**Bilag 2**

**Løsningsbeskrivelse**

# Kravtabell

Formatet på kravtabellene er som følger:

| Kundens krav | | | Leverandørens svar | |
| --- | --- | --- | --- | --- |
| Nr. | Krav-type | Beskrivelse | Oppfylles (Ja/Nei/  Delvis) | Dokumentasjonskrav |
|  |  |  |  |  |

Nr.: Kravets løpenummer

Kravtype: Se tabell nedenfor.

Beskrivelse: Tekst som beskriver kravet.

Oppfylles: I hvilken grad Leverandøren kan tilfredsstille kravet (Ja, Nei, Delvis). For krav som besvares med Delvis, må det særskilt utdypes hva som ikke kan tilfredsstilles.

Dokumentasjonskrav: Beskriver hvordan Kunden mener kravet skal svares ut.

Kravtype:

|  |  |
| --- | --- |
| **Absolutte krav (A)** | Kravet er viktig og MÅ tilfredsstilles. Kravet er å anse som et minimumskrav og kan ikke oppfylles «delvis». |
| **Absolutte krav (A)\*** | Kravet er viktig og MÅ tilfredsstilles. Kravet er å anse som et minimumskrav som ikke kan oppfylles «delvis», men overoppfyllelse vil blir gjenstand for relativ vurdering. |
| **Ønskede krav (B)** | Kravet BØR tilfredsstilles, men det er ikke et absolutt krav. Svar vil likevel ha betydning for evaluering av tilbudet og kravet kan oppfylles «delvis». |

## Krav til leverandørens leveringsevne, kompetanseutvikling og merkantile rutiner

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Krav-type** | **Beskrivelse** | **Oppfylles**  **Ja/Nei/**  **Delvis** | **Dokumentasjonskrav** |
| 1 | A | **Kontinuitet i tjenesteleveranser til Stortinget**  Det er viktig for Stortinget at konsulentene som tilbys på avtalen har kompetanse om og kjennskap til Stortingets løsninger på IT- og informasjonssikkerhetsområdet.  Tilbyder skal derfor sørge for at leveransene på rammeavtalen har høy grad av kontinuitet. |  | Leverandør skal gi en kortfattet beskrivelse av hvordan de vil sørge for at bistanden fortrinnsvis leveres av faste konsulenter og at det er kontinuitet i leveransen når det kommer avropsforespørsel fra Kunden. |
| 2 | A | **Utvikle konsulentens kompetanse**  Området IT- og informasjons­sikkerhet er i stadig endring. Kunden ønsker å sikre seg at konsulentens kompetanse forvaltes og videreutvikles i henhold til markedets og Stortingets behov. |  | Leverandør skal gi en utfyllende beskrivelse av hvordan kompetanse videreutvikles i organisasjonen for å svare til markedets og Stortingets behov for øvrig.  Dersom Leverandør har et opplegg for å sertifisere konsulentene, ber vi om at dette beskrives her. |
| 3 | A | **Merkantil oppfølging**  Ha en godt utprøvd arbeidsmetodikk rundt merkantil etterlevelse av avtalen som skaper forutsigbarhet og gjennomførings-trygghet for kunden. Viktige punkter her er:   * Opprettelse og oppfølging av tildelingsavtaler for å sikre at alle konsulenter som er engasjerte av Kunden er på gyldige og signerte avrop * Kvalitetssikring av fakturaer og oppfølging av eventuelle avviste fakturaer * Sikre korrekt prisjustering på rammeavtalen overfor Kunden |  | Leverandøren skal beskrive hvordan leverandøren oppfyller sine forpliktelser knyttet til oppfølging av avrop, fakturering og prisjusteringer. |

## Krav til erfaring og faglig kompetanse hos konsulentene

Det er en forventning om at Leverandøren kan levere tilstrekkelig med kompetanse innen informasjonssikkerhet som er relevant for Kunden. De generelle kravene gjelder for alle innleide konsulenter og regnes som «grunnmuren» i erfaring og faglig kompetanse.

Konsulentens roller er i denne kravtabellen delt opp i to områder. De er definert som rolle nummer 1- **«strategisk IT- informasjonssikkerhet»** og rolle nummer 2 – **«operativ IT- informasjonssikkerhet»**.

Kravene som stilles for å fylle rolle nummer 1 og 2 er summen av de generelle kravene påplusset de særegne kravene til henholdsvis rolle 1 og rolle 2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Krav-type** | **Beskrivelse** | **Oppfylles**  **Ja/Nei/**  **Delvis** | **Dokumentasjonskrav** |
| 4 | A | **Generelle krav** til konsulentene i rollene nedenfor som skal oppfylles   * Relevant utdannelse fra høgskole eller universitet. God relevant erfaring kan i enkelte tilfeller kompensere for manglende utdannelse. * Må kunne sikkerhetsklareres til for HEMMELIG etter sikkerhetsloven * Gode norskkunnskaper (både skriftlig og muntlig) * Minimum fem års erfaring innenfor området informasjonssikkerhet * Minimum tre års erfaring med ISO/IEC 27001-standarden for informasjonssikkerhet |  | Bekreftes |
| 5  5A  5B | A\* | **Rolle 1 -** **«strategisk informasjonssikkerhet»**  Leverandør må tilby tre konsulenter innenfor rolle 1 (det er mulig å tilby samme konsulent innen begge kategorier).  **Absolutte krav til konsulentenes kompetanse/erfaring:**   * Konsulentene skal ha erfaring fra utarbeidelse av risiko- og sårbarhetsanalyser vedrørende komplekse IT-systemer og IT infrastruktur * Konsulentene skal ha erfaring fra utforming og oppfølging av styringssystem for informasjonssikkerhet (ISMS), herunder utforming a relevante dokumenter knyttet til dette * Konsulenten skal ha erfaring med å gjøre verdivurderinger av IT-løsninger/tjenester * Konsulenten skal ha relevant erfaring fra arbeid med IT-sikkerhetsrevisjon * Konsulenten skal være godt kjent med NSM’s grunnprinsipper for IKT-sikkerhet   **Ønskelig kompetanse/erfaring:**     * Konsulentene bør ha erfaring fra rådgivning innen beste praksis for overvåking og rapportering vedrørende sikkerhetsbrudd og hendelser * Konsulentene bør ha erfaring med organisering av sikkerhetsarbeid, herunder kontinuitets og beredskapsplanlegging * Konsulenten bør ha erfaring fra deltakelse i IRT * Konsulenten bør ha erfaring med personvern (GDPR) fra et IT-sikkerhetsperspektiv |  | Leverandør skal oppgi tre navngitte konsulenter som oppfyller de absolutte kravene slik de er stilt opp i krav 5 A) og som best mulig oppfyller kravene i krav 5 B).  Navnene skal suppleres med CV på de tilbudte konsulentene + beskrivelse av tre-fem nærmere beskrevne referanseoppdrag (**NB**: Bruk vedlagt mal, vedlegg 1, for å dokumentere de tre-fem referanseoppdragene) |
| 6  6A  6B | A\* | **Rolle 2 - «operativ informasjonssikkerhet»**.  Leverandør må tilby tre konsulenter innenfor rolle 2 (det er mulig å tilby samme konsulent innen begge kategorier).      **Absolutte krav til konsulentenes kompetanse/erfaring:**   * Konsulentene skal ha operativ erfaring med gjennomføring av sikkerhetsgjennomganger/revisjoner, sikkerhetstester, og penetrasjonstester * Konsulentene skal ha operativ erfaring med gjennomføring av tiltak etter sikkerhetsgjennomganger/revisjoner, sikkerhetstester, og penetrasjonstester * Konsulenten skal ha god forståelse for IT-infrastruktur og sammenhengen med IT-sikkerhetsarkitektur   **Ønskelig kompetanse/erfaring:**     * Konsulentene bør ha erfaring med standarder for identitet og tilgangskontroll * Konsulentene bør ha erfaring med Public Key Infrastructure for utstedelse, administrasjon og bruk av digitale sertifikater * Konsulentene bør ha erfaring med standarder for sikker koding/programmering med fokus på hvordan utvikle sikrere programmer * Konsulentene bør ha erfaring med Sans 20 Critical Controls for Cyber Defence og NSMs grunnprinsipper for IKT sikkerhet * Konsulentene bør ha erfaring fra deltakelse i IRT |  | Leverandør skal oppgi tre navngitte konsulenter som oppfyller de absolutte kravene slik de er stilt opp i krav 6 A) og som best mulig oppfyller kravene i krav 6 B).  Navene skal suppleres med CV på de tilbudte konsulentene + beskrivelse av tre-fem nærmere beskrevne referanseoppdrag (**NB**: Bruk vedlagt mal, vedlegg 1, for å dokumentere de tre-fem referanseoppdragene) |