

M0161 Mall för redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av Skrivare som tjänst och produkt

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	3
4 Tekniska krav	6
Informationssäkerhetskrav på upphandlingsföremålet	6
5 Tilldelningskriterier	7
Tilldelningskriterier avseende informationssäkerhet	7
6 Särskilda kontraktsvillkor.....	7
Villkor för informationssäkerhet vid fullgörande av ramavtalet.....	7

1 Inledning

Detta dokument redovisar krav och villkor avseende informationssäkerhet som använts i ramavtalsupphandling av Skrivare som tjänst och produkt. 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

Exempel på krav:

6.1.1.3 Datadelningsavtal

Krav kan exempelvis ställas på att Ramavtalsleverantör och Underleverantör ingår datadelningsavtal med Avropsberättigad.

6.1.1.11 Informationssäkerhet

Krav kan exempelvis ställas på krav på identifiering, möjlighet att sätta rättigheter och behörigheter samt loggning. Krav även komma att ställas på olika standarder

6.1.1.23 Personuppgiftsbiträdesavtal

Krav kan exempelvis ställas på att Ramavtalsleverantör och Underleverantör ingår Personuppgiftsbiträdesavtal med Avropsberättigad.

6.1.1.30 Säkerhet

Krav kan exempelvis ställas på fysisk säkerhet, informationssäkerhet och IT-säkerhet. Några exempel är att skrivaren inte tillåter fjärrstyrning, att hårddisken är krypterad eller säkerhetsinstruktioner som Konsult ska följa.

6.1.1.31 Säkerhetsskyddsavtal

Krav kan exempelvis ställas på att Ramavtalsleverantör och Underleverantör ingår Säkerhetsskyddsavtal med Avropsberättigad.

Följande villkor för fullgörande av kontraktet kan preciseras

Se ovan.

3 Kvalificeringskrav

Krav på ramavtalsleverantörens informationssäkerhetsarbete

Informationen hämtad från Upphandlingsdokument Ansökningsinbjudan avsnitt 4.1.6

4.1.6 Systematiskt informationssäkerhetsarbete

A. Process för bedömning av informationssäkerhetsrisker

Ledningssystemet för informationssäkerhet ska innehålla rutiner för fastställande och tillämpning av en process för bedömning av informationssäkerhetsrisker som upprättar och underhåller kriterier för riskacceptans och kriterier för bedömningar av informationssäkerhetsrisker. Processen ska säkerställa att upprepade bedömningar av informationssäkerhetsrisker genererar konsistenta, korrekta och jämförbara resultat.

Processen ska omfatta att informationssäkerhetsriskerna identifieras genom tillämpning av processen för bedömning av informationssäkerhetsrisker för att identifiera risker förknippade med förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystem för informationssäkerhet. Processen ska omfatta att informationssäkerhetsriskerna analyseras genom att bedöma de potentiella konsekvenser som skulle uppstå om riskerna som identifieras realiserar. Vidare ska den realistiska sannolikheten för förekomsten av de risker som identifieras bedömas och risknivåer fastställas. Informationssäkerhetsriskerna ska utvärderas och resultaten av riskanalyser jämföras med de fastställda riskkriterierna. De analyserade riskerna ska prioriteras för riskbehandling. Bedömningar av informationssäkerhetsrisker ska genomföras med planerade intervall eller när betydande förändringar föreslås eller uppstår, med hänsyn till de kriterier som fastställs.

B. Process för behandling av informationssäkerhetsrisker

Ledningssystemet för informationssäkerhet ska innehålla rutiner för fastställande och tillämpning av en process för behandling av informationssäkerhetsrisker för att välja ut lämpliga alternativ för behandling av informationssäkerhetsrisker, med hänsyn tagen till resultaten av riskbedömningen samt fastställande av alla säkerhetsåtgärder som är nödvändiga för att införa valda alternativ för behandling av informationssäkerhetsrisker.

Processen ska omfatta verifikation av att inga nödvändiga säkerhetsåtgärder har utelämnats. Processen ska leda till skapandet av ett uttalande om tillämplighet som innehåller de nödvändiga säkerhetsåtgärderna och motivering för inkludering samt om de är införda eller inte. Processen ska omfatta formulerandet av en plan för behandling av informationssäkerhetsrisker.

C. Process för upprättande och dokumentation av informationssäkerhetsmål

Ledningssystemet för informationssäkerhet ska innehålla rutiner för fastställande och tillämpning av en process för upprättande och dokumentation av informationssäkerhetsmål för relevanta funktioner och nivåer. Informationssäkerhetsmålen ska vara mätbara (om det är praktiskt möjligt), beakta tillämpliga informationssäkerhetskrav och resultat från riskbedömning och riskbehandling, kommuniceras samt uppdateras vid behov.

D. Process för lämpligheten, tillräckligheten och verkan av ledningssystem

Ledningssystemet för informationssäkerhet ska innehålla rutiner för fastställande och tillämpning av en process för att lämpligheten, tillräckligheten och verkan av ledningssystem för informationssäkerhet ständigt förbättras. Processen ska innefatta fastställande av vilka resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra ledningssystem för informationssäkerhet samt säkerställande av att resurserna tillhandahålls.

E. Roller, ansvar och befogenheter

Högsta ledningen ska säkerställa att roller, ansvar och befogenheter är identifierade och kommunicerade inom organisationen.

F. Kompetens och utbildning

Ledningssystemet för informationssäkerhet ska säkerställa att varje person som är anställd inom organisationen och som utför uppgifter som kan orsaka sådan påverkan som organisationen identifierat som betydande, har kompetens grundad på lämplig teoretisk och praktisk utbildning eller erfarenhet. Det gäller personer som i rollen som anställd eller på organisationens uppdrag utför uppgifter åt organisationen.

G. Lagkrav

Ledningssystemet för informationssäkerhet ska säkerställa organisationens åtagande om att följa lagkrav inom området.

H. Genomförande av interna revisioner

Ledningssystemet för informationssäkerhet ska innehålla rutiner för genomförande av interna revisioner med planerade intervall för att få information om huruvida ledningssystem för informationssäkerhet överensstämmer med kraven på ledningssystem för informationssäkerhet samt att ledningssystem för informationssäkerhet har införts och underhållits på ett ändamålsenligt sätt.

Sökande ska inkomma med bevis som styrker att kravet är uppfyllt.

Sökande kan välja att bifoga/fylla i direkt i Tendsign eller på begäran av Kammarkollegiet lämna uppgifterna som kompletterade dokument.

Som bevis för kravet ovan godtas:

- Ett certifikat för ett visst informationssäkerhetssystem
- en egenbeskrivning som är så utförlig att det tydligt framgår att punkterna A-H ovan är uppfyllda.



4 Tekniska krav

Informationssäkerhetskrav på upphandlingsföremålet

Informationen hämtad från Anbudsinbjudan Kravspecifikation kapitel 4.

4.3.5 Programvara för säker utskriftshantering

Anbudsgivaren ska kunna genomföra leveranser av skrivare som är kompatibla med som minst någon av nedan angivna Programvaror för säker utskriftshantering. Avropsberättigad kommer vid Avropsförfrågan kunna ange sitt behov av kompatibilitet enligt nedan angivna Programvaror för utskriftshantering. I det fall en skrivare har kompatibilitet med fler Programvaror för säker utskriftshantering än nedan ska även dessa anges. Dessa Programvaror för säker utskriftshantering kommer sedan att tillföras listan gällande val för Avropsberättigade vid Avrop. I det fall utbyte av skrivare sker enligt avsnitt Ersättning av Upphandlingsföremål, ska listan med Programvara för säker utskriftshantering revideras vid behov. Skrivare som har bredare kompatibilitet kommer därför att kunna motsvara fler typer av behov.

4.4.12 Krypterad hårddisk

Anbudsgivaren ska kunna leverera krypterade hårddiskar i samtlig Hårdvara som inkluderar en hårddisk, i det fall Avropsberättigad i sitt Avrop anger krav om krypterad hårddisk

4.4.14 Automatisk radering av utskriftsjobb

Anbudsgivaren ska kunna leverera skrivare (samt även andra Produkter där kravet är aktuellt) som kan hantera automatisk radering av icke utskrivna jobb. Det ska kunna gå att konfigurera Produkterna så att automatisk radering av utskriftsjobb sker till exempel varje natt.

4.4.15 Korthantering

Anbudsgivaren ska kunna leverera konsulter med kompetens som klarar av att integrera hantering för säker utskrift via kort, så att denna hantering kan rymmas på ett inpasseringskort, tjänstekort eller liknande.

4.4.21 Utskriftsradering

Anbudsgivaren ska kunna leverera skrivare i vilken man kan ta bort utskriftsjobb direkt vid skärmen på skrivaren.

4.4.29 Lagringsmedia

Anbudsgivaren ska vid utrantering eller utbyte av Hårdvara kunna avlägsna och till Avropsberättigad överlämna all lagringsmedia som varit en del av Hårdvara, om



Avropsberättigad begär det i Avropsförfrågan. Kravet gäller oavsett finansieringsform.

5 Tilldelningskriterier

Tilldelningskriterier avseende informationssäkerhet

Inga tilldelningskriterier avseende informationssäkerhet användes vid utvärderingen i ramavtalsupphandlingen.

6 Särskilda kontraktsvillkor

Villkor för informationssäkerhet vid fullgörande av ramavtalet

Inga särskilda kontraktsvillkor avseende informationssäkerhet ställdes i upphandlingen