M0161 Mall för redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av AV och distansmöten

Innehåll

1 Inledning

Detta dokument redovisar krav och villkor avseende informationssäkerhet som använts i ramavtalsupphandling av AV och distansmöten 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 upphandlingsförmålet, 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 upphandlingsförmål 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 villkor för fullgörande av kontraktet kan preciseras

- **7.1.27 Säkerhet**

  Exempelvis fysisk säkerhet, informationssäkerhet, signalskydd och IT-säkerhet.

- **7.1.28 Säkerhetsskyddsavtal**

  Exempelvis att Ramavtalsleverantör och Underleverantör ingår Säkerhetsskyddsavtal med Avropsberättigad.

3 Kvalificeringskrav

Krav på ramavtalsleverantörens informationssäkerhetsarbete

3.6.5 Systematiskt informationssäkerhetsarbete

1

Sökande ska ha ett strukturerat och dokumenterat ledningssystem för informationssäkerhet.

Ledningssystemet för informationssäkerhet ska omfatta samtliga delar av sökandes verksamhet som medverkar i fullgörandet av Ramavtalet.

Kravet uppfylls genom att sökande som kompletterade dokument på begäran inkommer med:

- Giltig certifikat enligt "Certifikat gällande informationssäkerhet" nedan, eller
- En beskrivning som ska vara så utförlig att det tydligt framgår att punkterna A-I är uppfyllda.

Certifikat gällande informationssäkerhet

Certifikat som godkänns är:

- Giltigt certifikat för ISO 27001
- Giltigt certifikat eller diplom från ett likvärdigt informationssäkerhetsledningssystem som uppfyller punkter A-I nedan samt reviderat och diplomerat eller certifierat av en oberoende tredjepart. Den oberoende tredjeparten ska vara godkänd av den organisation som står bakom diplomet eller certifikatet att utföra revisioner samt behörig att utfärda diplomeringar och/eller certifieringar i dennes namn.

För att vara ett godkänt certifikat enligt första punkten ska det vara utställt av ett ackrediterat certifieringsorgan. Exempel på ackrediterat certifieringsorgan som är medlem eller ansluten till någon av de internationella organisationerna för ackrediteringsorgan enligt nedan.

- EA (European co-operation for Accreditation),
- IAF (International Accreditation Forum) eller
- ILAC (International Laboratory Accreditation Cooperation).

Giltighetstid ska framgå av certifikatet eller diplomet. Om giltighetstid inte framgår ska ett signerat intyg bifogas från den oberoende tredjepart som utfärdat certifikatet eller diplomet, där det framgår att det är giltigt.

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 realiseras. 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 bedömning av informationssäkerhetsrisker

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 realiseras. 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 informationssäkerhetskriterierna ska genomföras med planerade intervall eller när betydande förändringar föreslås eller uppstår, med hänsyn till de kriterier som fastställs.

C Process för behandling av informationssäkerhetsrisker

Ledningssystem 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 ingå nödvändiga säkerhetsåtgärder har utlämnats. Processen ska led 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.

D 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 måste var mätbara (om det är praktiskt möjligt), beakta tillämpliga informationssäkerhetskrav och resultat från riskbedömning och riskbehandling, kommuniceras samt uppdateras vid behov.

E 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.

F Roller, ansvar och befogenheter

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

G Kompetens och utbildning

Ledningssystemet för informationssäkerhet ska säkerställas att varje person 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.

H Lagkrav

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

I Interna revisioner

Ledningssystemet för informationssäkerhet ska innehålla rutiner för genomförande av interna revisioner med planerade intervall för att få informations 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.

4 Tekniska krav

Informationssäkerhetskrav på upphandlingsföremålet

3.7.1 Skydd mot obehöriga - molntjänst

Sökande ska skydda information som hanteras och förvaras i lokaler för Publik molntjänst och för Privat molntjänst från obehöriga. Sökande ska ha rutiner för hur sådan information skyddas från obehöriga.

3.7.2 Autentisering - molntjänst

Sökande ska ha en teknisk lösning för Publik molntjänst och för Privat molntjänst som fungerar så att Avropsberättigad skyddas mot obehörig åtkomst genom autentisering.

3.7.3 Tvåfaktorsautentisering

Sökande ska kunna erbjuda tvåfaktorsautentisering för inloggning med högre säkerhet gällande Privat molntjänst.

3.7.4 Krypterad lagringsmedia

Sökande ska kunna erbjuda krypterad lagringsmedia (fast och löstagbar) som lagrar Avropsberättigad information i en Privat molntjänst.

3.7.5 Krypterad datorkommunikation

1

Sökande ska kunna erbjuda att information som överförs via datorkommunikation levererad i Publik molntjänst och Privat molntjänst skyddas med kryptering.

3.7.6 Säkerhetskopiering

Sökande ska kunna leverera Publik molntjänst och Privat molntjänst som lagrar Avropsberättigads information och som ska ha funktioner för att regelbundet överföra Avropsberättigads information till säkerhetskopior.

Sökande ska kunna återläsa Avropsberättigads information på begäran av Avropsberättigad eller vid behov enligt överenskommelse med Avropsberättigad.

3.7.7 Destruktion

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.

3.7.8 Loggning

Sökande ska ha en funktion för loggning av förändringar utförda av administratör i Publik molntjänst eller Privat molntjänst.

5 Tilldelningskriterier

Tilldelningskriterier avseende informationssäkerhet

3.9.5 Begränsningskriterium Konsultkompetens informationssäkerhet

Sökande bör förfoga över minst 2 konsulter som minst uppfyller kraven enligt nedan. Sökande kan ange maximalt 2 konsulter nedan.

Informationssäkerhetskompetensen ska vara hänförlig till kompetens inom området för ljud och bild.

För att erhålla mervärde ska angiven Konsult ha:

- kompetensnivå 4
- kompetens om hur riskanalyser genomförs
- kompetens gällande produkters möjlighet till skydd för information
- kompetens gällande intrångsskydd
- kompetens om skydd mot skadlig kod
- kompetens om hur rättigheter och behörighet hanteras
- kompetens om loggning av händelser
- kompetens att kunna ge råd gällande informationssäkerhetslösningar

Sökande kan välja att lämna in dessa uppgifter som kompletterade dokument eller att ange uppgifter som efterfrågas nedan.

6 Särskilda kontraktsvillkor

Inga utöver de som finns i mallarna.