

Redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av IT-konsulttjänster – IT-säkerhet

Innehåll

1 Inledning.....	1
2 Kravkatalog	2
Följande krav kan i ett avrop kompletteras med	2
3 Kvalificeringskrav.....	3
Krav på ramavtalsleverantörens informationssäkerhetsarbete	3
4 Tekniska krav	4
Informationssäkerhetskrav på upphandlingsföremålet	4

1 Inledning

Detta dokument redovisar krav och villkor avseende informationssäkerhet som använts i ramavtalsupphandling av IT-konsulttjänster – IT-säkerhet. 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 innehåller krav och villkor avseende informationssäkerhet som kan ligga till grund för kompletteringar och preciseringar vid avrop. Den avropsberättigade kan välja ut och formulera lämpliga krav.

**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

Ur kapitel Kravkatalog avsnitt Informationssäkerhet

Vid Avrop kan krav ställas på informationssäkerhet.

Exempel på krav som kan ställas inom området informationssäkerhet är: - skydd av information mot obehörig åtkomst genom autentisering och auktorisering (behörighet), - brandväggar finns för de system som nyttjas inom ramen för utförandet av tjänsterna, - loggar bevaras och granskas regelbundet, - skydd av loggningsverktyg och logginformation mot manipulation och obehörig åtkomst, - kryptering av fasta och löstagbara lagringsmedia som lagrar kunds information, - regelbunden säkerhetskopiering av information som är tillhandahållen eller av stor vikt för kunder, - certifieringar inom IT-säkerhet, både avseende Ramavtalsleverantör och Konsult.



Ur kapitel Kravkatalog avsnitt Informationssäkerhet

Vid Avrop kan krav ställas att Ramavtalsleverantör och eventuell Underleverantör ska ingå säkerhetsskyddsavtal med Avropsberättigad och registerkontroll av Konsulter. I de fall krav på säkerhetsskyddsavtal ställs väljer Avropsberättigad vilken nivå, 1–3, som krävs för Konsulttjänstens utförande.

Avsnitt Personuppgiftsbehandling:

Vid Avrop kan krav ställas på att Ramavtalsleverantör och eventuell Underleverantör ska ingå personuppgiftsbiträdesavtal med Avropsberättigad.

Avsnitt Säkerhetsskydd och registerkontroll av Konsult:

Vid Avrop kan krav ställas att Ramavtalsleverantör och eventuell Underleverantör ska ingå säkerhetsskyddsavtal med Avropsberättigad och registerkontroll av Konsulter. I de fall krav på säkerhetsskyddsavtal ställs väljer Avropsberättigad för vilken nivå, 1-3, som krävs för Konsulttjänstens utförande.

3 Kvalificeringskrav

Krav på ramavtalsleverantörens informationssäkerhetsarbete

Informationen hämtad från Upphandlingsdokument avsnitt 5.6.3.2 Informationssäkerhetsarbete.

Anbudsgivaren ska bedriva ett strukturerat och dokumenterat arbete med informationssäkerhet som minst omfattar den personal som nyttjas vid utförande av IT-konsulttjänster.

Inom ramen för informationssäkerhetsarbetet ska anbudsgivaren:

1. arbeta efter en upprättad och av ledningen beslutad informationssäkerhetspolicy,
2. ha fastställda och mätbara informationssäkerhetsmål,
3. arbeta med uppföljning av fastställda informationssäkerhetsmål,
4. ha rutiner för att identifiera och hantera risker utifrån fastställda informationssäkerhetsmål,
5. ha rutiner för hantering och rapportering vid säkerhetsincidenter,



6. ha en tydlig ansvarsfördelning inom organisationen gällande informationssäkerhetsarbetet,
7. säkerställa att anställda regelbundet informeras om hur information får hanteras,
8. säkerställa att anställda har teknisk tillgång till kundens data enbart i de fall det är nödvändigt för att kunna fullgöra uppdrag,
9. genomföra revisioner minst en gång per år av informationssäkerhetsarbetet och på begäran kunna visa upp relevant dokumentation som styrker uppfyllnad av kravet.

För att styrka ovanstående krav ska anbudsgivaren som kompletterande dokument inkomma med antingen:

1. ett giltigt certifikat för ISO 27001 (samt på förfrågan, eventuella bilagor),
2. en handling som påvisar ett likvärdigt informationssäkerhetssystem, som är certifierat av ett ackrediterat organ etablerat inom EES, eller
3. dokumentation som styrker kravuppfyllnad samt på vidare begäran även bilaga Informationssäkerhetsarbete – hänvisning dokumentation, med tydlig hänvisning till var i dokumentationen det framgår att var och en av punkterna 1–9 ovan är uppfyllda.

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

4 Tekniska krav

Informationssäkerhetskrav på upphandlingsföremålet

Avsnitt 4.1.2 Säkerhetsskyddsavtal och registerkontroll

Anbudsgivaren ska acceptera att det vid Avrop kan komma att ställas krav på att Ramavtalsleverantör och/eller Underleverantör ska ingå säkerhetsskyddsavtal med Avropsberättigad och att Konsult ska registerkontrolleras innan Konsulttjänsten påbörjas.

Ramavtalsleverantör och/eller Underleverantör är skyldig att följa samtliga bestämmelser i tecknat säkerhetsskyddsavtal och när det krävs se till att Konsult medverkar vid avtalad säkerhetsprövning. För det fall Konsult inte medges utföra arbete för den Avropsberättigade efter sådan prövning, ska Ramavtalsleverantör utan dröjsmål se till att annan likvärdig Konsult ställs till förfogande.

Säkerhetsskyddsavtal kan tecknas på olika nivåer beroende på vilken omfattning som krävs, nivån bestäms av Avropsberättigad. Upphandlingsdokumenten innehåller bilagor som är utkast för de olika nivåerna för säkerhetsskyddsavtal.