Bilaga
Utkast till
Säkerhetsskyddsavtal
(Nivå 2)

KAMMARKOLLEGIET

Innehåll

1 Parter

Namn på Kunds organisation:
Adress:
Telefonnummer:
Fax:
E-postadress:
Organisationsnummer:

Namn på leverantörs (Ramavtalsleverantör eller underleverantör) organisation:
Adress:
Telefonnummer:
Fax:
E-postadress:
Organisationsnummer:

Har tecknat detta Säkerhetsskyddsavtal.

2 Definitioner

Samtliga begrepp som används i detta Säkerhetsskyddsavtal är definierade i bilaga Allmänna villkor.

3 Inledning

Detta Säkerhetsskyddsavtal utgör en del av Ramavtalet Kommunikationstjänster inom tele- och datakom, med diarienummer 23.3-3081-17. Villkoren i detta

Säkerhetsskyddsavtal reglerar vilka säkerhetsskyddsåtgärder som leverantör ska vidta i samband med att Kontrakt ska fullgöras och/eller att Ramavtalsleverantör ska få ta del av Avropsförfrågan som innehåller hemliga uppgifter.

3.1 Leverantör ska samråda med Kund om osäkerhet uppstår angående vad som ska betraktas som hemliga uppgifter.

3.2 Kontrakt innebär att leverantör i Kunds lokaler eller av Kund anvisade områden eller lokaler kommer att hantera och förvara hemliga uppgifter.

3.3 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.

3.4 Detta Säkerhetsskyddsavtal avser säkerhetsskydd för uppgifter som hos Kund som 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.

3.5 Detta Säkerhetsskyddsavtal tillsammans med leverantörs säkerhets-skyddsinstruktion, om en sådan har upprättats och godkänts, reglerar vilka säkerhetsskyddsåtgärder som leverantör ska vidta i samband med Avropsförfrågan och när Kontrakt ska fullgöras.

3.6 Ekonomiska villkor avseende detta Säkerhetsskyddsavtal regleras i Kontrakt.

3.7 Detta Säkerhetsskyddsavtal är en förutsättning men utgör ingen utfästelse eller garanti för att Kund ska teckna Kontrakt med Ramavtalsleverantör.

3.8 Om det förekommer motstridiga uppgifter i Kontrakt gäller detta Säkerhets-skyddsavtal framför Kontrakt. Motsvarande skrivning ska även tas in i Kontrakt.

3.9 Ramavtalsleverantör får endast använda Underleverantör som har tecknat Säkerhetsskyddsavtal med Kund.

4 Säkerhetsskydds-organisation

4.1 Det ska finnas en säkerhetsskyddschef och en ställföreträdande säkerhetsskyddschef hos leverantör.

4.2 Säkerhetsskyddschefen ska i säkerhetsskyddsfrågor rörande fullgörande av Kontrakt vara direkt underställd leverantörs ledning.

4.3 Säkerhetsskyddschefen leder säkerhetsskyddsverksamheten hos leverantör och är kontaktperson i säkerhetsskyddsfrågor gentemot Kund. Hos leverantör ska det även finnas en systemsäkerhetsansvarig för it-system som är avsedda för behandling av hemliga uppgifter.

5 Säkerhetsskyddsåtgärder

5.1 Leverantör ska upprätta en säkerhetsskyddsinstruktion när Säkerhetsskyddsavtal har undertecknats.

5.2 Eventuella förändringar eller tillägg i säkerhetsskyddsinstruktion ska godkännas av Kund.

5.3 Leverantör ska dokumentera de säkerhetsskyddsåtgärder som har vidtagits i samband med fullgörande av Kontrakt.

6 Behörighet

6.1 Behöriga att ta del av hemliga uppgifter är endast personer som:
(a) Bedöms pålitliga från säkerhetssynpunkt
(b) Har tillräckliga kunskaper om säkerhetsskydd
(c) Behöver uppgifterna för fullgörande av Kontrakt eller arbete i den verksamhet där de hemliga uppgifterna förekommer

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

7 Informationssäkerhet

7.1 Kund ska klargöra för leverantör i vilken utsträckning handlingar med mera som leverantör tar del av innehåller hemliga uppgifter.

7.2 Om hemliga uppgifter uppkommer under fullgörande av Kontrakt hos leverantör, ska leverantör vidta de säkerhetsskyddsåtgärder som är nödvändiga. Leverantör ska utan dröjsmål meddela Kund om hemliga uppgifter har uppkommit samt vilka säkerhetsskyddsåtgärder som har vidtagits.

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

7.4 Leverantör bör klargöra för Kund i vilken utsträckning uppgifter avseende affärs- eller driftsförhållanden som överlämnas till Kund är att anse som hemliga, samt varför leverantör kan komma att lida skada om dessa röjs (enligt offentlighets- och sekretesslagen). Leverantör är dock medveten om att Kund ändå kan vara skyldig att lämna ut sådana uppgifter.

7.5 Leverantör får inte utan Kunds tillstånd offentliggöra att det träffat ett Säkerhetsskyddsavtal. Denna information får därmed inte användas i marknadsföring eller på annat sätt.

7.6 Leverantör får inte utan Kunds tillstånd lämna uppgifter till massmedia som rör Kontrakt och som enligt Kund 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, enligt avsnitt 6, har tillträde.

7.7 Hemliga uppgifter får endast hanteras i it-system som har godkänts för sådan hantering av Kund. Beträffande hemliga uppgifter i it-miljö gäller för Kontrakts fullgörande bestämmelserna i avsnitt 8 alternativt Kunds it-säkerhetsbestämmelser.

8 Hemliga uppgifter i it-miljö

Informationen i detta avsnitt 8 motsvarar Säkerhetspolisens bilaga 1 till Säkerhetsskyddsavtal. Innehållet i bilagan är valbar för Säkerhetsskyddsavtal nivå 2. Det som har avtalats avseende hemliga uppgifter gäller även för kvalificerat hemliga uppgifter, om inte annat anges.

8.1 Hemliga uppgifter får endast hanteras i it-system som har godkänts för sådan hantering av Kund. It-system får inte tas i drift förrän Kund har godkänt it-system för behandling av hemliga uppgifter. Inför godkännandet ska it-system granskas för att verifiera att det uppfyller kraven på säkerhetsskydd. Vid granskningen är det särskilt viktigt att granska om it-system samverkar med andra it-system. Granskningen ska ske av annan än den som uppförde it-system. Granskningen ska dokumenteras.

8.2 Leverantör ska dokumentera mål och riktlinjer för säkerheten i it-system från anskaffning till avveckling. Leverantör 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 Kund.

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

8.4 En okrypterad dataförbindelse får användas för hemliga uppgifter inom ett område eller en lokal som disponeras av leverantör om leverantör har vidtagit och dokumenterat betryggande åtgärder mot obehörig avlyssning, och under förutsättning att Kund har godkänt detta.

8.5 Hemliga uppgifter får inte behandlas i ett it-system som har externa nätverks-kopplingar om inte Kund har godkänt detta.

8.6 Om Kund godkänt externa nätverkskopplingar får hemliga uppgifter sändas via ett elektroniskt kommunikationsnät endast om ett av Försvarsmakten godkänt signal-skyddssystem (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 Kund innan sändning förekommer.

8.7 Leverantör ska utse en systemsäkerhetsansvarig som ansvarar för säkerheten i det it-system som ska hantera hemliga uppgifter.

8.8 Hemliga uppgifter i it-system ska så långt praktiskt möjligt hanteras på samma sätt som hemliga fysiska handlingar. Hemliga elektroniska handlingar ska märkas enligt anvisningar i säkerhetsskyddsinstruktion. En kvalificerat hemlig elektronisk handling får inte skickas elektroniskt. Anvisningar om övrig hantering av elektroniska hemliga handlingar anges i den av leverantör upprättade och av Kund godkända säkerhetsskyddsinstruktion.

8.9 Om it-system 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-system. Om it-system utgörs av en fristående dator som nyttjas av flera personer ska det vid varje användning finnas ett behörighets-kontrollsystem 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-system. Denna förteckning ska sparas för att spårbarhet ska kunna uppnås i efterhand. Förteckningen ska överlämnas till

Kund när Kontrakt är avslutat. It-system ska logga användaridentitet, datum och tidpunkt för inloggning och utloggning samt användaraktiviteter i övrigt som är av betydelse för säkerheten i it-system. Leverantör ska dokumentera hur säkerhetsloggar ska analyseras. Kund ska godkänna anvisningarna. Säkerhetsloggarna ska överlämnas till Kund när Kontrakt är avslutat.

8.10 Innan ny information tillförs it-system ska informationen kontrolleras så att den inte innehåller skadlig kod. Programvara som skyddar mot skadlig kod ska uppdateras kontinuerligt. Leverantör ska dokumentera skyddet mot skadlig kod och Kund ska godkänna skyddet.

8.11 It-system ska vara försett med intrångsskydd och funktioner för intrångsdetektering. Leverantör ska dokumentera intrångsskyddet och intrångsdetekteringen, och Kund ska godkänna intrångsskyddet och intrångsdetekteringen.

8.12 Leverantör ska analysera och dokumentera behovet av skydd mot röjande signaler. Kund ska godkänna analysen. Om det behövs ska it-system ha ett betryggande skydd mot röjande signaler. It-system ska vara försedda med betryggande skydd mot obehörig avlyssning.

8.13 Leverantör ska dokumentera rutiner för hantering, rapportering och uppföljning av incidenter av betydelse för säkerheten i eller kring it-system. Kund ska godkänna incidenthanteringen.

8.14 Säkerhetskopior ska tas regelbundet enligt en av leverantör dokumenterad rutin, och förvaras avskilt från den plats där berört it-system finns. Säkerhetskopiorna ska testas regelbundet och förvaras i ett godkänt säkerhetsskåp. Säkerhetskopiorna bör krypteras. Kund ska godkänna rutinerna för säkerhetskopiering.

8.15 Leverantör ska bedöma och dokumentera den längsta tid som it-system kan vara ur funktion utan att fullgörande av Kontrakt i väsentlig omfattning störs. Leverantör ska också bedöma och dokumentera vilken reservrutin som ska användas om det inträffar. Kund ska godkänna kontinuitetsplanen.

8.16 Skrivare ska vara placerad i nära anslutning till och inom synhåll från den dator där utskriften upprättas.

8.17 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 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 fullgörande av Kontrakt 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 Kund för destruering, alternativt förstöras enligt Kunds anvisningar.

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

8.18 Vid service och underhåll av lagringsmedier som innehåller hemliga uppgifter får leverantör endast använda personal som är behörig att ta del av hemliga uppgifter enligt detta Säkerhetsskyddsavtal.

9 Tillträdesbegränsning

9.1 Kunds bestämmelser om tillträdesbegränsning gäller för leverantörs personal som ska delta vid fullgörande av Kontrakt.

9.2 Leverantör får inte utan Kunds godkännande byta eller använda andra lokaler, områden eller motsvarande för fullgörande av Kontrakt.

9.3 Endast behöriga personer som har godkänts av Kund får ha tillträde till de lokaler, områden eller motsvarande där fullgörande av Kontrakt genomförs. Det åligger leverantörs personal att följa Kunds tillträdesbestämmelser.

10 Säkerhetsprövning

10.1 Innan en person får del av hemliga uppgifter ska leverantör 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.

10.2 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.

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

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

10.5 Leverantör ska utan dröjsmål anmäla till Kund om en registerkontrollerad person hos leverantör lämnar uppdraget som är en del av fullgörande av Kontrakt. Kund ska utan dröjsmål anmäla till Säkerhetspolisen att personen har lämnat uppdraget som är en del av fullgörande av Kontrakt.

10.6 Leverantör ska till Kund anmäla omständigheter som kan vara av betydelse för bedömningen av en säkerhetsprövad persons lämplighet och pålitlighet.

10.7 Om en person som har säkerhetsprövats inom ramen för detta Säkerhetsskyddsavtal under fullgörande av Kontrakt befinns olämplig från säkerhetssynpunkt, ska leverantör 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.

10.8 Innan en person får del av hemliga uppgifter ska leverantör 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

11 Intern utbildning och kontroll

11.1 Kund ska före i Kontrakt överenskommet samarbete påbörjas ge lämplig utbildning i säkerhetsskyddsfrågor till de personer hos leverantör som kan komma att få del av hemliga uppgifter eller tillträde till lokaler, områden eller motsvarande där säkerhetskänslig verksamhet bedrivs. Därefter ansvarar leverantör för att dessa personer ges behövlig och fortlöpande utbildning. Utbildningen ska bland annat behandla:
(a) Hot och risker som från säkerhetssynpunkt föreligger mot eller är förknippade

med fullgörande av Kontrakt.
(b) Säkerhetsskyddsåtgärder som enligt leverantörs säkerhetsskyddsinstruktion ska vidtas mot föreliggande hot och risker.

11.2 Kund kan vid behov och efter särskild framställan medverka i viss utbildning som leverantör ger.

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

11.4 Leverantör ska omedelbart underrätta Kund om inträffade eller befarade händelser och omständigheter som kan påverka säkerhetsskyddet vad avser fullgörande av Kontrakt och personer som faller under detta Säkerhetsskyddsavtal.

12 Tillsyn

12.1 Kund har rätt att kontrollera att de i säkerhetsskyddsinstruktion alternativt Kunds bestämmelser redovisade och avtalade säkerhetsskyddsbestämmelserna följs. Vid en sådan tillsyn kan Kund biträdas av en representant från Säkerhetspolisen och/eller Försvarsmakten.

12.2 Tillsynen ska ske under Arbetsdag under normal kontorstid eller på plats och tid enligt särskild överenskommelse. Tillsynen får inte vara mer ingripande för leverantör än vad som är nödvändigt.

13 Kostnader

13.1 Leverantör ska bära eventuella kostnader som uppkommer med anledning av detta Säkerhetsskyddsavtal om inget annat avtalats i Kontrakt.

13.2 Ändring av Kontrakt ska ske enligt avsnitt 38 (Ändringar och tillägg) i Allmänna villkor.

14 Övrigt

14.1 Hemliga uppgifter som har tillförts eller uppkommit under fullgörande av Kontrakt ska även efter att Säkerhetsskyddsavtal upphört, eller till dess att Kund meddelar något annat, omfattas av tystnadsplikt.

14.2 Leverantör ska informera berörd personal om innebörden av tystnadsplikten och säkerhetsskyddet samt se till att personalen undertecknar sekretessförbindelser. Dessa förvaras hos leverantör så länge Kontrakt är giltigt och ska kunna kontrolleras av Kund under Kontraktstid. När Kontrakt avslutas lämnas sekretessförbindelserna till Kund.

14.3 Leverantör ska utan dröjsmål anmäla till Kund 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 leverantör råkar i ekonomiska svårigheter eller försätts i konkurs.

14.4 Samtliga handlingar, materiel eller övrigt som innehåller hemliga uppgifter och som har anknytning till Kontrakt är Kunds egendom om inget annat har avtalats. Dessa handlingar eller dylikt ska senast i samband med fullgjort Kontrakt återlämnas till Kund eller vid den tidpunkt som Kund och leverantör särskilt har kommit överens om.

15 Avtalsperiod

15.1 Detta Säkerhetsskyddsavtal träder i kraft vid undertecknandet och gäller tills vidare eller till dess det skriftligen sägs upp av Kund eller leverantör.

15.2 Säkerhetsskyddsavtal kan dock inte ensidigt sägas upp till en tidigare tidpunkt än den dag då Kontrakt har avslutats eller alla hemliga uppgifter har återlämnats till Kund.

15.3 Kund kan dock ensidigt säga upp detta Säkerhetsskyddsavtal liksom Kontrakt med omedelbar verkan om leverantör frångår detta Säkerhetsskyddsavtal.

Detta Säkerhetsskyddsavtal har upprättats i två likalydande exemplar varav Kund och leverantör har tagit var sitt.

Kund

Namn (fullständigt):
Befattning:
Ort och datum:

.....

Namnteckning

Leverantör

Namn (fullständigt):
Befattning:
Ort och datum:

.....

Namnteckning