgott säkerhetsskydd hos leverantören.

För att tillgodose kravet på säkerhetsskydd när sådan verksamhet utförs på uppdrag av en myndighet, ska den uppdragsgivande myndigheten träffa ett skriftligt avtal – säkerhetsskyddsavtal – med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det enskilda fallet. Denna process benämns säkerhetsskyddad upphandling.

I lagen om offentlig upphandling (LOU) respektive lagen om upphandling inom områdena vatten, en-

ergi, transporter och posttjänster (LUF) regleras hur en upphandling ska genomföras.

Ibland används också begreppen outsourcing och offshoring. Båda inbegrips dock i begreppet upphandling.

För upphandlingar som omfattas av sekretess eller andra särskilda begränsningar med hänsyn till rikets säkerhet tillämpas endast 15–16 kap. i LOU och LUF.

Säkerhetsskyddad upphandling får inte utnyttjas i konkurrensbegränsande eller annat diskriminerande syfte.

Ett företag får inte utan myndighetens tillstånd offentliggöra att det har träffat ett säkerhetsskyddsavtal. Denna information får därmed inte användas i marknadsföring eller på annat sätt.

2 Säkerhetsskydd

2.1 VAD ÄR SÄKERHETSSKYDD?

Med säkerhetsskydd avses:
1. Skydd mot brott som kan hota rikets säkerhet
2. Skydd av hemliga uppgifter
3. Skydd mot terroristbrott enligt 2 § lagen om straff för terroristbrott (terrorism), även om brot tet inte hotar rikets säkerhet.

Säkerhetsskydd innebär alltså att myndigheter och andra som säkerhetsskyddslagstiftningen gäller för ska vidta förebyggande åtgärder för att skydda mot brott som kan hota rikets säkerhet, såsom spionerі och sabotage.

Hemliga uppgifter som rör rikets säkerhet ska också skyddas. Offentlighets- och sekretesslagen ger inga anvisningar om hur sådana uppgifter ska hanteras. Detta regleras i stället i säkerhetsskyddslagstiftningen.

Säkerhetsskyddet omfattar också skydd mot terrorism. I vissa fall utgör terroristbrott ett hot mot rikets säkerhet, i andra fall inte. Med terroristbrott avses endast allvarliga angrepp utförda i avsikt att rasera de grundläggande principerna för en fungerande demokrati. De gärningar som kan utgöra terroristbrott är bland annat mord, dråp, grov skadegörelse, mordbrand, sabotage och spridande av gift eller smitta. Ett skydd mot terroristbrott ligger därför under alla förhållanden nära värnet om rikets säkerhet.

Verksamhet som omfattas av säkerhetsskyddslagstiftningen ska ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Skyddsvärda resurser ska regelbundet inventeras i en så kallad säkerhetsanalys.

Säkerhetsskyddet ska förebygga:
1. Att hemliga uppgifter obehörigen röjs, änd ras eller förstörs (informationssäkerhet)
2. Att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som avses i punkt 1 eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning)
3. Att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning).

Säkerhetsskyddet ska även i övrigt förebygga terrorism.

Utbildning och kontroll är andra viktiga delar i det förebyggande säkerhetsskyddsarbetet.

Bestämmelser om säkerhetsskydd finns i säkerhetsskyddslagen, säkerhetsskyddsförordningen samt i föreskrifter och allmänna råd som meddelas av Rikspolisstyrelsen och Försvarsmakten för sina specifika ansvars- och tillsynsområden. En myndighet kan också meddela egna föreskrifter inom sitt verksamhetsområde om verkställigheten av säkerhetsskyddslagen.

2.1.1 Säkerhetsanalys

5 § säkerhetsskyddslagen
5 § säkerhetsskyddsförordningen
2 § lagen om straff för terroristbrott
1 kap. 5 § RPSFS 2010:03
Kap. 1.3 Säkerhetsskydd – en vägledning

Av myndighetens säkerhetsanalys ska det framgå:
- Vilka uppgifter i verksamheten som ska hållas hemliga med hänsyn till rikets säkerhet
- Vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller till skydd mot terrorism
- Vilka IT-system som behandlar hemliga uppgifter eller som behöver skyddas mot terrorism.

Resultatet av säkerhetsanalysen ska dokumenteras och revideras regelbundet.

Säkerhetsanalysen utgör grunden för säkerhetsskyddsarbetet på en myndighet. Analysen ska definiera vad som är skyddsvärt och varför det är skyddsvärt. Det kan även vara av betydelse att i säkerhetsanalysen ange vilka verksamheter som inte behöver ett säkerhetsskydd. En väl dokumenterad säkerhetsanalys ger spårbarhet i säkerhetsskyddsarbetet, vilket är viktigt vid exempelvis förändringar i hotbild, myndighetens verksamhet eller organisation. Denna analys utgör också ett beslutsunderlag för myndighetens ledning när beslut fattas om verksamhetens säkerhetsskydd.

2.1.2 Informationssäkerhet

9 § säkerhetsskyddslagen
9–13 §§ säkerhetsskyddsförordningen
1 kap. 6 §, 2–4 kap. RPSFS 2010:03
Kap. 2–4 Säkerhetsskydd – en vägledning

Hemliga uppgifter ska skyddas oavsett vilken form de har. Hemliga uppgifter kan framgå av ett visst förhållande (resurser och verksamhet av vilka det framgår planläggning, belägenhet, beredskap, intresseinriktning, effekt med mera), av en anläggning (för en viss funktion eller verksamhet iordningställt markområde, byggnad eller annat utrymme samt för verksamheten erforderliga installationer såsom datahall med mera) eller av ett föremål (handling eller materiel).

Myndigheter ska förvara sina hemliga uppgifter på ett säkert sätt, så att obehöriga inte kan komma åt dem. En hemlig handling i skrift eller bild ska förvaras i ett förvaringsutrymme med sådan skyddsnivå att den inte obehörigen röjs, ändras eller förstörs. Materiel som innehåller hemliga uppgifter ska så långt det är möjligt hanteras på samma sätt som hemliga handlingar. Materiel innefattar även digitala lagringsmedier. Det är viktigt att utöver de enskilda hemliga uppgifterna även bedöma den totala mängden hemliga uppgifter vid utformningen av säkerhetsskyddet.

När hemliga uppgifter hanteras i IT-system är det viktigt att det sker på ett säkert sätt. För att uppnå detta behövs dels styrdokument som reglerar utformning och användning av IT-system, dels tekniska lösningar som uppfyller kraven för IT-system. Styrdokument, som beslutats av myndighetens chef, ska definiera mål, riktlinjer och instruktioner för förvaltning, drift och användning. Det ska även finnas en systemsäkerhetsansvarig som är utsedd av myndighetens chef.

Begreppet IT-system inkluderar utöver ordinära datorer och nätverksutrustning även till exempel kopiatorer och mobiltelefoner.

Innan ett IT-system som innehåller hemliga uppgifter anskaffas eller förändras ska en översiktlig analys genomföras för att fastställa vilket framtida säkerhetsskydd systemet behöver. Analysen ska även innehålla de åtgärder som behöver vidtas för att uppnå ett nödvändigt säkerhetsskydd. Analysen ska dokumenteras.

Utformningen av säkerhetsskyddet för ett eller flera sammankopplade IT-system som innehåller hemliga uppgifter innebär som regel att dessa är separerade från andra IT-system. Det betyder att IT-systemet inte kan kommunicera, varken trådbundet eller trådlöst, med andra IT-system.

Vid utformning av säkerhetsskydd för IT-system är det viktigt att anpassa följande:
- Behörighetskontroll
- Säkerhetslogg
- Skydd mot skadlig kod
- Intrångsdetektering
- Skydd mot intrång
- Skydd mot röjande signaler
- Skydd mot obehörig avlyssning
- Incidenthantering
- Säkerhetskopiering
- Kontinuitetsplan
- Hantering av elektroniska hemliga handlingar
- Hantering av digitala lagringsmedier.

För att bekräfta att säkerheten för IT-systemet i verkligheten uppfyller ställda krav ska det granskas. Det innebär att någon som inte har deltagit vid utformningen av IT-systemet kontrollerar att säkerhetskraven på IT-systemet är uppfyllda. Granskningen ska genomföras och dokumenteras innan driftgodkännandet. Vid granskningen är det särskilt viktigt att klargöra om IT-systemet kommunicerar med andra IT-system. Om det är fallet ska

det noggrant undersökas hur och till vilka system det kommunicerar.

Kan nödvändigt skydd inte uppnås ska myndigheten av säkerhetsskäl avstå från ett IT-system.

2.1.3 Tillträdesbegränsning

10 § säkerhetsskyddslagen
5 kap. RPSFS 2010:03
Kap. 5 Säkerhetsskydd – en vägledning

Tillträdesbegränsning ska hindra att obehöriga får tillgång till platser där det finns hemliga uppgifter eller där det bedrivs verksamhet som har betydelse för rikets säkerhet. Tillträdesbegränsning kan också användas för att förhindra terroristattentat samt skydda personer eller egendom mot angrepp och våldsbrott. Myndigheter ska utforma sin tillträdesbegränsning så att allmänhetens rätt att röra sig fritt inte inskränks mer än nödvändigt. Behovet av skydd ska styra utformningen.

Tillträdesbegränsningen kan gälla både för utomstående och för egna medarbetare. Medarbetarna får då enbart tillgång till lokaler eller områden som de har behov av för sitt arbete.

Bestämmelser om förbud mot tillträde till skyddsobjekt finns i lagen (1990:217) om skydd för samhällsviktiga anläggningar.

2.1.4 Säkerhetsprövning

11–13, 17–19 §§ säkerhetsskyddslagen
14, 18–19, 38 §§ säkerhetsskyddsförordningen
6 och 8 kap. RPSFS 2010:03
Kap. 6 och 8 Säkerhetsskydd – en vägledning

Säkerhetsprövning ska göras innan en person deltar i verksamhet som har betydelse för rikets säkerhet eller som är viktig att skydda mot terrorism. Prövningen ska klarlägga om personen är lojal och pålitlig från säkerhetssynpunkt.

Säkerhetsprövning ska grunda sig på:
- Personlig kännedom om den som prövningen gäller
- Uppgifter som framgår av till exempel betyg, intyg och referenser
- Uppgifter från registerkontroll och särskild personutredning som kan ingå som en del i prövningen.

Registerkontroll ska göras vid säkerhetsprövning som gäller deltagande i verksamhet som har placerats i säkerhetsklass. Registerkontroll innebär att uppgifter hämtas från register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller polisdatalagen (1998:622). Vid registerkontroll hämtas också de personuppgifter in som Rikspolisstyrelsen eller Säkerhetspolisen behandlar, utan att de ingår i ovan nämnda register.

Ett uppdrag kan placeras i säkerhetsklass 1, 2 eller 3. Det är viktigt att komma ihåg att det är uppdraget som placeras i en viss säkerhetsklass, inte personen som ska utföra det.

Skulle det komma fram uppgifter vid registerkontrollen som är av betydelse för uppdraget som personen ska delta i, kan dessa komma att lämnas ut till den myndighet som har beslutat om registerkontrollen. Registerkontrolldelegationen, som är en del av Säkerhets- och integritetsskyddsnämnden, beslutar om utlämnande av uppgifter i varje enskilt ärende.

Myndigheten som beslutar om registerkontroll av någon som inte ska delta i den egna verksamheten ska vid behov samråda med arbetsgivaren för att få ytterligare underlag för bedömningen av den anställdes pålitlighet från säkerhetssynpunkt eller då beslut efter registerkontrollen ska meddelas. Uppgifterna ska hanteras med stor varsamhet och endast delges arbetsgivarens säkerhetsskyddsansvariga och övriga som oundgängligen behöver uppgifterna.

2.1.5 Intern utbildning och kontroll

30 § säkerhetsskyddslagen
9 kap. RPSFS 2010:03
Kap. 9 Säkerhetsskydd – en vägledning

En förutsättning för ett effektivt säkerhetsskydd är att samtliga medarbetare på en arbetsplats får grundläggande utbildning i frågor om säkerhetsskydd. Utbildningen ska klargöra varför och hur man ska vidta skyddsåtgärder mot hot av olika slag. Utbildningen bör genomföras så att det skapas en positiv och aktiv inställning till säkerhetsskydd samt ett ökat säkerhetsmedvetande hos målgruppen. Ytterligare utbildning bör ges till dem som direkt befattar sig med hemliga uppgifter eller har sin arbetsplats förlagd på ett område där säkerhetskänslig verksamhet bedrivs.

Vid varje myndighet ska det finnas en plan för utbildning i säkerhetsskydd. Denna plan bör även omfatta utbildning för de företag med vilka myn-

digheten har träffat säkerhetsskyddsavtal. En förteckning bör också föras – företagsvis – över säkerhetsprövade personer som har genomgått utbildning i säkerhetsskydd, på samma sätt som görs avseende myndighetens egna anställda.

Varje myndighet ska ha en plan för intern kontroll av säkerhetsskyddet. Kontrollens syfte är att utröna om bestämmelserna om säkerhetsskydd efterlevs vid den egna myndigheten och att skyddsnivån är jämn och tillräckligt hög. Planen bör även omfatta kontroll av de företag med vilka myndigheten har träffat säkerhetsskyddsavtal. Myndigheten ska föra protokoll över varje kontroll. Protokollen ska förvaras samlade på myndigheten.

2.1.6 Tillsyn

31 § säkerhetsskyddslagen
41–42 §§ säkerhetsskyddsförordningen
9 kap. 4–6 §§ RPSFS 2010:03
Kap. 9 Säkerhetsskydd – en vägledning

Säkerhetsskyddet hos företag som har träffat säkerhetsskyddsavtal ska kontrolleras av den myndighet som har ingått avtalet. Försvarsmakten och Säkerhetspolisen kan också i samråd med myndigheten utföra kontroll av säkerhetsskyddet.

2.1.7 Föreskrifter och råd

33 § säkerhetsskyddslagen
43–45 §§ säkerhetsskyddsförordningen
1 kap. 5 § RPSFS 2010:03
Kap. 11 Säkerhetsskydd – en vägledning

För att underlätta hanteringen vid säkerhetsprövning och säkerhetsskyddad upphandling rekommenderas att myndigheten beslutar om interna bestämmelser. Verkställighetsföreskrifter kan också regleras i myndighetens arbetsordning.

När det gäller säkerhetsskyddad upphandling bör myndigheten dokumentera exempelvis handläggningsrutiner i samband med säkerhetsbedömning, säkerhetsprövning samt avslutande av uppdrag som har omgetts av säkerhetsskydd.

2.2 VARFÖR SKA MYNDIGHETER TRÄFFA SÄKERHETSSKYDDSAVTAL?

8 § säkerhetsskyddslagen
7 och 15 §§ säkerhetsskyddsförordningen
7 kap. RPSFS 2010:03

Utgångspunkten för säkerhetsskyddslagstiftningen är att de intressen som lagstiftningen slår vakt om ska ha samma skydd oavsett på vilket sätt verksamheten bedrivs. I detta sammanhang får det förstås så att myndighetens hemliga uppgifter ska ges samma säkerhetsskydd hos anbudsgivare och leverantör som de har på myndigheten. När det i en upphandling förekommer hemliga uppgifter, har myndigheten ansvaret för att det finns ett fullgott säkerhetsskydd.

Myndigheter ska därför genomföra säkerhetsskyddad upphandling när en anbudsgivare eller en leverantör kan få del av hemliga uppgifter. Myndigheten och företaget ska då träffa ett skriftligt avtal om de säkerhetsskyddsåtgärder som behövs i det särskilda fallet. Om förfrågningsunderlaget innehåller hemliga uppgifter innebär det att ett säkerhetsskyddsavtal måste tecknas redan innan anbudsgivaren kan få del av förfrågningsunderlaget. Ett företag, enskilt eller offentligt, som vill konkurrera om ett upphandlingskontrakt måste acceptera myndighetens uppfattning att ett säkerhetsskyddsavtal krävs.

Att ett säkerhetsskyddsavtal har slutits innebär inte att säkerhetsskyddslagen blir tillämplig på företagets verksamhet. Ett företag som redan omfattas av säkerhetsskyddslagen, genom att det allmänna utövar ett rättsligt bestämmande inflytande eller på grund av att verksamhet av betydelse för rikets säkerhet bedrivs av företaget, kan inte genom villkor i ett säkerhetsskyddsavtal få mindre långtgående åligganden än vad som följer av lagen. Det finns emellertid inget som hindrar att säkerhetsskyddet utökas eller i övrigt preciseras till vad som behövs i det aktuella uppdraget. Ett säkerhetsskyddsavtal måste under alla förhållanden ingås när förutsättningarna är sådana som anges ovan.

3 Processen säkerhetsskyddad upphandling

Detta kapitel redovisar hur en säkerhetsskyddad upphandling kan genomföras. Flödesschemat på nästa sida illustrerar processen dels när förfrågningsunderlaget innehåller hemliga uppgifter, dels när förfrågningsunderlaget inte innehåller hemliga uppgifter.

3.1 SÄKERHETSBEDÖMNING

5 § säkerhetsskyddsförordningen
1 kap. 5–6 §§, 7 kap. 2–3 §§ RPSFS 2010:03
Kap. 1.3 Säkerhetsskydd – en vägledning

En myndighet som avser att begära in anbud eller genomföra en upphandling måste ta ställning till om det i anbudet eller upphandlingen förekommer hemliga uppgifter. Om så är fallet, ska dessa uppgifter ha samma säkerhetsskydd hos företaget där uppdraget eller tjänsten utförs som hos myndigheten. Ansvaret för detta ligger på myndigheten.

I vissa fall kan uppdragets karaktär, omfattning eller komplexitet medföra att det finns behov av att inför ett anbud eller en upphandling göra en särskild säkerhetsanalys avseende det aktuella uppdraget. Denna analys bör utgå från myndighetens säkerhetsanalys. Resultatet av den för uppdraget genomförda analysen bör dokumenteras i en säkerhetsplan. Denna säkerhetsplan utgör sedan underlag för bedömning om ett säkerhetsskyddsavtal ska träffas för det aktuella anbudet eller upphandlingen.
Av säkerhetsplanen bör det också framgå vilka säkerhetsskyddsåtgärder som bedöms som nödvändiga i det aktuella anbudet eller upphandlingen.

Myndighetens säkerhetsskyddschef bör samverka med den som ansvarar för myndighetens upphandling redan i anskaffningsplaneringen. En sådan samverkan bidrar till att myndighetens säkerhetsskyddade upphandlingar planeras och förbereds i god tid.

Nivån på säkerhetsskyddet samt övriga krav på säkerhetsskydd bör anges redan i förfrågningsunderlaget, eftersom upphandlingen normalt måste göras om ifall den upphandlande myndigheten finner det nödvändigt att väsentligt ändra kraven under upphandlingens gång.

Utmynnar säkerhetsbedömningen inför en förestående upphandling i att något säkerhetsskydd inte behövs, kan ändå bedömningen vara att det är lämpligt att vidta vissa säkerhetsskyddsåtgärder. Dessa åtgärder kan till exempel bestå av utbildning av personalen eller information om tystnadsplikt. Krav på sådana säkerhetsskyddsåtgärder kan då ingå i affärsavtalet.

3.2 VAL AV UPPHANDLINGSFORM

Upphandlingsreglerna, en introduktion

Upphandling som rör rikets säkerhet regleras i 15 kap. LOU och LUF.

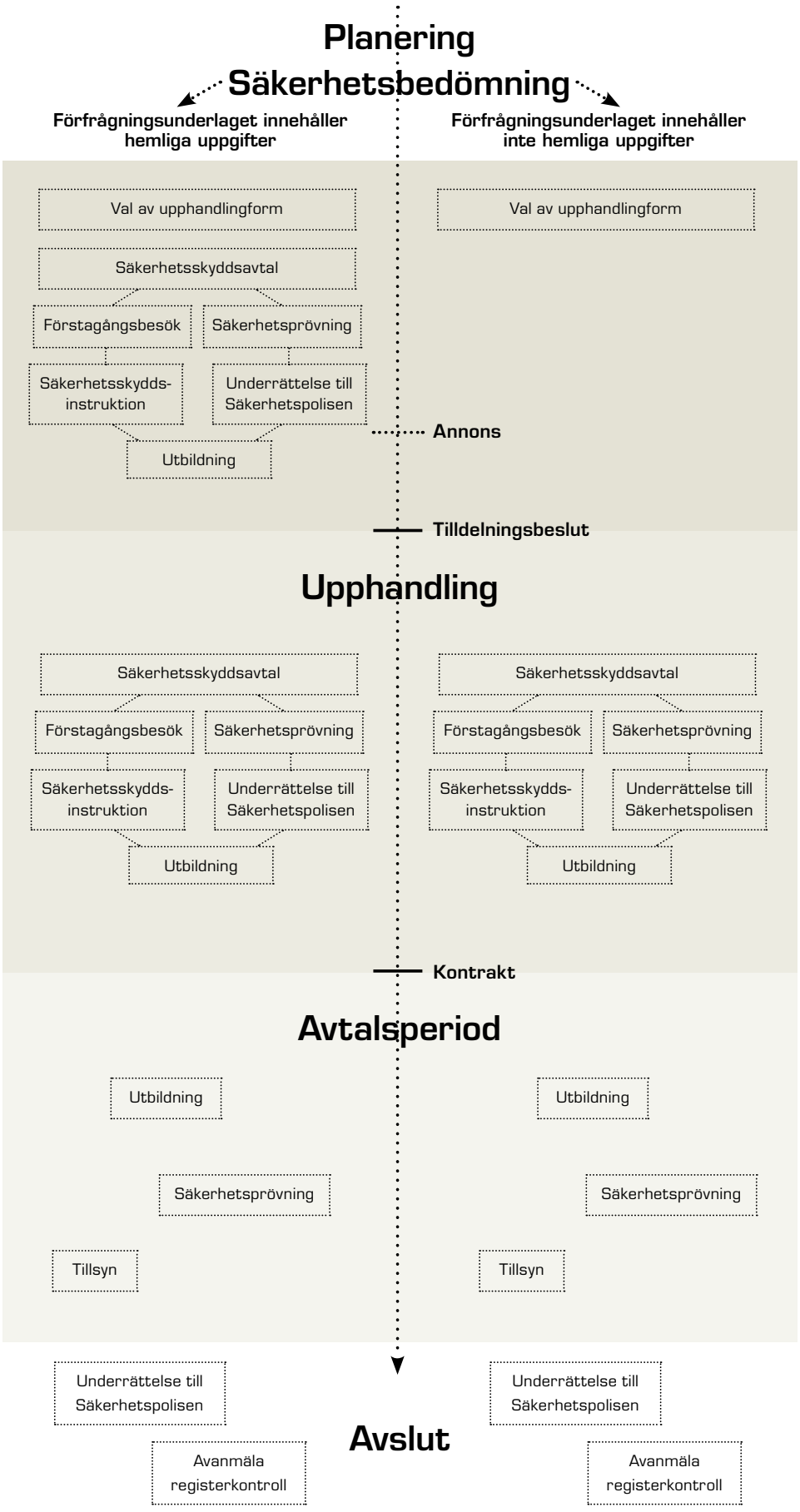
En upphandling enligt 15 kap. LOU och LUF ska göras genom förenklat förfarande eller urvalsförfarande. I vissa fall får också direktupphandling användas. Undantag från bestämmelserna i dessa kapitel får i enskilda fall beslutas av regeringen. Försvarets materielverk, FRA och Säkerhetspolisen får också själva besluta om vissa undantag.

3.3 SÄKERHETSSKYDDSAVTAL

8 § säkerhetsskyddslagen
15 § säkerhetsskyddsförordningen
7 kap. 6 § RPSFS 2010:03
Kap. 7 Säkerhetsskydd – en vägledning

I säkerhetsskyddsavtalet, som ska vara skriftligt, regleras vilka säkerhetsskyddsåtgärder som ska vidtas i den aktuella upphandlingen.

Om säkerhetsskyddslagen är tillämplig på anbudsgivaren eller företaget, exempelvis på grund av att de bedriver verksamhet av betydelse för rikets säkerhet, kan skyldighet enligt lagen inte inskränkas genom säkerhetsskyddsavtalet. Myndigheten bör oavsett om lagen är tillämplig eller inte träffa avtal med anbudsgivaren eller företaget och precisera vilket säkerhetsskydd som krävs i det särskilda fallet.


Planering
Säkerhetsbedömning
Förfrågningsunderlaget innehåller hemliga uppgifter
Förfrågningsunderlaget innehåller inte hemliga uppgifter
Val av upphandlingform
Säkerhetsskyddsavtal
Förstagångsbesök
Säkerhetsprövning
Säkerhetsskydds-instruktion
Underrättelse till Säkerhetspolisen
Utbildning
Annons
Val av upphandlingform
Tilldelningsbeslut
Upphandling
Säkerhetsskyddsavtal
Förstagångsbesök
Säkerhetsprövning
Säkerhetsskydds-instruktion
Underrättelse till Säkerhetspolisen
Utbildning
Säkerhetsskyddsavtal
Förstagångsbesök
Säkerhetsprövning
Säkerhetsskydds-instruktion
Underrättelse till Säkerhetspolisen
Utbildning
Kontrakt
Avtalsperiod
Utbildning
Säkerhetsprövning
Tillsyn
Utbildning
Säkerhetsprövning
Tillsyn
Underrättelse till Säkerhetspolisen
Avanmäla registerkontroll
Avslut
Underrättelse till Säkerhetspolisen
Avanmäla registerkontroll

Säkerhetsskyddsavtalen kan delas in i tre nivåer beroende på var uppdraget ska genomföras:

- Nivå 1
  Företaget kommer att hantera och förvara hemliga uppgifter i sina egna lokaler.

- Nivå 2
  Företaget kommer att hantera och förvara hemliga uppgifter i myndighetens lokaler eller av myndigheten anvisade områden eller lokaler.

- Nivå 3
  Företaget kan komma att få del av hemliga uppgifter i myndighetens lokaler eller av myndigheten anvisade områden eller lokaler.

Vid förhandlingar om säkerhetsskyddsavtal företräds det allmänna av den myndighet som avser att begära in anbud eller träffa avtal. Myndighetens säkerhetsskyddschef eller annan säkerhetsansvarig ska medverka vid förhandlingen.

Innehåller förfrågningsunderlaget hemliga uppgifter ska ett säkerhetsskyddsavtal träffas redan innan underlaget lämnas ut till anbudsgivaren.

I annat fall ska ett säkerhetsskyddsavtal träffas senast innan affärsavtalet träffas. Anledningen är att det ska finnas ett tillfredsställande säkerhetsskydd innan företaget får del av hemliga uppgifter. Notera också att beroende på vilket men ett eventuellt röjande av hemlig uppgift kan medföra kan säkerhetsskyddsåtgärderna variera, oavsett vilken nivå avtalet har.

Avtalsmallarna i bilagorna A–C måste alltid anpassas till det aktuella uppdraget och de säkerhetsskyddsåtgärder som har bedömts vara nödvändiga.

Har myndigheten träffat ett säkerhetsskyddsavtal inför en anbudsinfordran ska detta revideras i den utsträckning som behövs innan affärsavtalet träffas.

Myndigheten ska träffa säkerhetsskyddsavtal med såväl huvudleverantör som eventuella underleverantörer. En huvudleverantör kan aldrig gentemot myndigheten ansvara för säkerhetsskyddet hos en underleverantör.

Säkerhetsskyddsavtalet bör i tillämpliga delar innehålla överenskommelse om:
- Säkerhetsskyddsorganisation
- Säkerhetsskyddsinstruktion
- Informationssäkerhet
- Behörighet
- Tillträdesbegränsning
- Säkerhetsprövning inklusive placering i säkerhetsklass och registerkontroll
- Utbildning och kontroll
- Tillsyn
- Fördelning av kostnaderna för säkerhetsskyddet
- Tystnadsplikt
- Äganderättsförhållanden
- Avtalsperiod.

Säkerhetsskyddsavtalet utgör också grunden för uppdragets placering i säkerhetsklass och beslut om registerkontroll.

Hänvisning till bilagor
Mall säkerhetsskyddsavtal (nivå 1) – bilaga A
Mall säkerhetsskyddsavtal (nivå 2) – bilaga B
Mall säkerhetsskyddsavtal (nivå 3) – bilaga C

3.4 SÄKERHETSSKYDDSINSTRUKTION

7 kap. 6 § RPSFS 2010:03
Kap. 7.3 Säkerhetsskydd – en vägledning

När ett säkerhetsskyddsavtal har träffats ska företaget upprätta en säkerhetsskyddsinstruktion. I instruktionen ska företaget redovisa vilka säkerhetsskyddsåtgärder som kommer att vidtas för att uppfylla kraven i säkerhetsskyddsavtalet. Det betyder att företaget ska reglera sitt säkerhetsskydd kring den kommande hanteringen och förvaringen av hemliga uppgifter.

Säkerhetsskyddsinstruktionen ska godkännas av myndigheten. I de fall företaget ska utföra arbete i myndighetens lokaler eller i lokaler som har anvisats av myndigheten (säkerhetsskyddsavtal nivå 2 och 3) får myndigheten medge att en säkerhetsskyddsinstruktion inte behöver upprättas. I dessa fall ska myndighetens säkerhetsskyddsbestämmelser gälla. Det åligger berörd personal inom företaget att noggrant följa gällande bestämmelser om säkerhetsskydd.

Av såväl säkerhetsskyddsavtalet som säkerhetsskyddsinstruktionen ska framgå att kontroll av säkerhetsskyddet hos företaget får utföras av myndigheten. Det ska också framgå att kontroll även får utföras av Säkerhetspolisen och/eller Försvarsmakten i samråd med myndigheten.

Innehållet i säkerhetsskyddsinstruktionen ska grunda sig på de krav som ställs i säkerhetsskyddsavtalet och de närmare bestämmelser som gäller på myndigheten beträffande hantering och förvaring av

hemliga uppgifter. Information om vilka säkerhetsskyddsåtgärder myndigheten bedömer vara nödvändiga bör ges vid förstagångsbesöket (se kapitel 3.8).

Av säkerhetsskyddsinstruktionen bör det exempelvis framgå:
- Hur myndighetens säkerhetsskyddsorganisation är utformad
- Rutin för handläggning av säkerhetsprövning
- Regler och rutiner kring informationssäkerhet
- Tillträdesbegränsning
- Utbildningsplan för anställda
- Rutiner avseende internkontroll.

Myndigheten bör tillhandahålla ett underlag för utarbetandet av instruktionen. Viss ledning avseende innehållet i säkerhetsskyddsinstruktionen kan också fås från RPSFS 2010:03.

3.5 UNDERRÄTTELSE TILL SÄKERHETSPOLISEN

7 kap. 8 § RPSFS 2010:03
Kap. 7.5 Säkerhetsskydd – en vägledning

En myndighet ska utan dröjsmål underrätta Säkerhetspolisen om säkerhetsskyddsavtal som har träffats och om säkerhetsskyddsavtal som har upphört. Detta sker enklast genom att använda blanketten *Underlag säkerhetsskyddad upphandling* (SÄPO 070). Blanketten kan hämtas på Säkerhetspolisens webbplats, www.sakerhetspolisen.se.

En myndighet som övertar en pågående säkerhetsskyddad upphandling från en annan myndighet, och därmed även säkerhetsskyddsansvaret, ska upprätta ett eget säkerhetsskyddsavtal med företaget för uppdraget. Även detta ska snarast anmälas till Säkerhetspolisen.

3.6 SÄKERHETSPRÖVNING AV FÖRETAGETS LEDNING

11–13, 17–19 §§ säkerhetsskyddslagen
14, 18–19, 38 §§ säkerhetsskyddsförordningen
7 kap. 4–5 §§ RPSFS 2010:03
Kap. 7 Säkerhetsskydd – en vägledning

Innan myndigheten lämnar ut hemliga uppgifter till ett företag ska myndigheten göra en säkerhetsprövning och, om uppdraget är placerat i säkerhetsklass, låta göra en registerkontroll av företagets ledning. Ett säkerhetsskyddsavtal måste träffas innan registerkontroll får genomföras.

Företagsledningen och företagets säkerhetschef säkerhetsprövas av myndigheten. Myndigheten bestämmer i vilken omfattning som den som har säkerhetsprövats, och i förekommande fall registerkontrollerats, får användas i uppdraget. Detta bör närmare regleras i säkerhetsskyddsavtalet. Under ett uppdrags genomförande ska personella förändringar i styrelse och ledning som avses få del av uppgifterna alltid resultera i en ny säkerhetsprövning.

Innan registerkontroll får genomföras ska den som prövningen gäller ha lämnat sitt samtycke till kontrollen. För att den som ger sitt samtycke ska förstå vad registerkontroll innebär är det viktigt att myndigheten lämnar information till den som ska kontrolleras. Informationen bör åtminstone omfatta i vilka register som kontrollen görs. Samtycket bör dokumenteras och bevaras, eftersom samtycket även gäller för nya kontroller och utredningar så länge som den kontrollerade innehar samma uppdrag.

En framställan om registerkontroll ska göras på de blanketter som finns på Säkerhetspolisens webbplats, www.sakerhetspolisen.se. Företag ska bifoga ett registreringsbevis från Bolagsverket tillsammans med underlaget för registerkontroll. Registreringsbeviset ska inte vara äldre än 3 månader.

Kravet på svenskt medborgarskap gäller inte för personal som anlitas i uppdrag med säkerhetsskyddsavtal.

Den allmänna bedömningen av företagets lämplighet bör dock ha gjorts innan säkerhetsskyddsavtalet ingås. Detta kan exempelvis ske i samband med kvalificering inom ramen för upphandlingsprocessen. Uppgifter om hur företaget sköter sina skatter och avgifter kan erhållas från Skatteverket, blankett *SKV 4820*.

För ytterligare information om säkerhetsprövning, se kapitel 2.

3.7 SEKRETESSFÖRBINDELSE

8 § säkerhetsskyddsförordningen
7 kap. 7 § RPSFS 2010:03
Kap. 7.6 Säkerhetsskydd – en vägledning

För hemliga uppgifter gäller tystnadsplikt. Tystnadsplikt innebär att det är förbjudet att röja eller utnyttja hemliga uppgifter vare sig det sker muntligen eller på annat sätt. Av detta följer att det även är otillåtet att röja hemliga uppgifter för kollegor som inte har behov av uppgifterna för utförande

av uppdraget samt att förevisa hemliga föremål för obehöriga. Tystnadsplikten gäller även efter anställningens eller uppdragets upphörande.

Myndigheten, eller den som myndigheten bestämmer, ska upplysa berörda personer om:
- Innebörden och räckvidden av den tystnadsplikt som gäller för de hemliga uppgifterna i uppdraget
- Eventuella föreskrifter i säkerhetsskyddsinstruktionen
- Innebörden av begreppet behörig
- Straffbestämmelserna i 19 kap. brottsbalken avseende brott mot rikets säkerhet.

Myndigheten ska också se till att en sekretessförbindelse undertecknas. Undertecknande av sekretessförbindelse är en skriftlig bekräftelse på att uppdragstagaren har informerats om innebörden av tystnadsplikten och säkerhetsskyddet. En sekretessförbindelse som tecknas med företagets säkerhetsskyddsansvarige (säkerhetsskyddschefen) ska förvaras hos myndigheten. Övriga sekretessförbindelser förvaras hos den som är säkerhetsskyddsansvarig hos företaget så länge uppdraget pågår. När uppdraget är slutfört lämnas även dessa förbindelser till myndigheten.

När uppdraget avslutas är det lämpligt att påminna om att tystnadsplikten kvarstår. Detta kan ske genom ett nytt undertecknande av sekretessförbindelse.

Tystnadsplikten ska regleras i säkerhetsskyddsavtalet.

Hänvisning till bilaga
Exempel på sekretessförbindelse – bilaga D

3.8 FÖRSTAGÅNGSBESÖK

7 kap. 5 § RPSFS 2010:03
Kap. 7.2 Säkerhetsskydd – en vägledning

Om hemliga uppgifter ska lämnas ut till ett företag som ska hantera och förvara uppgifterna i egna lokaler, ska myndigheten genomföra ett besök hos företaget.

Detta kallas förstagångsbesök. Syftet är att kontrollera att lokalerna och förvaringsutrymmena är lämpliga från säkerhetsskyddssynpunkt. Kontrollen bör utgå från den genomförda säkerhetsanalysen eller säkerhetsplanen, där det framgår vilka krav som ska ställas på säkerhetsskyddet.

Vid förstagångsbesöket bör myndigheten också skaffa allmän information om företagets förmåga att hantera hemliga uppgifter.

Ett protokoll ska upprättas över vad som har framkommit och iakttagits vid förstagångsbesöket från säkerhetsskyddssynpunkt. Av protokollet bör framgå:
- Adressuppgifter
- Säkerhetsskyddsorganisation
- Företagets verksamhet
- Fastighetsägare
- Lokalernas utformning (yta, våningsplan, andra hyresgäster etc.)
- Tillträdesbegränsningar (dörrar, fönster, larm, lås, hantering av kort, koder och nycklar, passersystem, besöksrutiner, vaktbolag etc.)
- Hantering och förvaring av hemliga uppgifter (datorer, säkerhetsskåp, kopiatorer, skrivare etc.).

Om ställda säkerhetsskyddskrav inte är uppfyllda, måste företaget besökas på nytt för att kontrollera att bristerna har åtgärdats innan företaget kan godkännas för hantering och förvaring av hemliga uppgifter.

Vid förstagångsbesöket kan även en första utbildning av den personal som ska delta i uppdraget genomföras.

3.9 AFFÄRSAVTAL

I affärsavtalet avseende de ekonomiska villkoren ska det göras en hänvisning till säkerhetsskyddsavtalet. En klausul ska alltid tas in i affärsavtalet som fastställer att säkerhetsskyddsavtalet gäller framför affärsavtalet om det förekommer motstridiga uppgifter i affärsavtalet. Hela förfarandet med den säkerhetsskyddade upphandlingen måste vara klart innan något arbete påbörjas eller hemliga uppgifter lämnas ut.

3.10 SÄKERHETSPRÖVNING AV ÖVRIGA I UPPDRAGET

När affärsavtalet har träffats ska säkerhetsprövning och, om uppdraget är placerat i säkerhetsklass, registerkontroll ske av övriga anställda på företaget som ska delta i uppdraget och som kan antas komma att få del av hemliga uppgifter. Ska företaget ansvara för säkerhetsprövningen av sina anställda och informationen om registerkontroll, ska formerna för detta regleras i säkerhetsskyddsavtalet.

Myndigheten bestämmer i vilken omfattning som den som har säkerhetsprövats, och i förekommande fall registerkontrollerats, får användas i uppdraget. Detta bör närmare regleras i säkerhetsskyddsavtalet. Under ett uppdrags genomförande ska personella förändringar bland anställda som avses få del av uppgifterna alltid resultera i en ny säkerhetsprövning. Innan registerkontroll får genomföras ska den som prövningen gäller ha lämnat sitt samtycke till kontrollen. För att den som ger sitt samtycke ska förstå vad registerkontroll innebär är det viktigt att myndigheten eller företaget lämnar information till den som ska kontrolleras. Informationen bör åtminstone omfatta i vilka register som kontrollen görs. Samtycket bör dokumenteras och bevaras, eftersom samtycket även gäller för nya kontroller och utredningar så länge som den kontrollerade innehar samma uppdrag.

En framställan om registerkontroll ska göras på de blanketter som finns på Säkerhetspolisens webbplats, www.sakerhetspolisen.se.

Myndigheten bör dokumentera vilka personer som är föremål för säkerhetsprövning. Ett sådant dokument underlättar hanteringen av registerkontroller, till exempel avanmälan.

För ytterligare information om säkerhetsprövning, se kapitel 2.

3.11 UTBILDNING

9 kap. 1 § RPSFS 2010:03
Kap. 9 Säkerhetsskydd – en vägledning

En förutsättning för ett effektivt säkerhetsskydd är att den personal som ska delta i uppdraget får grundläggande utbildning i säkerhetsskydd. Utbildningen ska främst syfta till att klargöra varför skyddsåtgärder ska vidtas mot hot av olika slag, samt säkerställa att behörig personal har tillräcklig kunskap rörande säkerhetsskyddet i det aktuella uppdraget.

Myndighetens utbildningsplan bör därför även omfatta utbildning för de företag med vilka myndigheten har träffat säkerhetsskyddsavtal. Utbildning av den personal som ska delta i uppdraget kan genomföras dels vid förstagångsbesöket, dels innan uppdraget påbörjas.

Utbildningen bör bland annat omfatta:
- hotbild
- behörighet
- informationssäkerhet
- tillträdesskydd
- säkerhetsprövning inklusive registerkontroll
- tystnadsplikt
- övriga åtgärder enligt säkerhetsskyddsinstruktionen.

3.12 INTERN KONTROLL OCH TILLSYN

41–42 §§ säkerhetsskyddsförordningen
9 kap. 4–6 §§ RPSFS 2010:03

Företaget bör fortlöpande kontrollera att endast behöriga personer deltar i uppdraget, att åtgärderna i säkerhetsskyddsavtalet och säkerhetsskyddsinstruktionen vidtas, och att personal som deltar i uppdraget får regelbunden utbildning i säkerhetsskyddsfrågor. Protokoll bör föras över genomförda kontroller.

Företaget ska omedelbart underrätta myndigheten om inträffade eller befarade händelser och omständigheter som kan påverka företagets säkerhetsskydd. Företagets skyldigheter avseende detta bör regleras i säkerhetsskyddsavtalet.

Myndigheten ska kontrollera att företaget har vidtagit de avtalade säkerhetsskyddshöjande åtgärderna och genomfört en säkerhetsskyddsutbildning med de personer som kommer att få del av hemliga uppgifter i uppdraget. Denna kontroll kan om myndigheten önskar genomföras i samråd med Säkerhetspolisen och/eller Försvarsmakten.

Myndighetens plan för intern kontrollverksamhet bör även omfatta kontroll av de företag med vilka myndigheten har träffat säkerhetsskyddsavtal. Myndigheten bör föra protokoll över varje kontroll. Protokollen bör förvaras samlade hos myndigheten.

Formerna för tillsyn bör regleras i säkerhetsskyddsavtalet.

3.13 UPPDRAGETS AVSLUTANDE

7 kap. 7–8 §§ RPSFS 2010:03
Kap. 7.4 Säkerhetsskydd – en vägledning

När företaget har fullgjort uppdraget som har omgetts av säkerhetsskydd ska myndigheten säga upp säkerhetsskyddsavtalet. Det bör finnas rutiner för vilka åtgärder som ska vidtas när ett säkerhetsskyddsavtal sägs upp. Det är också lämpligt att i säkerhetsskyddsavtalet reglera vem som ska ansvara för dessa åtgärder.

Det är viktigt att säkerställa att företaget återlämnar information och utrustning med mera till myndigheten när uppdraget har slutförts. Personer som har deltagit i uppdraget ska återlämna nycklar och passerkort, och i förekommande fall bör koder till larm ändras samt behörighet i IT-system avslutas.

Myndigheten ska genom information till företaget och dess personal säkerställa att det som har avtalats om tystnadsplikt består. Detta kan ske genom ett nytt undertecknande av sekretessförbindelsen.

Myndigheten ska slutligen underrätta Säkerhetspolisen om att säkerhetsskyddsavtalet har upphört att gälla och avanmäla samtliga registerkontroller som är kopplade till uppdraget.

4 Säkerhetsskyddad upphandling med utländskt företag m.m.

8 § säkerhetsskyddslagen
17 § säkerhetsskyddsförordningen
Kap. 3.7 och 10 Säkerhetsskydd – en vägledning

Det finns inga hinder i säkerhetsskyddslagen för att i ett uppdrag använda ett utländskt företag eller en utländsk medborgare, som därmed kan få del av hemliga uppgifter. Särskild hänsyn bör dock tas till svårigheten att genomföra en adekvat och trovärdig säkerhetsprövning. Normalt bör det här ställas högre krav på inhämtning av referenser än om säkerhetsprövningen gäller en svensk medborgare. Detsamma bör gälla i de fall där personen i fråga har vistats en längre tid utomlands, även om han eller hon är svensk medborgare. När det gäller utlämnande av uppgifter och handlingar måste också bestämmelserna i offentlighets- och sekretesslagen beaktas.

Om det uppkommer ett behov av att i ett uppdrag delge hemliga uppgifter till ett företag i ett annat land torde krävas att regeringen ger sitt tillstånd till utlämnande av hemliga uppgifter samt att ett generellt bi- eller multilateralt säkerhetsskyddsavtal har träffats. Ett sådant säkerhetsskyddsavtal reglerar säkerhetsskyddet mellan länderna baserat på respektive lands nationella bestämmelser samt rutiner för industrisäkerhetsskyddssamarbete. Finns det inget sådant säkerhetsskyddsavtal med landet i fråga måste myndigheten få ett bemyndigande av regeringen att teckna ett projektspecifikt säkerhetsskyddsavtal med en utländsk myndighet.

Denna myndighet kan ansvara för genomförandet och kontrollen av säkerhetsskyddet vid det utländska företaget. Processen bör planeras i god tid.

Uppgift om vilka länder som har tecknat säkerhetsskyddsavtal med Sverige finns hos Nationella säkerhetsmyndigheten (NSA) vid Utrikesdepartementets sekretariat för säkerhet, sekretess och beredskap.

Offshoring och outsourcing

Globaliseringen och utvecklingen av elektroniska kommunikationsnätverk ger stora möjligheter att få olika tjänster utförda var som helst i världen. Detta har blivit allt vanligare inom IT-området och leder till utkontraktering av tjänster, så kallad outsourcing (som är när en extern aktör utför utvecklings-, underhålls- eller driftsarbete av system) och offshoring (som är när outsourcing sker till en aktör i ett annat land).

För svenska myndigheter innebär offshoring att svenska staten riskerar en sämre kontroll över samhällsviktiga system eftersom möjligheterna att säkerhetspröva personal och utnyttja svenska kontrollinstrument är begränsade i utlandet. Det är dessutom svårare för svenska myndigheter att bedöma hotbilden i de länder till vilka man har utkontrakterat verksamhet. Om det internationella säkerhetsläget förändras, vilket kan gå snabbt, saknas i värsta fall såväl kompetens som kapacitet och tid för att kunna flytta hem verksamheten till Sverige.

Outsourcing innebär ofta att flera kunders system och information blandas i samma fysiska datorsystem. Olika kunders data kan därför hamna i samma lagringsmiljöer, switchar, routrar och brandväggar. Ofta söker leverantören kostnadsbesparingar som leder till att system förs samman och virtualiseras, det vill säga att ett fysiskt system uppträder som flera logiska. Det innebär att en kunds externa webbserver kan placeras på samma fysiska maskin som en annan kunds interna databasserver ligger. Detta medför en ökad risk då en störning i en kunds system kan orsaka störningar även i andra kunders system.

Att ha tillräcklig kontroll över leverantörens driftspersonal är också svårt. Vilka rättigheter har de att komma åt kunders information? Hur stor omsättning har leverantören på sin personal? I hur stor utsträckning använder man sig av konsulter? Dessa frågor har kunden ofta ingen eller liten insyn i. När en stor mängd information från flera olika myndigheter och företag världen över hamnar hos en enskild leverantör riskerar den dessutom att bli en central punkt för till exempel andra länders underrättelseinhämtning.

Säkerhetsfrågor måste i dessa sammanhang lyftas fram och avspeglas i såväl affärsavtalet som säkerhetsskyddsavtalet. Innan myndigheter lägger ut tjänster till andra aktörer och länder bör de genomföra årliga och genomgripande säkerhetsanalyser. När det gäller verksamhet som är viktig för det svenska samhället och som rör rikets säkerhet bör de särskilt beakta offentlighets- och sekretesslagens bestämmelser om utlämnande av uppgifter och möjligheten att genomföra och kontrollera säkerhetsskyddet. Offshoring bör endast ske efter särskilda överväganden och de säkerhetsrisker som det kan innebära måste noggrant övervägas. Risken finns att myndigheten utgår från vissa förutsättningar medan leverantören inte inkluderar något utöver det som parterna uttryckligen har kommit överens om.

Säkerhetsskyddsavtal vid internationellt försvarssamarbete

I detta sammanhang kan också nämnas att Försvarets materielverk får träffa avtal om säkerhetsskydd med ett svenskt företag om det är nödvändigt för att företaget ska kunna delta i internationellt samarbete kring utveckling eller produktion av försvarsmateriel. Detta rör sig dock inte om säkerhetsskyddad upphandling i den mening som avses i denna vägledning, utan om säkerhetsklarering (facility security clearance) för ett svenskt företag som ska delta i internationellt försvarssamarbete.

När det gäller civilt internationellt samarbetet finns för närvarande ingen författningsreglering. Uppkommer behov av säkerhetsklarering med mera vid sådant samarbete hänvisas till NSA vid Utrikesdepartementets sekretariat för säkerhet, sekretess och beredskap.

Utländska beteckningar

Uppgifter som andra stater, utländska myndigheter och mellanfolkliga organisationer har klassificerat som TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED bör hanteras som hemliga uppgifter. Observera att andra beteckningar än de ovan nämnda kan förekomma enligt internationella överenskommelser.

I allmänhet kan handlingar märkta TOP SECRET eller motsvarande hanteras som kvalificerat hemliga handlingar, SECRET eller motsvarande och CONFIDENTIAL eller motsvarande som hemliga handlingar, samt RESTRICTED eller motsvarande som hemliga handlingar vars röjande endast kan antas medföra ringa men för rikets säkerhet. Motsvarande gäller även för andra lagringsmedier och materiel som har märkts med sådan utländsk beteckning.

Bilaga A

Mall säkerhetsskyddsavtal (nivå 1)

[Myndigheten], org.nr [111111-1111], [Alfagatan 1], [111 11] [Stockholm],
som företräder staten, nedan kallad Myndigheten

och

[Företaget AB], org.nr [222222-2222], [Betagatan 2], [222 22] [Stockholm],
nedan kallat Företaget träffar följande avtal om säkerhetsskydd.

1. Bakgrund

Myndigheten och Företaget avser att ingå ett avtal avseende alternativt Företaget ska få del av förfrågningsunderlag [diarienummer eller liknande] angående projektet [projektnamn], nedan kallat Uppdraget.

[Beskrivning av Uppdraget]

Uppdraget innebär att Företaget i sina egna lokaler kommer att hantera och förvara hemliga uppgifter.

Säkerhetsskyddet ska förebygga a) att hemliga uppgifter obehörigen röjs, ändras, görs otillgängliga för behöriga eller förstörs (informationssäkerhet), b) att obehöriga får tillgång till hemliga uppgifter eller verksamhet som har betydelse för rikets säkerhet (tillträdesbegränsning), och c) att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning). Andra säkerhetsskyddsåtgärder är utbildning och kontroll.

Detta avtal avser säkerhetsskydd för uppgifter som på Myndigheten omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet. En sådan uppgift benämns fortsättningsvis hemlig uppgift. En hemlig uppgift kan framgå av en handling, ett visst förhållande, en anläggning eller föremål av olika slag.

2. Avtalets omfattning

Detta säkerhetsskyddsavtal tillsammans med Företagets säkerhetsskyddsinstruktion reglerar vilka säkerhetsskyddsåtgärder som Företaget ska vidta i samband med Uppdraget.

De ekonomiska villkoren avseende Uppdraget regleras i ett kontrakt, nedan kallat Affärsavtalet.

Detta säkerhetsskyddsavtal är en förutsättning men utgör ingen utfästelse eller garanti för att Myndigheten ska teckna Affärsavtal med Företaget.

Om det förekommer motstridiga uppgifter i Affärsavtalet gäller detta säkerhetsskyddsavtal framför Affärsavtalet. Motsvarande skrivning ska även tas in i Affärsavtalet.

Företaget får endast använda underleverantörer som har tecknat säkerhetsskyddsavtal med Myndigheten.

3. Säkerhetsskyddsorganisation

Det ska finnas en säkerhetsskyddschef och en ställföreträdande säkerhetsskyddschef på Företaget. Säkerhetsskyddschefen ska i Uppdragets säkerhetsskyddsfrågor vara direkt underställd Företagets ledning. Säkerhetsskyddschefen leder säkerhetsskyddsverksamheten inom Företaget och är kontaktperson i säkerhetsskyddsfrågor gentemot Myndigheten. På Företaget ska det även finnas en systemsäkerhetsansvarig för IT-system som är avsedda för behandling av hemliga uppgifter.

4. Säkerhetsskyddsåtgärder

Företaget ska upprätta en säkerhetsskyddsinstruktion när säkerhetsskyddsavtalet har undertecknats.

Säkerhetsskyddsinstruktionen inklusive eventuella förändringar eller tillägg i säkerhetsskyddsinstruktionen ska godkännas av Myndigheten.

Företaget ska dokumentera de säkerhetsskyddsåtgärder som har vidtagits i Uppdraget.

5. Behörighet

Behöriga att ta del av hemliga uppgifter är endast personer som

- Bedöms pålitliga från säkerhetssynpunkt
- Har tillräckliga kunskaper om säkerhetsskydd
- Behöver uppgifterna för sitt uppdrag eller arbete i den verksamhet där de hemliga uppgifterna förekommer.

Hemliga uppgifter får endast delges personer som har säkerhetsprövats och godkänts av Myndigheten.

6. Informationssäkerhet

Myndigheten ska klargöra för Företaget i vilken utsträckning handlingar med mera som överlämnas till Företaget innehåller hemliga uppgifter.

Om hemliga uppgifter uppkommer under Uppdragets utförande på Företaget, ska Företaget vidta de säkerhetsskyddsåtgärder som är nödvändiga. Företaget ska utan dröjsmål meddela Myndigheten om hemliga uppgifter har uppkommit samt vilka säkerhetsskyddsåtgärder som har vidtagits.

Myndigheten ska alltid godkänna utrymmen som används vid hantering och förvaring av hemliga uppgifter.

Hemliga uppgifter får endast hanteras i IT-system som har godkänts för sådan hantering av Myndigheten. Beträffande hemliga uppgifter i IT-miljö gäller för Uppdraget bestämmelserna i bilaga 1.

Företaget bör klargöra för Myndigheten i vilken utsträckning uppgifter avseende affärs- eller driftsförhållanden som överlämnas till Myndigheten är att anse som hemliga, samt varför Företaget kan komma att lida skada om dessa röjs (enligt offentlighets- och sekretesslagen [2009:400]). Företaget är dock medvetet om att Myndigheten ändå kan vara skyldig att lämna ut sådana uppgifter.

Företaget får inte utan Myndighetens tillstånd lämna uppgifter till massmedia som rör Uppdraget och som enligt Myndigheten innehåller hemlig uppgift. Detsamma gäller för publicering i broschyrer, tidskrifter, böcker, filmer etc., samt vid föredrag, utställningar och förevisningar dit personer som inte är behöriga (punkt 5) har tillträde.

Företaget får inte utan Myndighetens tillstånd offentliggöra att det träffat ett säkerhetsskyddsavtal. Denna information får därmed inte användas i marknadsföring eller på annat sätt.

7. Tillträdesbegränsning

Myndigheten ska i samråd med Företaget fastställa nivån på tillträdesskyddet för de lokaler och områden eller motsvarande som Företaget avser att använda vid genomförandet av Uppdraget. Detta ska ske innan Företaget får del av hemliga uppgifter eller den säkerhetskänsliga verksamheten påbörjas.

Företaget får inte utan Myndighetens godkännande byta eller använda andra lokaler, områden eller motsvarande för Uppdragets genomförande.

Endast behöriga personer som har godkänts av Myndigheten får ha tillträde till de lokaler, områden eller motsvarande där Uppdraget genomförs.

8. Säkerhetsprövning

Innan en person får del av hemliga uppgifter ska Företaget genom säkerhetsprövning pröva vederbörandes lojalitet och pålitlighet från säkerhetssynpunkt. Säkerhetsprövningen ska omfatta varje person som får del av hemliga uppgifter, oavsett om de blir föremål för registerkontroll enligt säkerhetsskyddslagen (1996:627) eller inte.

Säkerhetsprövningen ska omfatta en personbedömning samt inhämtande av betyg, intyg och referenser. Är befattningen placerad i säkerhetsklass ska säkerhetsprövningen även omfatta registerkontroll och i vissa fall särskild personutredning.

Säkerhetsprövningen ska dokumenteras av Företaget och på begäran lämnas till Myndigheten. Tillsammans med uppgifter som har framkommit vid registerkontroll och särskild personutredning utgör säkerhetsprövningen underlag för Myndighetens beslut om att personen får anlitas. Företaget får inte anlita personen innan Företaget har fått del av Myndighetens beslut.

Innan en ansökan om registerkontroll skickas till Myndigheten ska Företaget särskilt informera den person som ska bli föremål för registerkontroll om vad kontrollen innebär. Företaget ska i samband med detta också inhämta personens samtycke till kontrollen. Samtycket ska dokumenteras och förvaras på Företaget.

Företaget ska utan dröjsmål anmäla till Myndigheten om en registerkontrollerad person på Företaget lämnar Uppdraget. Myndigheten ska utan dröjsmål anmäla till Säkerhetspolisen att personen har lämnat Uppdraget.

Företaget ska till Myndigheten anmäla omständigheter som kan vara av betydelse för bedömningen av en säkerhetsprövad persons lämplighet och pålitlighet.

Om en person som har säkerhetsprövats inom ramen för detta säkerhetsskyddsavtal under Uppdragets genomförande befinns olämplig från säkerhetssynpunkt, ska Företaget vidta de åtgärder som är lämpliga för att vederbörande inte ska få tillgång till hemliga uppgifter eller tillträde till lokaler, områden eller motsvarande där säkerhetskänslig verksamhet bedrivs.

9. Intern utbildning och kontroll

Myndigheten ska innan Uppdraget påbörjas ge lämplig utbildning i säkerhetsskyddsfrågor till de personer på Företaget som kan komma att få del av hemliga uppgifter eller tillträde till lokaler, områden eller motsvarande där säkerhetskänslig verksamhet bedrivs. Därefter ansvarar Företaget för att dessa personer ges behövlig och fortlöpande utbildning. Utbildningen ska bland annat behandla:

- Hot och risker som från säkerhetssynpunkt föreligger mot eller är förknippade med Uppdraget
- Säkerhetsskyddsåtgärder som enligt Företagets säkerhetsskyddsinstruktion ska vidtas mot föreliggande hot och risker.

Myndigheten kan vid behov och efter särskild framställan medverka i viss utbildning som Företaget ger.

Företaget ska fortlöpande kontrollera att endast behöriga personer som har godkänts av Myndigheten anlitas och att säkerhetsskyddet avseende informationssäkerhet och tillträdesbegränsning iakttas, samt att skyddsnivån är jämn och tillräckligt hög.

Företaget ska omedelbart underrätta Myndigheten om inträffade eller befarade händelser och omständigheter som kan påverka säkerhetsskyddet vad avser Uppdraget och personer som faller under detta avtal.

10. Tillsyn

Myndigheten har rätt att kontrollera att de i säkerhetsskyddsinstruktionen redovisade och avtalade säkerhetsskyddsbestämmelserna följs. Vid en sådan tillsyn kan Myndigheten biträdas av en representant från Säkerhetspolisen och/eller Försvarsmakten. Tillsynen ska ske under Företagets ordinarie kontorstid eller på plats och tid enligt särskild överenskommelse. Tillsynen får inte vara mer ingripande för Företaget än vad som är nödvändigt.

11. Kostnader

Företaget ska bära eventuella kostnader som uppkommer med anledning av detta säkerhetsskyddsavtal om inget annat avtalas i Affärsavtalet.

12. Övrigt

Hemliga uppgifter som har tillförts eller uppkommit under Uppdragets genomförande ska även efter att avtalet har upphört, eller till dess att Myndigheten meddelar något annat, omfattas av tystnadsplikt.

Företaget ska informera berörd personal om innebörden av tystnadsplikten och säkerhetsskyddet samt se till att personalen undertecknar sekretessförbindelser. Dessa förvaras på Företaget så länge Uppdraget pågår. När Uppdraget är slutfört lämnas sekretessförbindelserna till Myndigheten.

Företaget ska utan dröjsmål anmäla till Myndigheten när någon förändring sker beträffande firma, organisationsnummer, styrelse, verkställande direktör, revisor, post- och besöksadress eller telefonnummer. Avser ändringen firma, organisationsnummer, styrelse, verkställande direktör eller revisor ska ett nytt registreringsbevis bifogas anmälan. En anmälan ska också göras om ägarförhållandena ändras, om Företaget råkar i ekonomiska svårigheter eller försätts i konkurs.

Samtliga handlingar, materiel eller övrigt som innehåller hemliga uppgifter och som har anknytning till Uppdraget är Myndighetens egendom om inget annat har avtalats. Dessa hand-

lingar eller dylikt ska senast i samband med fullgjort Uppdrag återlämnas till Myndigheten eller vid den tidpunkt som parterna särskilt har kommit överens om.

13. Avtalsperiod

Detta säkerhetsskyddsavtal träder i kraft vid undertecknandet och gäller tills vidare eller till dess det skriftligen sägs upp av endera parten. [Uppsägningstid]

Avtalet kan dock inte ensidigt sägas upp till en tidigare tidpunkt än den dag då Uppdraget har slutförts eller alla hemliga uppgifter har återlämnats till Myndigheten.

Myndigheten kan dock ensidigt säga upp detta avtal liksom Affärsavtalet med omedelbar verkan om Företaget frångår detta avtal.

Detta avtal har upprättats i två likalydande exemplar varav parterna har tagit var sitt.

[Ort] den [datum och år]

[MYNDIGHETEN]	**[FÖRETAGET AB]**
.....	.....
[Anna Andersson]	**[Birgit Bertilsson]**

Bilaga 1 till säkerhetsskyddsavtal

Bestämmelser avseende informationssäkerhet för hemliga uppgifter i IT-miljö

1. Allmänt

Denna bilaga innehåller bestämmelser avseende hantering av hemliga uppgifter i IT-miljö som rör Uppdraget. Det som har avtalats avseende hemliga uppgifter gäller även för kvalificerat hemliga uppgifter, om inte annat anges.

Hemliga uppgifter får endast hanteras i IT-system som har godkänts för sådan hantering av Myndigheten.

Företaget ska samråda med Myndigheten om osäkerhet uppstår angående vad som ska betraktas som hemliga uppgifter.

Företaget ska dokumentera mål och riktlinjer för säkerheten i IT-system från anskaffning till avveckling. Företaget ska även dokumentera instruktioner för användning, förvaltning och drift av IT-system som är avsedda för behandling av hemliga uppgifter. Dokumentationen avseende mål och riktlinjer samt instruktionerna ska godkännas av Myndigheten.

IT-system får inte tas i drift förrän Myndigheten har godkänt systemen för behandling av hemliga uppgifter. Inför godkännandet ska IT-systemet granskas för att verifiera att det uppfyller kraven på säkerhetsskydd. Vid granskningen är det särskilt viktigt att granska om IT-systemet samverkar med andra IT-system. Granskningen ska ske av annan än den som uppförde systemet. Granskningen ska dokumenteras.

2. IT-system för behandling av hemliga uppgifter

Ett IT-system kan utgöras av en fristående dator som har en löstagbar hårddisk, eller ett fysiskt separat nätverk med flera datorer.

En okrypterad dataförbindelse får användas för hemliga uppgifter inom ett område eller en lokal som disponeras av Företaget om Företaget har vidtagit och dokumenterat betryggande åtgärder mot obehörig avlyssning, och om Myndigheten har godkänt detta.

Hemliga uppgifter får inte behandlas i ett IT-system som har externa nätverkskopplingar om inte Myndigheten har medgett annat.

Om Myndigheten medger externa nätverkskopplingar får hemliga uppgifter sändas via ett elektroniskt kommunikationsnät endast om ett av Försvarsmakten godkänt signalskyddssystem (kryptosystem) används. Sändningen måste också ske enligt de bestämmelser som gäller för den aktuella sekretessnivån. Det är viktigt att försäkra sig om till vilket IT-system de hemliga uppgifterna ska skickas. Samråd ska ske med Myndigheten innan sändning förekommer.

3. Systemsäkerhetsansvarig

Företaget ska utse en systemsäkerhetsansvarig som ansvarar för säkerheten i det IT-system som ska hantera hemliga uppgifter.

4. Hantering av elektroniska hemliga handlingar

Hemliga uppgifter i IT-system ska så långt praktiskt möjligt hanteras på samma sätt som hemliga handlingar. Hemliga elektroniska handlingar ska märkas enligt anvisningar i säkerhetsskyddsinstruktionen.

En kvalificerat hemlig elektronisk handling får inte skickas elektroniskt.

Anvisningar om övrig hantering av elektroniska hemliga handlingar anges i den av Företaget upprättade och av Myndigheten godkända säkerhetsskyddsinstruktionen.

5. Behörighetskontroll och säkerhetsloggning

Om IT-systemet utgörs av ett nätverk ska ett behörighetskontrollsystem användas där alla användare är unikt identifierbara och har ett personligt aktivt kort eller en säkerhetsdosa för att logga in i IT-systemet.

Om IT-systemet utgörs av en fristående dator som nyttjas av flera personer ska det vid varje användning finnas ett behörighetskontrollsystem eller föras en förteckning i en kvittenslista. Alternativt kan varje individuell användare ha varsin löstagbar hårddisk.

Det ska finnas en förteckning över vilka som har behörighet att använda IT-systemet. Denna förteckning ska sparas för att spårbarhet ska kunna uppnås i efterhand. Förteckningen ska överlämnas till Myndigheten när Uppdraget är avslutat.

IT-systemet ska logga användaridentitet, datum och tidpunkt för inloggning och utloggning samt användaraktiviteter i övrigt som är av betydelse för säkerheten i systemet. Företaget ska dokumentera hur säkerhetsloggar ska analyseras. Myndigheten ska godkänna anvisningarna. Säkerhetsloggarna ska överlämnas till Myndigheten när Uppdraget är avslutat.

6. Skydd mot skadlig kod

Innan ny information tillförs IT-systemet ska informationen kontrolleras så att den inte innehåller skadlig kod. Programvara som skyddar mot skadlig kod ska uppdateras kontinuerligt. Företaget ska dokumentera skyddet mot skadlig kod och Myndigheten ska godkänna skyddet.

7. Intrångsdetektering och skydd mot intrång

IT-systemet ska vara försett med intrångsskydd och funktioner för intrångsdetektering. Företaget ska dokumentera intrångsskyddet och intrångsdetekteringen, och Myndigheten ska godkänna skyddet och detekteringen.

8. Skydd mot röjande signaler och obehörig avlyssning

Företaget ska analysera och dokumentera behovet av skydd mot röjande signaler. Myndigheten ska godkänna analysen. Om det behövs ska IT-systemet ha ett betryggande skydd mot röjande signaler.

IT-system ska vara försedda med betryggande skydd mot obehörig avlyssning.

9. Incidenthantering

Företaget ska dokumentera rutiner för hantering, rapportering och uppföljning av incidenter av betydelse för säkerheten i eller kring ett IT-system. Myndigheten ska godkänna incidenthanteringen.

10. Säkerhetskopiering
Säkerhetskopior ska tas regelbundet enligt en av Företaget dokumenterad rutin, och förvaras avskilt från den plats där det berörda IT-systemet finns. Säkerhetskopiorna ska testas regelbundet och förvaras i ett godkänt säkerhetsskåp. Säkerhetskopiorna bör krypteras. Myndigheten ska godkänna rutinerna för säkerhetskopiering.

11. Kontinuitetsplan
Företaget ska bedöma och dokumentera den längsta tid som IT-systemet kan vara ur funktion utan att Uppdraget i väsentlig omfattning störs. Företaget ska också bedöma och dokumentera vilken reservrutin som ska användas om det inträffar. Myndigheten ska godkänna kontinuitetsplanen.

12. Hantering av utskrifter
Skrivare eller plotter ska vara placerad i nära anslutning till och inom synhåll från den dator där utskriften upprättas.

13. Hantering av digitala lagringsmedier
En dator med inbyggd hårddisk ska vara inlåst i ett godkänt säkerhetsskåp (SS 3492). Har datorn en löstagbar hårddisk ska hårddisken förvaras i säkerhetsskåpet. Även andra lagringsmedier såsom disketter, CD- eller DVD-skivor och USB-minnen, som innehåller eller har innehållit hemliga uppgifter, ska förvaras i säkerhetsskåp. Endast behörig personal får ha tillgång till säkerhetsskåpet.

Ett lagringsmedium som innehåller eller har innehållit hemliga uppgifter får endast återanvändas inom Uppdraget av behörig personal. Ett sådant lagringsmedium får endast användas i utrustning som har godkänts för hantering av hemliga uppgifter.

Ett lagringsmedium som innehåller eller har innehållit hemliga uppgifter ska vara försett med en varaktig hemligbeteckning. En förteckning ska föras som beskriver innehållet på lagringsmediet, för att underlätta utredning av vilka uppgifter som har förlorats vid en eventuell förlust av lagringsmediet. Lagringsmedier ska inventeras på samma sätt som hemliga handlingar.

När ett lagringsmedium utrangeras ska det överlämnas till Myndigheten för destruering, alternativt förstöras enligt Myndighetens anvisningar.

Ett lagringsmedium får inte lämna Företagets lokaler utan Myndighetens godkännande. Om ett lagringsmedium medförs från Företagets lokaler ska det hållas under omedelbar uppsikt eller förvaras på ett sätt som motsvarar den säkerhetsskyddsnivå som gäller för förvaring av lagringsmediet inom Företagets lokaler. Under transport ska, i förekommande fall, den hemliga uppgiften krypteras med av Myndigheten godkänd kryptoprodukt.

14. Underhåll
Vid service och underhåll av lagringsmedier som innehåller hemliga uppgifter får Företaget endast använda personal som är behörig att ta del av hemliga uppgifter enligt säkerhetsskyddsavtalet.

Bilaga B

Mall säkerhetsskyddsavtal (nivå 2)

[Myndigheten], org.nr [111111-1111], [Alfagatan 1], [111 11] [Stockholm], som företräder staten, nedan kallad Myndigheten

och

[Företaget AB], org.nr [222222-2222], [Betagatan 2], [222 22] [Stockholm], nedan kallat Företaget träffar följande avtal om säkerhetsskydd.

1. Bakgrund

Myndigheten och Företaget avser att ingå ett avtal avseende alternativt Företaget ska få del av förfrågningsunderlag [diarienummer eller liknande] angående projektet [projektnamn], nedan kallat Uppdraget.

[Beskrivning av Uppdraget]

Uppdraget innebär att Företaget i Myndighetens lokaler eller av Myndigheten anvisade områden eller lokaler kommer att hantera och förvara hemliga uppgifter.

Säkerhetsskyddet ska förebygga a) att hemliga uppgifter obehörigen röjs, ändras, görs otillgängliga för behöriga eller förstörs (informationssäkerhet), b) att obehöriga får tillgång till hemliga uppgifter eller verksamhet som har betydelse för rikets säkerhet (tillträdesbegränsning), och c) att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning). Andra säkerhetsskyddsåtgärder är utbildning och kontroll.

Detta avtal avser säkerhetsskydd för uppgifter som på Myndigheten omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet. En sådan uppgift benämns fortsättningsvis hemlig uppgift. En hemlig uppgift kan framgå av en handling, ett visst förhållande, en anläggning eller föremål av olika slag.

2. Avtalets omfattning

Detta avtal tillsammans med Företagets säkerhetsskyddsinstruktion (om en sådan har upprättats) reglerar vilka säkerhetsskyddsåtgärder som Företaget ska vidta i samband med Uppdraget.

De ekonomiska villkoren avseende Uppdraget regleras i ett kontrakt, nedan kallat Affärsavtalet.

Detta säkerhetsskyddsavtal är en förutsättning men utgör ingen utfästelse eller garanti för att Myndigheten ska teckna Affärsavtal med Företaget om Uppdraget.

Om det förekommer motstridiga uppgifter i Affärsavtalet gäller detta säkerhetsskyddsavtal framför Affärsavtalet. Motsvarande skrivning ska även tas in i Affärsavtalet.

Företaget får endast använda underleverantörer som har tecknat säkerhetsskyddsavtal med Myndigheten.

3. Säkerhetsskyddsorganisation

Det ska finnas en säkerhetsskyddschef och en ställföreträdande säkerhetsskyddschef på Företaget. Säkerhetsskyddschefen ska i Uppdragets säkerhetsskyddsfrågor vara direkt underställd Företagets ledning. Säkerhetsskyddschefen leder säkerhetsskyddsverksamheten inom Företaget och är kontaktperson i säkerhetsskyddsfrågor gentemot Myndigheten. På Företaget ska det även finnas en systemsäkerhetsansvarig för IT-system som är avsedda för behandling av hemliga uppgifter.

4. Säkerhetsskyddsåtgärder

Företaget ska upprätta en säkerhetsskyddsinstruktion när ett säkerhetsskyddsavtal har träffats.

Eventuella förändringar eller tillägg i säkerhetsskyddsinstruktionen ska godkännas av Myndigheten.

Företaget ska dokumentera de säkerhetsskyddsåtgärder som har vidtagits i Uppdraget.

5. Behörighet

Behöriga att ta del av hemliga uppgifter är endast personer som

- Bedöms pålitliga från säkerhetssynpunkt
- Har tillräckliga kunskaper om säkerhetsskydd
- Behöver uppgifterna för sitt uppdrag eller arbete i den verksamhet där de hemliga uppgifterna förekommer.

Hemliga uppgifter får endast delges personer som har säkerhetsprövats och godkänts av Myndigheten.

6. Informationssäkerhet

Myndigheten ska klargöra för Företaget i vilken utsträckning handlingar med mera som Företaget tar del av innehåller hemliga uppgifter.

Om hemliga uppgifter uppkommer under Uppdragets utförande på Företaget, ska Företaget vidta de säkerhetsskyddsåtgärder som är nödvändiga. Företaget ska utan dröjsmål meddela Myndigheten om hemliga uppgifter har uppkommit samt vilka säkerhetsskyddsåtgärder som har vidtagits.

Företaget får endast hantera och förvara hemliga uppgifter i av Myndigheten anvisade och godkända utrymmen. Hemliga uppgifter får inte medföras från Myndigheten eller från av Myndigheten anvisade områden eller lokaler.

Hemliga uppgifter får endast hanteras i IT-system som har godkänts för sådan hantering av Myndigheten. Beträffande hemliga uppgifter i IT-miljö gäller för Uppdraget bestämmelserna i bilaga 1 alternativt Myndighetens IT-säkerhetsbestämmelser.

Företaget bör klargöra för Myndigheten i vilken utsträckning uppgifter avseende affärs- eller driftsförhållanden som överlämnas till Myndigheten är att anse som hemliga, samt varför Företaget kan komma att lida skada om dessa röjs (enligt offentlighets- och sekretesslagen [2009:400]). Företaget är dock medvetet om att Myndigheten ändå kan vara skyldig att lämna ut sådan uppgifter.

Företaget får inte utan Myndighetens tillstånd lämna uppgifter till massmedia som rör Uppdraget och som enligt Myndigheten innehåller hemlig uppgift. Detsamma gäller för publicering i broschyrer, tidskrifter, böcker, filmer etc., samt vid föredrag, utställningar och förevisningar dit personer som inte är behöriga (punkt 5) har tillträde.

Företaget får inte utan Myndighetens tillstånd offentliggöra att det träffat ett säkerhetsskyddsavtal. Denna information får därmed inte användas i marknadsföring eller på annat sätt.

7. Tillträdesbegränsning

Myndighetens bestämmelser om tillträdesbegränsning gäller för Företagets personal som ska delta i Uppdraget.

Företaget får inte utan Myndighetens godkännande byta eller använda andra lokaler, områden eller motsvarande för Uppdragets genomförande.

Endast behöriga personer som har godkänts av Myndigheten får ha tillträde till de lokaler, områden eller motsvarande där Uppdraget genomförs. Det åligger Företagets personal att följa Myndighetens tillträdesbestämmelser.

8. Säkerhetsprövning

Innan en person får del av hemliga uppgifter ska Företaget genom säkerhetsprövning pröva vederbörandes lojalitet och pålitlighet från säkerhetssynpunkt. Säkerhetsprövningen ska omfatta varje person som får del av hemliga uppgifter, oavsett om de blir föremål för registerkontroll enligt säkerhetsskyddslagen (1996:627) eller inte.

Säkerhetsprövningen ska omfatta en personbedömning samt inhämtande av betyg, intyg och referenser. Är befattningen placerad i säkerhetsklass ska säkerhetsprövningen även omfatta registerkontroll och i vissa fall särskild personutredning.

Säkerhetsprövningen ska dokumenteras av Företaget och på begäran lämnas till Myndigheten. Tillsammans med uppgifter som har framkommit vid registerkontroll och särskild personutredning utgör säkerhetsprövningen underlag för Myndighetens beslut om att personen får anlitas. Företaget får inte anlita personen innan Företaget har fått del av Myndighetens beslut.

Innan en ansökan om registerkontroll skickas till Myndigheten ska Företaget särskilt informera den person som ska bli föremål för registerkontroll om vad kontrollen innebär. Företaget ska i samband med detta också inhämta personens samtycke till kontrollen. Samtycket ska dokumenteras och förvaras på Företaget.

Företaget ska utan dröjsmål anmäla till Myndigheten om en registerkontrollerad person på Företaget lämnar Uppdraget. Myndigheten ska utan dröjsmål anmäla till Säkerhetspolisen att personen har lämnat Uppdraget.

Företaget ska till Myndigheten anmäla omständigheter som kan vara av betydelse för bedömningen av en säkerhetsprövad persons lämplighet och pålitlighet.

Om en person som har säkerhetsprövats inom ramen för detta säkerhetsskyddsavtal under Uppdragets genomförande befinns olämplig från säkerhetssynpunkt, ska Företaget vidta de åtgärder som är lämpliga för att vederbörande inte ska få tillgång till hemliga uppgifter eller tillträde till lokaler, områden eller motsvarande där säkerhetskänslig verksamhet bedrivs.

9. Intern utbildning och kontroll

Myndigheten ska innan Uppdraget påbörjas ge lämplig utbildning i säkerhetsskyddsfrågor till de personer på Företaget som kan komma att få del av hemliga uppgifter eller tillträde till lokaler, områden eller motsvarande där säkerhetskänslig verksamhet bedrivs. Därefter ansvarar Företaget för att dessa personer ges behövlig och fortlöpande utbildning. Utbildningen ska bland annat behandla:

- Hot och risker som från säkerhetssynpunkt föreligger mot eller är förknippade med Uppdraget
- Säkerhetsskyddsåtgärder som enligt Företagets säkerhetsskyddsinstruktion alternativt Myndighetens bestämmelser ska vidtas mot föreliggande hot och risker.

Myndigheten kan vid behov och efter särskild framställan medverka i viss utbildning som Företaget ger.

Företaget ska fortlöpande kontrollera att endast behöriga personer som har godkänts av Myndigheten anlitas och att säkerhetsskyddet avseende informationssäkerhet och tillträdesbegränsning iakttas, samt att skyddsnivån är jämn och tillräckligt hög.

Företaget ska omedelbart underrätta Myndigheten om inträffade eller befarade händelser och omständigheter som kan påverka säkerhetsskyddet vad avser Uppdraget och personer som faller under detta avtal.

10. Tillsyn

Myndigheten har rätt att kontrollera att de i säkerhetsskyddsinstruktionen alternativt Myndighetens bestämmelser redovisade och avtalade säkerhetsskyddsbestämmelserna följs. Vid en sådan tillsyn kan Myndigheten biträdas av en representant från Säkerhetspolisen och/eller Försvarsmakten. Tillsynen ska ske under Företagets ordinarie kontorstid eller på plats och tid enligt särskild överenskommelse. Tillsynen får inte vara mer ingripande för Företaget än vad som är nödvändigt.

11. Kostnader

Företaget ska bära eventuella kostnader som uppkommer med anledning av detta säkerhetsskyddsavtal om inget annat avtalas i Affärsavtalet.

12. Övrigt

Hemliga uppgifter som har tillförts eller uppkommit under Uppdragets genomförande ska även efter att avtalet har upphört, eller till dess att Myndigheten meddelar något annat, omfattas av tystnadsplikt.

Företaget ska informera berörd personal om innebörden av tystnadsplikten och säkerhetsskyddet samt se till att personalen undertecknar sekretessförbindelser. Dessa förvaras på Företaget så länge Uppdraget pågår. När Uppdraget är slutfört lämnas sekretessförbindelserna till Myndigheten.

Företaget ska utan dröjsmål anmäla till Myndigheten när någon förändring sker beträffande firma, organisationsnummer, styrelse, verkställande direktör, revisor, post- och besöksadress eller telefonnummer. Avser ändringen firma, organisationsnummer, styrelse, verkställande direktör eller revisor ska ett nytt registreringsbevis bifogas anmälan. En anmälan ska också göras om ägarförhållandena ändras, om Företaget råkar i ekonomiska svårigheter eller försätts i konkurs.

Samtliga handlingar, materiel eller övrigt som innehåller hemliga uppgifter och som har anknytning till Uppdraget är Myndighetens egendom om inget annat har avtalats. Dessa handlingar eller dylikt ska senast i samband med fullgjort Uppdrag återlämnas till Myndigheten eller vid den tidpunkt som parterna särskilt har kommit överens om.

13. Avtalsperiod

Detta säkerhetsskyddsavtal träder i kraft vid undertecknandet och gäller tills vidare eller till dess det skriftligen sägs upp av endera parten. [Uppsägningstid]

Avtalet kan dock inte ensidigt sägas upp till en tidigare tidpunkt än den dag då Uppdraget har slutförts eller alla hemliga uppgifter har återlämnats till Myndigheten.

Myndigheten kan dock ensidigt säga upp detta avtal liksom Affärsavtalet med omedelbar verkan om Företaget frångår detta avtal.

Detta avtal har upprättats i två likalydande exemplar varav parterna har tagit var sitt.

[Ort] den [datum och år]

[MYNDIGHETEN]	**[FÖRETAGET AB]**
.....	.....
[Anna Andersson]	**[Birgit Bertilsson]**

Bilaga C

Mall säkerhetsskyddsavtal (nivå 3)

[Myndigheten], org.nr [111111-1111], [Alfagatan 1], [111 11] [Stockholm], som företräder staten, nedan kallad Myndigheten

och

[Företaget AB], org.nr [222222-2222], [Betagatan 2], [222 22] [Stockholm], nedan kallat Företaget träffar följande avtal om säkerhetsskydd.

1. Bakgrund

Myndigheten och Företaget avser att ingå ett avtal avseende alternativt Företaget ska få del av förfrågningsunderlag [diarienummer eller liknande] angående projektet [projektnamn], nedan kallat Uppdraget.

[Beskrivning av Uppdraget]

Uppdraget innebär att Företaget i Myndighetens lokaler eller av Myndigheten anvisade områden eller lokaler kan få del av hemliga uppgifter.

Säkerhetsskyddet ska förebygga a) att hemliga uppgifter obehörigen röjs, ändras, görs otillgängliga för behöriga eller förstörs (informationssäkerhet), b) att obehöriga får tillgång till hemliga uppgifter eller verksamhet som har betydelse för rikets säkerhet (tillträdesbegränsning), och c) att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning). Andra säkerhetsskyddsåtgärder är utbildning och kontroll.

Detta avtal avser säkerhetsskydd för uppgifter som på Myndigheten omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet. En sådan uppgift benämns fortsättningsvis hemlig uppgift. En hemlig uppgift kan framgå av en handling, ett visst förhållande, en anläggning eller föremål av olika slag.

2. Avtalets omfattning

Detta avtal tillsammans med Företagets säkerhetsskyddsinstruktion (om en sådan har upprättats) reglerar vilka säkerhetsskyddsåtgärder som Företaget ska vidta i samband med Uppdraget.

De ekonomiska villkoren avseende Uppdraget regleras i ett kontrakt, nedan kallat Affärsavtalet.

Detta säkerhetsskyddsavtal är en förutsättning för men utgör ingen utfästelse eller garanti för att Myndigheten ska teckna Affärsavtal med Företaget om Uppdraget.

Om det förekommer motstridiga uppgifter i Affärsavtalet gäller detta säkerhetsskyddsavtal framför Affärsavtalet. Motsvarande skrivning ska även tas in i Affärsavtalet.

Företaget får endast använda underleverantörer som har tecknat säkerhetsskyddsavtal med Myndigheten.

3. Säkerhetsskyddsorganisation

Det ska finnas en säkerhetsskyddschef och en ställföreträdande säkerhetsskyddschef på Företaget. Säkerhetsskyddschefen ska i Uppdragets säkerhetsskyddsfrågor vara direkt underställd Företagets ledning. Säkerhetsskyddschefen leder säkerhetsskyddsverksamheten inom Företaget och är kontaktperson i säkerhetsskyddsfrågor gentemot Myndigheten. På Företaget ska det även finnas en systemsäkerhetsansvarig för IT-system som är avsedda för behandling av hemliga uppgifter.

4. Säkerhetsskyddsåtgärder

Företaget ska upprätta en säkerhetsskyddsinstruktion när ett säkerhetsskyddsavtal har träffats.

Eventuella förändringar eller tillägg i säkerhetsskyddsinstruktionen ska godkännas av Myndigheten.

Företaget ska dokumentera de säkerhetsskyddsåtgärder som har vidtagits i Uppdraget.

5. Behörighet

Behöriga att ta del av hemliga uppgifter är endast personer som

- Bedöms pålitliga från säkerhetssynpunkt
- Har tillräckliga kunskaper om säkerhetsskydd
- Behöver uppgifterna för sitt uppdrag eller arbete i den verksamhet där de hemliga uppgifterna förekommer.

Hemliga uppgifter får endast delges personer som har säkerhetsprövats och godkänts av Myndigheten.

6. Informationssäkerhet

Myndigheten ska klargöra för Företaget i vilken utsträckning handlingar med mera som Företaget kan få del av innehåller hemliga uppgifter.

Om hemliga uppgifter uppkommer under Uppdragets utförande på Företaget, ska Företaget vidta de säkerhetsskyddsåtgärder som är nödvändiga. Företaget ska utan dröjsmål meddela Myndigheten om hemliga uppgifter har uppkommit samt vilka säkerhetsskyddsåtgärder som har vidtagits.

Företaget får endast hantera och förvara hemliga uppgifter i av Myndigheten anvisade och godkända utrymmen. Hemliga uppgifter får inte medföras från Myndigheten eller från av Myndigheten anvisade områden eller lokaler.

Hemliga uppgifter får endast hanteras i IT-system som har godkänts för sådan hantering av Myndigheten. Beträffande hemliga uppgifter i IT-miljö gäller för Uppdraget bestämmelserna i bilaga 1 alternativt Myndighetens IT-säkerhetsbestämmelser.

Företaget bör klargöra för Myndigheten i vilken utsträckning uppgifter avseende affärs- eller driftsförhållanden som överlämnas till Myndigheten är att anse som hemliga, samt varför Företaget kan komma att lida skada om dessa röjs (enligt offentlighets- och sekretesslagen [2009:400]). Företaget är dock medvetet om att Myndigheten ändå kan vara skyldig att lämna ut sådana uppgifter.

Företaget får inte utan Myndighetens tillstånd lämna uppgifter till massmedia som rör Uppdraget och som enligt Myndigheten innehåller hemlig uppgift. Detsamma gäller för publice-

ring i broschyrer, tidskrifter, böcker, filmer etc., samt vid föredrag, utställningar och förevisningar dit personer som inte är behöriga (punkt 5) har tillträde.

Företaget får inte utan Myndighetens tillstånd offentliggöra att det träffat ett säkerhetsskyddsavtal. Denna information får därmed inte användas i marknadsföring eller på annat sätt.

7. Tillträdesbegränsning

Myndighetens bestämmelser om tillträdesbegränsning gäller för Företagets personal som ska delta i Uppdraget.

Företaget får inte utan Myndighetens godkännande byta eller använda andra lokaler, områden eller motsvarande för Uppdragets genomförande.

Endast behöriga personer som har godkänts av Myndigheten får ha tillträde till de lokaler, områden eller motsvarande där Uppdraget genomförs. Det åligger Företagets personal att följa Myndighetens tillträdesbestämmelser.

8. Säkerhetsprövning

Innan en person får tillträde till lokaler eller områden där han eller hon kan få del av hemliga uppgifter ska Företaget genom säkerhetsprövning pröva vederbörandes lojalitet och pålitlighet från säkerhetssynpunkt. Säkerhetsprövningen ska omfatta varje person som får tillträde till lokaler eller områden där han eller hon kan få del av hemliga uppgifter, oavsett om de blir föremål för registerkontroll enligt säkerhetsskyddslagen (1996:627) eller inte.

Säkerhetsprövningen ska omfatta en personbedömning samt inhämtande av betyg, intyg och referenser. Är befattningen placerad i säkerhetsklass ska säkerhetsprövningen även omfatta registerkontroll och i vissa fall särskild personutredning.

Säkerhetsprövningen ska dokumenteras av Företaget och på begäran lämnas till Myndigheten. Tillsammans med uppgifter som har framkommit vid registerkontroll och särskild personutredning utgör säkerhetsprövningen underlag för Myndighetens beslut om att personen får anlitas. Företaget får inte anlita personen innan Företaget har fått del av Myndighetens beslut.

Innan en ansökan om registerkontroll skickas till Myndigheten ska Företaget särskilt informera den person som ska bli föremål för registerkontroll om vad kontrollen innebär. Företaget ska i samband med detta också inhämta personens samtycke till kontrollen. Samtycket ska dokumenteras och förvaras på Företaget.

Företaget ska utan dröjsmål anmäla till Myndigheten om en registerkontrollerad person på Företaget lämnar Uppdraget. Myndigheten ska utan dröjsmål anmäla till Säkerhetspolisen att personen har lämnat Uppdraget.

Företaget ska till Myndigheten anmäla omständigheter som kan vara av betydelse för bedömningen av en säkerhetsprövad persons lämplighet och pålitlighet.

Om en person som har säkerhetsprövats inom ramen för detta säkerhetsskyddsavtal under Uppdragets genomförande befinns olämplig från säkerhetssynpunkt, ska Företaget vidta de åtgärder som är lämpliga för att vederbörande inte ska få tillträde till lokaler, områden eller motsvarande där han eller hon kan få tillgång till hemliga uppgifter.

9. Intern utbildning och kontroll

Myndigheten ska innan Uppdraget påbörjas ge lämplig utbildning i säkerhetsskyddsfrågor till de personer på Företaget som kan komma att få tillträde till lokaler, områden eller motsvarande där han eller hon kan få del av hemliga uppgifter. Därefter ansvarar Företaget för att dessa personer ges behövlig och fortlöpande utbildning. Utbildningen ska bland annat behandla:

- Hot och risker som från säkerhetssynpunkt föreligger mot eller är förknippade med Uppdraget
- Säkerhetsskyddsåtgärder som enligt Företagets säkerhetsskyddsinstruktion alternativt Myndighetens bestämmelser ska vidtas mot föreliggande hot och risker.

Myndigheten kan vid behov och efter särskild framställan medverka i viss utbildning som Företaget ger.

Företaget ska fortlöpande kontrollera att endast behöriga personer som har godkänts av Myndigheten anlitas och att säkerhetsskyddet avseende informationssäkerhet och tillträdesbegränsning iakttas, samt att skyddsnivån är jämn och tillräckligt hög.

Företaget ska omedelbart underrätta Myndigheten om inträffade eller befarade händelser och omständigheter som kan påverka säkerhetsskyddet vad avser Uppdraget och personer som faller under detta avtal.

10. Tillsyn

Myndigheten har rätt att kontrollera att de i säkerhetsskyddsinstruktionen alternativt Myndighetens bestämmelser redovisade och avtalade säkerhetsskyddsbestämmelserna följs. Vid en sådan tillsyn kan Myndigheten biträdas av en representant från Säkerhetspolisen och/eller Försvarsmakten. Tillsynen ska ske under Företagets ordinarie kontorstid eller på plats och tid enligt särskild överenskommelse. Tillsynen får inte vara mer ingripande för Företaget än vad som är nödvändigt.

11. Kostnader

Företaget ska bära eventuella kostnader som uppkommer med anledning av detta säkerhetsskyddsavtal om inget annat avtalas i Affärsavtalet.

12. Övrigt

Hemliga uppgifter som har tillförts eller uppkommit under Uppdragets genomförande ska även efter att avtalet har upphört, eller till dess att Myndigheten meddelar något annat, omfattas av tystnadsplikt.

Företaget ska informera berörd personal om innebörden av tystnadsplikten och säkerhetsskyddet samt se till att personalen undertecknar sekretessförbindelser. Dessa förvaras på Företaget så länge Uppdraget pågår. När Uppdraget är slutfört lämnas sekretessförbindelserna till Myndigheten.

Företaget ska utan dröjsmål anmäla till Myndigheten när någon förändring sker beträffande firma, organisationsnummer, styrelse, verkställande direktör, revisor, post- och besöksadress eller telefonnummer. Avser ändringen firma, organisationsnummer, styrelse, verkställande direktör eller revisor ska ett nytt registreringsbevis bifogas anmälan. En anmälan ska också göras om ägarförhållandena ändras, om Företaget råkar i ekonomiska svårigheter eller försätts i konkurs.

Samtliga handlingar, materiel övrigt som innehåller hemlig uppgift och som har anknytning till Uppdraget är Myndighetens egendom om inget annat har avtalats. Dessa handlingar eller dylikt ska senast i samband med fullgjort Uppdrag återlämnas till Myndigheten eller vid den tidpunkt som parterna särskilt har kommit överens om.

13. Avtalsperiod

Detta säkerhetsskyddsavtal träder i kraft vid undertecknandet och gäller tills vidare eller till dess det skriftligen sägs upp av endera parten. [Uppsägningstid]

Avtalet kan dock inte ensidigt sägas upp till en tidigare tidpunkt än den dag då Uppdraget har slutförts eller alla hemliga uppgifter har återlämnats till Myndigheten.

Myndigheten kan dock ensidigt säga upp detta avtal liksom Affärsavtalet med omedelbar verkan om Företaget frångår detta avtal.

Detta avtal har upprättats i två likalydande exemplar varav parterna har tagit var sitt.

[Ort] den [datum och år]

[MYNDIGHETEN]	**[FÖRETAGET AB]**
.....	.....
[Anna Andersson]	**[Birgit Bertilsson]**

Bilaga D

Exempel på sekretessförbindelse – säkerhetsskyddad upphandling

Uppdraget angående …… innebär att du får/kan få del av uppgifter som hos uppdragsgivaren (myndigheten) omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet (hemliga uppgifter). För dessa uppgifter gäller tystnadsplikt.

Tystnadsplikt innebär att det är förbjudet att röja eller utnyttja hemliga uppgifter vare sig det sker muntligen eller på annat sätt. Det är även otillåtet att röja hemliga uppgifter för kollegor som inte har behov av uppgiften för utförande av Uppdraget och att till exempel förevisa hemliga föremål för obehöriga.

Jag bekräftar att jag har:
- Upplysts om räckvidden och innebörden av den tystnadsplikt som gäller för mig som anställd på …… avseende hemliga uppgifter
- Upplysts om innebörden av begreppet behörig och vad detta innebär i fråga om att lämna hemliga uppgifter till en annan person oavsett hur detta sker
- Informerats om straffbestämmelserna i 19 kap. brottsbalken avseende brott mot rikets säkerhet.

Jag …… (namn, personnummer, befattning) förbinder mig att iaktta tystnadsplikt avseende alla hemliga uppgifter som jag får del av i samband med Uppdraget.

Tystnadsplikten gäller även efter att anställningen eller Uppdraget har upphört.

……
Egenhändig namnteckning

Information enligt ovan har meddelats av undertecknad.

…… ……
Underskrift **Namnförtydligande**

Jag har idag, med anledning av att min anställning (eller motsvarande) kommer att upphöra, informerats om den tystnadsplikt som gäller för alla hemliga uppgifter som jag fått del av i samband med Uppdraget.

……
Egenhändig namnteckning

Information enligt ovan har meddelats av undertecknad.

…… ……
Underskrift **Namnförtydligande**

Bilaga E

Begreppsförklaringar

Begreppen i denna vägledning används med nedanstående innebörd. Observera att begreppen kan definieras på annat sätt i andra sammanhang. I förekommande fall refereras i definitionen till relevant bestämmelse (se bilaga F).

AFFÄRSAVTAL	Ett avtal med ekonomiska villkor som sluts mellan en myndighet och ett företag. Benämns som kontrakt i LOU och LUF. 2 kap. 10 § LOU och LUF.
DIREKTUPPHANDLING	Ett förfarande utan krav på anbud. Direktupphandling får endast användas om kontraktets värde är lågt eller om det finns synnerliga skäl. 2 kap. 23 §, 15 kap. 3 § LOU och 2 kap. 26 §, 15 kap. 3 § LUF.
FÖRENKLAT FÖRFARANDE	Ett förfarande där alla leverantörer har rätt att delta, deltagande leverantörer ska lämna anbud och den upphandlande myndigheten får förhandla med en eller flera anbudsgivare. 2 kap. 24 §, 15 kap. 3 § LOU och 2 kap. 27 §, 15 kap. 3 § LUF.
FÖRETAG	Aktiebolag, handelsbolag, föreningar och andra juridiska personer samt enskilda firmor med vilka en myndighet avser att träffa ett säkerhetsskyddsavtal. Benämns leverantör i LOU och LUF. 7 kap. 1 § RPSFS 2010:03, 2 kap. 11 § LOU och LUF.
FÖRFRÅGNINGSUNDERLAG	Ett underlag för anbud som en upphandlande myndighet tillhandahåller en leverantör. 2 kap. 8 § LOU.
FÖRSTAGÅNGSBESÖK	Ett besök av myndigheten hos företaget i syfte att förvissa sig om att företagets lokaler och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt. 7 kap. 5 § RPSFS 2010:03.
HEMLIG UPPGIFT	Uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet. 4 § säkerhets skyddsförordningen.
INFORMATIONSSÄKERHET	Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet. Informationssäkerhet innefattar bland annat IT-säkerhet.
IT-SÄKERHET	Säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation. IT-säkerhet är en del av informationssäkerhet.

KONTRAKT	Se begreppet affärsavtal.
MYNDIGHET	I denna vägledning avses stat, kommun och landsting som omfattas av 8 § säkerhetsskyddslagen.
OFFENTLIG UPPHANDLING	De åtgärder som vidtas av en upphandlande myndighet i syfte att tilldela ett kontrakt eller ingå ett ramavtal avseende varor, tjänster eller byggentreprenader. 2 kap. 13 § LOU.
OFFSHORING	Ett företag flyttar produktion av varor eller tjänster, till exem pel utveckling, underhåll och/eller drift av IT-system, till ett annat land.
OUTSOURCING	Utförandet av hela eller delar av funktioner som tidigare legat inom det egna företaget, till exempel telefonväxel, städning och stödfunktioner, överlåts till en underleverantör inom landet.
RAMAVTAL	Ett avtal som ingås mellan en eller flera upphandlande myndigheter och en eller flera leverantörer i syfte att fastställa villkoren för senare tilldelning av kontrakt under en given tidsperiod. 2 kap. 15 § LOU och 2 kap. 16 § LUF.
SEKRETESS	Förbud att röja uppgift oavsett om det sker muntligt, genom att allmänna handlingar lämnas ut eller på annat sätt. Offentlighets- och sekretesslagen.
SÄKERHETSANALYS	Myndigheter och andra som säkerhetsskyddsförordningen gäller för ska undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av denna undersökning – säkerhetsanalysen – ska dokumenteras. 5 § säkerhetsskyddsförordningen.
SÄKERHETSPLAN	Inför ett anbud eller en upphandling finns ibland behov av att göra en säkerhetsanalys av det aktuella uppdraget. Denna analys utgår från myndighetens säkerhetsanalys. Resultatet av analysen benämns i denna vägledning säkerhetsplan.
SÄKERHETSSKYDDSAVTAL	Ett skriftligt avtal mellan en myndighet och anbudsgivare eller leverantör som reglerar vilka säkerhetsskyddsåtgärder (informationssäkerhet inklusive IT-säkerhet, tillträdesbegränsning, säkerhetsprövning, utbildning och kontroll) som bedöms nödvändiga för den enskilda upphandlingen. 8 § säkerhetsskyddslagen.
SÄKERHETS-SKYDDSINSTRUKTION	Av företaget upprättade bestämmelser eller riktlinjer som redovisar vilka säkerhetsskyddsåtgärder som kommer att vidtas för att uppfylla kraven i säkerhetsskyddsavtalet. Säkerhetsskyddsinstruktionen och förändringar i den ska alltid godkännas av myndigheten. 7 kap. 6 § RPSFS 2010:03.

UPPHANDLINGSSEKRETESS	Anbudsansökningar och anbud omfattas av så kallad absolut sekretess. Absolut sekretess innebär att uppgifter ur anbudsansökningar och anbud inte får lämnas ut under upphandlingsprocessen till annan än den som har lämnat anbudet eller ansökan enligt offentlighets- och sekretesslagen.
URVALSFÖRFARANDE	Ett förfarande där alla leverantörer har rätt att ansöka om att få lämna anbud, den upphandlande myndigheten inbjuder vissa leverantörer att lämna anbud och den upphandlande myndigheten får förhandla med en eller flera anbudsgivare. 2 kap. 25 § LOU och 2 kap. 28 § LUF.

Bilaga F

Referenser

I denna vägledning finns hänvisningar till bestämmelser och publikationer som listas nedan. Listan innehåller även andra relevanta publikationer. För aktuell lagtext, se www.lagrummet.se.

Lagar, förordningar och föreskrifter

Försvarsmaktens föreskrifter om säkerhetsskydd; FFS 2003:7

Lagen (2007:1091) om offentlig upphandling [klassiska sektorn]
– *förkortas i texten LOU*

Lagen (2003:148) om straff för terroristbrott

Lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster [försörjningssektorn]
– *förkortas i texten LUF*

Offentlighets- och sekretesslagen (2009:400)

Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd; RPSFS 2010:03
– *förkortas i texten RPSFS 2010:03*

Säkerhetsskyddsförordningen (1996:633)

Säkerhetsskyddslagen (1996:627)

Säkerhetspolisens tillsynsområde

Säkerhetsskydd – en vägledning (Säkerhetspolisen 2009, www.sakerhetspolisen.se)

Försvarsmaktens tillsynsområde

Riktlinjer för sekretessbedömning inom Försvarsmakten (H SÄK Sekrbed 1999)

Handbok för Försvarsmaktens säkerhetstjänst i säkerhetsskydd (H SÄK Skydd 2007)

Försvarsmaktens föreskrifter om säkerhetsskydd; FFS 2003:7

Upphandling

Upphandlingsreglerna, en introduktion (Konkurrensverket 2008, www.konkurrensverket.se)

Övrigt

Industrisäkerhetsskyddsmanual (FMV/Säkerhetsskydd 2004, www.fmv.se/security)

Säkerhetspolisen

Säkerhetspolisen

Box 12312, 102 28 Stockholm
Tfn 010-568 70 00 Fax 010-568 70 10
E-post sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se