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.