Säkerhetsskyddsavtal SUA nivå 1

mellan

Affärsverket svenska kraftnät (”SvK”)
Postadress: Box 1200, 172 24 Sundbyberg
Besöksadress: Sturegatan 1, Sundbyberg
nedan kalla SvK
och **FÖRETAGET XXX**
Adress:
Organisationsnummer:

Svenska kraftnät (SvK) och **FÖRETAGET XXX** träffar följande avtal om säkerhetsskydd i samband med förvaring av sekretessinformation ang **Projekt/uppdrag XXX**

Detta avtal reglerar det säkerhetsskydd som med hänsyn till rikets säkerhet skall tillämpas beträffande det uppdrag som FÖRETAGET XXX skall utföra åt SvK enligt särskilt affärsavtal, i vilket hänvisning skall ske till detta avtal.

Detta säkerhetsskyddsavtal är en förutsättning, men utgör ingen utfästelse eller garanti för att SvK skall teckna affärsavtal med FÖRETAGET XXX om uppdraget.

Uppdraget innebär att FÖRETAGET XXX i sina egna lokaler kommer att hantera och förvara hemliga uppgifter av betydelse för rikets säkerhet. För utförligare underlag se ”Projektsäkerhetsinstruktion XXX”.

Detta säkerhetsskyddsavtal omfattar erforderliga säkerhetsskyddsåtgärder, som FÖRETAGET XXX skall iakttaga, främst avseende informationssäkerhet, inklusive IT-säkerhet, säkerhetsprövning, tillträdesbegränsning, intern utbildning och kontroll, tillsyn samt uppdragsspecifika tillägg.

Sekretess kan, om FÖRETAGET XXX så begär och i den utsträckning 31 kap 16-17 § offentlighets- och sekretesslagen (2009:400) medger, gälla hos SvK för uppgifter som överlämnas till SvK.

Parterna förbinder sig att beträffande uppdraget
iakttaga,
- dels bestämmelserna i detta säkerhetsskyddsavtal,
- dels bestämmelserna i den säkerhetsskyddsinstruktion som har upprättats och fastställts av FÖRETAGET XXX och godkänts av SvK den

ansvarar genom säkerhetsskyddschefen: ……
Tel: ……för att ovanstående bestämmelser följs hos FÖRETAGET XXX

Kontaktperson vid Svenska kraftnät är XXX.

1. **Allmänt**

1.1 Detta avtal jämte den av FÖRETAGET XXX upprättade och fastställda och av SvK godkända säkerhetsskyddsinstruktionen skall ligga till grund för säkerhetsskyddet inom FÖRETAGET XXX i anledning av uppdraget för SvK. Eventuella ändringar av eller tillägg till säkerhetsskyddsinstruktionen skall godkännas av SvK för att vara gällande.

1.2 FÖRETAGET XXX ansvarar för att överenskommet säkerhetsskydd genomförs och efterlevs inom FÖRETAGET XXX

1.3 Samtliga handlingar, disketter, materiel, modeller eller liknande som har anknytning till uppdraget, och överlämnats av SvK skall såvitt inget annat avtalats, anses som SvK egendom.

1.4 Senast i samband med slutredovisningen av uppdraget skall FÖRETAGET XXX till SvK återlämna samtliga till uppdraget hörande handlingar, disketter, materiel, modeller eller liknande.

2. **Säkerhetsskyddsorganisation**

2.1 Vid FÖRETAGET XXX skall det finnas en säkerhetsskyddschef och en ersättare för denne (ställföreträdande säkerhetsskyddschef). Säkerhetsskyddschefen skall i säkerhetsskyddsfrågor vara direkt underställd FÖRETAGET XXX s ledning.

2.2 Säkerhetsskyddsverksamheten inom FÖRETAGET XXX skall ledas av säkerhetsskyddschefen. Säkerhetsskyddschefen är kontaktman i säkerhetsskyddsfrågor gentemot SvK.

2.3 Vid FÖRETAGET XXX skall det finnas en registrator.

2.4 FÖRETAGET XXX s säkerhetsorganisation och utsedda säkerhetsansvariga skall framgå av FÖRETAGET XXX s säkerhetsskyddsinstruktion.

3. **Informationssäkerhet**

3.1 Det åligger SvK att skriftligen meddela FÖRETAGET XXX vad som är hemligt i uppdraget. Hemlig uppgift enligt säkerhetsskyddsförordningen (1996:633) är uppgift som omfattas av Offentlighets – och sekretesslagen (2009:400)och som rör rikets säkerhet. Vid beslut om ändring av skyddsnivån skall SvK snarast underrätta FÖRETAGET XXX . Röjande av hemlig uppgift kan medföra åtal enligt, 19 kap BrB.

3.2 Personal som av FÖRETAGET XXX avses användas för arbete åt SvK skall ur säkerhetssynpunkt vara behörig att ta del av hemlig uppgift. Behörig att ta del av hemlig uppgift är endast den som:

- bedöms pålitlig ur säkerhetssynpunkt
- har tillräckliga kunskaper om säkerhetsskydd

- behöver uppgifterna för sitt arbete i den verksamhet där de hemliga uppgifterna förekommer.

3.3 För genomförande av uppdraget får FÖRETAGET XXX endast använda personal eller underleverantörer som godkänts av SvK. Detsamma gäller för FÖRETAGET XXX eventuella samtliga övriga enheter (centrala, regionala och lokala).

3.4 All personal som skall delta i uppdraget skall innan detta påbörjas informeras om innebörden och räckvidden av tystnadsplikten samt intyga detta genom att underteckna ett personligt sekretessbevis.
Undertecknade sekretessbevis skall hanteras och förvaras av FÖRETAGET XXX på betryggande sätt så att de inte kan åtkommas av obehöriga.

3.5 Förvaringsutrymmen av lägst säkerhetsskåpsstandard (SS 3492) för hemliga uppgifter som handlingar, disketter och materiel skall godkännas av SvK för att få användas.

3.6 Inventering av hemlig handling och hemligt material som utlånats till behörig person och inventering av expeditioner och arkiv skall ske vid behov genom FÖRETAGET XXX försorg. Inventeringsrapport skall dock avges till SvK minst en gång/år.

3.7 Handling och materiel som innehåller hemlig uppgift får endast förstöras genom SvK:s försorg eller enligt överenskommelse med SvK.

Före beslut av SvK om förstöring skall kontroll ske att handlingarna ej erfordras för fullgörande av eventuella garanti- eller serviceåtaganden.

Verkställd förstöring skall framgå av anteckningar i register över hemliga handlingar. Handlingar som ej förstörts skall redovisas till SvK enligt punkt 1.4 ovan.

3.8 Hemliga uppgifter, som ingår i uppdraget får inte delges annan myndighet, företag eller enskild utan SvK skriftliga godkännande.

3.9 Innan uppgift inom ramen för detta avtal genom FÖRETAGET XXX lämnas till massmedia eller för publicering i broschyrer, tidskrifter, böcker, filmer eller liknande skall FÖRETAGET XXX kontrollera med SvK att det inte rör hemliga uppgifter.
Vad här sagts skall gälla även vid föredrag, utställning och förevisning, dit annan än från säkerhetssynpunkt behöriga äger tillträde.

4. Säkerhetsprövning

4.1 FÖRETAGET XXX skall innan enskild person delges hemlig uppgift genom säkerhetsprövning pröva vederbörandes lämplighet och pålitlighet från säkerhetsskyddssynpunkt.

Säkerhetsprövning omfattar:

- Allmän personkännedom.
- Referenser.
- Betyg, intyg och liknande.

Vid inplacering i säkerhetsklass

- Godkännande av SvK efter genomförd registerkontroll.

4.2 Säkerhetsprövningen enligt punkten 4.1 skall dokumenteras av FÖRETAGET XXX och vid begäran lämnas över till SvK. Den utgör därefter underlag för bedömning av inplacering i säkerhetsklass och för SvK:s beslut efter genomförd registerkontroll.

4.3 Den som avses bli föremål för registerkontroll skall av FÖRETAGET XXX informeras om detta samt ge sitt skriftliga samtycke till registerkontroll. *Detta krävs inte vid omkontroll av tidigare kontrollerad person i samma befattning och säkerhetsklass.* Vid begäran om registerkontroll skall FÖRETAGET XXX insända fullständiga personuppgifter till SvK samt bekräftelse på att berörd person upplysts om samt lämnat sitt skriftliga samtycke till den begärda registerkontrollen.

4.4 FÖRETAGET XXX skall avvakta med att anlita registerkontrollerad person intill dess FÖRETAGET XXX delgivits SvKs beslut efter verkställd registerkontroll. FÖRETAGET XXX skall följa SvK beslut

4.5 FÖRETAGET XXX skall utan dröjsmål anmäla till SvK om en säkerhetsklassad person vid FÖRETAGET XXX byter befattning, lämnar det aktuella uppdraget eller avslutar sin anställning.

4.6 FÖRETAGET XXX skall till SvK anmäla omständigheter som kan vara av betydelse för bedömning av en säkerhetsprövad persons lämplighet och pålitlighet.

4.7 Om en person som säkerhetsprövats inom ramen för detta avtal, under uppdragets genomförande befinns olämplig ur säkerhetssynpunkt, skall FÖRETAGET XXX vidta de åtgärder som är lämpliga för att vederbörande inte skall få tillgång till hemliga uppgifter.

5. Tillträdesbegränsning

5.1 SvK fastställer i samråd med FÖRETAGET XXX nivån på tillträdesbegränsningen för de lokaler och områden som FÖRETAGET XXX avser utnyttja för genomförande av uppdraget, innan den säkerhetsskyddade verksamheten får påbörjas.

5.2 Om FÖRETAGET XXX under uppdragets genomförande avser att utnyttja andra lokaler skall detta omgående anmälas till SvK för fastställande av nivån på säkerhetsskyddet för de nya lokalerna.

5.3 Om besökare till tillträdesbegränsat område kan antas komma att få del av hemliga uppgifter skall SvK godkännande inhämtas före besöket. Med besökare avses varje person som inte redan är behörig enligt villkoren i punkterna 3.3.

6. IT-säkerhet

6.1 Innan användning av datorstöd påbörjas skall samråd ske med SvK. Vid IT-användning gäller säkerhetsbestämmelser som framgår av handbok för

Försvarsmaktens Säkerhetsskyddstjänst Informationsteknologi (H Säk IT 2006) samt ev övriga, av SvK skriftligen redovisade krav.

7. Intern utbildning och kontroll

7.1 Personal som kan komma att få del av hemliga uppgifter skall innan uppdraget påbörjas och därefter fortlöpande ges erforderlig utbildning genom FÖRETAGET XXX försorg angående:

- hot och risker som kan föreligga med anledning av verksamheten,
- sekretessförhållanden,
- innebörden och räckvidden av tystnadsplikten,
- tillträdesregler,
- övriga säkerhetsskyddsåtgärder som enligt de av SvK meddelade säkerhetsskyddsbestämmelserna skall vidtas mot föreliggande hot och risker.

Den grundläggande utbildningen skall med angivande av utbildningsdatum skriftligt bekräftas till SvK

Vid behov och efter framställan kan SvK medverka i viss del av utbildningen.

7.2 FÖRETAGET XXX skall fortlöpande kontrollera att endast behörig personal anlitas och att säkerhetsskyddet avseende informationssäkerhet och tillträdesbegränsning iakttas samt att skyddsnivån är jämn och tillräckligt hög.

7.3 FÖRETAGET XXX skall hålla SvK underrättad om inträffade eller befarade händelser och omständigheter, som kan påverka säkerhetsskyddet vad avser uppdrag och anställda som faller under detta avtal.

8. Tillsyn

8.1 SvK har rätt att kontrollera att de redovisade och avtalade säkerhetsskydds-bestämmelserna efterföljs. Vid sådan kontroll kan även representant för Säkerhetspolisen delta och utföra denna i samråd med beställaren.

9. Kostnader

9.1 Kostnader som inte reglerats särskilt i detta säkerhetsskyddsavtal, men som uppkommer på grund av detsamma, skall regleras i affärsavtalet mellan SvK och FÖRETAGET XXX

10. Giltighet

10.1 Detta avtal träder i kraft vid undertecknandet och gäller tills vidare intill det skriftligen sägs upp av endera parten. Avtalet kan dock inte ensidigt sägas upp före den dag, då uppdrag som omfattas av detta avtal slutförts. SvK kan dock ensidigt häva avtalet, om FÖRETAGET XXX frångår detta eller dess anda.

10.2 Hemliga uppgifter som erhållits eller uppkommit under fullgörande av uppdrag, som omfattas av detta avtal, skall även efter avtalets upphörande hemlighållas tills dess annat meddelas av SvK.

10.3 FÖRETAGET XXX skall utan dröjsmål anmäla till SvK när någon ändring sker beträffande firmanamn, organisationsnummer, post- och besöksadress samt, styrelse övrig ledning, säkerhetsansvariga och revisorer. Detsamma gäller vid ändrade ägareförhållanden eller om FÖRETAGET XXX råkar i ekonomiska svårigheter eller försätts i konkurs. Aktuellt registreringsbevis, som är högst tre månader gammalt, skall bifogas anmälan.

10.4 Av detta säkerhetsskyddsavtal är två likalydande exemplar upprättade och utväxlade.

.....	.....
Ort och datum	Ort och datum
Svenska Kraftnät	FÖRETAGET XXX
_____	_____
Bemyndigad avtalstecknare	Firmatecknare
_____	_____
Namnförtydligande	Namnförtydligande

Bilaga 1 till säkerhetsskyddsavtal

Bestämmelser avseende informationssäkerhet för hemliga uppgifter i IT-miljö

1. **Allmänt**

1.1 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.

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

1.3 FÖRETAGET XXX ska samråda med SvK om osäkerhet uppstår angående vad som ska betraktas som hemliga uppgifter

1.4 FÖRETAGET XXX ska dokumentera mål och riktlinjer för säkerheten i IT-system från anskaffning till avveckling. FÖRETAGET XXX 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 SvK.

1.5 IT-system får inte tas i drift förrän SvK 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**

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

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

2.2 Hemliga uppgifter får inte behandlas i ett IT-system som har externa nätverkskopplingar om inte SvK har medgett annat. Om SvK medger externa nätverkskopplingar får hemliga uppgifter sändas via ett elektroniskt kommunikationsnät endast om ett 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 SvK innan sändning förekommer.

3. Systemsäkerhetsansvarig

3.1 FÖRETAGET XXX ska utse en systemsäkerhetsansvarig som ansvarar för säkerheten i det IT-system som ska hantera hemliga uppgifter. Detta skall dokumenteras och en kontaktlista skall upprättas.

4. Hantering av elektroniska hemliga handlingar

4.1 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.

4.2 En kvalificerat hemlig elektronisk handling får inte skickas elektroniskt.

4.3 Anvisningar om övrig hantering av elektroniska hemliga handlingar anges i den av FÖRETAGET XXX upprättade och av SvK godkända säkerhetsskyddsinstruktionen.

5. Behörighetskontroll och säkerhetsloggning

Säkerhetsfunktionen behörighetskontroll syftar till att identifiera och autenticera en användare samt styra åtkomsten till de delar i IT-systemet som användaren har behörighet att ta del av. Säkerhetsfunktionen för behörighetskontroll kan implementeras genom användandet av olika policys eller kombinationer av dessa som grund.

5.1 Om IT-systemet utgörs av ett nätverk ska ett behörighetskontrollsystem användas där alla användare är unikt identifierbara och har ett personligt aktivt kort, en säkerhetsdosa för engångslösenord eller vanligt lösenord för att logga in i IT-systemet. Systemet skall tillhandahålla mekanismer för byte av lösenord. Lösenordet ska vara tidsbegränsat. Vid upprepande autenticeringsfel skall konton låsas och administratören notifieras. Vidare skall manuell upplåsning ske endast av behörig administratör.

5.2 Endast behörig administratör ska förvalta behörighetskontrollsystemet och sköta dess säkerhetsinställningar

5.3 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 SvK när Uppdraget är avslutat.

5.4 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 XXX ska dokumentera hur säkerhetsloggar analyseras. SvK ska godkänna anvisningarna. Säkerhetsloggarna ska överlämnas till SvK när Uppdraget är avslutat.

5.5 IT-systemets loggar skall vara i läsbar format och skall möjliggöra verktygsbaserad granskning av registrerade händelser. Säkerhetskopiering av säkerhetsloggen skall vara möjligt.

5.6 IT-systemet skall säkerställa att registrerade händelser inte raderas, skrivs över eller på annat sätt förstörs eller ändras.

6. **Skydd mot skadlig kod**

6.1 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.

6.2 FÖRETAGET XXX ska dokumentera skyddet mot skadlig kod och SvK ska godkänna skyddet.

7. **Intrångsdetektering och skydd mot intrång**

Detta syftar till att på ett kontrollerat sätt ge åtkomst till olika tjänster i ett IT-system, både från insidan och från utsidan av det skyddade IT-systemet. Detta kontrollerade sätt kan åstadkommas genom att tillåta, neka och/eller genom att omdirigera informationsflödet genom intrångsskyddet.
Det finns i huvudsak två principiellt olika sätt att implementera intrångsskydd. Den första lösningen är att låta inkommande och utgående informationsflöde passera genom någon form av filter som då baserat på regler avgör om informationen skall få passera igenom filtret eller inte. Filter kan implementeras olika avancerat och därmed utgöra olika styrka på intrångsskyddet.
Den andra lösningen är att använda vissa typer av krypto som genom att dekryptera inkommande informationsflöde kan avgöra om dekrypteringen gått rätt till och därmed tillåta informationen att passera in i IT-systemet. Det utgående informationsflödet krypteras på motsvarande sätt och för att kunna ta del av informationen måste sålunda den mottagande parten ha tillgång till rätt nyckel.

7.1 IT-systemet ska vara försett med intrångsskydd och funktioner för intrångsdetektering. FÖRETAGET XXX ska dokumentera intrångsskyddet och intrångsdetekteringen, och SvK ska godkänna skyddet och detekteringen.

7.2 Intrångsskyddet skall begränsa vilken information som får överföras genom säkerhetsfunktionen genom att kontrollera både inkommande och utgående informationsflöde och säkerställa att information inte överförs utan att de konfigurerade filter anropas och används.

8. **Skydd mot skadlig kod**

Skyddet mot skadlig kod kan implementeras på olika sätt där det vanligaste skyddet är att använda programvara för detektering av skadlig kod, s.k. antivirusprogramvara. Det är dock inte det enda skyddet som kan implementeras i IT-system utan det går också att använda integritetskontroller för subjekt och objekt samt använda konfigurationsstyrning av mjukvara. Alternativ till att använda antivirusprogramvara är att endast tillåta sådan mjukvara som är trovärdig, dvs. där källan är känd och utvärderad, eller att endast tillåta signerad mjukvara. Den senare ställer stora krav på att veta vilka subjekt och objekt som verksamheten behöver och därmed skall tillåtas samt att det finns ett förtroende för den part som signerar mjukvaran.

8.1 Skyddet mot skadlig kod skall förhindra all åtkomst till IT-systemets resurser av sådana objekt som innehåller skadlig kod samt säkerställa detektering av skadlig kod genom kontroll av inkommande och utgående informationsflöde samt att ingen överföring kan ske utan att kontrollmekanismen används.

8.2 Som kontrollmekanism skall användas en definitionsfil.

8.3 Skyddet skall, om detektering av skadlig kod sker, automatiskt kunna vidta åtgärder. Sådana åtgärder skall vad gäller definitionsfil, omfatta placering av subjekt eller objekt i karantän samt notifiera behörig administratör och behörig användare.

8. Skydd mot röjande signaler och obehörig avlyssning

8.1 FÖRETAGET XXX ska analysera och dokumentera behovet av skydd mot röjande signaler. SvK ska godkänna analysen. Om det behövs ska IT-systemet ha ett betryggande skydd mot röjande signaler.

8.2 IT-system ska vara försedda med betryggande skydd mot obehörig avlyssning som t.ex. kryptering.

9. Incidenthantering

9.1 FÖRETAGET XXX ska dokumentera rutiner för hantering, rapportering och uppföljning av incidenter av betydelse för säkerheten i eller kring ett IT-system. SvK ska godkänna incidenthanteringen.

10. Säkerhetskopiering

10.1 Säkerhetskopior ska tas regelbundet enligt en av FÖRETAGET XXX dokumenterad rutin, och förvaras avskilt från den plats där det berörda IT-systemet finns.

10.2 Säkerhetskopiorna ska testas regelbundet och förvaras i ett godkänt säkerhetsskåp

10.3 Säkerhetskopiorna bör krypteras. SvK ska godkänna rutinerna för säkerhetskopiering.

11. Kontinuitetsplan

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

12. Hantering av utskrifter

12.1 Skrivare eller plotter ska vara placerad i nära anslutning till och inom synhåll från den dator där utskriften upprättas. Tillgång till utrustning för utskrift skall begränsas till de för uppdraget deltagande resurser.

13. Hantering av digitala lagringsmedia

13.1 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 USA-minnen, som innehåller eller har innehållit hemliga uppgifter, ska förvaras i säkerhetsskåp. Endast behörig personal får ha tillgång till säkerhetsskåpet

13.2 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.

13.3 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.

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

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

14. Underhåll

14.1 Vid service och underhåll av lagringsmedier som innehåller hemliga uppgifter får FÖRETAGET XXX endast använda personal som är behörig att ta del av hemliga uppgifter enligt säkerhetsskyddsavtalet.