Inkoop
Conformiteitenlijst Eisen

Rijksdienst Caribisch Nederland

Bezoekadres
APNA gebouw
Kaya International z/n
Kralendijk, Bonaire
Caribisch Nederland

Meer informatie
aanbesteding@rijksoverheid.nl

BIJLAGE	2
Kenmerk	PR15904

1 Eisen

Aan alle in deze bijlage genoemde eisen dient onvoorwaardelijk voldaan te zijn. Indien een Inschrijver niet voldoet aan een eis, wordt de Inschrijver uitgesloten en wordt de Inschrijving ter zijde gelegd.

Eis 1: U gaat akkoord met de ARBIT-2022.

Eis 2: U gaat akkoord met de concept Raamovereenkomst, bijlage 9.

Eis 3: U gaat akkoord met de concept Nadere Overeenkomst, bijlage 12.

Eis 4: U gaat akkoord met de concept Verwerkersovereenkomst, bijlage 15.

Eis 5: U gaat akkoord met de concept Nadere Offerteaanvraag, bijlage 11.

Eis 6: U beschikt over de meest recente ISO 9001 of gelijkwaardig, (een kwaliteitshandboek), waarmee de Inschrijver aantoont dat hij in staat is om consequent zijn dienstverlening te leveren die voldoen aan eisen van de klant en de wet, en waaruit volgt dat er zorg is voor klanttevredenheid door processen gericht op continue verbetering en het voorkomen van non-conformiteit

Eis 7: U beschikt over de meest recente ISO/IEC 27001 of gelijkwaardig. Bij gelijkwaardig is Inschrijver in het bezit is van een, door een erkend onafhankelijk instituut uitgegeven, certificaat voor het voldoen aan de meest recente of daarop aansluitende versie van een vergelijkbaar erkend normenkader, ondersteund door een onafhankelijk instituut, of de Inschrijver kan middels een schriftelijke verklaring van maximaal 2000 woorden aantonen dat:

a) het proces van informatiebeveiliging in zijn onderneming zodanig is geborgd, dat de continuïteit van de dagelijkse operatie is geborgd;
b) vertrouwelijke persoons- of bedrijfsgegevens door zijn Personeel en/of Derden worden beschermd conform de in de geheimhoudingsverklaring en verwerkingsovereenkomst benoemde voorwaarden;
c) de eigen infrastructuur van de Inschrijver weerbaar is tegen cybersecurity-dreigingen, zoals malware en kwetsbaarheden in verouderde gebruikte software;
d) de Inschrijver in staat is tot tijdige detectie van en adequate reactie op security-incidenten binnen zijn onderneming/organisatie.

Eis 8: De door u in te zetten medewerkers beschikken over een Certified Ethical Hacker (CEH) of gelijkwaardig. Bij gelijkwaardig zijn de medewerkers van Inschrijver in het bezit van een certificaat of diploma waarmee zij aantonen kwetsbaarheden in kaart te kunnen brengen en in staat zijn om gericht te adviseren over organisatorische, technische en personele cybersecuritymaatregelen.

Eis 9: U gaat ermee akkoord dat na afroep van de Nadere Opdracht, door middel van de Nadere Offereteaanvraag, de uitvoering van de pentest uiterlijk binnen twee maanden kan worden gestart.

Eis 10: U gaat ermee akkoord dat een geplande pentest door de Opdrachtgever tot twee weken van te voren kosteloos mag worden verplaatst.

Eis 11: U kunt of u bent in staat om op verzoek van Opdrachtgever remote te kunnen werken.

Eis 12: U kunt ten minste, maar niet uitsluitend, de volgende methodieken uitvoeren: white box, grey box en black box. Deze voert u uit volgens de op het moment van uitvoeren geldende normering.

Eis 13: U verklaart dat al uw medewerkers in het bezit zijn van een geldige VOG, niet ouder dan zes (6) maanden.

Eis 14: U verklaart dat iedere nieuwe medewerker die beschikbaar wordt gesteld voor deze Prestatie voorafgaand aan de indiensttreding aan u VOG dient te overhandigen.

Eis 15: U gaat er mee akkoord dat facturatie achteraf plaatsvindt op basis van de in de Nadere overeenkomst afgesproken tarieven, tenzij in de Nadere overeenkomst anders is overeengekomen.

Eis 16: Ieder kwartaal wordt een gastcollege gegeven aan het MBO Bonaire door een Opdrachtnemer die een Nadere Opdracht voor het uitvoeren van een pentest wint, waarbij de pentest op Bonaire uitgevoerd moet worden in het betreffende kwartaal. Wanneer een Opdrachtnemer een Nadere Offerteaanvraag wint, dan zal het gastcollege in afstemming met Opdrachtnemer, Opdrachtgever en het MBO Bonaire gepland worden.

Het kan voorkomen dat eenzelfde Opdrachtnemer meerdere gastcolleges geeft in een jaar, wanneer hij meerdere Nadere Opdrachten gegund krijgt. Indien er geen pentesten gepland zijn door SSO CN in een kwartaal, dan vindt er geen gastcollege plaats.

Eis 17: U verklaart dat alleen degenen die betrokken zijn bij de uitvoering van de pentest (binnen de Nadere overeenkomst) de resultaten van deze test zullen zien, en deze niet verder worden gedeeld binnen en buiten de organisatie.

Eis 18: U stemt er mee in dat de security specialist (pentester) na het uitvoeren van de testen alle resultaten zal analyseren en aanvullen met additionele informatie over eventueel gevonden kwetsbaarheden zoals de exacte locatie(s), het risico en de impact van de gevonden kwetsbaarheid op de integriteit en vertrouwelijkheid van de data in het systeem, als onderdeel van de Nadere overeenkomst.

Eis 19: U stemt er mee in dat de bevindingen na de analyse in een rapportage worden opgenomen aangevuld met een accuraat advies voor het verbeteren van de beveiliging.

Eis 20: Het gegeven advies voor het oplossen van de gevonden kwetsbaarheden is altijd specifiek toegespitst op de systemen van Opdrachtgever.

Eis 21: De resultaten uit het rapport zullen persoonlijk met de betrokkenen bij Opdrachtgever worden besproken. Bij deze bespreking zal in elk geval de uitvoerend security specialist (pentester) aanwezig zijn om alle vragen omtrent het onderzoek te beantwoorden.

Eis 22: Alle opgeleverde testrapportages worden na afronding door de uitvoerende security specialist (pentester) nogmaals bekeken door een tweede security specialist van Opdrachtnemer. Dit om te verifiëren of alle controles grondig zijn uitgevoerd en de informatie die wordt verschaft aangaande het verhelpen van de gevonden kwetsbaarheden correct is beschreven. Opdrachtgever kan vragen naar bewijslast hiervan.

Eis 23: Opdrachtnemer beschikt over een mechanisme/informatiesysteem waarop beveiligd bestanden met Opdrachtgever kunnen worden uitgewisseld. Dit mechanisme moet door Opdrachtgever worden goedgekeurd alvorens dit gebruikt kan worden. Opdrachtgever kan op enig moment een ander mechanisme voorschrijven aan Inschrijver voor het uitwisselen van bestanden.

Eis 24: Alle documentatie, waaronder offertes, plannen van aanpak, rapportages en testresultaten worden in de Nederlandse taal opgesteld.

Eis 25: Alle inhoudelijke informatie voortkomend uit en benodigd voor security testen moet daarom opgeslagen worden op een plek waar het Nederlandse recht van toepassing is.

Dit geldt voor:
- Rapportages;
- Overzichten van bevindingen;
- Technische en niet technische documentatie ten behoeve van security testen;
- Broncode.

Penetratietest tools:
Voor eventueel te gebruiken penetratietest tools geldt, dat deze geen gebruik mogen maken van opslag van data inclusief eventuele metadata in een Cloud omgeving.

(Security) Code review:
Specifiek voor (security) code reviews geldt, dat eventueel gebruikte code review tools geen gebruik mogen maken van cloud faciliteiten, onder Nederlandse wetgeving moeten vallen en in een afgeschermde omgeving moeten staan.

Eis 26: Wanneer Opdrachtnemer tijdens het uitvoeren kwetsbaarheden met een groot risico signaleert, CVSS Score High (>7.0) en/ of Critical (>9.0), dient Opdrachtnemer dit direct bij de contactpersoon van Opdrachtgever te melden, zodat Opdrachtgever hier actie op kan nemen.

Eis 27: Wanneer Opdrachtnemer tijdens het onderzoek merkt dat er onbedoeld een onderbreking of verstoring is veroorzaakt op een component of dienstverlening van Opdrachtgever als gevolg van zijn handelen, wordt van Opdrachtnemer verwacht dat het onderzoek wordt gestopt.

Eis 28: De beveiligingsopdrachten dienen, tenzij anders aangegeven in de nadere offerteaanvraag, te toetsen dat het IT-systeem voldoet aan:
- de meest recente OWASP Top 10;
- de meest recente CWE/SANS TOP 25 Most Dangerous Software Errors;
- de meest recente NCSC ICT Beveiligingsrichtlijnen voor Webapplicaties 2024;
- de meest recente Baseline Informatiebeveiliging Overheid;
- de meest recente NEN-EN-ISO/IEC 27001 en NEN-EN-ISO/IEC 27002 (allen voor zover van toepassing op het te onderzoeken IT-systeem),

Eis 29: Alle prijzen zijn inclusief alle bijkomende kosten (all-in). Dat betekent dat de Opdrachtgever, behalve de door de Inschrijver geoffreerde tarieven, niets aan de Inschrijver verschuldigd is.

Eis 30: De prijzen zijn exclusief reis- en verblijfkosten die Opdrachtnemer maakt voor het uitvoeren van pentesten op Bonaire. Onder reis- en verblijfkosten wordt verstaan vliegtickets (maximaal economy class), hotelovernachtingen (maximaal drie sterren), auto huur (maximaal huurklasse economy) en toeristenbelasting. Opdrachtnemer dient facturen en betaalbewijzen te kunnen overleggen om de reis- en verblijfkosten vergoed te krijgen.

Eis 31: De Opdrachtnemer is in staat een Rapportage van hoge kwaliteit op te stellen, waarin minimaal de volgende rapportagevereisten aan bod komen:

Managementsamenvatting:

- Een beknopt overzicht voor senior management met de belangrijkste bevindingen, risico's, impact, en aanbevelingen;
- Samenvatting van de belangrijkste kwetsbaarheden en hun mogelijke impact op de organisatie.

Scope en Doelstellingen:
- Gedetailleerde beschrijving van de scope van de Pentest, inclusief welke systemen, netwerken, applicaties, en IP-adressen zijn getest;
- Specificatie van de methodologie en doelstellingen van de Pentest, bijvoorbeeld het testen van specifieke kwetsbaarheden of het evalueren van de beveiligingshouding.

Methodologie en Testprocedures:
- Beschrijving van de gebruikte testmethoden (black-box, white-box, grey-box) en tools;
- Gedetailleerd overzicht van de testprocedures, inclusief de gebruikte technieken en stappen die zijn genomen tijdens de Pentest;
- Overzicht van de geleverde accountinformatie (zoals tokens, acoountnamen en passwords).

Overzicht van Bevindingen:
- Gedetailleerde lijst van alle geïdentificeerde kwetsbaarheden, gecategoriseerd op risiconiveau (bijv. kritiek, hoog, medium, laag);
- Voor elke kwetsbaarheid moet een beschrijving, impactanalyse, risicobeschrijving en bewijs van het probleem (bijv. screenshots of logs) worden opgenomen;
- Prioritering van de kwetsbaarheden op basis van de waarschijnlijkheid van exploitatie en de impact op het systeem;
- Gedetailleerde technische beschrijvingen van hoe kwetsbaarheden zijn geïdentificeerd en geëxploiteerd;
- Informatie over de exploitability van elke kwetsbaarheid, inclusief stappen die zijn genomen om de exploitatie te demonstreren.

Aanbevelingen voor Mitigatie en Herstel:
- Specifieke, gedetailleerde aanbevelingen voor het verhelpen van elke kwetsbaarheid, inclusief technische oplossingen en beleidsaanpassingen.

Logbestanden en Bewijsmateriaal:
- Opname van relevante logbestanden, foutmeldingen, en andere gegevens die de bevindingen ondersteunen;
- Screenshots, netwerkdumps, of andere bewijzen van exploitatie om de bevindingen te valideren.

Overzicht van gebruikte tools en technieken:
- Gedetailleerde lijst van de tools en scripts die zijn gebruikt tijdens de Pentest, inclusief hun versienummers en configuratie-instellingen;
- Een beschrijving van de tools die tijdens de Pentest zijn ingezet

Documentatie van Beperkingen en Aannames:
- Vermelding van eventuele beperkingen die de Pentest hebben beïnvloed (bijv. beperkte toegang, netwerkbeperkingen);
- Beschrijving van aannames die zijn gemaakt tijdens de test en hun mogelijke impact op de resultaten.

Communicatie en Incidentbeheer:
- Overzicht van eventuele incidenten die zich tijdens de Pentest hebben voorgedaan en de genomen maatregelen;
- Aanbevelingen voor verbeteringen in incidentbeheer en communicatie tijdens toekomstige Pentests.

Conclusie en Eindbeoordeling:
- Algemene conclusie over de beveiligingsstatus van de geteste systemen;
- Eindbeoordeling en samenvatting van de belangrijkste risico's en aanbevolen verbeteringen.

Eis 32: Het staat opdrachtnemer vrij om opdrachtgever tussentijds te adviseren over innovatieve mogelijkheden voor wat betreft het opleveren van de rapportages.

Eis 33: Opdrachtnemer biedt een voorziening zodat gegevens rondom de Pentest en rapportages tussen de Aanbestedende dienst en Opdrachtnemer versleuteld en met integriteitscontrole uitgewisseld worden.

Eis 34: Opdrachtnemer vernietigt resultaten en bevindingen uit de Pentest standaard na maximaal twaalf (12) maanden. Na twaalf (12) maanden dient Opdrachtnemer een vernietigingsverklaring te overhandigen aan Opdrachtgever als bewijs van het vernietigen van de resultaten en bevindingen uit de Pentest.

Eis 35: Er mag op geen enkele manier sprake zijn van belangenverstrengeling. Als zich toch belangenverstrengeling voor kan doen, dan dient Opdrachtnemer dit direct uit eigen beweging te melden.

Eis 36: Wederpartij voorziet Opdrachtgever van updates over de voortgang van de werkzaamheden met betrekking tot het uitvoeren van de pentesten (volgnummer(s).

Eis 37: Opdrachtnemer en Opdrachtgever hebben één keer per jaar een evaluatiegesprek, waarbij Opdrachtnemer Opdrachtgever meeneemt in de ontwikkelingen die in de markt spelen onder andere op het gebied van methodieken om pentesten uit te voeren.

Hiermee verklaart Inschrijver onvoorwaardelijk te voldoen aan alle in deze bijlage genoemde eisen.

Indien een Inschrijver niet voldoet aan een eis, valt de Inschrijver af en wordt deze verder niet in de beoordeling en gunning meegenomen.

Naam organisatie	
Naam ondertekeningbevoegd persoon	
Datum	
Handtekening	