



^[1] **Selectieleidraad Dienst Informatiebeveiliging**

AICT-2022-0037

[2] Voorwoord

Deze Selectieleidraad hoort bij de mededingingsprocedure met onderhandeling, als bedoeld in artikel 2.30 e.v. van de Aanbestedingswet, voor een Dienst Informatiebeveiliging bestaande uit twee percelen:

- het ter beschikking stellen, configureren, beheren en (door)ontwikkelen van een centraal Netwerkknooppunt (P1), en
- het ter beschikking stellen, beheren en (door)ontwikkelen van Generieke security diensten (P2).

De gemeente Amsterdam is voornemens om per perceel een Overeenkomst te gunnen aan één Inschrijver. U kunt zich op basis van deze Selectieleidraad aanmelden als Gegadigde. U dient daartoe een Verzoek tot Deelname in te dienen.

De uiterste datum en tijd voor het inleveren van een Verzoek tot Deelname is 30 november 2022.

In deze Selectieleidraad treft u alle informatie en instructies aan om een Verzoek tot Deelname voor te bereiden en in te dienen.

Wij wensen u veel succes met de uitwerking.

[3] Inhoud

[4]

1 Begrippen	5
2 De Opdracht	8
2.1 Leeswijzer	8
2.2 Doelstelling	8
2.3 De Opdrachtgever	9
2.4 De Opdrachtnemers	9
2.5 Marktconsultatie	9
2.6 Beoordelingsteam	10
2.7 Varianten	10
2.8 Beschrijving van de Dienst Informatiebeveiliging	10
2.8.1 Aanleiding en achtergrond	10
2.8.2 Algemene kengetallen	11
2.8.3 Scope Netwerkknooppunt (P1)	11
2.8.4 Scope Generieke security diensten (P2)	14
2.9 Vorm, duur en waarde van de Overeenkomsten	20
2.10 Randvoorwaarden voor gunning van de percelen betreffende leverancier	21
2.11 Planning op hoofdlijnen	22
3 Voorschriften bij de aanbesteding	24
3.1 Algemene voorschriften	24
3.2 Aanbestedingsprocedure en procesgang	24
3.3 Voorwaarden	24
3.4 Keuze aanbestedingsprocedure	25
3.5 Elektronische communicatie via TenderNed	25
3.6 Communicatie met betrekking tot deze aanbesteding	26
3.7 Voorbehoud	26
3.8 Vragenronde	26
3.9 Onvolkomenheden, procedurefouten, onduidelijkheden en (tegen)strijdigheden	27
3.10 Volledigheid en indeling aanmelding	27
3.11 Intellectueel eigendom, geheimhouding, publiciteit en taal	28
3.12 Sluitingsdatum voor aanmeldingen	29
3.13 Voorschriften betreffende de wijze van indiening van de Verzoeken tot Deelname	29
3.14 Beoordeling van de aanmeldingen	30
3.15 Herstel van fouten en omissies, verduidelijking	30
3.16 Klachtenregeling	30
3.17 Geschillen	31
3.17.1 Nederlands recht	31
3.17.2 Rechtsbescherming en opschortende termijn	31
3.18 Verzoek tot Deelname door een combinatie	32

3.19 Aanmelden met beroep op derden.....	32
3.20 Onderaannemers.....	32
3.21 Concurrentie bevorderende maatregelen.....	33
3.22 Belangenverstrengeling.....	33
3.23 Sanctiepakket Rusland.....	33
4 Selectieprocedure	35
4.1 Beoordeling van de aanmelding.....	35
4.2 Selecteren Gegadigden	35
4.3 Bekend maken resultaat beoordeling	35
4.4 Opvragen bewijsmiddelen.....	36
5 Eisen ten aanzien van Gegadigde	36
5.1 Uitsluitingsgronden	36
5.1.1 Bewijsmiddelen.....	37
5.2 Geschiktheidseisen.....	37
5.2.1 Financieel economische draagkracht	37
5.2.2 Verzekering	38
5.2.3 Technische bekwaamheid.....	38
5.2.4 Kerncompetenties voor het Netwerkknooppunt.....	39
5.2.5 Kerncompetenties voor Generieke security diensten	40
5.3 Verificatie bewijsstukken	41
6 Selectiecriteria	42
6.1 Algemeen	42
6.2 Selectiecriteria voor het Netwerkknooppunt (P1)	42
6.3 Selectiecriteria voor Generieke security diensten (P2)	45
6.4 Ranking en selectiebesluit	48
6.5 Het gunningscriterium van de aanbesteding.....	48
6.5.1 Kwaliteit	49
6.5.2 Globale uitwerking kwaliteitscriteria	49
7 Bijlagen	51
7.1 Gemeentelijke Inkoopvoorwaarden bij IT 2020 [GIBIT 2020] van de VNG	51
7.2 Amsterdamse bepalingen bij de Algemene Inkoopvoorwaarden	51
7.3 Referentiesjabloon Netwerkknooppunt (P1)	51
7.4 Referentiesjabloon Generieke security diensten (P2)	51

1 Begrippen

Algemene Inkoopvoorwaarden Amsterdamse bepalingen	Gemeentelijke Inkoopvoorwaarden bij IT 2020 [GIBIT 2020] van de VNG (Bijlage 7.1). De Amsterdamse bepalingen bij de Algemene Inkoopvoorwaarden (Bijlage 7.2)
APT	Advanced Persistent Threat
Aw	Aanbestedingswet 2012, wet van 1 november 2012, houdende regels omtrent aanbestedingen. Deze wet is op 8 november 2012 gepubliceerd in het Staatsblad nummer 542 en per 1 juli 2016 gewijzigd in verband met implementatie van de aanbestedingsrichtlijnen 2014/23/EU, 2014/24/EU en 2014/25/EU.
Beschrijvend Document	Het document dat de behoeftestelling van de Gemeente verwoordt en naar de geselecteerde Gegadigden (de Inschrijvers) wordt gezonden voor het maken en indienen van een Inschrijving.
Bijlage(n)	Document(en) dat (die) in en/of bij de Selectieleidraad is (zijn) gevoegd. Deze Bijlagen vormen een onlosmakelijk onderdeel van de Selectieleidraad.
CCC	Cloud Competence Center
CSIRT	Computer Security Emergency Response Team
Gegadigde	Iedere onderneming, samenwerkingsvorm (combinatie), of hoofdopdrachtnemer in samenwerking met onderaannemers die een Verzoek tot Deelname indient of voornemens is een Verzoek tot Deelname in te dienen om in aanmerking te komen voor deelname aan de gunningsfase van deze Europese aanbesteding.
Gemeente	Gemeente Amsterdam
Generieke security diensten	De generieke security diensten zoals beschreven in paragraaf 2.8.4.
Gunningscriterium	Het gunningscriterium in deze aanbestedingsprocedure is de 'economisch meest voordelige inschrijving' (EMVI, zie artikel 2.114 Aw) op basis van de beste prijs-kwaliteitverhouding en wordt in het Beschrijvend Document nader uitgewerkt.
HenT (Infrastructurele) dienst	Hosting en Technische applicatiebeheer Een van de (Infrastructurele) diensten zoals beschreven par. 2.8.1 van deze Selectieleidraad, maar ook SaaS diensten en toekomstige diensten in het kader van ontwikkelingen zoals IoT, robotisering, etc.
Inschrijver	De Gegadigde die met toepassing van de selectieprocedure, zoals beschreven in deze Selectieleidraad, door de Gemeente is

	geselecteerd voor deelname aan de gunningsfase. De geselecteerde Gegadigden (Inschrijvers) ontvangen daartoe van de Gemeente het Beschrijvend Document.
Inschrijving	De bindende aanbieding die Inschrijvers op basis van het Beschrijvend Document indienen.
KPI	Key Performance Indicator
Minimumvereisten	De minimale vereisten waaraan een Gegadigde dient te voldoen om in aanmerking te komen voor deelname aan de gunningsfase van deze aanbestedingsprocedure.
MISP	Malware Information Sharing Platform
Mitre Att&ck	Kennis framework voor het vastleggen van tactieken en technieken die door actoren gebruikt worden.
NCSC	Nationaal Cyber Security Centrum
Netwerkknooppunt	Het netwerkknooppunt zoals beschreven in paragraaf 2.8.3.
NDN	Nationaal Detectie Netwerk
Nota van Inlichtingen	Document waarin de geanonimiseerde vragen en antwoorden op vragen van Gegadigden zijn opgenomen, evenals eventuele wijzigingen van de Selectieleidraad en/of Bijlagen. De Nota van Inlichtingen maakt integraal en bindend onderdeel uit van de Selectieleidraad en prevaleert boven de bepalingen van de Selectieleidraad. Indien er meer versies van de Nota van Inlichtingen worden gepubliceerd, dan prevaleert in geval van tegenstrijdigheid tussen de versies het bepaalde in de meest recente versie.
Opdracht	De opdracht tot het verzorgen van een Netwerkknooppunt (Perceel 1) en Generieke security diensten (Perceel 2) ten behoeve van de Gemeente, zoals aangekondigd op TenderNed met referentienummer AICT 2022-0037 en nader omschreven in hoofdstuk 2 van deze Selectieleidraad.
Opdrachtnemer	De Inschrijver aan wie de Gemeente de Opdracht gunt.
Overeenkomst	De overeenkomst die tussen Opdrachtnemer en Opdrachtgever zal worden gesloten en waarop de Algemene Inkoopvoorwaarden en de Amsterdamse bepalingen van toepassing zullen zijn.
Selectiecriteria	Criteria die, indien nodig, na de toetsing van het Verzoek tot Deelname aan de Uitsluitingsgronden en Minimumvereisten worden gebruikt om het aantal geselecteerde Gegadigden/ Inschrijvers te beperken tot vijf.
Selectieleidraad	Dit document met Bijlagen, met daarin een beschrijving van en toelichting op de organisatie van de Gemeente, de scope van de Opdracht, de te volgen procedure, de Uitsluitingsgronden, de Minimumvereisten en de van toepassing zijnde Selectiecriteria.
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center

Uitsluitingsgronden	De gronden van uitsluiting zoals genoemd in de artikelen 2.86 en 2.87 Aw.
Uniform Europees Aanbestedingsdocument	Het formulier 'Uniform Europees Aanbestedingsdocument' als bedoeld in artikel 2.84 Aw waarin Gegadigde zonder voorbehoud verklaart dat geen van de door de Gemeente aangeduide Uitsluitingsgronden van toepassing zijn op Gegadigde en dat zij voldoet aan bepaalde door de Gemeente aangeduide geschiktheidseisen.
Verzoek tot Deelname	Het document waarin een Gegadigde te kennen geeft deel te willen nemen aan deze Europese aanbesteding, vergezeld van alle documenten die Gegadigde aanbiedt ter beantwoording van het gestelde in deze Selectieleidraad.

2 De Opdracht

Voor u ligt de Selectieleidraad ter zake van de Europese aanbesteding Dienst Informatiebeveiliging ten behoeve van de gemeente Amsterdam. Opdrachtgever is de directeur Digitale Voorzieningen.

Bij de Europese aanbesteding treden als procesbegeleiders op:
de heer P. Pirson (Lead Buyer ICT) en mevrouw Z. Yilmaz (Lead Buyer ICT).

In deze selectiefase dient alle communicatie te verlopen via de berichtenbox van TenderNed.

2.1 Leeswijzer

In deze Selectieleidraad wordt achtereenvolgens ingegaan op het onderwerp van de aanbesteding en de te volgen procedure. In hoofdstuk 2 wordt de Opdracht op hoofdlijnen beschreven. Hoofdstuk 3 geeft de algemene voorschriften weer. Hoofdstuk 4 bevat de selectieprocedure en hoofdstuk 5 verwoordt de Minimumvereisten zoals die voor Gegadigden worden gehanteerd. Hoofdstuk 6 beschrijft de Selectiecriteria en in hoofdstuk 7 wordt ten slotte een opsomming gegeven van de Bijlagen. Deze Bijlagen zijn in separaat bijgevoegd.

2.2 Doelstelling

De Opdracht Dienst Informatiebeveiliging bestaat uit 2 percelen:

- het ter beschikking stellen, configureren, beheren en (door)ontwikkelen van een Netwerkknooppunt (P1), en
- het ter beschikking stellen, beheren en (door)ontwikkelen van Generieke security diensten (P2).

Na afronden van de aanbesteding heeft de Gemeente:

- 1) voor beide percelen een (strategisch) partner die in staat is om de gevraagde dienstverlening te leveren, inclusief het continu blijven van de beveiligingsmaatregelen aan het wijzigende dreigingsbeeld en het wijzigende ICT-landschap van de Gemeente en inclusief het beheer en onderhoud van de onderliggende oplossingen en tooling, zodanig dat de dienstverlening voldoet en blijft voldoen aan nationale en Amsterdamse beveiligingsrichtlijnen, de ICT-visie van de Directie Digitale Voorzieningen en haar ambitie, doelstellingen, uitgangspunten en randvoorwaarden
- 2) een succesvol uitgevoerde transitie van de huidige Dienst ADP naar de nieuw te contracteren Dienst Informatiebeveiliging;
- 3) de beschikking over operationeel en kwalitatief goede dienstverlening tegen beheersbare en overzichtelijke kosten.

- 4) voor beide percelen een rechtmatig contract voor de duur van 5 jaar met optionele verlenging van 2 x 2 jaar.

2.3 De opdrachtgever

Amsterdam is een grootstedelijke gemeente in de Nederlandse provincie Noord-Holland. De Gemeente telt 882.633 inwoners (30 september 2022, Bron: CBS[1]) en is de grootste stad van Nederland. Amsterdam vormt samen met 32 andere gemeenten de Metropoolregio Amsterdam. In de regio wonen meer dan 2.500.000 mensen.

De gemeente Amsterdam kent een voor Nederland bijzonder bestuurlijk stelsel: de gemeente is verdeeld in stadsdelen, op dit moment zijn dat er zeven. Op 24 maart 2022 is daar het stadsgebied Weesp bij gekomen na een gemeentelijke herindeling.

De gemeente Amsterdam telt momenteel ongeveer 22.500 medewerkers en streeft ernaar deze een afspiegeling te laten zijn van de bevolking.

Voor meer informatie over de gemeente Amsterdam verwijzen we u naar de website www.amsterdam.nl.

2.4 De Opdrachtnemers

De Gemeente zoekt twee Opdrachtnemers die ervoor zorgen dat de (ICT) diensten van de Gemeente door de oplossingen, diensten en resources die Opdrachtnemer levert op een adequate manier zijn beveiligd tegen (cyber) security dreigingen in lijn met het actuele dreigingsbeeld voor de Gemeente. Het doel is om met de Dienst Informatiebeveiliging de stad veilig te maken en te houden.

De doelstelling van deze aanbesteding is dat de Gemeente per perceel één leverancier contracteert die in staat is de betreffende dienstverlening te leveren, inclusief continue actualisatie van de beveiligingsmaatregelen aan het wijzigende dreigingsbeeld, het beheer en onderhoud van de onderliggende oplossingen en tooling, zodanig dat de Dienst Informatiebeveiliging voldoet en blijft voldoen aan nationale en Amsterdamse beveiligingsrichtlijnen, de ICT-visie en de ambitie, doelstellingen, uitgangspunten en randvoorwaarden van de Directie Digitale Voorzieningen.

2.5 Marktconsultatie

Ter voorbereiding op de Europese aanbesteding heeft de Directie Digitale Voorzieningen van de Gemeente een marktconsultatie uitgevoerd. Deze bestond uit twee fasen:

1. Een plenaire bijeenkomst waarin de Gemeente de marktpartijen heeft geïnformeerd over de behoefte van de Gemeente en over de scope van de Opdracht. Ook heeft de Gemeente de

aanbesteding toegelicht. Tenslotte was er voor de marktpartijen gelegenheid voor het geven van hun zienswijze op de door Gemeente voorgestelde scope en aanpak en voor het stellen van vragen. Dertien marktpartijen hebben zich aangemeld voor de plenaire bijeenkomst.

2. Op basis van door de marktpartijen ingevulde vragenlijsten zijn zes marktpartijen geselecteerd waar 1-op-1-gesprekken mee zijn gevoerd. Het doel van deze gesprekken was om de gegeven antwoorden op de vragenlijst en de zienswijze van de marktpartij op de onderhavige aanbesteding in meer detail te bespreken. In de gesprekken zijn de volgende onderwerpen aan bod gekomen:
 - a. Afbakening van de diensten en indeling van de aanbesteding in percelen;
 - b. Migratie en implementatie van het Netwerkknooppunt en de Generieke security diensten;
 - c. Hosting van achterliggende oplossingen en tooling;
 - d. Bijblijven van de Generieke security diensten met het actueel dreigingslandschap en;
 - e. Duurzaamheid.

De bevindingen uit de marktconsultatie zijn waar relevant verwerkt in deze Selectieleidraad en worden indien nodig meegenomen bij het opstellen van het Beschrijvend Document.

2.6 Beoordelingsteam

Voor deze aanbesteding is een beoordelingsteam samengesteld waarin zowel materiedeskundigen als deskundigen op het gebied van Europees aanbesteden, contracteren, financiële en juridische zaken zijn verenigd. Dit betreft een indicatief uitgangspunt. De Gemeente kan de samenstelling van het beoordelingsteam wijzigen.

2.7 Varianten

De Gemeente staat geen varianten toe (zie artikel 2.83 Aw).

2.8 Beschrijving van de Dienst Informatiebeveiliging

2.8.1 Aanleiding en achtergrond

In het 'ICT-huis' van de Gemeente zijn de zes bouwlagen van de gehele ICT-landschap opgenomen, te weten:

- 1) WAN en (W)LAN (ANET) voor de interne connectiviteit tussen gebouwen;
- 2) Applicatie Hosting en Datacenter services (HenT en CCC) voor de hosting en het technisch applicatiebeheer van zowel on premise als cloud applicaties;
- 3) Amsterdam Digitale Poort (ADP) voor de beveiliging van het interne netwerk tegen dreigingen vanuit het externe netwerk;

- 4) Amsterdam Digitale Werkomgeving (ADW) voor de werkplek van de medewerkers;
- 5) Generieke, Gemeenschappelijke en Specifieke Applicaties;
- 6) Toegangsbeheer, dit is onderdeel van iedere bouwlaag.

De Gemeente heeft de lagen 1 tot en met 4 als diensten uitbesteed bij 4 (strategisch) partners. De huidige overeenkomst voor de dienst ADP die invulling geeft aan laag 3 van het ICT-huis expireert per 14 oktober 2023. Ook wordt er op korte termijn een nieuw visiedocument ontwikkeld voor de Directie Digitale Voorzieningen, waarbij enkele wijzigingen worden doorgevoerd van het huidige ICT-huis. De belangrijkste wijzigingen zijn:

- De derde bouwlaag zal niet meer ADP heten, maar Informatiebeveiliging. Deze bouwlaag bestaat uit alle generieke informatiebeveiligingsonderdelen die logischerwijs geen onderdeel zijn van de overige diensten;
- Toegangsbeheer, voorheen laag 6, zal geen aparte bouwlaag meer vormen, maar onderdeel worden van de bouwlaag Informatiebeveiliging.

Dit betekent dat het nieuwe ICT-huis uit 5 lagen zal bestaan die leiden tot de volgende (Infrastructurele) diensten:

- 1) WAN en (W)LAN voor de interne connectiviteit tussen gebouwen (ANET);
- 2) Applicatie Hosting en Datacenter services voor de hosting en het technisch applicatiebeheer van zowel on premise als cloud applicaties (HenT en CCC);
- 3) Amsterdam Digitale Werkomgeving voor de werkplek van de medewerkers (ADW);
- 4) Netwerkknooppunt voor de beveiliging van het interne netwerk tegen dreigingen;
- 5) Generieke security diensten.

De (Infrastructurele) diensten 4 en 5 zijn als separate percelen onderwerp van deze aanbesteding Dienst Informatiebeveiliging.

2.8.2 Algemene kengetallen

De Gemeente heeft op dit moment ongeveer 22.500 medewerkers en kent ongeveer 1200 actieve applicaties. Binnenkort zal de GGD Amsterdam gebruik gaan maken van de (Infrastructurele) diensten van de Gemeente waardoor het aantal medewerkers met ongeveer 1200 toe zal nemen. Het aantal applicaties varieert over de afgelopen jaren, waarbij de verwachting is dat dit de komende jaren ook het geval zal zijn.

2.8.3 Scope Netwerkknooppunt (P1)

Het Netwerkknooppunt is het centrale punt waarover het netwerkverkeer van alle (Infrastructurele) diensten van de Gemeente verloopt. Over het Netwerkknooppunt wordt al het netwerkverkeer doorgevoerd, gerouteerd en ontsloten. Het Netwerkknooppunt voorziet op een flexibele, schaalbare en betrouwbare wijze in de zgn. externe connectiviteit, de connectiviteit tussen de Gemeente en andere netwerken en organisaties. Het Netwerkknooppunt dient flexibel te zijn, omdat de ICT (infrastructuur) van de Gemeente aan verandering onderhevig is. Hierdoor is het van

belang dat eventuele diensten op een efficiënte wijze aangesloten kunnen worden en dat het Netwerkknooppunt schaalbaar is. Daarnaast is het belangrijk dat het Netwerkknooppunt een betrouwbare en robuuste inrichting kent ter voorkoming van zogeheten 'single-points-of-failure' (onder andere minimaal twee (2) Points of Presence (POP) in Nederland).

Het gemeentelijke ICT-landschap kent een multi-sourcing constructie. Dit betekent dat delen van de ICT (infrastructuur), conform het eerder toegelichte ICT-huis, zijn uitbesteedt aan verschillende (strategisch) partners. De uitdaging in deze constructie is dat het gemeentelijke ICT-landschap wel moet werken als één geheel. Organisatorisch betekent dit dat de (strategisch) partners nauw samen werken om ervoor te zorgen dat de verschillende delen ook technisch naadloos op elkaar aansluiten.

De connectiviteit van de Gemeente is opgesplitst in twee delen, namelijk de interne en de externe connectiviteit, waarbij de externe connectiviteit onderdeel is van het Netwerkknooppunt. Dit betekent voor de Gegadigde dat het succes van de externe connectiviteit mede afhangt van de aansluiting op de interne connectiviteitsdienst en de samenwerking met de betreffende (strategisch) partner.

Al het internetverkeer dient via het Netwerkknooppunt te verlopen, hetzij via een proxy, hetzij via een koppeling. Zowel de organisatie van de proxy als het realiseren van de koppeling is onderdeel van de Opdracht voor het Netwerkknooppunt. Verkeer wordt geïnspecteerd, versleutelde verbindingen worden geïnspecteerd, en aanvallen worden voorkomen. De realisatie van de verbindingen en het (fysiek) aansluiten van netwerk- en partnerkoppelingen vallen ook binnen scope van de Opdracht.

Mailrelay

Een aantal applicaties (± 10) van de Gemeente beschikt nog niet over een veilige mailoplossing die voldoet aan de standaarden die vereist zijn voor veilige mail. Om het toch mogelijk te maken om op een veilige manier te mailen vanuit deze applicaties is een mailrelay onderdeel van het Netwerkknooppunt. De mailrelay ondersteunt de standaarden DKIM, DMARC en SPF. Gegadigde begeleidt en ondersteunt bij het aansluiten van de applicaties op de mailrelay en bewaakt de beveiligingsmaatregelen van de mailrelay, zoals authenticatie.

Zero Trust

Het Netwerkknooppunt ondersteunt het Zero Trust Security Model, op basis van het principe "vertrouw nooit, verifieer altijd". Dit model stapt daarmee af van de al oude gedachte dat de interne omgeving veiliger is dan de onveilige externe omgeving. "Zero Trust" biedt hierop een antwoord door het toepassen van een gelaagde authenticatie en autorisatie methode en het continu monitoren van alle activiteiten op het netwerk, de systemen, applicaties en gebruik/apparatuur binnen de scope van het Netwerkknooppunt (netwerkmonitoring). Het toegangsbeheer van het model wordt geïmplementeerd door monitoring van toegang, detectie van ongeoorloofde toegang en beveiliging hiervan bij alle netwerkdiensten.

Voor applicaties/ informatiesystemen die het Zero Trust Security Model nog niet ondersteunen voorziet het Netwerkknooppunt in segmentatie, verkeersbeperking en inspectie tussen de interne netwerken.

Beveiliging Netwerkknooppunt

Het Netwerkknooppunt dient te zijn voorzien van netwerkbeveiliging die ervoor zorgt dat het netwerk is beveiligd conform de vereisten vanuit de Baseline Informatiebeveiliging Overheid (BIO) en de NEN7510. Om dit te bewerkstelligen voorziet Gegadigde in ieder geval in de beveiligingscomponenten Anti DDos oplossing, IPS/IDS, firewalling en een applicatie proxy (zie hierna). Voor monitoring van de security moet het Netwerkknooppunt als logbron worden incident aangesloten op de overkoepelende monitoring en response dienst van de Gemeente (zie par.2.8.4).

1. Anti DDos

In het kader van netwerkbeveiliging neemt Gegadigde passende maatregelen tegen (distributed) denial of service aanvallen voor ondersteunende servers en netwerkinfrastructuur binnen de scope van het Netwerkknooppunt Om de beschikbaarheid van online diensten en websites binnen het Amsterdam domein te kunnen waarborgen, biedt Gegadigde daarnaast een centrale anti DDOS oplossing.

2. IPS/IDS

Inbraak preventie systeem (IPS) en inbraakdetectiesysteem (IDS) houden het netwerk constant in de gaten. IPS/ IDS identificeren, loggen en voorkomen zo mogelijk security incidenten op het netwerk.

3. Firewalling

Binnen het Netwerkknooppunt zorgt firewalling voor de analyse van alle inkomende en uitgaande databestanden, beschermt de gemeentelijke infrastructuur en blokkeert het netwerkverkeer ingeval van risico's/gevaar.

4. Applicatie proxy

De Gemeente heeft een aantal diensten die intern gepositioneerd zijn in de eigen datacenters of in de datacenters van partners. Deze diensten bieden (web)applicaties en API's die voor intern gebruik geschikt zijn. Als onderdeel van het Netwerkknooppunt dienen deze (web)applicaties en API's benaderbaar te zijn gemaakt voor het internet door middel van applicatie proxies. Per applicatie wordt ondersteuning verwacht in de vorm van certificaten aanvragen, verkeerstroom aanpassingen en de aansluiting op de monitoring en response dienst.

Hosting

De hosting valt binnen de scope van het Netwerkknooppunt. Omdat de Gemeente bezig is om haar datacenters uit te faseren, kan Gegadigde het Netwerkknooppunt niet hosten in een van deze datacenters, maar dient Gegadigde gebruik te maken van een extern datacenter.

Bij de keuze voor de locatie van de hosting dient Gegadigde er rekening mee te houden dat het Netwerkknooppunt fysiek aangesloten moet worden op het interne netwerk van de Gemeente. Dit heeft tot gevolg dat het niet mogelijk is om het Netwerkknooppunt in de cloud te hosten. Componenten die geen fysieke verbinding nodig hebben dienen bij voorkeur wel in de cloud te worden gehost vanwege de strategie van de Gemeente om te hosten in de cloud, tenzij. Dit geldt bijvoorbeeld voor de hiervoor genoemde beveiligingscomponenten.

Threat intelligence

De Gemeente maakt gebruik van het Nationaal Detectie Netwerk (NDN) van het NCSC. Hierdoor moet Gegadigde het Netwerkknooppunt aansluiten op het NDN en de hiervoor bestemde MISP server van de Gemeente. De scope voor perceel 2 (par. 2.8.4) bevat meer informatie over het NDN en de MISP server.

Ontwerp en adviesdiensten

Binnen de Gemeente spelen er vaak projecten en initiatieven (met andere woorden: nieuwe aansluitingen) waarin verkeersstromen en de veiligheid van de verkeersstromen moet worden gerealiseerd. Om dit te kunnen realiseren kunnen er ontwerpen nodig zijn zoals bijvoorbeeld de uitwerking van de doelarchitectuur voor de nieuwe verkeersstroom. Daarnaast is er behoefte aan advisering tijdens dergelijke trajecten. Zowel ontwerpen als adviseringstrajecten vallen binnen de scope van de dienst.

Kengetallen voor het Netwerkknooppunt

De kengetallen voor het huidige externe netwerk en het bijbehorende verkeersplein (wat wordt omgedoopt tot Netwerkknooppunt) zijn:

- een redundante internettoegang van 10 Gbps;
- 8 redundante partnerkoppelingen;
- 4 closed user group circuits ten behoeve van het datapunt;
- 35 VPN communities;
- 4 datacenter locaties;
- 6 datacenter redundante interconnects;
- ongeveer 80 netwerkverbindingen.

2.8.4 Scope Generieke security diensten (P2)

De Gemeente hanteert het uitgangspunt dat iedere (strategisch) partner verantwoordelijk is voor de veiligheid van haar eigen (Infrastructurele) dienst. De beveiligingsmaatregelen die iedere (strategisch) partner daarvoor neemt, vallen niet onder de Generieke security diensten.

De Gemeente heeft behoefte aan volgende Generieke security diensten:

- 1) Cyber threat intelligence dienst;
- 2) Monitoring en incident response dienst;
- 3) Overkoepelende kwetsbaarheden management dienst;
- 4) Coördinated responsible disclosure dienst (hackers loket);
- 5) Automated malware analysis dienst.

Samenhangende diensten

De Opdrachtnemer dient deze vijf diensten zoveel mogelijk als samenhangend geheel uit te voeren, waardoor de output van de (individuele) diensten optimaal kan worden gebruikt. Een ander belangrijk aspect van deze dienstverlening is dat Opdrachtnemer deze gedurende de looptijd van

de Overeenkomst blijft doorontwikkelen om bij te blijven bij de actuele dreigingen. Dit geldt bijvoorbeeld voor het actueel houden van use-cases en play-books en ook het life cycle management van de onderliggende oplossingen en tooling moet worden geborgd.

Zo moet het bijvoorbeeld mogelijk zijn om use-cases binnen de monitoring en incident response dienst te actualiseren op basis van gewijzigde dreigingen vanuit de Cyber threat intelligence dienst.

Cyber threat intelligence dienst

Het hart van de Generieke security diensten is de cyber threat intelligence dienst. Threat intelligence is het verzamelen/verspreiden/delen van op feiten gebaseerde informatie over dreigingen, met als doel om het ontstane risico zo snel mogelijk af te dekken en mogelijke schade tot een minimum te beperken.

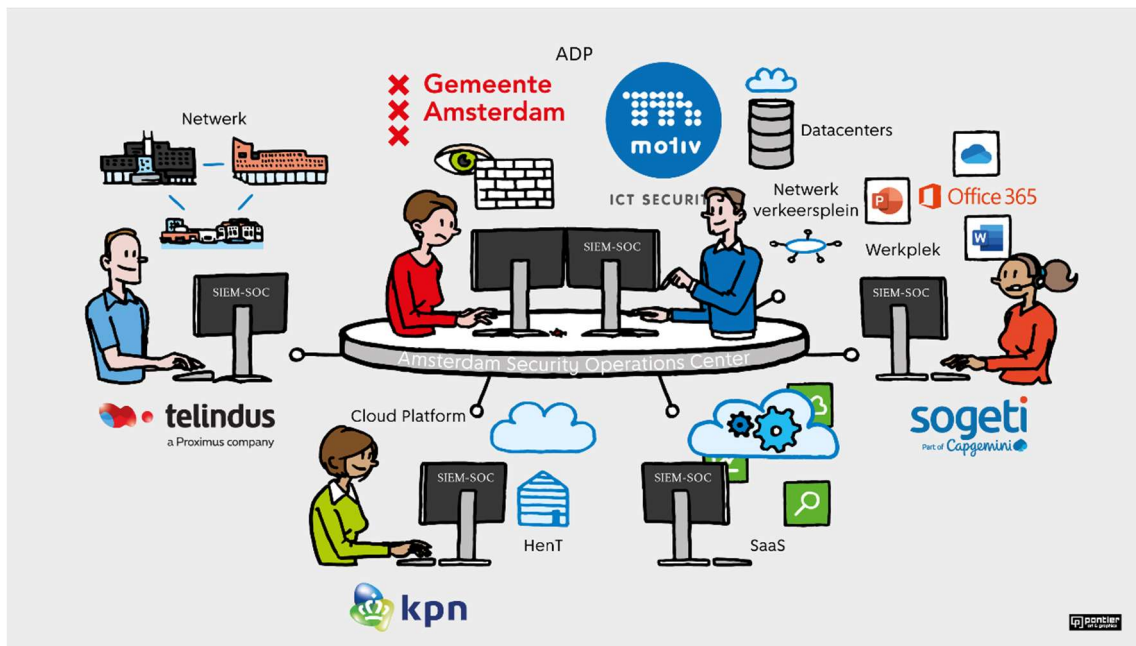
Het ophalen van dreigingsinformatie gebeurt door gebruik te maken van onder andere een commerciële service, het aansluiten op het Nationaal Detectie Netwerk (NDN) van het NCSC en het in kaart brengen van dreigingen specifiek voor de Gemeente.

Het aansluiten op het NDN is georganiseerd door een MISP server. Gegadigde organiseert de hosting en het beheer van de MISP server van de Gemeente. Hierdoor is het voor het NCSC duidelijk als een specifieke dreiging wordt gemeld vanuit de gemeente Amsterdam.

De commerciële threat intelligence service inclusief het aansluiten daarvan op de threat intelligence dienst is onderdeel van de Opdracht. De commerciële threat intelligence dienst haalt dreigingsinformatie op vanuit onder andere het internet en het dark web (dark web hunting) en rapportages over Advanced Persistent Threats (APT's) en hun modus operandi.

Monitoring en incident response dienst

De huidige monitoring en incident response dienst kent een kleinere scope dan de gewenste scope, namelijk de monitoring en de response van de externe connectiviteit + de twee datacenters van de Gemeente, datacenter 1 en datacenter 2 (DC1 en DC2), het zogeheten Amstel SOC.



Figuur 1 : Huidige decentrale security monitoring en response dienst per (strategisch) partner

Logbronnen van de huidige security monitoring en response dienst zijn:

- Antivirus meldingen - McAfee
- Meldingen van foutieve en succesvolle loginpogingen – On premise Microsoft Active Directory
- Wat staat waar en welke systemen zijn (in) actief – Infoblox
- Remote access – Cisco ISE
- IDS sensor node van het type Darktrace op het koppelvvlak Amstel Data Center DC 1/ DC 2 gericht op servers en beheer

Overige kengetallen van de huidige security monitoring en response dienst zijn:

- 1 TB opslag binnen het centrale SOC platform + real time analyseren van gemiddeld 1400 gebeurtenissen per seconde (De BIO kent een verplichting om log data die gerelateerd is aan een incident 3 jaar te bewaren, voor de NEN7510 geldt 5 jaar);
- 30 use-cases op basis van het Magma framework, gemapt naar het Mitre Att&ck framework;
- 6000 te analyseren IP-adressen.

De gewenste scope van de security monitoring en incident response dienst is een uitbreiding van de scope van de huidige dienst, zoals hiervoor beschreven naar alle (Infrastructurele) diensten van de Gemeente.



Figuur 2: Toekomstige onafhankelijke security monitoring en response dienst

Om de beveiliging van de (Infrastructurele) diensten van de Gemeente te borgen wil de Gemeente de stap zetten naar een onafhankelijke security monitoring en incident response dienst.

De security monitoring en incident response dienst draagt zorg voor de 24x7 monitoring en response op security incidenten binnen alle (Infrastructurele) diensten.

De security monitoring en incident response dienst moet worden aangesloten op meerdere logbronnen voor monitoring van de (Infrastructurele) diensten, zodat correlatie van security gebeurtenissen mogelijk is. Het vaststellen van de gewenste logbronnen zal in samenspraak tussen Opdrachtnemer en de Gemeente gebeuren. De organisatie van de dienst bestaat uit een aantal medewerkers van de Gemeente voor de tactische regie en medewerkers van Opdrachtnemer voor de operationele regie en operationele werkzaamheden.

Om de security monitoring en incident response werkzaamheden uit te kunnen voeren zijn er een aantal oplossingen ondergebracht onder de dienst:

- 1) Het Security Information en Event Managementsysteem (SIEM) voor correlatie van logging en gebeurtenissen (meldingen);
- 2) Een Security Orchestration, Automation and Responsesysteem (SOAR) voor geautomatiseerde afhandeling van security incidenten;
- 3) Extended Detection and Response (XDR) om snel geautomatiseerd in te kunnen grijpen bij security incidenten op endpoints;
- 4) Een management platform voor de afhandeling van (potentiële) security incidenten.

Hierbij is het aan Inschrijver om een keuze te maken voor een specifieke invulling van de gevraagde oplossingen. Vanuit hun tactische regierol kunnen de medewerkers van de Gemeente ook gebruik maken van de oplossingen en de tooling.

De security monitoring en response dienst is een 24 x 7 full-service dienst waarbij zoveel mogelijk afhankelijkheden zijn weggenomen door deze onder te brengen in de dienst. Zo is het uitvoeren van digitaal forensisch onderzoek en het Computer Security Incident Response Team (CSIRT) onderdeel van de dienst waardoor het mogelijk is om de responsetijd op cyber security incidenten zo kort mogelijk te houden. In geval van een security incident zorgt het CSIRT team voor snel handelen met als doel om de schade zoveel mogelijk te beperken, reduceren en snel herstel van de dienstverlening te bevorderen. Het CSIRT team is onderdeel van de security monitoring en responsdienst. Het uitvoeren van digitaal forensisch onderzoek voortvloeiend uit security incidenten heeft als doel het analyse en incident response proces te ondersteunen met een verdere diepgaandere analyse dan de dienst kan bieden.

Voor het waarborgen van de kwaliteit van onder andere de use-cases is ontwikkeling, integratie, automatisering en validatie en testen van use-cases door simulatie van een aanval (purple teaming) ook onderdeel van de monitoring en incident response dienst.

Use-cases zijn gemapt op het Mitre Att&ck framework. Hierbij is het belangrijk dat zowel use-cases als play-books blijven bij de actuele dreigingen en ook het life cycle management is gewaarborgd.

Buiten scope: De stadsbrede security monitoring en response dienst¹ is geen onderdeel van de gewenste scope voor de security monitoring en incident response dienst zoals hierboven beschreven.

Kwetsbaarhedenmanagement dienst

De Gemeente vereist van iedere (strategisch) partner dat de geleverde (Infrastructurele) dienst veilig is en dat deze verantwoordelijk is voor het installeren van beveiligingspatches (patchmanagement). Om te kunnen ontdekken in welke gevallen deze patches noodzakelijk zijn, hebben (strategisch) partners vaak een kwetsbaarheden scanner draaien.

De kwetsbaarhedenmanagement dienst is de overkoepelende dienst voor kwetsbaarhedenmanagement waardoor de Gemeente een totaaloverzicht krijgt van de kwetsbaarheden binnen de IT (infrastructuur).

De coördinatie van patchverzoeken, inclusief bewaken van opvolging, richting andere (strategisch) partners is ook onderdeel van de dienst.

Onderdeel van kwetsbaarhedenmanagement dienst is een dashboard of tooling waarop informatie over alle kwetsbaarheden binnen de IT (Infrastructuur) wordt getoond. Het dashboard of tooling toont in ieder geval de volgende kwetsbaarheden:

- 1) Kwetsbaarheden vanuit andere (Infrastructurele) diensten. De (strategisch) partners die verantwoordelijk zijn voor deze diensten leveren deze informatie aan;

¹ Het is de ambitie van de Gemeente om in de toekomst de security en monitoring en response dienst uit te breiden naar een stadsbrede security en monitoring en response dienst, waaronder bijv. ook de organisatieonderdelen V&OR en Parkeren zullen vallen. Deze organisatieonderdelen gebruiken echter andere technieken dan binnen de scope van deze aanbesteding zijn voorzien, denk bijv. aan camera's onder bruggen, parkeerautomaten, etc. en vallen dan ook buiten de scope van de aanbesteding.

- 2) Kwetsbaarheden gevonden vanuit de coördinated responsible disclosure dienst;
- 3) Kwetsbaarheden vanuit PEN- en hacktesten. De Gemeente of de leverancier die de testen uitvoert levert deze informatie aan.

Door inzicht in de kwetsbaarheden en bewaking van de opvolging is de zorgplicht van de Gemeente op het gebied van technische kwetsbaarheden gewaarborgd (BIO control 12.6.1 en 12.6.1.1).

Input voor de kwetsbaarhedenmanagement dienst is de threat intelligence dienst. Aan de hand van de actuele dreigingen is het immers mogelijk om de prioriteit te bepalen van de gevonden kwetsbaarheden.

Coördinated responsible disclosure dienst

De Gemeente gaat binnenkort de coördinated responsible disclosure activeren op de website van de stad. Dit betekent dat ethisch hackers onder voorwaarden die de Gemeente heeft gesteld een poging mogen doen om kwetsbaarheden te ontdekken in de online diensten van de Gemeente. Als een ethisch hacker een kwetsbaarheid ontdekt meldt hij dit bij de Gemeente. Het administreren, registreren en coördineren van de opvolging van deze kwetsbaarheden naar de verantwoordelijke eigenaren van de Gemeente valt onder de coördinated responsible disclosure dienst.

Malware analysis platform dienst

Potentiële malware dient op een veilige manier onderzocht te worden buiten andere systemen om. Hiervoor is een automated malware analysis platform dienst met een veilige sandbox onderdeel van de Generieke security diensten. Ondanks dat het onderzoeken van potentiële malware zoveel mogelijk geautomatiseerd gebeurt is een webportal naar de sandbox ook onderdeel van de dienst, zodat de medewerkers van de Gemeente zelf, zonder tussenkomst van de leverancier, ook op een veilige manier potentiële malware kunnen onderzoeken.

De Gegadigde dient een malware analysis platform specifiek voor de Gemeente in te richten. De data binnen dit platform blijft van de Gemeente en het platform kan om deze reden ook geen onderdeel zijn van een gedeelde sandbox/malware dienst.

Cyber Fusion Center

De bovengenoemde Generieke security diensten zijn ondergebracht in een Cyber Fusion Center, binnen de organisatie van de Gemeente.

Het Cyber Fusion Center waakt over de beveiliging van het ICT-landschap van de Gemeente en houdt zich 24/7 bezig met het monitoren daarvan. Het Cyber Fusion Center staat daarnaast in verbinding met verschillende (externe) partijen die de Gemeente van data voorzien over mogelijke kwetsbaarheden en mogelijke dreigingen.

Het Cyber Fusion Center vertaalt deze data naar relevante acties en informatie voor de Gemeente of de leveranciers die een (Infrastructurele) dienst leveren, voorzien hen van adviezen en verlenen eventueel bijstand remote of op locatie middels het CSIRT. De organisatie van het Cyber Fusion Center bestaat uit medewerkers van de Gemeente en medewerkers van Opdrachtnemer. Hierbij is

het uitgangspunt dat de medewerkers van het Cyber Fusion Center zoveel mogelijk gezamenlijk op locatie werken in het Cyber Fusion Center van de Gemeente.

Hosting

Het is de verwachting dat Gegadigde voor het leveren van de Generieke security diensten gebruik maakt van oplossingen en tooling. Deze oplossingen en tooling, inclusief de hosting daarvan zijn integraal én contractueel onderdeel van de aangeboden dienstverlening. Dit betekent ook dat de leverancier voor de dienstverlening geen gebruik kan maken van reeds door de Gemeente met Microsoft of andere partijen, gesloten contracten betreffende o.a. omgevingen (tenants) en licenties. Uitgangspunt voor de hosting van oplossingen en tooling is 'cloud tenzij', waarbij de cloudvorm (public, private, community of hybride) vrij in te vullen is. Dit wil zeggen dat de leverancier aan de hand van de in de oplossingen en tooling te verwerken gegevens bepaalt welke vorm van hosting, gezien wet- en regelgeving waaronder de AVG, het meest passend is. Indien cloud niet mogelijk is dan dient dit te worden toegelicht. Ook de organisatie van de on premise hosting is onderdeel van het contract.

Buiten scope

Toegangsbeheer (IAM) valt niet binnen de scope van deze aanbesteding.

2.9 Vorm, duur en waarde van de Overeenkomsten

Voor de dienstverlening van de percelen 1 en 2 (Netwerkknooppunt en Generieke security diensten) zal een overeenkomst van Opdracht worden gesloten met een basis looptijd van 5 jaar met 2 maal de optie om 2 jaar te verlengen. De redenen waarom de Gemeente kiest voor deze relatief lange looptijd zijn:

- 1) de Opdrachtnemers zullen naar verwachting geruime tijd aanloopproblemen en -kosten hebben voordat de diensten optimaal functioneren. De gekozen looptijd stelt ze in staat om een gezonde businesscase op te stellen;
- 2) Voor de Gemeente is het voorbereiden en uitvoeren van een aanbesteding een intensief en langdurig proces, bij een kortere contractduur zal zij relatief kort op de huidige aanbesteding al moeten starten met een nieuwe aanbesteding.

Een globale inschatting van de waarde van het Netwerkknooppunt bedraagt 25 miljoen euro voor de totale looptijd van de Overeenkomst, inclusief verlenging.

Een globale inschatting van de waarde van de Generieke security diensten bedraagt 30 miljoen euro voor de totale looptijd van de Overeenkomst, inclusief verlenging.

2.10 Randvoorwaarden voor gunning van de percelen betreffende leverancier

Deze aanbestedingsprocedure voor de Dienst Informatiebeveiliging bestaat uit 2 percelen: 1) het Netwerkknooppunt en 2) Generieke security diensten. Binnenkort zal er een andere aanbestedingsprocedure worden gestart die deels parallel zal lopen met de aanbesteding Dienst Informatiebeveiliging. Deze tweede aanbesteding betreft ook twee percelen: 1) PEN- en hacktesting, en 2) Security consultancy. De twee procedures vertonen een samenhang in de zin dat er afhankelijkheden zijn bij de gunning van de percelen aan bepaalde leveranciers.

De Gemeente hanteert hierbij de volgende uitgangspunten:

- 1) De huidige (strategisch) partners van de Gemeente voor werkplekken (ADW), Applicatie Hosting en Datacenter services (HenT en CCC) en interne connectiviteit (ANET), komen niet in aanmerking voor de gunning van de Generieke security diensten (P2), voor PEN- en hacktesting (P3) en Security consultancy (P4) vanwege de geboden onafhankelijkheid van deze percelen.
- 2) Een partij die een bepaald perceel wint, komt niet in aanmerking voor gunning van de overige percelen. Toelichting:
 - a. De leverancier die het Netwerkknooppunt (P1) gaat verzorgen, kan niet ook verantwoordelijk zijn voor de Generieke security diensten (P2), omdat deze door een onafhankelijk leverancier moeten worden uitgevoerd. De leverancier(s) die de PEN- en hacktesting gaan verzorgen, testen tevens het Netwerkknooppunt en de leverancier voor Security consultancy geeft mogelijk ook advies over het Netwerkknooppunt;
 - b. De Generieke security diensten (P2) dienen door een onafhankelijk leverancier te worden uitgevoerd en deze leverancier komt daarom niet in aanmerking voor gunning van de overige percelen;
 - c. Het onder b. genoemde geldt ook voor de leveranciers voor PEN- en hacktesting;
 - d. De leverancier die Security consultancy gaat verzorgen, geeft mogelijk ook advies over het Netwerkknooppunt en de Generieke security diensten en daar is onafhankelijkheid belangrijk. Daarnaast betreft Security consultancy ook het uitvoeren van controles op de uitgevoerde PEN- en hacktesting. In dat laatste geval is onafhankelijkheid noodzakelijk.
- 3) Mocht een leverancier in deze aanbesteding Dienst Informatiebeveiliging meedingen naar zowel P1 als P2 en voor beide percelen als winnaar uit de bus komen, dan kiest de Gemeente welk perceel deze leverancier gegund krijgt. Hierbij geldt het uitgangspunt dat de Gemeente het perceel waarop de leverancier de hoogste kwaliteitsscore heeft behaald aan hem zal gunnen. Dit geldt ook voor de twee percelen uit de andere, samenhangende procedure voor PEN- en hacktesting en Security consultancy.

Hierna vindt u alvast een korte toelichting op de twee percelen: PEN- en hacktesting, en Security consultancy. Op basis van deze toelichting kan een leverancier een voorlopige inschatting maken welke opdrachten voor hem interessant zijn. Zowel PEN- en hacktesting als Security consultancy

zullen worden uitgevraagd als een dienstverleningsopdracht (met evt. een resultaatsverplichting). Voor beide percelen geldt dat de Gemeente geen afnameverplichting heeft.

Korte toelichting PEN- en hacktesting

PEN- en hacktesting betreft het uitvoeren van penetratietests en vulnerability scans. De Gemeente kan beide typen tests afnemen om meer inzicht te krijgen in het beveiligingsniveau van informatiesystemen en de beveiliging daarvan te kunnen verbeteren.

Onder een penetratietest verstaat de Gemeente een onderzoek naar de risico's en kwetsbaarheden van informatiesystemen, waarbij de gevonden kwetsbaarheden ook daadwerkelijk getoetst worden om de kwetsbaarheid aan te tonen (het controleren op false positives).

Bij een vulnerability scan worden de informatiesystemen alleen gescand op het mogelijk aanwezig zijn van kwetsbaarheden.

Voor PEN- en hacktesting zal er een raamovereenkomst met drie leveranciers worden afgesloten voor de duur van 4 jaar. Per nadere opdracht zal de Gemeente een zogenaamde mini competitie uitvoeren. De leveranciers die onderdeel uitmaken van de raamovereenkomst kunnen dan een aanbieding doen. De precieze voorwaarden waaronder deze mini competities worden uitgevoerd zijn op dit moment nog niet bekend. De verwachte (totale) contractwaarde voor PEN- en hacktesting is ruim 10 miljoen euro. De Gemeente behoudt zich het recht voor om deze waarde in de aanbesteding bij te stellen. Er zal geen afnameverplichting gelden.

Korte toelichting Security consultancy

De Gemeente heeft behoefte aan onafhankelijk en hoogwaardig advies op het gebied van informatiebeveiliging en concreet aan advies op de volgende onderdelen:

- Second opinions ten aanzien van security architectuur (high level design) vraagstukken en PEN- en hacktest rapportages;
- Reviews en advisering met betrekking tot te nemen cybersecurity maatregelen;
- Advies aan andere dienstonderdelen op het gebied van security, bijvoorbeeld bij Security by Design vraagstukken.

Voor Security consulting zal een raamovereenkomst met een leverancier worden afgesloten voor de duur van 4 jaar. De verwachte contractwaarde is ongeveer 5 miljoen euro. De Gemeente behoudt zich het recht voor om deze waarde in de aanbesteding bij te stellen. Er zal geen afnameverplichting gelden.

2.11 Planning op hoofdlijnen

De planning van deze aanbestedingsprocedure is als volgt:

Fase	Wat	Einddatum
Selectieleidraad	Publiceren Selectieleidraad	20-okt-22

Selectiefase	Indienen vragen voor Nota van Inlichtingen (versie 1)	28-okt-22
	Publiceren antwoorden op Nvi vragen (Nvi v1)	04-nov-22
	Indienen vragen voor Nota van Inlichtingen (versie 2)	11-nov-22
	Publiceren antwoorden op Nvi vragen (Nvi v2)	18-nov-22
	Uiterste inleverdatum Verzoeken tot Deelname	30-nov-22
	Beoordelen Verzoeken tot Deelname en bekendmaking top-5 Gegadigden	16-dec-22
	Einde standstill-periode Selectieleidraad	6-jan-23
Beschrijvend Document	Publiceren Beschrijvend Document	07-feb-23
Offertefase	Indienen initiële Inschrijving en start 'onderhandelingsfase'	20-mrt-23
	Inleverdatum definitieve Inschrijving	10-apr-23
	Voorlopige gunning en start standstill-periode	28-apr-23
	Einde standstill-periode	18-mei-23
	Ondertekenen Overeenkomst	25-mei-23

Tabel 1: Globale planning

3 Voorschriften bij de aanbesteding

3.1 Algemene voorschriften

Deze aanbesteding is officieel aangekondigd via www.tenderned.nl. Gemeente Amsterdam gebruikt TenderNed om wijzigingen of aanvullingen te communiceren aan de markt. Gegadigde is en blijft verantwoordelijk voor het volgen van TenderNed alsmede het aanvragen en downloaden van de relevante documenten.

Verder gelden de volgende algemene voorschriften:

- Het indienen van een Verzoek tot Deelname betekent dat Gegadigde instemt met de bepalingen van de aanbestedingsprocedure;
- Branchevoorwaarden of algemene voorwaarden van Gegadigde zijn uitdrukkelijk niet van toepassing;
- Op deze procedure is uitsluitend Nederlands recht van toepassing;
- Geschillen zullen worden beslecht door de bevoegde rechter bij de rechtbank in Amsterdam.

3.2 Aanbestedingsprocedure en procesgang

Deze aanbestedingsprocedure wordt uitgevoerd in de vorm van een Mededingingsprocedure met onderhandeling als bedoeld in artikel 2.30 e.v. Aw.

Op 29 juni 2022 is op TenderNed de marktconsultatie voor deze Opdracht gepubliceerd, met referentienummer AICT-2022-0037.

De Gemeente zal aan de hand van deze Selectieleidraad komen tot een kwalificatie en nadere selectie van vijf Gegadigden per perceel. De vijf geselecteerde Gegadigden (we noemen ze vanaf dat moment Inschrijvers) ontvangen het Beschrijvend Document en op basis daarvan kunnen ze hun initiële Inschrijving opstellen en indienen.

3.3 Voorwaarden

Door indiening van uw Verzoek tot Deelname op de wijze zoals in deze Selectieleidraad beschreven, wordt u Gegadigde voor de aanbestedingsprocedure van Gemeente en aanvaardt u zonder voorbehoud alle in deze Selectieleidraad (inclusief Bijlagen) en in de Nota van Inlichtingen gestelde voorwaarden.

3.4 Keuze aanbestedingsprocedure

Zowel het Netwerkknooppunt (P1) als de Generieke security diensten (P2) betreffen complexe dienstverlening, inclusief onderliggende oplossingen en tooling, die in grote mate moeten worden aangepast aan de specifieke situatie binnen de Gemeente. Bijkomende aspecten die de Gemeente in deze context relevant acht, zijn het ontwerpen (vormgeven en faseren) van de migratie- en implementatietrajecten in het complexe multi-sourcing ICT-landschap van de Gemeente en het inrichten van de samenwerking en de communicatie van de nieuwe leverancier met de zittende (strategisch) partners van de overige (Infrastructurele) diensten op operationeel, tactisch en strategisch niveau.

Voor deze aanbesteding heeft de Gemeente dan ook gekozen voor de mededingingsprocedure met onderhandeling. De Aanbestedingswet en de richtlijnen laten in dit geval voldoende ruimte voor het gebruik van deze procedure. De aanbesteding heeft immers betrekking op complexe aankopen van geavanceerde producten waarbij aanpassings- of ontwerpactiviteiten noodzakelijk zijn. Leveranciers kunnen niet in de behoefte van de Gemeente voorzien door het enkele leveren van beschikbare standaardoplossingen. In Considerans 43 van RICHTLIJN 2014/24/EU worden grote ICT-projecten expliciet als voorbeeld genoemd voor de toepassing van bijzondere procedures.

Door de complexiteit van de Opdracht bestaat de kans dat leveranciers bepaalde aspecten van de behoefte over het hoofd zien, waardoor de offertes niet optimaal aansluiten bij de wensen van de Gemeente. Het gebruik van de mededingingsprocedure met onderhandeling stelt de Gemeente in staat om deze risico's te mitigeren. Ze kan met de Inschrijvers in gesprek gaan om te verifiëren of er in hun initiële Inschrijving voldoende rekening is gehouden met de belangrijkste wensen van de Gemeente en op welke wijze dit is gedaan. Na deze gesprekken hebben de leveranciers de mogelijkheid om een definitieve Inschrijving in te dienen.

3.5 Elektronische communicatie via TenderNed

De Gemeente kiest er in deze aanbesteding voor om de schriftelijke communicatie met Gegadigden uitsluitend langs elektronische weg te laten plaatsvinden. Om die reden:

- zijn de Selectieleidraad en alle Bijlagen via TenderNed openbaar en vrij toegankelijk gemaakt;
- dienen verzoeken om inlichtingen uitsluitend via TenderNed te worden ingediend;
- zullen de Nota van Inlichtingen en alle overige documenten uitsluitend via TenderNed worden verspreid;
- dient Gegadigde zijn Verzoek tot Deelname via TenderNed in te dienen;
- vindt alle overige schriftelijke communicatie met Gegadigden via TenderNed plaats.

Voor vragen over het gebruik van TenderNed kan Gegadigde direct contact opnemen met de helpdesk van TenderNed.

NB Om via TenderNed te kunnen deelnemen aan deze aanbesteding dienen Gegadigden over een zogenaamde 'e-Herkenning' te beschikken. Gegadigde wordt, indien hij nog niet over e-Herkenning beschikt, geadviseerd deze tijdig aan te vragen. Voor meer informatie verwijzen we naar

<https://www.tenderned.nl/cms/voor-ondernemingen/starten-met-tenderned/eherkenning-gebruiken>.

3.6 Communicatie met betrekking tot deze aanbesteding

Het is Gegadigde niet toegestaan contact op te nemen met medewerkers van de Gemeente en/of andere deelnemers aan het projectteam en het beoordelingsteam, anders dan de contactpersonen. Alle communicatie verloopt via de procesbegeleider, dhr. P. Pirson of mevr. Z. Yilmaz, via de berichtenmodule in TenderNed.

Indien bovengenoemde regels worden overtreden, kan dit tot onmiddellijke uitsluiting van verdere deelneming leiden, ongeacht de fase van de aanbesteding.

Alle correspondentie in het kader van deze aanbesteding dient voorzien te zijn van het referentienummer van deze aanbesteding op TenderNed, te weten: AICT-2022-0037.

3.7 Voorbehoud

De in deze Selectieleidraad gestelde criteria zijn gebaseerd op de huidige en op dit moment bekende toekomstige situatie bij de Gemeente. Gegadigden kunnen geen rechten ontleen aan de in deze Selectieleidraad genoemde planning, aantallen of specificaties. Deze dienen slechts ter indicatie van de te contracteren diensten en als basis voor de vergelijking van de verschillende Verzoeken tot Deelname.

De Gemeente behoudt zich het recht voor om het aanbestedingstraject tot de ingangsdatum van de Overeenkomst geheel of gedeeltelijk, tijdelijk of definitief te stoppen.

3.8 Vragenronde

Vragen ter verduidelijking van deze aanbesteding dienen uiterlijk op de in de planning genoemde datum en tijd, onder vermelding van de naam van de aanbesteding, via TenderNed ingediend te worden bij de contactpersoon. Vragen die na deze datum binnenkomen worden in beginsel niet beantwoord en worden niet verder in behandeling genomen bij de beoordeling. Gegadigde dient bij vragen nauwkeurig aan te geven op welk deel van de Selectieleidraad de vraag betrekking heeft, onder vermelding van het paginanummer.

De Gemeente beantwoordt de door Gegadigden/Inschrijvers gestelde vragen, geanonimiseerd in twee versies van de Nota van Inlichtingen. Deze Nota van Inlichtingen wordt op TenderNed gepubliceerd.

Indien een Gegadigde het niet eens is met delen van een artikel uit de Algemene Inkoopvoorwaarden of de Amsterdamse bepalingen kan hij, gemotiveerd en voorzien van een alternatief tekstvoorstel, een verzoek tot aanpassing indienen. De Gemeente beoordeelt dit alternatief en geeft in de Nota van Inlichtingen een antwoord dat bindend is voor alle Inschrijvers. De definitieve Nota van Inlichtingen maakt daarna onlosmakelijk deel uit van deze Selectieleidraad.

De Nota van Inlichtingen vormt samen met de Selectieleidraad het enige uitgangspunt van deze aanbesteding. Mondelinge toezeggingen of afspraken hebben geen rechtskracht, tenzij deze schriftelijk zijn bevestigd door de contactpersoon.

3.9 Onvolkomenheden, procedurefouten, onduidelijkheden en (tegen)strijdigheden

Dit document met de bijbehorende Bijlagen is met grote zorg samengesteld. De Gemeente verzoekt Gegadigde eventuele onvolkomenheden, vermeende procedurefouten, onduidelijkheden en/of (tegen)strijdigheden betreffende de documenten terstond, doch uiterlijk op de datum en het tijdstip waarop de schriftelijke gestelde vragen moeten zijn ingediend en overigens ook conform het bepaalde in paragraaf 3.8 bij de contactpersoon te melden. Deze termijn wordt gehanteerd om de Gemeente in de gelegenheid te stellen vragen te beantwoorden, een bezwaar te toetsen en Gegadigde een redelijke termijn te geven eventuele aanpassingen te kunnen verwerken. De Gemeente verzoekt Gegadigde evenwel om niet tot het laatste moment te wachten met het stellen van vragen.

Indien na de sluitingsdatum van het indienen van de Verzoeken tot Deelname blijkt dat de aanbestedingsdocumentatie onvolkomenheden en/of procedurefouten en/of onduidelijkheden en/of (tegen)strijdigheden bevat en deze zijn niet door Gegadigde gemeld, dan zal dit in het voordeel van Gemeente worden uitgelegd. De Gegadigde heeft in dat geval zijn rechten verwerkt om zich op die onvolkomenheden en/of procedurefouten en/of onduidelijkheden en/of (tegen)strijdigheden (al dan niet in rechte) te beroepen. Kennelijke fouten of omissies in de tekst van de aanbestedingsdocumentatie binden Gemeente in geen geval.

3.10 Volledigheid en indeling aanmelding

Het Verzoek tot Deelname dient volledig en rechtsgeldig te zijn: alle gevraagde bewijsstukken en andere informatie moet zijn bijgesloten en Gegadigde wordt verzocht alle in deze Selectieleidraad vermelde vragen, zowel algemeen als specifiek te beantwoorden. Daarnaast dient Gegadigde bevoegd te zijn tot het aangaan van de in deze Selectieleidraad bedoelde Overeenkomst.

Het is niet toegestaan vaste teksten en indelingen in formulieren en Bijlagen te wijzigen. Het Verzoek tot Deelname dient conform het overzicht in onderstaande Tabel 2 te worden opgebouwd:

Bestandsnaam	Omschrijving	Aanleveren in format
101 Verzoek tot Deelnames-brief_<naam Gegadigde>	Rechtsgeldig ondertekend en in de Nederlandse taal opgesteld Verzoek tot Deelname waarin: beschrijving samenwerking met derde partijen (indien van toepassing); eventuele bijzonderheden omtrent het Verzoek tot Deelname; en volmacht (indien van toepassing).	Pdf-formaat (maximaal 2 pagina's a4)
102 Beantwoording vragen_<naam Gegadigde>	Beantwoording van de vragen uit de paragrafen 6.2 en/of 6.3.	Pdf-formaat
103x Referentie-sjabloon	Ingevulde referentiesjablonen. Nummer de exemplaren op al naar gelang de hoeveelheid die wordt ingeleverd: 103a, 103b, etc.	Bijlagen 7.3 en 7.47.4
104 Uittreksel-Handelsregister <naam Gegadigde>	Uittreksel(s) uit het Handelsregister (niet ouder dan drie maanden bij het moment van indienen van de Verzoek tot Deelname).	Pdf-formaat
N.v.t.	Uniform Europees Aanbestedingsdocument	Via TenderNed

Tabel 2: Inleverinstructie

Het Verzoek tot Deelname dient te worden ondertekend door één of meer personen die bevoegd zijn de onderneming te binden. De bevoegdheid dient te kunnen worden vastgesteld aan de hand van de gegevens uit het Handelsregister. In geval een combinatie een Verzoek tot Deelname indient dan dient het Verzoek tot Deelname door alle deelnemers aan de combinatie te worden ondertekend. Het is toegestaan een volmacht aan het Verzoek tot Deelname toe te voegen in verband met de vertegenwoordigingsbevoegdheid.

De Gemeente behoudt zich het recht voor om een onvolledig Verzoek tot Deelname niet verder in behandeling te nemen.

3.11 Intellectueel eigendom, geheimhouding, publiciteit en taal

Behoudens uitzonderingen door de Auteurswet gesteld, mag zonder schriftelijke toestemming van de Gemeente niets uit dit document worden verveelvoudigd (anders dan voor het doel van deze aanbesteding) door middel van druk, fotokopie of anderszins.

Alle informatie uit deze Selectieleidraad en andere documenten behorend bij deze aanbesteding of verkregen in de hierop volgende contacten mag uitsluitend gebruikt worden om antwoorden te formuleren op de gestelde vragen. Het is niet toegestaan de informatie te gebruiken voor andere doeleinden. Publiciteit door Gegadigde met betrekking tot deze aanbesteding is alleen toegestaan na schriftelijke voorafgaande toestemming van Gemeente.

Alle door Gegadigde aangeboden informatie en documentatie wordt eigendom van de Gemeente. De Gemeente zal alle verkregen informatie uit deze procedure vertrouwelijk behandelen en niet gebruiken voor andere doeleinden dan beschreven, tenzij Gegadigde anders vermeldt.

De voertaal in de Gemeente is overwegend Nederlands. Gegadigde bevestigt door het indienen van een Verzoek tot Deelname dat de accountmanager en alle medewerkers die tijdens het aanbestedingstraject en in een eventuele latere fase van uitvoering van de dienstverlening contact hebben met de medewerkers van de Gemeente de Nederlandse taal beheersen.

Alle correspondentie en documentatie die door de Gemeente wordt opgesteld zal alleen in het Nederlands worden uitgegeven. Correspondentie en documentatie van Gegadigde wordt alleen geaccepteerd als die in het Nederlands is opgesteld. Uitzondering wordt gemaakt voor documenten die oorspronkelijk in een andere taal zijn opgesteld, bijvoorbeeld technische omschrijving van materiaal, jaarverslag, verzekeringspolis, bankgarantie etc. In voorkomend geval kan de Gemeente om een officiële vertaling verzoeken. Eventuele kosten zijn dan voor rekening van Gegadigde.

3.12 Sluitingsdatum voor aanmeldingen

De sluitingsdatum voor het indienen van een Verzoek tot Deelname voor deze aanbesteding is 30 november 2022.

3.13 Voorschriften betreffende de wijze van indiening van de Verzoeken tot Deelname

- Het Verzoek tot Deelname (inclusief de te overleggen ingevulde Bijlagen en bijbehorende documenten) dient via TenderNed te worden aangeleverd.
- Het Verzoek tot Deelname dient geparafeerd en ondertekend te zijn door (een) rechtsgeldig(e) vertegenwoordiger van Gegadigde. Dit wordt na bekendmaking van het resultaat van beoordelen geverifieerd aan de hand van het door Gegadigde ondertekende Uniform Europees Aanbestedingsdocument en het te verstrekken uittreksel uit het register van de Kamer van Koophandel. Uit dit uittreksel moet de tekenbevoegdheid van de ondertekenaar duidelijk blijken. Het uittreksel uit het Handelsregister mag op het moment van indienen van de Verzoek tot Deelname niet ouder zijn dan drie maanden.
- De Gegadigde dient voor het aanleveren van de gevraagde informatie gebruik te maken van de formulieren die daarvoor bestemd zijn en die zijn toegevoegd in de Bijlagen. Antwoorden die ingediend worden in afwijkende formats kunnen worden uitgesloten van beoordeling.

Verzoeken tot Deelname die niet voldoen aan bovengenoemde voorschriften kunnen als ongeldig terzijde worden gelegd.

3.14 Beoordeling van de aanmeldingen

Na de sluitingstermijn wordt de aanmeldingskluis in TenderNed geopend en worden de Verzoeken tot Deelname beoordeeld. De Gemeente streeft ernaar om op de datum opgenomen in de planning de beoordeling af te ronden en Gegadigde schriftelijk van het resultaat van beoordelen in kennis te stellen.

3.15 Herstel van fouten en omissies, verduidelijking

De Gemeente verklaart Verzoeken tot Deelname die niet voldoen aan de eisen, voorwaarden en formuleren zoals vastgelegd in deze Selectieleidraad ongeldig, behoudens het bepaalde in deze paragraaf.

Mocht blijken dat in een Verzoek tot Deelname informatie ontbreekt, dan kan de Gemeente besluiten om het gebrek aan overgelegde gegevens te laten herstellen, afhankelijk van de ernst van het gebrek (alleen bij kleine omissies kan de Gemeente om aanvulling verzoeken). De Gemeente is daartoe op geen enkele manier verplicht. De Gemeente behoudt zich tevens het recht voor om verduidelijking, toelichting of aanvulling van een Verzoek tot Deelname of andere informatie te vragen, dit ter uitsluitende beoordeling door de Gemeente. De Gemeente is ook daartoe op geen enkele manier verplicht.

De Gemeente kan alle informatie die door een Gegadigde ter beschikking wordt gesteld (ook die afkomstig van derden) op juistheid controleren, onder meer door derden te benaderen. Mocht uit die verificatie blijken dat een Gegadigde onjuiste informatie heeft verstrekt in zijn Verzoek tot Deelname, dan kan de Gemeente die Gegadigde uitsluiten van (verdere) deelname aan de aanbesteding.

Gegadigde dient binnen de door de Gemeente aangegeven termijn te reageren. Het aangeleverde maakt vervolgens onlosmakelijk onderdeel uit van het Verzoek tot Deelname van Gegadigde. Indien een dergelijke reactie niet, niet op tijd en/of niet volledig ontvangen is, dan kan dit leiden tot uitsluiting van verdere deelname aan de aanbesteding.

3.16 Klachtenregeling

Tijdens de aanbestedingsprocedure kan een situatie ontstaan waarbij bij een belanghebbende ontevredenheid ontstaat over het handelen van de Gemeente. Voor deze situatie beschikt de Gemeente over een klachtenprocedure.

Een belanghebbende kan gemotiveerd een klacht indienen op het e-mailadres: ictaanbestedingen.ict@amsterdam.nl.

De Gemeente is vrij om al dan niet te besluiten tot opschorting van de procedure. Een klacht is een schriftelijke melding van een natuurlijke of rechtspersoon, die belang heeft bij deze aanbesteding. In de klacht geeft de Gegadigde/Inschrijver gemotiveerd aan over welke punten hij een klacht heeft. Een klacht moet duidelijk als zodanig worden benoemd.

Een klacht is geen verzoek tot het verkrijgen van inlichtingen. Een verzoek om inlichtingen heeft een neutraal karakter en is gericht op verduidelijking. Vragen en verzoeken gericht op verduidelijking dienen tijdig ingebracht te worden zoals beschreven in paragraaf 3.8.

Het volgen van deze klachtenprocedure kan tot gevolg hebben dat klachten die in onderling overleg opgelost kunnen worden niet nodeloos aan de rechter worden voorgelegd.

3.17 Geschillen

3.17.1 Nederlands recht

Op eventuele geschillen naar aanleiding van deze aanbestedingsprocedure, de selectie, de gunning en de Overeenkomst is uitsluitend Nederlands recht van toepassing. Geschillen dienen te worden voorgelegd aan de bevoegde rechter te Amsterdam.

3.17.2 Rechtsbescherming en opschortende termijn

Indien een ondernemer zich niet kan verenigen met de inhoud van de aanbestedingstukken, de beantwoording van vragen in het kader van de Nota van Inlichtingen of de reactie van de Gemeente op klachten van ondernemer, dan dient de ondernemer voor de in de planning, zoals te vinden in paragraaf 2.11 genoemde inleverdatum een kort geding aanhangig te maken op straffe van verval van recht.

Indien een Gegadigde/Inschrijver rechtsmaatregelen wil treffen tegen de selectie/gunningsbeslissing van de Gemeente, dient de Inschrijver uiterlijk op de in de planning, zoals te vinden in paragraaf 2.11 genoemde datum einde standstill-periode, door betekening van een dagvaarding een kort geding bij de Rechtbank in Amsterdam aanhangig te hebben gemaakt. Een kopie van de dagvaarding dient zo snel mogelijk aan de contactpersoon van deze aanbesteding te worden gemaild. Indien niet binnen de bezwaartermijn na de dag van verzending van de selectie/gunningsbeslissing een kort geding aanhangig is gemaakt, kan de Gemeente overgaan tot het sluiten van de Overeenkomst. Inschrijvers kunnen na het verstrijken van de opschortende termijn geen rechtsmaatregelen meer treffen ten aanzien van de selectie/gunningsbeslissing van de Gemeente.

3.18 Verzoek tot Deelname door een combinatie

Een combinatie bestaat uit meerdere hoofdopdrachtnemers die gezamenlijk als één Gegadigde een Verzoek tot Deelname indienen. Indien het Verzoek tot Deelname geschiedt door een combinatie, dan dient elk lid van een combinatie een volledig ingevuld en ondertekend exemplaar van het Uniform Europees Aanbestedingsdocument in te dienen. Voorts dient elk lid van de combinatie in Deel 2, 4 en 5 van het Uniform Europees Aanbestedingsdocument aan te geven voor welke geschiktheidseisen een beroep op zijn onderneming wordt gedaan.

Na de datum van indienen van het Verzoek tot Deelname is het niet meer mogelijk om een al gevormde combinatie te wijzigen, tenzij dit geschiedt na schriftelijke toestemming van de Gemeente. Het verzoek om wijziging zal in ieder geval worden afgewezen indien de wijziging volgens de Gemeente in strijd is met het (Europese) aanbestedingsrecht.

Ondernemingen die in combinatie aanmelden zijn hoofdelijk aansprakelijk voor de nakoming van alle uit de Overeenkomst voortvloeiende verplichtingen. Bij eventuele gunning van de Opdracht aan een combinatie, zal deze combinatie een rechtsvorm aannemen, waarmee de Gemeente de Overeenkomst zal sluiten. De combinatie dient tevens een penvoerder aan te wijzen.

3.19 Aanmelden met beroep op derden

Gegadigde kan zich voor het voldoen aan de gestelde eisen ook beroepen op de financieel economische draagkracht dan wel technische en/of beroepsbekwaamheid van derden. Een voorwaarde bij het beroep op deze derde(n) is dat Gegadigde kan aantonen dat hij daadwerkelijk kan beschikken over de voor die Opdracht noodzakelijke middelen van deze derde(n).

Zowel in geval van intra-concernrelaties als in geval van een genomineerde onderaannemer dient Gegadigde in Deel 2, 4 en 5 het Uniform Europees Aanbestedingsdocument aan te geven voor welke geschiktheidseisen Gegadigde een beroep op deze derde(n) doet.

Het wijzigen van een 'genomineerde derde' gedurende de aanbestedingsprocedure of de looptijd van de Overeenkomst is slechts mogelijk na schriftelijke toestemming van de Gemeente. Gegadigde dient hierom tijdig schriftelijk een verzoek te doen aan de Gemeente. Het verzoek zal in ieder geval worden afgewezen als de wijziging volgens Gemeente in strijd is met het (Europese) aanbestedingsrecht.

3.20 Onderaannemers

Gegadigde dient in zijn Verzoek tot Deelname tevens op te geven of, en zo ja wie, Gegadigde voornemens is voor de uitvoering van de Opdracht in te zetten als onderaannemer. Een onderaannemer is een partij die onder de verantwoordelijkheid van de Opdrachtnemer werkzaamheden zal verrichten in het kader van de Opdracht.

Het wijzigen van een onderaannemer gedurende de offertefase (dus na afloop van de selectiefase) of gedurende de looptijd van de Overeenkomst is slechts mogelijk na schriftelijke toestemming van de Gemeente. Inschrijver/Opdrachtnemer dient hiervoor tijdig schriftelijk een verzoek te doen aan de Gemeente. Het verzoek zal in ieder geval worden afgewezen als de wijziging volgens de Gemeente in strijd is met het (Europese) aanbestedingsrecht.

3.21 Concurrentie bevorderende maatregelen

Het is toegestaan dat een geïnteresseerde onderneming bij meerdere Verzoeken tot Deelname betrokken is, mits dit niet strijdig is met het onderstaande:

- Ondernemingen kunnen slechts éénmaal als Gegadigde aanmelden, hetzij als individuele (zelfstandige) onderneming, hetzij in een combinatie met andere ondernemingen.
- Indien meerdere ondernemingen binnen één concern geïnteresseerd zijn, is het deelnemen aan de aanbestedingsprocedure slechts mogelijk indien zij zich inschrijven als één Gegadigde.
- Indien meerdere ondernemingen binnen één concern bij meerdere Gegadigden betrokken zijn, dient de moedermaatschappij te bepalen welke onderneming binnen het concern zich terugtrekt. Indien de moedermaatschappij een keuze binnen zeven kalenderdagen na een verzoek daartoe door de Gemeente achterwege laat, zal door de Gemeente worden overgegaan tot een keuze op basis van loting.

3.22 Belangenverstrengeling

De Gemeente kan een ondernemer van (verdere) deelname aan de aanbestedingsprocedure uitsluiten als:

- deze aan de zijde van de Gemeente betrokken is, of is geweest, bij de (voorbereiding van de) aanbesteding,
- deze zich bedient van ondernemingen, adviseurs, medewerkers en andere (rechts)personen die betrokken zijn of zijn geweest bij de (voorbereiding van de) aanbesteding. Datzelfde geldt als (rechts)personen uit de groep van de Ondernemer een dergelijke betrokkenheid hebben of hadden.

De Gemeente zal een ondernemer niet uitsluiten als die aantoont dat onder de omstandigheden van het concrete geval de mededinging door bedoelde betrokkenheid niet is of wordt belemmerd.

3.23 Sanctiepakket Rusland

In het vijfde EU-sanctiepakket van vrijdag 8 april 2022 hebben de lidstaten afgesproken dat het verboden is voor aanbestedende diensten en speciale sectorbedrijven om nieuwe opdrachten te gunnen aan Russische partijen gevestigd in de Russische Federatie, met inbegrip van dochters in de

Europese Unie gevestigd die door deze partijen gecontroleerd of aangestuurd worden. Als gevolg hiervan zal de Gemeente een ondernemer van verdere deelname van de aanbestedingsprocedure uitsluiten als:

- a. De onderneming gedreven wordt voor rekening van een Russisch onderdaan of een in Rusland gevestigde natuurlijk persoon, rechtspersoon, entiteit of lichaam.
- b. De onderneming voor meer dan 50% direct of indirect in handen is van een entiteit als bedoeld in 3.23 onder a.
- c. De onderneming handelt of op aanwijzing van een entiteit als bedoeld in 3.23 onder a.
- d. De onderneming gebruik maakt van een onderaannemer, leverancier of andere entiteit, waarbij de prestatie van deze betrokkenen meer dan 10% van de onderhavige Opdracht vertegenwoordigt terwijl tevens voor deze betrokkenen een van bovenstaande vragen a t/m c met "ja" beantwoord moet worden

Door het indienen van een Verzoek tot Deelname verklaart Gegadigde dat geen van de bepalingen 3.6 a t/m d op zijn onderneming van toepassing zijn. Mocht uit een screening van de Gemeente blijken dat deze bepalingen wel van toepassing zijn op Opdrachtnemer na het sluiten van de Overeenkomst is de Gemeente gerechtigd de Overeenkomst per direct te beëindigen.

4 Selectieprocedure

De mededingingsprocedure met onderhandeling is een procedure in twee fases. De eerste fase, waarin de Gegadigden worden geselecteerd, is openbaar. In de tweede fase worden de geselecteerde Gegadigden/Inschrijvers uitgenodigd voor deelname aan de gunningsfase en mogen ze een Inschrijving indienen. Hieronder vindt Gegadigde informatie over de selectieprocedure.

4.1 Beoordeling van de aanmelding

De ontvangen Verzoeken tot Deelname worden beoordeeld door het beoordelingsteam. De beoordeling bestaat uit een aantal fases:

1. Vaststellen van de volledigheid en juistheid van het Verzoek tot Deelname;
2. Beoordelen dat Uitsluitingsgronden niet op Gegadigde van toepassing zijn en dat Gegadigde voldoet aan de geschiktheidseisen 5;
3. Selecteren Gegadigden;
4. Bekend maken resultaat van de beoordeling.

4.2 Selecteren Gegadigden

Indien de toets zoals bedoeld in paragraaf 4.1 onder 1 en 2 niet leidt tot uitsluiting c.q. ongeldigverklaring, wordt het Verzoek tot Deelname verder inhoudelijk beoordeeld. Er worden maximaal vijf Gegadigden geselecteerd voor deelname aan de gunningsfase. Dat betekent dat, indien meer dan vijf Gegadigden aan de gestelde Uitsluitingsgronden en minimumvereisten voldoen, de Gemeente het aantal Gegadigden op basis van de Selectiecriteria, zoals beschreven in hoofdstuk 66 zal terugbrengen tot vijf.

4.3 Bekend maken resultaat beoordeling

De Gegadigden zullen op de hoogte worden gesteld van het resultaat van de beoordeling.

De geselecteerde Gegadigden worden geïnformeerd over het feit dat ze zijn geselecteerd en dat ze worden uitgenodigd tot het doen van een Inschrijving.

De Gegadigden die niet voldoen of niet zijn geselecteerd worden daar schriftelijk over geïnformeerd. Zij ontvangen schriftelijk de resultaten van de uitgevoerde beoordeling, inclusief de individuele plaats in de rangorde (waarbij de namen van de andere Gegadigden om commerciële redenen anoniem blijven).

De Gemeente is niet verplicht om documenten die betrekking hebben op deze aanbesteding, zoals resultaten van individuele beoordelingen, vergelijkingen en adviezen binnen het beoordelingsteam betreffende kwalificatie en gunning, aan Gegadigden bekend te maken.

4.4 Opvragen bewijsmiddelen

De Gemeente kan gebruik maken van de mogelijkheid om naar aanleiding van het ingevulde Uniform Europees Aanbestedingsdocument de vooraf benoemde bewijsmiddelen op te vragen ter verificatie. In paragraaf 5.1.1 staat vermeld welke bewijsmiddelen de Gemeente in dat geval op zal kunnen vragen.

5 Eisen ten aanzien van Gegadigde

De Gegadigden worden op basis van het ingediende Verzoek tot Deelname beoordeeld. Dit hoofdstuk geeft de Uitsluitingsgronden en de Geschiktheidseisen weer waaraan de organisatie van Gegadigde dient te voldoen. De Gemeente wijst Gegadigde erop dat alle in deze Selectieleidraad gevraagde gegevens juist, volledig, op correcte wijze en op tijd dienen te worden aangeleverd. Indien sprake is van het overleggen van onjuiste, onvolledige dan wel niet correcte aanbieding van de gevraagde gegevens, kan dit leiden tot uitsluiting.

5.1 Uitsluitingsgronden

Het ingediende Verzoek tot Deelname van de Gegadigde wordt eerst gecontroleerd op Uitsluitingsgronden. De Uitsluitingsgronden zijn opgenomen in het Uniform Europees Aanbestedingsdocument (Bijlage 7.2). Indien op een Gegadigde een Uitsluitingsgrond van toepassing is, en de Gemeente besluit geen toepassing te geven aan artikel 2.88 Aw, wordt het betreffende Verzoek tot Deelname terzijde gelegd en komt dit niet in aanmerking voor verdere (inhoudelijke) beoordeling.

Gegadigde verklaart door het invullen en ondertekenen van het Uniform Europees Aanbestedingsdocument dat de omstandigheden zoals benoemd in deze verklaring niet op de onderneming van Gegadigde van toepassing zijn en dat Gegadigde in de verificatiefase (na voorlopige gunning) de eventueel verlangde bewijsstukken/verklaringen zoals bedoeld in artikel 2.89 Aw op het eerste verzoek van de Gemeente kan verstrekken. Het gebruik van het Uniform Europees Aanbestedingsdocument houdt in dat de selectiefase of inschrijffase van een aanbesteding voor de Uitsluitingsgronden en de Geschiktheidseisen slechts het Uniform Europees Aanbestedingsdocument afgegeven wordt, zonder dat er nadere informatie wordt verstrekt. Doel van het Uniform Europees Aanbestedingsdocument is dat alleen van de geselecteerde Gegadigden

de inlichtingen en gegevens uit het Uniform Europees Aanbestedingsdocument worden geverifieerd.

5.1.1 Bewijsmiddelen

Om te bewijzen dat van de in het UEA genoemde omstandigheden geen sprake is, dienen de volgende bewijsstukken te worden overlegd.

- Gegadigde kan door middel van een uittreksel uit het handelsregister aantonen dat de uitsluitingsgrond als bedoeld in Deel 3 onder punt C van het 'Uniform Europees Aanbestedingsdocument' op hem niet van toepassing is.
- Gegadigde kan door middel van een Gedragsverklaring Aanbesteden, die op het tijdstip van het indienen van de Verzoek tot Deelname niet ouder is dan twee jaren, aantonen dat de Uitsluitingsgronden, voor zover het een onherroepelijke veroordeling of een onherroepelijke beschikking wegens overtreding van de mededingingsregels betreft, op hem niet van toepassing zijn. Een Gedragsverklaring Aanbesteden kan worden aangevraagd via <https://www.justis.nl/producten/gedragsverklaring-aanbesteden-gva>. Dit bewijsmiddel dient eerst te worden afgegeven nadat de Gemeente hiertoe een verzoek doet.
- Gegadigde kan door middel van een verklaring van de Belastingdienst, die op het tijdstip van het indienen van het Verzoek tot Deelname niet ouder is dan zes maanden, aantonen dat de Uitsluitingsgrond, bedoeld in Deel 2 onder punt B van het 'Uniform Europees Aanbestedingsdocument' niet op hem van toepassing is. Dit bewijsmiddel dient eerst te worden afgegeven nadat de Gemeente hiertoe een verzoek doet.

Indien een ondertekend Uniform Europees Aanbestedingsdocument geen deel uitmaakt van het Verzoek tot Deelname wordt het Verzoek tot Deelname uitgesloten van verdere beoordeling.

5.2 Geschiktheidseisen

Daarna wordt de geschiktheid van Gegadigde voor de uitvoering van de dienstverlening vastgesteld. Voor het bepalen van de geschiktheid zijn diverse criteria vastgesteld. Alle Geschiktheidseisen betreffen minimumeisen. Dit houdt in dat voor iedere eis afzonderlijk een op onderhavige aanbesteding afgestemd minimum is vastgesteld waaraan Gegadigde moet voldoen. Het Verzoek tot Deelname van een Gegadigde die niet voldoet aan één of meerdere van deze eisen wordt terzijde gelegd en komt niet in aanmerking voor verdere (inhoudelijke) beoordeling.

5.2.1 Financieel economische draagkracht

In Deel 4 van het Uniform Europees Aanbestedingsdocument verklaart Gegadigde dat zijn onderneming voldoet aan de gestelde eisen met betrekking tot financieel economische draagkracht.

- (i) Jaarrekeningen. Ter toetsing van de financiële draagkracht dient er op basis van de vastgestelde en door een accountant goedgekeurde jaarrekeningen van de afgelopen drie jaar (2019, 2020 en 2021) geen sprake te zijn van negatief (eigen) vermogen. Indien het (eigen) vermogen positief is door het verstrekken van achtergestelde leningen (aansprakelijk vermogen) met korte looptijd (tot drie jaar) wordt het (eigen) vermogen als zijnde negatief beschouwd.
- (ii) Jaarrekeningen. In de meest recente jaarrekening is geen sprake van continuïteitsrisico (blijkens een continuïteitsparagraaf).
- (iii) Risico's. Bij de onderneming van Gegadigde is op dit moment of in de nabije toekomst geen sprake van aanwezige c.q. mogelijke risico's die de continuïteit van de organisatie kunnen beïnvloeden.

5.2.2 Verzekering

Gegadigde beschikt over een adequate verzekering voor beroepsaansprakelijkheid (BAV). De Gegadigde dient per gebeurtenis voor minimaal 2.500.000 euro verzekerd te zijn. Gegadigde dient verzekerd te blijven gedurende de duur van de Overeenkomst. Daarnaast dient Gegadigde marktconform verzekerd te zijn voor bedrijfsaansprakelijkheid (AVB).

5.2.3 Technische bekwaamheid

De Gemeente stelt in dit kader minimeisen aan Gegadigden op het gebied van technische bekwaamheid. De Gemeente kan van Gegadigde eisen om de opgegeven informatie naar aanleiding van het gestelde in deze paragraaf nader te onderbouwen dan wel van bewijzen te voorzien.

De technische bekwaamheid wordt voornamelijk bepaald door de wijze waarop de kwaliteitsborging en kwaliteitscontrole is georganiseerd in de organisatie van Gegadigde.

- (i) De beveiliging van informatie van de te verwerken gegevens wordt voornamelijk bepaald door de wijze waarop deze kwaliteitsborging en kwaliteitscontrole is georganiseerd in de organisatie van Gegadigde. Daarbij dient vanzelfsprekend te worden voldaan aan de gestelde wettelijke kaders. Gegadigde dient te beschikken over een informatie-beveiligingssysteem dat door een officiële certificeringsinstantie is gecertificeerd op basis van NEN-ISO: 27001: 2013 met een bijbehorende VVT-verklaring welke de gehele scope (ontwikkelen, technisch beheren, hosten) afdekt.

Gegadigde kan worden verzocht één van de volgende bewijsmiddelen te verstrekken:

- a. een afschrift van een geldig NEN-ISO 27001 certificaat met bijbehorende VVT-verklaring of vergelijkbaar.

- (ii) Referenties, voorzien van een door een referent te ondertekenen 'tevredenheidsverklaring' waarmee Gegadigde de in onderstaande paragrafen 5.2.4 en/of 5.2.5 genoemde kerncompetenties aantoont.

Per kerncompetentie dient Gegadigde één (1) referentie te verstrekken. Een referentieopdracht moet zijn uitgevoerd in de drie jaar voorafgaand aan de uiterste datum van indienen van het Verzoek tot Deelname. De referentieopdracht hoeft niet te zijn afgerond. Voor het indienen van de referenties dient u gebruik te maken van de referentiesjablonen in Bijlagen 7.3 en 7.4.

NB. De in de referentiesjablonen beschreven competenties dienen met meetbare prestatie-indicatoren te worden onderbouwd: accuraat, verifieerbaar, onweerlegbaar/ niet betwistbaar, vertaling naar de betreffende opdracht, (prestatie)metingen in termen van getallen, percentages of tijd.

- (iii) De Gegadigde is voor de eigen bedrijfsvoering ten minste in het bezit van een gecertificeerd milieumanagementsysteem zoals ISO 14001, EMAS, of gelijkwaardig.

Gelijkwaardigheid van een milieumanagementsysteem kan worden aangetoond op basis van de volgende criteria:

- Kwantificeerbare impact voor de gehele bedrijfsvoering van de Gegadigde,
- Onafhankelijk getoetste resultaten.

5.2.4 Kerncompetenties voor het Netwerkknooppunt

Kerncompetentie 1

Het gedurende een periode van minimaal 3 jaar bij een gemeente met minimaal 100.000 inwoners of een overheidsinstelling met minimaal 5.000 medewerkers ter beschikking stellen, configureren, beheren en (door)ontwikkelen van een Netwerkknooppunt in een multi-sourcing omgeving. Onder multi-sourcing omgeving verstaat de Gemeente een IT-infrastructuur van een organisatie waarvan naast het Netwerkknooppunt ten minste 1 ander onderdeel is uitbesteedt aan een leverancier anders dan de leverancier van het Netwerkknooppunt.

Toelichting In deze kerncompetentie is het van belang dat de leverancier inhoudelijke kennis en ervaring heeft met het ontwerpen van en verbinding leggen met overheidskoppelingen en -API's. Deze maken gebruik van open standaarden en overheidsstandaarden. Dit wijkt af van een Netwerkknooppunt in de commerciële sector, vandaar dat de Gemeente deze kerncompetentie heeft beperkt tot gemeenten en overheidsinstellingen van een bepaalde omvang.

Kerncompetentie 2

Het gedurende een periode van minimaal 3 jaar bij een gemeente met minimaal 100.000 inwoners of een overheidsinstelling met minimaal 5.000 medewerkers beveiligen van een Netwerkknooppunt conform wettelijke regelgeving voor de overheid voor informatiebeveiliging, de Baseline Informatiebeveiliging Overheid (BIO) en NEN7510.

Toelichting In deze kerncompetentie is het van belang dat de leverancier inhoudelijke kennis en ervaring heeft met het beveiligen van een Netwerkknooppunt conform wettelijke regelgeving voor de overheid voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Commerciële organisaties hebben niet te maken met de BIO, vandaar dat de Gemeente deze kerncompetentie heeft beperkt tot gemeenten en overheidsinstellingen van een bepaalde omvang.

Kerncompetentie 3

In de afgelopen drie jaar bij een gemeente met minimaal 100.000 inwoners, een overheidsinstelling met minimaal 5.000 medewerkers of een commerciële organisatie met minimaal 5.000 medewerkers een veilige ontsluiting van connectiviteit hebben geïmplementeerd op basis van het Zero Trust Security Model (zie paragraaf 2.8.3 voor meer informatie over dit model).

5.2.5 Kerncompetenties voor Generieke security diensten

Kerncompetentie 1

Het gedurende een periode van minimaal 3 jaar bij een gemeente met minimaal 100.000 inwoners of een andere overheidsinstelling met minimaal 5.000 medewerkers ter beschikking stellen, beheren en (door)ontwikkelen van ten minste drie van de vijf in paragraaf 2.8.4 beschreven security diensten, waarbij in ieder geval de threat intelligence dienst deel uitmaakt van de dienstverlening.

Toelichting Het dreigingsbeeld van de overheid is afwijkend van het dreigingsbeeld van een commerciële organisatie. Er zijn uitsluitend overheidsorganisaties voor threat intelligence aangesloten op het Nationaal Detectie Netwerk van het NCSC. Daarnaast geldt voor alle security diensten dat deze de Gemeente moeten beveiligen conform wettelijke regelgeving voor de overheid voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Commerciële organisaties hebben niet te maken met de BIO, vandaar dat de Gemeente deze kerncompetentie heeft beperkt tot gemeenten en overheidsinstellingen van een bepaalde omvang.

Kerncompetentie 2

Het gedurende een periode van minimaal 3 jaar bij een gemeente met minimaal 100.000 inwoners, een overheidsinstelling met minimaal 5.000 medewerkers of een commerciële organisatie met minimaal 5.000 medewerkers ter beschikking stellen en beheren van ten minste drie van de vijf in paragraaf 2.8.4 beschreven security diensten, waarbij de leverancier ervoor zorgt dat de aangeboden diensten de Gemeente voortdurend en op adequate wijze blijven beschermen tegen het actuele dreigingslandschap en blijven aansluiten bij de IT infrastructuur van opdrachtgever, zonder dat de Gemeente hiervoor aanvullende diensten moet afnemen. Dit geldt ook voor de aan de diensten onderliggende oplossingen en tooling, inclusief de configuratie hiervan, waarbij de oplossingen en tooling op efficiënte wijze blijven werken.

Kerncompetentie 3

Het gedurende een periode van minimaal 3 jaar bij een gemeente met minimaal 100.000 inwoners, een overheidsinstelling met minimaal 5.000 medewerkers of een commerciële organisatie met minimaal 5.000 medewerkers ter beschikking stellen en beheren van ten minste drie van de vijf in

betreffende paragraaf in de scope beschreven security diensten, waarbij de security diensten zo zijn ingericht dat deze een samenhangend geheel vormen. Met samenhangend geheel wordt bedoeld dat de output van de ene security dienst als input dient voor een of meer andere diensten. Een bijvoorbeeld hiervan is het gebruik van dreigingsinformatie vanuit de Cyber threat intelligence dienst als input voor de ontwikkeling van nieuwe use cases in de Monitoring en incident response dienst.

In deze kerncompetentie wordt de output van iedere dienst minimaal (eventueel handmatig) gebruikt als input voor ten minste één van de andere twee diensten. Bij de betreffende referentie dient een voorbeeld rapportage te worden gevoegd inclusief de samenhang van deze diensten (bijvoorbeeld de mapping van dreigingen vanuit de threat intelligence dienst naar de ontwikkeling van nieuwe use-cases in de monitoring en responsdienst).

Kerncompetentie 4

Het gedurende een periode van minimaal 3 jaar bij een gemeente met minimaal 100.000 inwoners, of een overheidsinstelling met minimaal 5.000 medewerkers leveren van een monitoring en incident response dienst, zoals beschreven in paragraaf 2.8.4, waarbij ten minste één van de drie afhankelijke dienstonderdelen (forensisch onderzoek, CSIRT team en de ontwikkeling, integratie, automatisering en validatie van use cases) onderdeel is van de dienst. Dit om zo min mogelijk afhankelijkheden van andere diensten te creëren, waardoor een snelle response op security incidenten mogelijk is.

Toelichting Het dreigingsbeeld van de overheid is afwijkend van het dreigingsbeeld van een commerciële organisatie. Daarnaast is de wijze waarop wordt omgegaan met security incidenten afwijkend omdat overheden met elkaar samenwerken via het Nationaal Detectienetwerk. De Gemeente heeft deze kerncompetentie daarom beperkt tot gemeenten en overheidsinstellingen van een bepaalde omvang.

5.3 Verificatie bewijsstukken

Voor het verlichten van de administratieve lasten voor zowel Gegadigde als de Gemeente, dienen alleen Gegadigden die zijn geselecteerd om door te gaan naar de volgende fase (gunning), uiterlijk één (1) week na dagtekening van het schriftelijke verzoek hiertoe van de Gemeente de bij het Uniform Europees Aanbestedingsdocument behorende bewijsstukken aan te leveren.

De Gemeente kan tot het einde van de gunningsfase om verduidelijking vragen.

Indien de inhoud van de gevraagde bewijsstukken van een Gegadigde niet overeenkomt met wat in het Uniform Europees Aanbestedingsdocument is gesteld, wordt het betreffende Verzoek tot Deelname ongeldig verklaard en wordt Gegadigde alsnog uitgesloten van verdere deelname aan deze aanbestedingsprocedure. In dat geval komen de eerstvolgende Gegadigden in rangorde (de nummer '6', '7', ...) alsnog in aanmerking voor deelname.

6 Selectiecriteria

Dit hoofdstuk verwoordt per perceel een aantal vragen dat betrekking heeft op de organisatie van de Gegadigde. Tenzij expliciet anders vermeld, dienen alle voor een bepaald perceel relevante vragen te worden beantwoord.

6.1 Algemeen

Indien meer dan vijf Gegadigden aan de gestelde minimumvereisten voldoen wordt het aantal teruggebracht naar vijf door het vaststellen van een rangorde op basis van de antwoorden op de Selectiecriteria.

In de paragrafen 6.2 en 6.3 worden vragen gesteld over de kwaliteit van de organisatie van de onderneming van Gegadigde. De door Gegadigden in het kader van het Verzoek tot Deelname aangeleverde informatie wordt door het beoordelingsteam beoordeeld.

Nadere toelichting beoordeling Selectiecriteria

De Gemeente hecht veel waarde aan een degelijke, consistente en verifieerbare onderbouwing van de antwoorden, waarmee Gegadigde aantoont dat hij hetgeen hij beschrijft waar kan maken, of waar heeft gemaakt. De onderbouwing is bondig en dient plaats te vinden aan de hand van informatie, documentatie, praktijkvoorbeelden, referenties en dergelijke. De beschrijving hiervan moet in het antwoord worden opgenomen. Verwijzingen naar bijlagen, handboeken en/of websites zijn niet toegestaan. Indien hiernaar wordt verwezen, worden de teksten hiervan niet meegenomen in de beoordeling. Aspecten van een antwoord dat niet voldoende onderbouwd is, worden door de Gemeente in beginsel buiten beschouwing gelaten.

Naast de onderbouwing van het antwoord beoordeelt de Gemeente het antwoord op relevantie, toepasbaarheid en haalbaarheid.

6.2 Selectiecriteria voor het Netwerkknooppunt (P1)

Criterium 1 De Gemeente is op zoek naar een leverancier met voldoende kennis en expertise van het ter beschikking stellen, configureren, beheren en (door)ontwikkelen van een Netwerkknooppunt in een multi-sourcing omgeving. Zie paragraaf 2.8.3 voor meer informatie over multi-sourcing.

Gegadigde kan op basis van maximaal twee (2) referenties aantonen hoe breed zijn ervaring is met netwerken in complexe multi-sourcing omgevingen.

Beoordelingsmethodiek:

- Indien een referentie een multi-sourcing omgeving betreft waarin naast het Netwerkknooppunt twee andere onderdelen zijn uitbesteedt aan verschillende leveranciers anders dan de leverancier van het Netwerkknooppunt: 4 punten.

- Indien een referentie een multi-sourcing omgeving betreft waarin naast het Netwerkknooppunt meer dan twee andere onderdelen zijn uitbesteedt aan verschillende leveranciers anders dan de leverancier van het Netwerkknooppunt: 8 punten.

De maximale score is 16 punten voor twee referenties.

Criterium 2 Gegadigde dient doorlopend zorg te dragen voor de continuïteit en kwaliteit van het Netwerkknooppunt, ook indien de aangesloten uitbestede, (Infrastructurele) diensten wijzigen, zonder dat de Gemeente hiervoor aanvullende diensten hoeft af te nemen.

Dit betekent dat er gedurende de looptijd van de Overeenkomst met een zekere regelmaat snelle wijzigingen in het Netwerkknooppunt moeten worden doorgevoerd, zoals het openzetten van een poort of het aanpassen van routeringen.

Om haar expertise en ervaring op dit vlak aan te tonen, kan Gegadigde een referentie aanleveren van een gemeente met minimaal 100.000 inwoners of een andere overheidsinstelling met minimaal 5.000 medewerkers, waarbij zij het bij deze organisatie geïmplementeerde proces beschrijft waarmee zij borgt dat het Netwerkknooppunt up-to-date blijft en aan blijft sluiten bij de aangesloten, uitbestede (Infrastructurele) diensten.

Het antwoord op deze vraag wordt beoordeeld op basis van de volgende schaal:

- 0 punten - geen wijzigingsproces voor het Netwerkknooppunt ingericht;
- 4 punten - wijzigingsproces voor het Netwerkknooppunt en gedocumenteerd;
- 8 punten - wijzigingsproces voor het Netwerkknooppunt ingericht en gedocumenteerd, inclusief prioriteringsmogelijkheden;
- 12 punten - risico gebaseerd wijzigingsproces voor het Netwerkknooppunt ingericht.

Maximaal 12 punten voor een referentie.

Criterium 3 De Gemeente is op zoek naar een leverancier met voldoende kennis en expertise van het beveiligen van het Netwerkknooppunt voor de Gemeente. Zie paragraaf 2.8.3 voor meer informatie over de beveiliging van een Netwerkknooppunt.

Gegadigde kan op basis van maximaal twee (2) referenties aantonen hoeveel ervaring hij heeft met de beveiliging van een Netwerkknooppunt. De referenties dienen afkomstig te zijn van een gemeente met minimaal 100.000 inwoners of een andere overheidsinstelling met minimaal 5.000 medewerkers.

Beoordelingsmethodiek:

- 3 punten - een referentie betreft een ISO27001 of NEN7510 certificering of gelijkwaardig.
- 3 extra punten - een referentie toont aanvullend aan dat de opzet, het bestaan en werking van de bij 1. gecertificeerde processen is geborgd, bijvoorbeeld door een ISAE3402 type 2 verklaring niet ouder dan een (1) jaar.

Maximaal 12 punten voor twee referenties.

Criterium 4 De Gemeente is op zoek naar een leverancier met voldoende kennis en expertise van het Zero Trust Security Model voor connectiviteit. Zie paragraaf 2.8.3 voor meer informatie over dit model.

Om haar expertise en ervaring op dit vlak aan te tonen, kan Gegadigde maximaal twee (2) referenties aanleveren van een gemeente met minimaal 100.000 inwoners of een andere overheidsinstelling met minimaal 5.000 medewerkers, waarbij zij een veilige ontsluiting van connectiviteit hebben geïmplementeerd op basis van het Zero Trust Security Model. Iedere referentie dient te worden voorzien van het plan van aanpak op basis waarvan de implementatie is uitgevoerd.

Beoordelingsmethodiek:

- 8 punten per volledige referentie, inclusief plan van aanpak.

Maximaal 16 punten voor twee referenties.

Criterium 5 De ICT-infrastructuur van de Gemeente is complex en uitdagend, waardoor het belangrijk is dat de kennis van de leverancier voor het Netwerkknooppunt up-to-date en kwalitatief hoogwaardig is.

Beschrijf in welke mate u kennis op het gebied van netwerktechnieken en ontwikkelingen binnen connectiviteit, zoals netwerkarchitectuur, governance en delivery, actief uitdraagt. Hierbij kunt u bijvoorbeeld benoemen of u actief deelneemt/bijdraagt aan relevante communities, aan events en seminars, of publiceert in vakbladen.

Bij deze vraag scoort u hoger a) naarmate het uitdragen van de betreffende kennis minder gerelateerd is aan uw dagelijkse werkzaamheden, b) naarmate uw kennissessies niet alleen gericht zijn op uw eigen medewerkers, maar een groter en/of diverser publiek bereiken, c) naarmate uw kennis wordt uitgedragen via meer gerenommeerde kanalen/gremia, zoals een publicatie in een (wetenschappelijk) tijdschrift of een keynote bij een bepaalde conferentie en d) indien u al dan niet samen met partners en al dan niet in een eigen lab, zelf onderzoek doet op het betreffende vakgebied.

Gegadigde dient deze vraag te beantwoorden in maximaal 1000 woorden. Al het meerdere zal niet in de beoordeling worden meegenomen.

De maximale score voor het antwoord op deze vraag is 12 punten; maximaal 3 punten voor ieder aspect a t/m d.

Criterium 6 De Gemeente kiest ervoor om de CO₂-prestatieladder als kader te hanteren om een duurzame partij te selecteren. De niveaus zijn beschreven in de vigerende versie van de Handreiking Aanbesteden uitgegeven door Stichting Klimaatvriendelijk Aanbesteden & Ondernemen (SKAO). Hoe hoger het aangeboden CO₂-ambitieniveau van Gegadigde is, hoe hoger de score op dit Selectie criterium.

Hiervoor wordt de volgende onderverdeling gehanteerd:

Trede	Punten
CO ₂ -prestatieladder trede 1	0

CO ₂ -prestatieladder trede 2	0
CO ₂ -prestatieladder trede 3	3
CO ₂ -prestatieladder trede 4	4
CO ₂ -prestatieladder trede 5	8

Gegadigde kan aantonen aan een bepaald niveau te voldoen door een CO₂-bewust certificaat in te dienen bij het Verzoek tot Deelname. Heeft Gegadigde géén CO₂-bewust certificaat, dan dient Gegadigde aan te tonen dat aan de trede wordt voldaan door het overhandigen van een verklaring van een onafhankelijke instelling. Bij het overhandigen van een verklaring van een onafhankelijke instelling ligt de bewijslast bij Gegadigde om aan te tonen dat in de beoordeling door deze onafhankelijke instelling een vergelijkbare methode is gehanteerd in de beoordeling als wordt gedaan bij de certificering van het CO₂-bewust certificaat.

Onderstaande tabel geeft per Selectie criterium het maximaal te behalen punten:

	Selectie- criterium	Max. aantal punten
C1: Ter beschikking stellen, configureren, beheren en (door)ontwikkelen van een Netwerkknooppunt in een multi-sourcing omgeving.	1	16
C2: Garanderen van de continuïteit en kwaliteit van het Netwerkknooppunt	2	12
C3: Voldoende kennis en expertise van het beveiligen van het Netwerkknooppunt	3	12
C4: Voldoende kennis en expertise van het Zero Trust Security Model voor connectiviteit.	4	16
C5: Up-to-date en kwalitatief hoogwaardige kennis van het Netwerkknooppunt.	5	12
C6: Duurzame eigen organisatie	6	8

De schaal waarop de vragen worden beoordeeld is bij iedere vraag afzonderlijk aangegeven.

De behaalde scores worden bij elkaar opgeteld en de vijf Gegadigden met de hoogste totaalscore komen in aanmerking voor deelname aan de gunningsfase.

6.3 Selectiecriteria voor Generieke security diensten (P2)

Criterium 1 De Gemeente is op zoek naar een leverancier met voldoende kennis en expertise van het leveren van security diensten, waarbij de security diensten als een samenhangend geheel zijn ingericht en zijn gemapt naar Mitre Att&ck. Met samenhangend geheel bedoelt de Gemeente dat de output van de ene security dienst (handmatig of automatisch) als input dient voor een of meer andere diensten. Een voorbeeld van samenhang is het gebruik van dreigingsinformatie vanuit de cyber threat intelligence dienst als input voor de ontwikkeling van nieuwe use cases in de monitoring en incident response diens.

Gegadigde kan op basis van maximaal 3 referenties aantonen hoe breed zijn ervaring is met samenhangende security diensten.

De op dit Selectiecriterium te behalen score is als volgt:

- 1 punt voor iedere naar Mitre Att&ck gemapte dienst (max. 5 punten)
- ½ punt voor iedere output van een bepaalde dienst die handmatig als input voor een andere dienst wordt gebruikt (max. 10 punten).
- ½ punt extra voor iedere output van een bepaalde dienst die automatisch als input voor een andere dienst wordt gebruikt (max. 10 punten).

Criterium 2 De Gemeente is op zoek naar een leverancier met voldoende kennis en expertise van cyber threat intelligence als all-in dienst (zie paragraaf 2.8.4), waarbij de cyber threat intelligence dienst haar dreigingsinformatie ophaalt uit meer dan één bron.

Om haar expertise en ervaring op dit vlak aan te tonen, kan Gegadigde maximaal 3 referenties aanleveren van een door haar geleverde threat intelligence dienst, waarbij de dreigingsinformatie uit een of meerdere bronnen wordt opgehaald. De Gemeente onderscheidt de volgende bronnen:

- Internet,
- Dark web,
- NDN,
- Eigen SOC van opdrachtgever.

De score op dit Selectiecriterium is 1 punt voor de bronnen Internet, NDN en Eigen SOC van opdrachtgever en 2 punten voor de bron Dark web, voor iedere referentie. De maximale score is dan 15 voor de drie referenties (3x5).

Criterium 3 Het dreigingslandschap van de Gemeente is constant in beweging en de security diensten dienen de Gemeente ten alle tijden te beschermen tegen het actuele dreigingslandschap, zonder dat de Gemeente hiervoor aanvullende diensten hoeft af te nemen. Daardoor zijn er gedurende de looptijd van het contract met een zekere regelmaat snelle wijziging in security diensten gewenst, bijvoorbeeld wijzigingen in de use cases op het SIEM platform en wijzigingen in de play books voor de security incident monitoring dienst.

Om haar expertise en ervaring op dit vlak aan te tonen, kan Gegadigde een referentie aanleveren van een gemeente met minimaal 100.000 inwoners of een andere overheidsinstelling met minimaal 5.000 medewerkers, waarbij zij het bij deze organisatie geïmplementeerde proces beschrijft waarmee zij borgt dat de security diensten up-to-date blijven en blijven beschermen tegen het actuele dreigingslandschap.

Het antwoord op deze vraag wordt beoordeeld op basis van de volgende schaal:

- 0 punten - geen wijzigingsproces voor security diensten ingericht;
- 4 punten - wijzigingsproces voor security ingericht en gedocumenteerd;
- 8 punten - wijzigingsproces voor security diensten ingericht en gedocumenteerd, inclusief prioriteringsmogelijkheden;
- 12 punten - risico gebaseerd wijzigingsproces voor security diensten ingericht;
- 16 punten - geautomatiseerd risico gebaseerd wijzigingsproces voor security diensten ingericht.

Criterium 4 De security omgeving van de Gemeente is complex en uitdagend, waardoor het belangrijk is dat de kennis van de leverancier voor security diensten up-to-date en kwalitatief hoogwaardig is. Beschrijf de wijze waarop u dit borgt in uw organisatie.

- 1) Geef aan of ten minste 70% van uw security personeel aantoonbaar in het bezit is van erkende marktcertificeringen voor security personeel.
Met een positief antwoord op onderdeel 1) van deze vraag scoort u 4 punten. Op verzoek van de Gemeente dient u hiervoor een bewijsmiddel aan te leveren.
- 2) Beschrijf in welke mate u kennis op het gebied van security actief uitdraagt. Hierbij kunt u bijvoorbeeld benoemen of u actief deelneemt/bijdraagt aan relevante communities, aan events en seminars, of publiceert in vakbladen.

Bij deze vraag scoort u hoger naarmate het uitdragen van de betreffende kennis minder gerelateerd is aan uw dagelijkse werkzaamheden, naarmate uw kennissessies niet alleen gericht zijn op uw eigen medewerkers, maar een groter en/of diverser publiek bereiken, naarmate uw kennis wordt uitgedragen via meer gerenommeerde kanalen/gremia, zoals een publicatie in een (wetenschappelijk) tijdschrift of een keynote bij een bepaalde conferentie en indien u al dan niet samen met partners en al dan niet in een eigen lab, zelf onderzoek doet op het betreffende vakgebied.

Gegadigde dient dit onderdeel 2 van deze vraag te beantwoorden in maximaal 1000 woorden. Al het meerdere zal niet in de beoordeling worden meegenomen.

De maximale score voor dit onderdeel 2 van deze vraag is 8 punten.

Criterium 5 Aanbesteder heeft ervoor gekozen de CO₂-prestatieladder als kader te hanteren om de duurzaamste partij te selecteren. De niveaus zijn beschreven in de vigerende versie van de Handreiking Aanbesteden uitgegeven door Stichting Klimaatvriendelijk Aanbesteden & Ondernemen (SKAO). Hoe hoger het aangeboden CO₂-ambitieniveau van Gegadigde is, hoe hoger de score op dit Selectiecriteria.

Hiervoor wordt de volgende onderverdeling gehanteerd:

Trede	Punten
CO ₂ -prestatieladder trede 1	0
CO ₂ -prestatieladder trede 2	0
CO ₂ -prestatieladder trede 3	3
CO ₂ -prestatieladder trede 4	4
CO ₂ -prestatieladder trede 5	8

Gegadigde kan aantonen aan een bepaald niveau te voldoen door een CO₂-bewust certificaat in te dienen bij het Verzoek tot Deelname. Heeft Gegadigde géén CO₂-bewust certificaat, dan dient Gegadigde aan te tonen dat aan de trede wordt voldaan door het overhandigen van een verklaring van een onafhankelijke instelling. Bij het overhandigen van een verklaring van een onafhankelijke instelling ligt de bewijslast bij Gegadigde om aan te tonen dat in de beoordeling door deze onafhankelijke instelling een vergelijkbare methode is gehanteerd in de beoordeling als wordt gedaan bij de certificering van het CO₂-bewust certificaat.

Onderstaande tabel geeft per Selectie criterium het maximaal te behalen punten:

	Selectie- criterium	Max. aantal punten
Voldoende kennis en expertise van het leveren van security diensten, waarbij de security diensten als een samenhangend geheel zijn ingericht en zijn gemapt naar Mitre Att&ck.	1	25
Voldoende kennis en expertise van threat intelligence als all-in dienst	2	15
Bescherming tegen het actuele dreigingslandschap	3	16
Borging van de up-to-date kennis van security diensten	4	12
Duurzame eigen organisatie	5	8

De schaal waarop de vragen worden beoordeeld is bij iedere vraag afzonderlijk aangegeven.

De behaalde scores worden bij elkaar opgeteld en de vijf Gegadigden met de hoogste totaalscore komen in aanmerking voor deelname aan de gunningsfase.

6.4 Ranking en selectiebesluit

Het beoordelingsteam kent de scores in consensus toe. Op basis van deze beoordeling en de uitkomst van de verificatie en screening zullen de beste vijf Gegadigden worden uitgenodigd deel te nemen aan de volgende fase van de aanbesteding. In geval meerdere Gegadigden gelijk op de vijfde plaats eindigen, zal de hoogste score op het belangrijkste criterium de doorslag geven, waarbij een criterium als belangrijker wordt beschouwd indien de maximale score voor het betreffende criterium hoger is. Indien twee criteria voor een bepaald perceel dezelfde maximale score hebben, dan geldt het lager genummerde criterium als belangrijker. Voor P1 geldt bijv. dat C1 en C4 een maximale score van 16 hebben, waarbij C1 lager genummerd is en daarmee belangrijker. Indien dit niet tot een verschil leidt tussen Gegadigden, dan zal er worden geloot welke Gegadigde wordt uitgenodigd om deel te nemen. Iedere Gegadigde ontvangt een brief met afwijzing van dan wel verzoek tot verdere deelname.

De volgorde waarin de vijf Gegadigden zijn geëindigd, speelt in het verdere proces geen rol meer.

6.5 Het gunningscriterium van de aanbesteding

Ten behoeve van het vervolg van de aanbesteding na de selectiefase, de gunningsfase, licht de Gemeente in dit hoofdstuk de gunningscriteria voor die fase alvast op hoofdlijnen toe.

Het gaat hierbij om een indicatie, in het later te publiceren Beschrijvend Document kunnen nog wijzigingen worden doorgevoerd. Daarnaast zullen de gunningscriteria in het Beschrijvend Document meer detail bevatten.

Conform art. 2.114 Aw 2012 zal de Gemeente de Opdracht gunnen op grond van de naar het oordeel van de Gemeente economisch meest voordelige inschrijving. De economisch meest voordelige inschrijving wordt door de Gemeente vastgesteld op basis van de beste prijs-kwaliteitverhouding (BPKV). De precieze invulling van dit criterium zal worden vastgesteld in het Beschrijvend Document. Naar verwachting zal er gebruik worden gemaakt van een bij de Opdracht, of bij een perceel passende variant van de basisformule 'P/Q', waardoor de Opdracht wordt gegund aan de inschrijver die de laagste prijs per eenheid kwaliteit vraagt. Om te voorkomen dat een Inschrijver de Opdracht gegund krijgt met een zeer scherp geprijsde oplossing die voor de Gemeente echter kwalitatief niet acceptabel is, zal waarschijnlijk een minimumkwaliteit worden geëist.

6.5.1 Kwaliteit

De kwaliteit van de Inschrijvingen van de op de handen zijnde procedure wordt beoordeeld middels vier sub-gunningscriteria. Het algehele gunningscriterium is mogelijk als volgt opgebouwd:

Gunningscriteria	Weging
Kwaliteit	100
Architectuurontwerp aangeboden oplossingen en tooling	25
Plan van aanpak Migratie-Implementatie	25
Wensen uit Programma van Eisen en Wensen	40
Service Level Agreement	10

Deze indeling en weging is voorlopig. In het Beschrijvend Document zullen deze definitief worden gemaakt.

6.5.2 Globale uitwerking kwaliteitscriteria

Subcriterium 1: Architectuur onderliggende oplossingen en tooling

Om de gevraagde dienstverlening te kunnen leveren zal de Inschrijver gebruik moeten maken van (samenhangende) oplossingen en tooling. Hierbij zullen er ook koppelingen tot stand moeten worden gebracht met informatiesystemen binnen de Gemeente. Onderdeel van de Inschrijving is een architectuurontwerp van de aangeboden oplossingen, tooling en koppelingen.

Subcriterium 2: Plan van aanpak voor migratie-implementatie

Opdrachtgever wil door de Inschrijver ontzorgd worden. Inschrijver levert een Plan van aanpak voor migratie-Implementatie met daarin:

- De projectorganisatie;
- Het tijdschema van de implementatie;
- Een overzicht van potentiële risico's en de door Inschrijver te nemen mitigerende maatregelen;
- De wijze waarop Inschrijver het Netwerkknooppunt gaat inrichten om het te laten aansluiten bij de uitbestede (Infrastructurele) dienst voor interne connectiviteit en de overige uitbestede (Infrastructurele) diensten.

Subcriterium 3: Meerwaarde van de geleverde diensten

Een van de doelstellingen die de Gemeente in deze aanbesteding nastreeft is het selecteren van een Inschrijver die met de gevraagde dienstverlening zoveel mogelijk meerwaarde creëert voor de Gemeente, bovenop de minimum gestelde eisen die al in het programma van eisen en wensen zijn opgenomen. De geleverde meerwaarde zal worden bepaald door het beoordelen van de antwoorden van de Inschrijver op de wensen van de Gemeente. Deze zullen worden opgenomen in het Programma van Eisen en Wensen. De wensen kunnen betrekking hebben op diverse onderwerpen.

De wensen voor het Netwerkknooppunt (P1) kunnen bijvoorbeeld betrekking hebben op de wijze waarop de Inschrijver zorgt dat het Netwerkknooppunt en de netwerk beveiligingsdiensten flexibel, schaalbaar en betrouwbaar blijven en in lijn met het informatiebeveiligingsbeleid van de Gemeente. Een ander mogelijk onderwerp is de wijze waarop projecten binnen het Netwerkknooppunt worden uitgevoerd, inclusief de implementatie van kostenmanagement.

De wensen voor de Generieke security diensten (P2) kunnen betrekking hebben op de wijze waarop de individuele diensten (zoals beschreven in paragraaf 2.8.4) worden ingericht en uitgevoerd en de mate waarin leverancier de Generieke security diensten als samenhangend geheel kan inrichten en uitvoeren. Een ander mogelijk onderwerp is de implementatie van een adequaat project- en kostenmanagement.

Subcriterium 4: SLA

De voor Opdrachtgever relevante beheereisen (KPI's) zullen in het Beschrijvend Document in het Programma van Eisen en Wensen worden opgenomen. Van Inschrijver wordt verwacht dat hij deze zal inpassen in zijn 'standaard' SLA, aangevuld met door de Inschrijver aangeboden KPI's. Dit SLA zal, met de aanvullend ingebrachte KPI's, worden beoordeeld.

7 Bijlagen

7.1 Gemeentelijke Inkoopvoorwaarden bij IT 2020 [GIBIT 2020] van de VNG

7.2 Amsterdamse bepalingen bij de Algemene Inkoopvoorwaarden

7.3 Referentiesjabloon Netwerkknooppunt (P1)

7.4 Referentiesjabloon Generieke security diensten (P2)