



Redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling Datorer, mobiltelefoner och surfplattor

Innehåll

1 Inledning.....	1
2 Kravkatalog	3
Följande krav kan i ett avrop kompletteras med	3
Följande villkor för fullgörande av kontraktet kan preciseras.....	3
3 Kvalificeringskrav.....	3
Krav på ramavtalsleverantörens informationssäkerhetsarbete	Fel! Bokmärket är inte definierat.
4 Tekniska krav	4
Informationssäkerhetskrav på upphandlingsföremålet	8
5 Tilldelningskriterier	8
Tilldelningskriterier avseende informationssäkerhet	9
6 Särskilda kontraktsvillkor.....	9
Villkor för informationssäkerhet vid fullgörande av ramavtalet.....	9

1 Inledning

Detta dokument redovisar krav, kriterier och villkor avseende informationssäkerhet som använts i ramavtalsupphandling Datorer, mobiltelefoner och surfplattor. Det innehåller även krav som kan ställas vid avrop. Dokumentet är avsett att ge en bild av hur frågor avseende informationssäkerhet hanterats i den aktuella ramavtalsupphandlingen.

Krav och villkor är hämtade från upphandlingsunderlag och ramavtal. För de fullständiga dokumenten hänvisas till information om respektive ramavtalsområde på avropa.se.



Kraven och villkoren är här indelade på följande sätt:

Kravkatalog

Kravkatalogen erbjuder möjlighet för avropsberättigad att själv ställa krav, kriterier och villkor avseende informationssäkerhet. Den avropsberättigade kan välja ut och formulera lämpliga krav, kriterier och/eller villkor utifrån den egna verksamhetens behov.

Kvalificeringskrav

Kvalificeringskrav är obligatoriska krav på leverantören som ska vara uppfyllda redan när anbud lämnas in.

Tekniska krav

Tekniska krav avser obligatoriska krav på upphandlingsföremålet, produkten och eller tjänsten ställda i ramavtalsupphandlingen. Dessa krav kan vara uttryckta som "ska-krav".

Tilldelningskriterier

Tilldelningskriterier avser krav på egenskaper hos upphandlingsföremålet, produkten och eller tjänsten, som gett ett mervärde i ramavtalsupphandlingen, exempelvis poäng, påslag eller avdrag. Dessa krav kan vara uttryckta som "bör-krav".

Särskilda kontraktsvillkor

Särskilda kontraktsvillkor är krav och villkor som leverantör och upphandlingsföremål ska uppfylla vid ramavtalets fullgörande. Dessa villkor finns i ramavtalets Huvuddokument och i Allmänna villkor samt i Kravkatalog. Även andra benämningar förekommer.

2 Kravkatalog

Följande krav kan i ett avrop kompletteras med

Krav avseende informationssäkerhet på upphandlingsföremålet

Vid Avrop kan krav, kriterier och villkor komma att ställas på informationssäkerhet, cybersäkerhet och säkerhet, exempelvis avseende kryptering, spårbarhet, behörigheter, administration, uppdateringar, användaridentiteter, autentisering och detekteringsförmåga, destruering, gallring, distansradering, radering, rensning, tillgänglighet, skydd mot avlyssning, lösenord, fysisk säkerhet, säkra transporter.

Vid Avrop kan krav, kriterier och villkor komma att ställas på att det vid leverans tillämpas regelverk, processer, rutiner och strukturer avseende informationssäkerhet.

Vid Avrop kan krav, kriterier och villkor komma att ställas på att Ramavtalsleverantör och Underleverantör ingår säkerhetsskyddsavtal med Avropsberättigad.

Följande villkor för fullgörande av kontraktet kan preciseras

Se texten i avsnitt om särskilda kontraktsvillkor.

3 Kvalificeringskrav

Informationssäkerhetskrav på sökande

4.1.4 Systematiskt informationssäkerhetsarbete

Sökanden ska bedriva ett systematiskt informationssäkerhetsarbete som minst har en koppling till Upphandlingsföremålet.

Sökanden ska vid tidpunkten för anbudsansökans inlämnande tillämpa ett strukturerat, dokumenterat och systematiskt informationssäkerhetsarbete i enlighet med gällande utgåva av ISO 27001, eller likvärdigt enligt punkt c nedan.

Inom ramen för det systematiska informationssäkerhetsarbetet ska sökanden arbeta efter en upprättad informationssäkerhetspolicy som har en koppling till Upphandlingsföremålet och som minst säkerställer:

1. att det finns fastställda informationssäkerhetsmål,
2. att sökanden arbetar med uppföljning av fastställda informationssäkerhetsmål,
3. att sökanden arbetar med att identifiera risker utifrån fastställda informationssäkerhetsmål,
4. att sökanden arbetar med att hantera risker utifrån fastställda informationssäkerhetsmål, och
5. att sökanden har fördelat resurser samt tilldelat behörighet och befogenheter vad gäller informationssäkerhetsarbetet i dessa delar.

För att styrka ovanstående krav ska sökanden som kompletterande dokument bifoga antingen:

- a. ett giltigt certifikat för ISO 27001 (samt på förfrågan, eventuella bilagor),
- b. en handling som påvisar ett likvärdigt informationssäkerhetssystem, som är certifierat av ett ackrediterat organ i något annat land inom EES, och som uppfyller punkterna 1–5 ovan, eller
- c. en egen utförlig beskrivning där det tydligt framgår att punkterna 1–5 ovan är uppfyllda.

Handlingen ska vara översatt till svenska, engelska, danska eller norska om originalhandlingen är upprättad på ett annat språk.

4.1.5.4 Destruering

Sökande ska kunna erbjuda destruktion av Hårdvara.

Sökande ska kunna säkerställa att Hårdvara eller del av Hårdvara destrueras så att lagrad information inte går att återskapa.

Det innebär att sökande minst ska kunna:

- montera bort lagringsmedia
- destruera lagringsmedia
- upprätta ett intyg i vilket det framgår att lagringsmedia är destruerat och på vilket sätt det är destruerat

Sökande ska kunna tillhandahålla destrueringsintyg.

Destrueringsintyget ska minst innehålla:

- Vilken typ av lagringsmedia, ange serienummer eller likvärdigt
- Datum för destruering
- Vilken metod som användes
- Garanti om att lagringsmedia är destruerat på ett sätt som gör att informationen på lagringsmediet inte kan återskapas

Sökande ska ange om kravet uppfylls via åberopat företag.

Sökande ska visa en mall som används vid upprättade av intyg för destruering genom att bifoga mallen nedan eller skicka in den som kompletterade dokument på begäran av Kammarkollegiet. Mallen ska minst innehålla uppgifter enligt punkterna ovan.

4.1.5.5 Säker borttagning av data på hårddisk

Sökande ska kunna erbjuda säker borttagning av data på hårddisk.

Sökande ska kunna ta bort data/information på ett sätt som vid var tid är det mest effektiva för att eftersträva att data/information inte kan återläsas eller återskapas.

Det innebär att sökande minst ska kunna:

- ta bort data/information på hårddisk på ett sätt som är det mest effektiva för att data/informationen inte kan återläsas eller återskapas
- upprätta ett intyg i vilket det framgår att säker borttagning av data på hårddisk är genomförd
- utföra borttagningen på plats hos kund eller i egna lokaler

Sökande ska kunna utfärda intyg för säker borttagning av data på hårddisk.

Intyget för säker borttagning av data ska minst innehålla:

- att data/informationen är borttagen på ett sätt som är det mest effektiva så att data/informationen inte går att återskapa eller återläsas
- information om vilken metod för borttagning som har används
- information om vilken programvara som används

Sökande ska ange om kravet uppfylls via åberopat företag.

Sökande ska visa en mall som används vid upprättade av intyg för säker borttagning av data på hårddisk genom att bifoga mallen nedan eller skicka in den som kompletterade dokument på begäran av Kammarkollegiet. Mallen ska minst innehålla uppgifter enligt punkterna ovan.

4.1.5.6.3 Säkerhetsspecialist

Sökande ska ha en organisation och kapacitet att hantera säkerhetsrelaterade krav, kriterier och villkor inom området.

Sökande ska förfoga över minst 1 Konsult som minst uppfyller kraven enligt nedan.

Konsulten ska minst vara på kompetensnivå 3 enligt kapitel *Kravkatalog* och ha kompetens inom området. Sökande ska ange namn på Konsult och Konsultens arbetsgivare. Om det är ett annat företag än sökande måste det företaget anges som ett åberopat företag.

Angiven Konsult ska ha säkerhetskompetens att:

- ge råd kring produkters säkerhetsfunktioner
- ge råd angående säker metod för borttagning av data
- upprätta rutiner för säkra transporter av exempelvis lagringsmedia innehållandes data
- ge säkerhetsråd inför anskaffning av produkter
- ge support gällande säkerhetsfrågor av levererade produkter

Sökande ska fylla i bilaga *Konsultkompetens* för bevis om teknisk kompetens enligt punkterna ovan. Bilagan kan bifogas ansökan eller lämnas som kompletterade dokument på begäran av Kammarkollegiet.

4.1.5.9.4 Referensuppdrag - Destruering

Sökande ska visa att denne har en organisation och kapacitet gällande uppdrag av säker destruering av valfritt antal hårddiskar. Med destruering avses fysiska moment som förstör hårddisken så att den inte går att använda.

Hårddiskarna kan ha destruerats hos kund eller hos sökande.

Ett intyg av säker destruering ska ha getts till referenten.

Om det är ett annat företag än sökande som utfört uppdraget ska det företaget anges som ett åberopat företag.

Informationen om referensuppdragen kan bifogas i ansökan nedan eller lämnas som kompletterade dokument på begäran av Kammarkollegiet.

4.1.5.9.5 Referensuppdrag - Borttagning av data från lagringsmedia

Sökande ska visa att denne har en organisation och kapacitet som kan ta bort data från lagringsmedia på Hårdvara på ett oåterkalleligt sätt som innebär att data/information inte kan återskapas.

Hårdvaran ska genomgått en fullständig radering av information och informationen får inte ha kunnat återläsas.

Sökande ska ange den metod som används och även hur metoden fungerar.

Om det är ett annat företag än sökande som utfört uppdraget ska det företaget anges som ett åberopat företag.

Informationen om referensuppdragen kan bifogas i ansökan nedan eller lämnas som kompletterade dokument på begäran av Kammarkollegiet.



5 Begränsningskriterier

5.1.10 Referensuppdrag - Säkra transporter

Sökande kan få poäng om sökande kan visa att denne har en organisation och kapacitet som kan hantera transporter av Hårdvara med lagringsmedia på ett säkert sätt.

Transporten ska ha skett på ett sätt att obehöriga inte fått tillträde till information på Hårdvaran. Sökande ska beskriva hur transporten har gått till.

Transporten ska minst innehålla

- Hårdvaran ska ha förvarats inlåsta på något sätt.
- Övervakning av Hårdvaran på något sätt, antingen manuellt eller digitalt

Om det är ett annat företag än sökande som utfört uppdraget ska det företaget anges som ett åberopat företag.

Informationen om referensuppdrag kan bifogas i ansökan nedan eller lämnas som kompletterade dokument på begäran av Kammarkollegiet.

4 Tekniska krav

Informationssäkerhetskrav på upphandlingsföremålet

Inga tekniska krav har ställts avseende informationssäkerhet.



5 Tilldelningskriterier

Tilldelningskriterier avseende informationssäkerhet

3.4.2 Säkerhet end-point

Anbudsgivaren kan erhålla poäng om anbudsgivaren kan erbjuda en säkerhetslösning för bärbara datorer, så kallad end-point säkerhet.

Hårdvaran ska minst skyddas med en proaktiv säkerhetslösning med automatisk detektion och respons vid misstänkta beteenden. Vid bekräftade hot ska larm kunna dirigeras till tekniker.

Exempel på åtgärder som automatiskt kan blockeras är:

- Skadlig kod/mjukvara som laddas ner
- Körning av misstänkta eller maskerade skript

Anbudsgivaren ska bifoga dokumentation som visar att kriteriet uppfylls. Exempel på dokumentation är produktblad.

6 Särskilda kontraktsvillkor

Villkor för informationssäkerhet vid fullgörande av ramavtalet

5.10.3 Säkerhet i Hårdvaras systemprogramvara

För Hårdvara som Ramavtalsleverantören erbjuder ska Ramavtalsleverantören under Ramavtalets löptid övervaka status för den i Sverige senast tillgängliggjorda versionen av respektive enhets systemprogramvara (där operativsystem och annan integrerad enhetsprogramvara ingår). Ramavtalsleverantören ska på anmodan av Kammarkollegiet samt Avropsberättigade organisationer lämna uppgift om vilken version av en Hårdvaras systemprogramvara som är den senast tillgängliga, hur den tillgängliggörs kunder samt vilket datum den först tillgängliggjordes kunder i Sverige. Hårdvara som Ramavtalsleverantör erbjuder ska regelbundet förse med säkerhetsuppdateringar så länge de erbjuds av



Ramavtalsleverantörens Underleverantör och/eller varumärkesägare.

Finns en offentliggjord sårbarhet i en Hårdvara (inklusive operativsystem, operativsystemkärna (kernel) och hårdvara såsom processor och nätkommunikation) som kan utnyttjas för obehörig åtkomst eller påverkan, och sårbarheten inte hanterats med någon åtgärd i den senast tillgängliggjorda versionen av systemprogramvaran, ska Ramavtalsleverantören genast meddela Kammarkollegiet där Ramavtalsleverantören antingen anmäler utbyte av Hårdvaran i fråga, alternativt informerar om att Ramavtalsleverantören genom kontakt med varumärkesägare undersöker lösningar. Målet är att på ett betryggande sätt säkerställa att Hårdvara som erbjuds regelbundet förses med säkerhetsuppdateringar.

6.6.2 Säkerhetsangivelser och policy

Ramavtalsleverantören ska vara väl införstådd med, samt följa Avropsberättigads säkerhetsangivelser vid tillträde till dennes lokaler.

Ramavtalsleverantör ska följa villkor i Avropsberättigads miljöpolicy som Avropsberättigad angivit i Kontrakt. Om Avropsberättigad så medger, får Ramavtalsleverantör istället uppfylla Ramavtalsleverantörs egen miljöpolicy.

Ramavtalsleverantör ska följa villkor i Avropsberättigads uppförandekod och andra etiska villkor som Avropsberättigad angivit i Kontrakt. Om Avropsberättigad medger det får Ramavtalsleverantör istället uppfylla Ramavtalsleverantörs egen uppförandekod och etiska villkor.

6.28 Säkerhet och Säkerhetsskyddsavtal

Ramavtalsleverantör ska följa de föreskrifter och riktlinjer för säkerhet och informationssäkerhet som anges i Ramavtalet och Kontraktet, eller som Avropsberättigad redovisar från tid till annan samt se till att berörd personal iakttar dessa föreskrifter. Process för och konsekvenser av ändringar i föreskrifter eller riktlinjer under Kontraktstid ska följa vad som framgår avsnitt *Ändringar av Kontraktet*. Om säkerhetsföreskrifterna förändras efter Kontraktets tecknande har Ramavtalsleverantör rätt till ersättning om Ramavtalsleverantör kan påvisa att förändringarna inneburit kostnadsökningar som uppgår till mer än 5 000 SEK per år.

Om Avrop enligt Avropsberättigad omfattas av säkerhetsskydd enligt säkerhetsskyddslagen (2018:585), ska tillämpliga bestämmelser i nämnda lag följas. Ramavtalsleverantören och berörd Underleverantör ska på begäran



ingå Säkerhetsskyddsavtal med Avropsberättigad på den nivå och enligt de villkor som Avropsberättigad bestämmer. I sådana fall är Kontraktets giltighet villkorad av att ett gällande Säkerhetsskyddsavtal föreligger mellan Avropsberättigad och Ramavtalsleverantören.

Ramavtalsleverantören har inte rätt till ersättning om Avropsberättigad säger upp Kontraktet till följd av att det saknas ett giltigt Säkerhetsskyddsavtal. Säkerhetsskyddsavtalet ska inte omfatta affärsmässiga villkor såsom avgifter, viten, betalning och liknande. Ramavtalsleverantör ska vara väl införstådd med, samt följa Avropsberättigads säkerhetsangivelser vid tillträde till Avropsberättigads lokaler.