
Bijlage 3 Programma van Eisen
Openbare Europese aanbesteding
PEN testen
Kadaster

Contractnummer: A24-104041

Datum: 12-06-2025

Bijlage 3 Programma van eisen

In deze bijlage zijn de eisen opgenomen die het Kadaster stelt aan de gevraagde dienstverlening. Aan deze eisen moet bij uitvoering van de Overeenkomst worden voldaan, tenzij uit de eis volgt dat bij Inschrijving aan de eis moet worden voldaan. Het niet voldoen aan een of meerdere eisen betekent uitsluiting van verdere beoordeling.

1.1 Dienstverlening algemeen

Nr.	Eisen
1	Opdrachtnemer is bereid om mee te werken aan een contractmanagementoverleg (CMO). Dit overleg heeft ten doel om de afspraken gemaakt in het contract te bewaken en eventueel verdere afspraken te maken. De frequentie is het eerste jaar 1 keer per kwartaal en na het eerste jaar 1 keer per jaar. De frequentie van het CMO kan in overleg tussen partijen worden aangepast. Opdrachtnemer levert minimaal jaarlijks een management rapportage. Naar aanleiding van deze management rapportage vindt een contractmanagementoverleg plaats, eventueel op locatie van de Aanbestedende dienst. In de management rapportage zijn de gegevens van de afzonderlijke Nadere Opdrachten opgenomen: • Naam van de aanvrager; • Afdeling van de aanvrager; • Korte beschrijving van de opdracht; • Totaalbedrag; • Aard van de dienstverlening (PEN test, follow-up PEN test en/of advies); • Normale aanvraag of spoedaanvraag; • Doorlooptijd dienstverlening (vanaf moment aanvraag tot decharge); • KPI's (nog nader af te stemmen met projectgroep). Daarnaast dient Opdrachtnemer ook generieke informatie toe te voegen, zoals: • Eventuele knelpunten of verbeteracties voortkomende uit evaluaties; • Trends en ontwikkelingen op het gebied van informatiebeveiliging. Na gunning is het voor het Kadaster mogelijk om aanvullingen of aanpassingen in de aan te leveren managementinformatie te laten doen, zonder meerkosten voor de het Kadaster.
2	Opdrachtnemer beschikt over een communicatie- en escalatie matrix. Na gunning zullen Opdrachtnemer en het Kadaster hierover afstemmen en dit vastleggen.
3	Het Kadaster heeft het recht een audit uit te voeren om de opzet, het bestaan en de werking van de beveiligingsmaatregelen te toetsen van Opdrachtnemer. Het Kadaster bepaald welk onafhankelijk en algemeen erkend bureau de audit uitvoert. Alle gegevens die door opdrachtnemer tijdens de uitvoering van penetratietests worden verkregen, gegenereerd, verzameld, verwerkt of opgeslagen, dienen uitsluitend binnen de Europese Economische Ruimte (EER) te worden bewaard en verwerkt.

1.2 Algemene eisen m.b.t. het proces

Nr.	Eisen
-----	-------

-
- 4 Opdrachtnemer levert één vaste contactpersoon die beschikt over technische security kennis en die bij alle gesprekken aanwezig is als verbindende factor tussen het Kadaster en de uitvoerende Professionals en zorgt voor continuïteit van kennis gedurende de contractduur. Bij langdurige afwezigheid of vertrek levert de Opdrachtnemer een vaste vervanger.

 - 5 In het beschrijvend document (paragraaf 1.3.1) staat het proces beschreven dat gevolgd wordt bij het uitvoeren van PEN testen en follow-up testen. De opdrachtnemer dient zich houden aan dit proces te conformeren.

 - 6 De PEN test wordt extern of indien nodig intern uitgevoerd.
 1. **Extern:** de PEN test wordt uitgevoerd vanaf een locatie over het publieke netwerk.
 2. **Intern:** de PEN test wordt uitgevoerd vanaf een door het Kadaster aangewezen locatie of vanaf een locatie van een leverancier/dienstverlener van Het Kadaster. Alle eventuele bijkomende kosten (zoals bijvoorbeeld reis- en verblijfskosten) kunnen niet apart verrekend worden en zijn onderdeel van de dienstverlening.

 - 7 Na de aanvraag voor een PEN test zal een intakegesprek binnen 5 werkdagen gepland worden.

 - 8 De Dienstverlening van Opdrachtnemer start een PEN test verzoek met een Nederlandstalig intakegesprek via teams. Tijdens dit intakegesprek wordt in samenspraak met de Opdrachtnemer vastgesteld wat de scope, diepgang en planning van de gevraagde dienst zal zijn. Na het uitvoeren van een intakegesprek levert Opdrachtnemer binnen of uiterlijk op de 10e werkdag een offerte op voor het uitvoeren van de gevraagde PEN test. Deze termijn start op de eerste werkdag nadat Opdrachtnemer de intake heeft uitgevoerd.

 - 9 Het intakegesprek wordt in overleg met het Kadaster ingepland en uitgevoerd. Opdrachtnemer brengt hier geen separate kosten voor in rekening; deze kosten zijn opgenomen in de tarieven voor de uitvoering van de Dienstverlening.

Tijdens het intakegesprek worden in ieder geval de volgende onderwerpen besproken:

 1. het doel van de Dienstverlening;
 - a. de onderzoeksvraag (bijv. welke typen kwetsbaarheden worden gevonden in een systeem, hoe ver kan een hacker binnendringen als hij een bepaalde hoeveelheid tijd heeft);
 2. de scope van de dienst;
 - a. de te onderzoeken applicaties en/of systemen en/of netwerk componenten;
 - b. technische gegevens (bijvoorbeeld IP-adressen en URL's);
 - c. aantallen databases, pagina's, invoervelden, RBAC rollen;
 - d. complexiteiten en speciale aandachtspunten bij het onderzoek;
 - e. onderdelen die expliciet niet worden getoetst;
 - f. Welke omgeving het betreft (ontwikkeling, test, acceptatie, productie);
 - g. Welke normenkaders getoetst moeten worden tijdens de test;
 - h. of het een hertest betreft waarbij resultaten van een eerdere PEN test dienen te worden meegenomen;
 - h. of een hertest noodzakelijk wordt gevonden nadat maatregelen zijn getroffen.
 3. de diepgang van het onderzoek (in hoeverre gebruik maken van kwetsbaarheden op de bewuste omgeving in 2f);
 4. het niveau van voorkennis (black, grey of white box);
 - a. welke informatie beschikbaar wordt gesteld door het Kadaster (afhankelijk van niveau van voorkennis).
 5. de locatie van uitvoering van de PEN test (intern of extern);
 6. communicatie;
 - a. de frequentie van tussentijds voortgangsoverleg;
-

-
7. indien gewenst het soort presentatie(s) en de doelgroep;
 - a. met inhoudelijke diepgang voor technici en security specialisten en/of;
 - b. voor lijnverantwoordelijken en proces-, data- of systeemeigenaren.
 8. of de test dusdanig moet worden uitgevoerd dat detectie van de test (en escalatie via een incident response proces) zoveel mogelijk vermeden wordt;
 9. werkafspraken:
 - a. wat Opdrachtnemer moet doen als er een kritieke kwetsbaarheid wordt gevonden (testen stoppen, rapporteren of doorgaan);
 10. eventuele randvoorwaarden tijdens de uitvoering, bijvoorbeeld dag op locatie;
 11. planningsafspraken;
 - a. de gewenste uitvoerdatum of data;
 - b. de tijden waarop de werkzaamheden worden uitgevoerd;
 - c. een einddatum van de oplevering van het rapport;
 - d. op welke momenten er niet getest mag worden;
 - e. contactpersonen en communicatiekanalen tijdens het uitvoeren van de Dienstverlening;
 - f. doorlooptijden, deadlines;
 - g. testlocatie, in beginsel in Nederland. In gezamenlijk overleg eventueel mogelijk om hier van af te wijken.
-
12. Contact gegevens voor het geval er vragen aan het technische team zijn tijdens de PEN test.
-
- 10 De offerte van Opdrachtnemer is time boxed (vaste tijd, vaste prijs) gespecificeerd en omvat alle gevraagde werkzaamheden voor de Dienstverlening, inclusief de rapportage, maar uitgezonderd een eventuele follow-up PEN test. De offerte zal de maximale tarieven zoals overeengekomen in de Raamovereenkomst niet overschrijden. De offerte omvat ten minste:
- de totaalprijs van de opdrachtomschrijving;
 - een omschrijving van de uit te voeren diensten;
 - een onderbouwing van het benodigd aantal dagen;
 - een specificatie van de uit te voeren werkzaamheden per dagdeel (een dagdeel is 4 uur);
 - een planning;
 - voorwaarden en garanties van dienstverlener t.a.v. de planning;
 - als bijlage een globaal testplan, inclusief risico's per test;
 - te gebruiken PEN test methodiek(en);
 - de namen, functies en certificeringen van Professionals die het zullen uitvoeren;
 - wederzijdse bereikbaarheid tijdens het testen;
 - vertrouwenspersonen (voor het melden van vertrouwelijke bevindingen);
 - locatie van uitvoering van de werkzaamheden (intern of extern);
 - overige relevante bepalingen uit het startgesprek.
-
- 11 Tot 10 werkdagen voor aanvang van de PEN test kan het Kadaster de Dienstverlening kosteloos annuleren of verplaatsen.
-
- 12 Indien er sprake is van spoed (bijvoorbeeld kritieke dienst, publieke security incidenten) dient Opdrachtnemer binnen 5 dagen te starten met de PEN test. Spoedaanvragen zijn zeer uitzonderlijk, in de afgelopen 5 jaren is het één keer voorgekomen. De uurtarieven zoals die door u worden opgenomen in het Prijzenblad zijn hier ook van toepassing, **hierop mag een toeslag van 25% worden berekend.**
-
- 13 Na afronding van de uitvoering van de PEN test levert Opdrachtnemer binnen 10 werkdagen een concept rapportage op.
-
- 14 Het opleveren van de rapportage wordt door Opdrachtnemer via een veilige bestandsoverdracht met het Kadaster gedeeld.
-

-
- 15 Opdrachtnemer staat toe dat het Kadaster de bevindingen uit de PEN test, inclusief onderliggende rapportages of delen daarvan, deelt met derden indien het Kadaster dit noodzakelijk acht voor de opvolging of beoordeling van de testresultaten. Het Kadaster draagt in een dergelijk geval de verantwoordelijkheid voor het verder verspreiden van deze informatie en de vertrouwelijkheid hiervan.
-
- 16 De bevindingen, aanbevelingen en conclusies van de PEN test dienen te worden opgeleverd in een Nederlandstalig, schriftelijke rapportage.
-
- 17 Het Kadaster eist dat tenminste de volgende onderwerpen onderdeel zijn van de rapportage:
1. een management samenvatting;
 2. inleiding;
 3. opdrachtoomschrijving;
 4. scope en doelstelling van de PEN test;
 5. uitvoeringsdata;
 6. onderzochte omgeving en objecten; applicaties en versienummers;
 7. de methoden, technieken en tools (inclusief versienummers) die gebruikt zijn;
 8. gebruikte parameters, tijdstippen waarop testen zijn uitgevoerd, IP-adres waarvandaan is getest);
 9. detailoverzicht van geconstateerde bevindingen met minimaal:
 - a. Bevinding, onderbouwing en mogelijke impact risico's;
 - b. Aanbeveling om de risico's te mitigeren;
 - c. Voor welke systemen/applicatie/op welke plekken binnen de applicatie, de bevinding van toepassing is;
 - d. Per bevinding een uniek volgnummer;
 - e. Score opbouw volgens het Common Vulnerability Scoring System (CVSS) 3.1 of 4.0;
 - f. Gebruikte methodiek en techniek om bevinding te reproduceren;
 - g. Om de volledigheid van het onderzoek aan te tonen, bevat de rapportage een totaaloverzicht van alle getoetste kwetsbaarheden, ook als het getoetste aan de gestelde eisen voldoet.
 - h. Indien gewenst: lijst met alle bevindingen en aanbevelingen inclusief CVSS in Excel toevoegen.
 10. conclusies en aanbevelingen.
-
- 18 Na de oplevering van het concept rapport is het, indien gewenst, mogelijk om de uitkomsten van een PEN test via een Teams meeting te bespreken, eventuele suggesties en/of verzoeken ter verduidelijking kunnen worden aangevuld en/of indien incorrect kunnen worden aangepast door Opdrachtnemer. Opdrachtnemer levert daarna een definitieve rapportage op.
-

1.3 Inhoudelijke eisen van de Dienstverlening

Nr. Eisen

- 19 Opdrachtnemer voert op verzoek van het Kadaster Dienstverlening uit op o.a.:
- Applicaties: waaronder maatwerkapplicaties, pakketimplementaties, web- en mobile applicaties, databases, webserver, servicebussen, etc.;
 - Applicatiediensten (applicaties 'as a service');
 - Infrastructuur: waaronder servers, besturingssystemen, netwerkapparatuur, -protocollen en – configuraties en beveiligingscomponenten;
 - Devices w.o. besturingssysteem en eventuele applicatiediensten;
 - Extern gehoste diensten;
 - Clouddiensten.
-
- 20 Bij de uitvoering van de Dienstverlening wordt door Opdrachtnemer minimaal getest op de aspecten:
- Kwetsbaar op onbeschikbaarheid;
 - Integriteit;
-

- Vertrouwelijkheid.

- 21 Opdrachtnemer toetst op verzoek van het Kadaster de objecten tenminste op kwetsbaarheden conform de meest recentelijk gepubliceerde OWASP top 10, SANS top 25, AVG, NCSC-richtlijnen voor webapplicaties en overige security richtlijnen indien relevant zoals SOC2, Logius norm (voor DigiD).
- 22 Opdrachtnemer voert op verzoek van het Kadaster de Dienstverlening uit met de hieronder genoemde niveaus van voorkennis.
 1. Black box: er worden vooraf geen gegevens beschikbaar gesteld over of toegang tot het te onderzoeken object. De test wordt uitgevoerd vanuit een ongeautoriseerd perspectief en benadert de realiteit van cyber criminelen het meest.
 2. Grey box: er worden beperkte gegevens over de applicatie(s) en infrastructuur beschikbaar gesteld. Ook kunnen er (test) login credentials worden beschikbaar gesteld. De PEN test wordt uitgevoerd vanuit het perspectief van iemand die normale toegang heeft (bemachtigd), waarbij geprobeerd kan worden buiten de gestelde kaders van dat account te treden.
 3. White box: additionele gegevens over de applicatie(s) en infrastructuur worden beschikbaar gesteld. Ook kunnen er (test) login credentials worden beschikbaar gesteld.
- 23 Opdrachtnemer informeert het Kadaster 1 week voor aanvang van de PEN test over de IP-adressen die worden gebruikt voor de PEN test alsmede de namen van de Professionals die de testen zullen uitvoeren, zodat het Kadaster voldoende tijd heeft voor aanvragen certificaten en/of whitelisting.
- 24 Wanneer Opdrachtnemer tijdens de uitvoering van de PEN test kwetsbaarheden met een critical vulnerability (CVSS) signaleert, dan dient Opdrachtnemer dit direct bij de contactpersoon van het Kadaster te melden, zodat het Kadaster hier actie op kan ondernemen.
- 25 Wanneer Opdrachtnemer tijdens de uitvoering van de PEN test merkt dat er onbedoeld een onderbreking of verstoring is veroorzaakt op een component of Dienstverlening van het Kadaster als gevolg van zijn handelen, wordt van Opdrachtnemer verwacht dat het onderzoek direct wordt gestopt. Opdrachtnemer maakt direct melding hiervan bij de voor dit onderzoek aangewezen contactpersoon van het Kadaster onder vermelding van alle relevante informatie.
- 26 Wanneer tijdens het uitvoeren van de Dienstverlening onbedoeld een verstoring is veroorzaakt verzorgt de contactpersoon van het Kadaster de communicatie en start de contactpersoon acties op zodat het proces kan worden hersteld. Vervolgens wordt met Opdrachtnemer overlegd of en met welk ander (minder riskant) deel van het onderzoek kan worden vervolgd tijdens het herstellen van het proces.
- 27 Een follow-up PEN test volgt het standaard PEN test proces. Veelal zal het Kadaster aan Opdrachtnemer vragen om een follow-up PEN test uit te voeren op een selectie van eerder gevonden kwetsbaarheden.
- 28 Het Kadaster draagt zorg voor de ondertekening van de vrijwaringsverklaring en afstemming met eventuele andere leveranciers van het Kadaster die deze vrijwaring voor akkoord moeten ondertekenen. Het Kadaster retourneert de ondertekende vrijwaringsverklaring met de opdrachtschrijving aan Opdrachtnemer voordat de werkzaamheden zullen starten.

1.4 Eisen m.b.t. uitvoerende Professionals

Nr. Eisen

- 29 Professionals van Opdrachtnemer dienen minimaal te beschikken over de volgende competenties:
 - Heeft HBO of universitair werk- en denkniveau;
 - Werkervaring in het (technisch-) domein waarop de dienstverlening wordt uitgevoerd zoals: Windows, AIX, Linux, Netwerken, (Cloud) web hosting, databases, Java, etc.;
 - Beheersing van de Nederlandse en/of Engelse taal in woord en geschrift;

- Beschikken over communicatieve skills, om in een contact, bijvoorbeeld bij gesprekken met klant, eindgebruiker, of medewerkers van het Kadaster, een correcte houding aan te nemen en in is staat de juiste bewoordingen te kiezen;
- Relevante werkervaring in het (zelfstandig) uitvoeren van PEN(follow-up) testen en/of adviesdiensten;
- Zelfstandig uitvoeren van de gevraagde dienstverlening;
- Optioneel: De Professional is in het bezit van vak gerelateerde certificaten in relatie tot PEN testen, gericht op het uitvoeren van PEN testen waaruit blijkt dat de Professional over de juiste competenties beschikt.

Voor de junior pentester gelden de aanvullende competenties:

- Onder regie van de senior uitvoeren van de gevraagde dienstverlening
- Het verrichten van de minder complexe werkzaamheden
- Enige ervaring met risicomanagement en/of informatiebeveiliging

Voor de senior pentester gelden de aanvullende competenties:

- Het verrichten van de zeer complexe werkzaamheden;
- Ruime ervaring met risicomanagement en/of informatiebeveiliging;
- **Ruime ervaring met projectmanagement;**
- Ruime ervaring met het samenwerken in multidisciplinaire teams en omgevingen;
- De Professional is in het bezit van een OSCP of een vergelijkbare certificering.

Voor de projectleider gelden de aanvullende competenties:

- Draagt eindverantwoordelijkheid voor de coördinatie en uitvoering van de dienstverlening binnen de opdracht;
- Beschikt over ruime ervaring in het aansturen van (technische) teams binnen het cybersecuritydomein;
- Heeft ervaring met klantcommunicatie op tactisch en strategisch niveau;
- Is in staat om te adviseren over prioriteiten, risico's en escalaties richting het Kadaster;
- Beschikt over aantoonbare ervaring met projectsturing binnen overheids- of vergelijkbare complexe omgevingen.

30	Opdrachtnemer zorgt ervoor dat altijd minimaal 1 Senior pentester onderdeel is van het PEN test team.
31	Opdrachtnemer zorgt ervoor dat zij over voldoende Professionals met de juiste competenties en kennis beschikken om de Dienstverlening voor Het Kadaster uit te voeren gedurende de looptijd van de dienstverlening, waarbij zij de capaciteit hebben om minimaal twee PEN testen (van verschillende offertes) tegelijk uit te kunnen voeren.
32	Opdrachtnemer dient bij aanvang van de Raamovereenkomst het team van Professionals op te geven inclusief vermelding van de specifieke expertise en brengt het Kadaster tijdig op de hoogte van vervanging en uitbreiding.
33	Professionals die betrokken zijn bij het uitvoeren van de dienstverlening dienen over een VOG beschikken, waaruit blijkt dat er geen bezwaren zijn voor de uitvoering van de dienstverlening. Opdrachtnemer moet dit periodiek rapporteren.
34	Opdrachtnemer brengt de Professionals die bij de uitvoering van een Nadere overeenkomst betrokken worden voor aanvang van een Nadere overeenkomst op de hoogte van de Gedragscode Integriteit Rijk (https://zoek.officiëlebekeendmakingen.nl/stcrt-2015-33770.html). De betrokken Professionals dienen deze Gedragscode Integriteit Rijk in acht te nemen.

- 35 Bij constatering van ongewenst gedrag van een ingezette Professional, waardoor de samenwerking met het Kadaster is verstoord, bij oneigenlijk gebruik en/of vernieling van middelen of gegevens van het Kadaster of overtreding van gedragsregels, procedures of (integriteit)instructies door de Professional heeft het Kadaster het recht te eisen dat deze persoon wordt vervangen door een ander gekwalificeerde Professional. De directe kosten van het oneigenlijke gebruik en/of de vernieling worden aan Opdrachtnemer in rekening gebracht. Te denken valt aan: diefstal, vernieling en oneigenlijk gebruik van voorzieningen.
- 36 Het Kadaster heeft het recht, in het geval dat een Professional die betrokken is bij de uitvoering van de Dienstverlening of Opdrachtnemer niet de vereiste documenten/verklaringen kan overleggen, de Professional te weigeren of de inzet van de Professional terstond te beëindigen, zonder dat de Opdrachtnemer aanspraak kan maken op enigerlei schadevergoeding.
- 37 Het Kadaster verwacht van Opdrachtnemer dat er door Professionals van Opdrachtnemer professioneel en deskundig wordt gehandeld tijdens het uitvoeren van de Dienstverlening om verstoringen aan het proces van het Kadaster te voorkomen. Desondanks realiseert het Kadaster zich dat de Dienstverlening altijd een risico met zich mee brengt en dat er toch een onverwachte verstoring kan optreden.

1.5 Informatie- en privacybeveiliging

Nr. Eisen

- 38 Opdrachtnemer garandeert strikte vertrouwelijkheid t.a.v. de uit te voeren Opdrachten voor het Kadaster.
- 39 De Opdrachtnemer mag alleen toegang krijgen tot de systemen die expliciet in de scope van de PEN test vallen.
- 40 Accounts en toegangsgegevens worden uitsluitend gebruikt voor het uitvoeren van de PEN test en worden na afloop verwijderd.
- 41 De Opdrachtnemer mag geen permanente accounts aanhouden binnen de IT-omgeving van het Kadaster.
- 42 Testdata (inclusief logging en screenshots) moet minimaal versleuteld worden opgeslagen en mag niet worden gedeeld met derden.
- 43 Alle testdata en tussenresultaten moeten binnen 30 dagen na afronding van de PEN test worden vernietigd.
- 44 Rapportages mogen uitsluitend in versleutelde vorm aan ~~de~~ het Kadaster worden geleverd en moeten binnen 612 maanden worden verwijderd bij de leverancier.
- 45 De Opdrachtnemer moet zijn eigen toegang tot de systemen registreren en bijhouden.
- 46 Het Kadaster heeft het recht om deze logs op te vragen.
- 47 Bij ongeautoriseerde toegangspogingen of afwijkingen moet de leverancier direct melding maken.
- 48 Het Kadaster verwerkt gegevens van particulieren en bedrijven. De omgang met deze gegevens vraagt een werkwijze die de vertrouwelijkheid en integriteit van deze gegevens waarborgt. Daarom gebruikt het Kadaster de "Baseline Informatiebeveiliging Overheid" (BIO) (bijlage 9) en het "Voorschrift Informatiebeveiliging Rijksdienst – bijzondere informatie 2013" (VIR-BI 2013) (bijlage 10) Inschrijver committeert zich aan de inhoud van Bijlage 9 en 10 van het Beschrijvend Document – BIO en VIR-BI 2013 en draagt er zorg voor dat tijdens de looptijd van de Overeenkomst de Diensten die worden aangeboden het basis beveiliging niveau, zoals beschreven in het BIO en de VIR-BI 2013, niet aantasten. De BIO sluit aan op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002).
- 49 Opdrachtnemer mag de persoonsgegevens uitsluitend verwerken in de Europese Economische Ruimte. Opdrachtnemer verwerkt geen Persoonsgegevens buiten de Europese Economische Ruimte, tenzij hij

daarvoor vooraf uitdrukkelijk expliciete en schriftelijk toestemming heeft verkregen van het Kadaster en tevens voldoet aan het gestelde in hoofdstuk 5 van de AVG.

- 50 Als de Opdrachtnemer onbedoeld persoonsgegevens tegenkomt, moet hij dit direct melden aan het Kadaster.
- 51 Opdrachtnemer heeft een procedure voor het melden van datalekken aan Het Kadaster op basis van de AVG, zodat Het Kadaster tijdig een melding kan doen bij de Autoriteit Persoonsgegevens
- 52 In het geval van een beveiligingsincident of datalek moet de Opdrachtnemer binnen 24 uur een melding doen **en binnen 48 uur** een impactanalyse leveren.
- 53 Social engineering mag alleen worden uitgevoerd als dit expliciet in de scope is opgenomen.
- 54 De Opdrachtnemer mag geen DoS/DDoS-tests uitvoeren op productieomgevingen tenzij expliciet toegestaan.
- 55 Kwetsbaarheden mogen niet worden gedeeld met derden of gebruikt voor andere doeleinden.

1.6 Eisen m.b.t. tarieven en facturering

Nr. Eisen

- 56 Opdrachtnemer vrijwaart het Kadaster voor eventuele aanspraken van een belastingdienst.
- 57 Indien Opdrachtnemer aangeeft geen btw in rekening te hoeven brengen, dan gaat Opdrachtnemer ermee akkoord dat de bewijsmiddelen ten aanzien van de reden die hieraan ten grondslag liggen, aan het Kadaster worden overlegd, binnen 20 dagen na diens verzoek hiertoe.
- 58 Opdrachtnemer is aansprakelijk voor de (extra) kosten inzake btw indien Opdrachtnemer deze ten onrechte niet, of voor een onjuist bedrag bij het Kadaster in rekening heeft gebracht. De verantwoordelijkheid voor een juiste btw-afracht ligt, behoudens het gestelde in de hierna genoemde zin, te allen tijde bij Opdrachtnemer. Wanneer het Kadaster een dienst afneemt van een buitenlandse onderneming en de prestatie wordt volgens de fiscale regelgeving geacht in Nederland te zijn verricht, dan is de Aanbestedende dienst zelf verantwoordelijk voor de afdracht van btw aan de Nederlandse fiscus over deze in Nederland verrichte dienst(en).
- 59 De prijs dient/de tarieven dienen 'all-in' te zijn. Daaronder zijn derhalve begrepen: de salariskosten, de overheadkosten (als onder meer huisvesting en salariskosten van niet productief personeel), de kosten voor ondersteunend werk, de kosten voor het gebruik van apparatuur (als onder meer pc's, die worden gemaakt ten gevolge van de Opdracht en de winst, de verzekeringskosten, reis- en verblijfkosten, etc. De tarieven dienen te worden uitgedrukt in euro's.
- 60 De tarieven kunnen na de initiële contractperiode van 2 jaren, jaarlijks per 1 september worden aangepast op basis van het 'CBS-prijsindexcijfer Dienstprijzen – Commerciële Dienstverlening en transport index 2021=100.

Voor de berekening van de te indexeren tarieven wordt de volgende formule gehanteerd: "Nieuwe prijs = Oude prijs x ([index] huidig jaar / [index] vorig jaar)". Het resultaat wordt afgerond op twee cijfers achter de komma.

Opdrachtnemer dient zijn voornemen voor prijsverhoging minimaal 3 maanden voor aanvangsdatum van de indexering schriftelijk bekend te maken aan het Kadaster. Gewijzigde tarieven gaan pas in na schriftelijke instemming van het Kadaster
- 61 De tarieven van reeds verstrekte Nadere Opdrachten binnen de Raamovereenkomsten mogen niet worden geïndexeerd.
- 62 Voorstellen voor het komende jaar die na 1 juni van het huidige jaar door Opdrachtnemer worden ingediend, zullen door het Kadaster niet meer in behandeling worden genomen.

-
- 63 De facturering vindt plaats na afronding en decharge van de Dienstverlening. Indien de Dienstverlening een grote omvang en/of doorlooptijd kent, dan kunnen er aanvullende afspraken worden gemaakt over de facturering. Het Kadaster dient hiervoor schriftelijk akkoord te geven.

Het Kadaster hanteert een betalingstermijn van 30 dagen na ontvangst van de factuur.

- 64 Op de factuur van Opdrachtnemer dienen ten minste de volgende gegevens te worden vermeld:
- Factuurdatum;
 - Het inkoopordernummer dat door het kadaster wordt verstrekt;
 - Omschrijving van de gefactureerde zaken.

Facturen worden als pdf-bestand en als XML/UBL-bestand (minimaal versie 2.1) verstuurd aan:
facturen@kadaster.nl.

- 65 Gedurende de uitvoering van de Raamovereenkomst mogen geen prijzen/kosten gefactureerd worden welke niet in de offerte opgegeven zijn, tenzij tussen partijen uitdrukkelijk anders wordt overeengekomen.
-