



Redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av Finansiell revision

1. 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.

Följande krav kan ett avrop kompletteras med

8.1.9 Säkerhetsskydd och registerkontroll

Vid avrop kan Avropsberättigad ställa krav på att säkerhetsskyddsavtal (SUA) ska ingås vid genomförande av uppdrag. Ramavtalsleverantör och eventuell Underleverantör ska i sådana fall teckna säkerhetsskyddsavtal, genomgå säkerhetsprövning och konsult ska registerkontrolleras innan uppdrag får påbörjas.

2. Kvalificeringskrav

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

Krav på ramavtalsleverantörens informationssäkerhetsarbete

5.6.5 Informationssäkerhetsarbete

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

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 bifoga 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 enligt punkt 1 och 2 ovan ska vara översatta till svenska, engelska, danska eller norska, om de ursprungligen är upprättade på ett annat språk.

Handlingen enligt punkt 3 ovan ska vara översatt till svenska om originalhandlingen är upprättad på ett annat språk.