Geschiktheidseisen

(Zoals bedoeld in artikel 2.90 t/m 2.98 Aanbestedingswet en deel IV Uniform Europees Aanbestedingsdocument)

Onderstaande worden de volgende geschiktheidseisen behandeld:

A. Financiële en economische draagkracht;
B. Technische bekwaamheid en beroepsbekwaamheid - Referenties;
C. Technische bekwaamheid en beroepsbekwaamheid - Certificering.

A. Financiële en economische draagkracht

De gegadigde dient bij aanmelding aan onderstaande eisen met betrekking tot financiële en economische draagkracht te voldoen. Gegadigde verklaart door ondertekening van het UEA formulier over onderstaande bewijstukken te beschikken. Gegadigde toont zijn financiële en economische draagkracht aan door middel van de volgende onderstaande bewijsstukken:

Bedrijfsaansprakelijkheidsverzekering

Een kopie verzekeringspolis of verzekeringscertificaat met betrekking tot de bedrijfsaansprakelijkheid (bewijs van verzekering tegen bedrijfsrisico's), die op het tijdstip van indiening niet ouder is dan één jaar, waaruit de hoogte van het te verzekeren bedrag blijkt met een minimum van € 5.000.000,- per aanspraak.

Gegadigde dient dit bewijsstuk binnen zeven kalenderdagen aan te leveren, op eerste aangeven van de aanbestedende dienst.

De Gegadigde aan wie is gegund, verplicht zich contractueel om de verzekering, die voldoet aan de vereisten, onder dezelfde voorwaarden en met minimaal de verzekerde bedragen te handhaven, gedurende de gehele contractperiode.

B. Technische bekwaamheid en beroepsbekwaamheid - Referenties

Referentieprojecten en kerncompetenties

Gegadigde moet de volgende drie (3) kerncompetenties hebben ingezet bij organisaties van vergelijkbare omvang en complexiteit (aan Aanbestedende dienst). Deze vergelijkbare omvang en complexiteit is voor de gevraagde dienstverlening gedefinieerd als:

- Waarbij de ICT-dienstverlening werd geleverd door minimaal vijf (5) ketenpartners (inclusief de ICT-afdeling van Aanbestedende dienst), waaronder één hostingpartij.
- Voor minimaal eenentwintighonderd (2.100) werkplekken, waarop de ICT-ketenpartners zowel on site (locaties waar de deelnemende gemeenten kantoor houden) als off site (meestal maar niet slechts 'thuiswerkplekken').
- Met een modulaire opbouw van de dienstverlening, waarbij in het bijzonder wordt bedoeld dat deelnemende gemeenten in voorkomende gevallen kunnen besluiten de gevraagde dienstverlening niet af te nemen.

Kerncompetentie 1: Geavanceerde Managed Detection and Response (MDR) dienstverlening

Gegadigde dient aantoonbare ervaring en expertise te hebben in het leveren van geavanceerde Managed Detection and Response (MDR) diensten, inclusief:

1. Proactieve monitoring en detectie van cyberbeveiligingsbedreigingen met behulp van geavanceerde technologieën zoals machine learning en gedragsanalyse.
2. Snelle en effectieve respons op geïdentificeerde beveiligingsincidenten, inclusief het uitvoeren van zowel geautomatiseerde als handmatige maatregelen om dreigingen te neutraliseren en eventuele schade te beperken. Het vermogen om geautomatiseerde responsmechanismen te implementeren is cruciaal om snel opkomende cyberaanvallen te bestrijden en de impact op de bedrijfscontinuïteit te minimaliseren.
3. Voortdurende verbetering van het beveiligingsniveau door middel van inzichten uit incidentanalyses en de implementatie van preventieve maatregelen om toekomstige aanvallen te voorkomen.
4. Aantoonbaar vermogen om samen te werken met interne en externe belanghebbenden, zoals IT-afdelingen, ketenpartners (andere dienstverleners in de ICT-leveringsketen), juridische teams en wetshandhavingsinstanties, om een gecoördineerde respons op cyberbeveiligingsincidenten te waarborgen.

Minimumvereisten:

Gegadigde dient één (1) referentie te verstrekken om de bovengenoemde ervaring en expertise te onderbouwen. Deze moeten de volgende informatie bevatten:

1. Een beschrijving van de uitgevoerde MDR-projecten, met inbegrip van de aard en de omvang van de opdracht, de technologieën en methodieken die zijn gebruikt, en de behaalde resultaten.
2. Een overzicht van de geleverde diensten, met een nadruk op de aanpak van proactieve monitoring, detectie, respons en continue verbetering in de context van cyberbeveiliging.
3. Een toelichting op de wijze waarop de Gegadigde heeft samengewerkt met andere belanghebbenden, zoals eerder genoemd, om een gecoördineerde en effectieve respons op cyberbeveiligingsincidenten te waarborgen.
4. Een uiteenzetting van de uitdagingen die de Gegadigde heeft ondervonden bij het uitvoeren van de MDR-diensten, en de strategieën die zijn toegepast om deze uitdagingen te overwinnen en succesvolle resultaten te bereiken.
5. Een voorbeeldrapportage waarmee gegadigde periodiek rapporteert over de dienstverlening.

Kerncompetentie 2: Auditing van ketenpartners op naleving van beveiligingsmaatregelen en patchbeheer

Gegadigde dient aantoonbare ervaring en expertise te hebben in het uitvoeren van audits bij ketenpartners, met name op het gebied van het implementeren van beveiligingspatches en andere door het NCSC en andere relevante instanties aanbevolen beveiligingsmaatregelen. Deze competentie omvat:

1. Het ontwikkelen en uitvoeren van auditplannen om de naleving van beveiligingsvoorschriften en best practices bij ketenpartners te beoordelen, met een focus op tijdige en effectieve implementatie van beveiligingspatches en -maatregelen.
2. Het toepassen van erkende auditmethodieken en -standaarden, zoals ISO 27001, NIST of andere relevante raamwerken, om een systematische en consistente beoordeling van de beveiligingspraktijken van ketenpartners te waarborgen.
3. Het identificeren en rapporteren van tekortkomingen en risico's in het beveiligingsbeheer van ketenpartners, inclusief aanbevelingen voor verbetering en het monitoren van de voortgang van de implementatie van verbetermaatregelen.
4. Effectieve communicatie en samenwerking met ketenpartners om bewustwording en naleving van beveiligingsnormen te bevorderen en een cultuur van continue verbetering op het gebied van cyberbeveiliging te ondersteunen.

5. Aantoonbaar vermogen om complexe en diverse ICT-leveringsketens te beoordelen en te beheren, met inbegrip van het vermogen om effectieve beveiligingsmaatregelen te implementeren in overeenstemming met de specifieke eisen en risico's van de betrokken organisaties.

Minimumvereisten:

Gegadigde dient één (1) referentie te verstrekken om de bovengenoemde ervaring en expertise te onderbouwen. Deze moeten de volgende informatie bevatten:

1. Een beschrijving van de uitgevoerde auditprojecten bij ketenpartners, met inbegrip van de aard en omvang van de opdracht, de toegepaste auditmethodieken en -standaarden, en de behaalde resultaten.
2. Een overzicht van de geïdentificeerde tekortkomingen en risico's in het beveiligingsbeheer van ketenpartners, evenals de aanbevolen en geïmplementeerde verbetermaatregelen.
3. Een toelichting op de wijze waarop de Gegadigde effectief heeft gecommuniceerd en samengewerkt met ketenpartners om naleving van beveiligingsnormen te bevorderen en een cultuur van continue verbetering op het gebied van cyberbeveiliging te ondersteunen.
4. Een uiteenzetting van de uitdagingen die de Gegadigde heeft ondervonden bij het uitvoeren van de audits bij ketenpartners en de strategieën die zijn toegepast om deze uitdagingen te overwinnen en succesvolle resultaten te bereiken.

Kerncompetentie 3: Uitvoeren van digitaal forensisch onderzoek bij bepaalde security incidenten

Gegadigde dient aantoonbare ervaring en expertise te hebben in het uitvoeren van digitaal forensisch onderzoek naar aanleiding van security incidenten. Deze competentie omvat:

1. Het uitvoeren van grondige, systematische en nauwkeurige analyses van security incidenten om de oorzaak, omvang en impact van de inbreuk vast te stellen, met behulp van geavanceerde forensische technieken en tools.
2. Het identificeren en veiligstellen van digitaal bewijsmateriaal in overeenstemming met de wettelijke vereisten en best practices, om de integriteit en bruikbaarheid van het bewijsmateriaal in eventuele juridische procedures te waarborgen.
3. Het analyseren en reconstrueren van de chronologie van security incidenten om de aanvalsvector, betrokkenheid van kwaadwillenden en eventuele verdere bedreigingen voor de organisatie te bepalen.

4. Het opstellen van gedetailleerde forensische rapporten en het presenteren van bevindingen aan relevante belanghebbenden, zoals het management, juridische teams en wetshandhavingsinstanties, op een duidelijke en begrijpelijke wijze.
5. Samenwerking met interne en externe partijen, zoals IT-afdelingen, beveiligingsteams en ketenpartners, om een gecoördineerde aanpak van het onderzoek en de respons op security incidenten te waarborgen en om herstel- en verbetermaatregelen effectief te implementeren.

Minimumvereisten:

Gegadigde dient één referentie te verstrekken om de bovengenoemde ervaring en expertise te onderbouwen. Deze moeten de volgende informatie bevatten:

1. Een beschrijving van de uitgevoerde digitaal forensisch onderzoekprojecten, met inbegrip van de aard en omvang van het onderzoek, de technieken en tools die zijn gebruikt, en de behaalde resultaten.
2. Een overzicht van de geïdentificeerde oorzaken, omvang en impact van de onderzochte security incidenten, evenals de geïmplementeerde herstel- en verbetermaatregelen.
3. Een toelichting op de wijze waarop de Gegadigde effectief heeft gecommuniceerd en samengewerkt met relevante belanghebbenden om een gecoördineerde aanpak van het onderzoek en de respons op security incidenten te waarborgen.
4. Een uiteenzetting van de uitdagingen die de Gegadigde heeft ondervonden bij het uitvoeren van het digitaal forensisch onderzoek en de strategieën die zijn toegepast om deze uitdagingen te overwinnen en succesvolle resultaten te bereiken.

Nadere bijzonderheden:

U dient per referentieopdracht de contactgegevens (zakelijke NAW-gegevens, telefoonnummer en e-mailadres) van de referent te vermelden;

Per kerncompetentie mag maximaal één referentie worden ingediend; een referentie mag wel ter aantoning van meerdere kerncompetenties worden ingezet.

De beschrijving van een referentieopdracht mag maximaal 700 woorden omvatten (i.e. 2 A4). Indien de beschrijving van een referentieopdracht twee kerncompetenties betreft, mag deze maximaal 1.400 woorden (i.e. 4 A4) omvatten, etc.;

De betreffende referentieopdrachten dienen maximaal 3 jaar oud te zijn, gerekend vanaf de in dit document vermelde geplande ingangsdatum van het contract, en, binnen deze periode, voor minimaal één (1) jaar door Gegadigde te zijn geleverd.

De opgegeven referentieprojecten dienen tot tevredenheid van de betreffende referent vakkundig als zelfstandig, verantwoordelijk en coördinerend hoofdaannemer uitgevoerd te zijn.

Aanbesteder heeft het recht om de door Gegadigde gedane opgave met betrekking tot de opgegeven referentie inhoudelijk te (laten) controleren door rechtstreeks aan de referent (inzage in) extra informatie te vragen. Daarnaast behoudt Aanbestedende dienst zich het recht voor om rechtstreeks met de referentie in contract te treden en een referentiebezoek te doen en/of (een) verificatiegesprek(ken) te voeren.

C. Technische bekwaamheid en beroepsbekwaamheid - certificering

Kwaliteitsborging ISO-9001 of gelijkwaardig

Gegadigde dient gecertificeerd te zijn volgens ISO-9001 of gelijkwaardig. Deze gelijkwaardigheid dient te worden aangetoond. Indien Gegadigde niet beschikt over een certificaat en zich ook niet in een certificeringtraject bevindt, kan worden volstaan met het overleggen van een eigen kwaliteitshandboek dat gelijkwaardig is aan een ISO 9001. Dit kwaliteitshandboek dient actueel en geldig te zijn, waarin zijn opgenomen de maatregelen die de organisatie treft om de kwaliteit te waarborgen en te controleren. Dit kwaliteitshandboek dient vergezeld te gaan van een bereidheidsverklaring van het management waaruit blijkt dat het management deze maatregelen onderschrijft en actief controleert. Gegadigde verklaart door ondertekening van het UEA formulier dat hij voldoet aan deze eis en beschikt over het gevraagde certificaat of gelijkwaardig. Gegadigde dient dit bewijsstuk binnen zeven kalenderdagen aan te leveren, op eerste aangeven van Gemeente Leiden.

NEN-ISO 27001

Een afschrift van een geldig NEN-ISO 27001 certificaat met bijbehorende Verklaring van Toepasselijkheid (VvT) of vergelijkbaar.

OSCP-certificaten of gelijkwaardig

Een manier om nader onderzoek te doen naar gedetecteerde IT-security incidenten is met ethical hackers. Gegadigde overlegt afschriften van OCSP-certificaten, of gelijkwaardig, van minimaal 3 ethical hackers die hij in dienst heeft.

Afschrift First of gelijkwaardig

Voor Incident Response/CERT overlegt Gegadigde een afschrift van First (Forum of Incident Response and Security Teams), Trusted Introducer (TI), Carnegie Mellon certificaat, of gelijkwaardig.

Beroepsbevoegdheid - Inschrijving in nationale beroep- of handelsregister

Gegadigde verklaart dat de onderneming is ingeschreven in het nationale beroep- of handelsregister van het land van herkomst volgens de eisen van het land waar de Gegadigde gevestigd is.

Gegadigde dient dit bewijsstuk binnen zeven kalenderdagen aan te leveren, op eerste aangeven van de aanbestedende dienst.