Vraagspecificatie Proces-Eisen (VSP) CIV
Ten behoeve van ARVODI

Van toepassing op de
Overeenkomst

Leveren Videobeelden ten behoeve van verkeersinformatie

2021

Zaaknummer 31163720

van de RWS-CIV

Datum	05-03-2021
Versie	1.2
Status	Definitief

RWS Informatie

Inhoud

Inleiding

Doel van dit document

Dit document bevat een beschrijving van de processen, waarmee Opdrachtnemer, al dan niet op basis van zijn (gecertificeerde) kwaliteitsmanagementsysteem voor verantwoordelijk is en waarmee Opdrachtnemer aantoonbaar de scope (tijd en kwaliteit) van deze overeenkomst doelmatig en efficiënt borgt.

Leeswijzer

Bij het lezen van dit document dient de lezer goed nota te nemen van het volgende:

- Eisen die gesteld worden, zijn te herkennen aan een nummer en een schuin afgedrukte tekst, de titel van de eis. De direct aansluitende tekst is de inhoudelijke eis;
- Alinea's die vooraf gegaan worden door "*Toelichting:* [….]" geven een nadere uitleg van de eis(en) die er boven staa(n)t. Het licht toe hoe de eis(en) geïnterpreteerd moet(en) worden en maken zodoende onderdeel uit van de eis;
- Alle andere tekst dient ter introductie, inleiding of verduidelijking die moet leiden tot een beter begrip van de context van de werkzaamheden.

Algemene eisen

Algemeen

Eis (1) : *Aanvullen van de eisen en voorkomen van hiaten*

De Opdrachtnemer wordt geacht om de in de Overeenkomst gestelde eisen ten behoeve van de Prestatie/Dienst zodanig aan te vullen of te verbeteren dat de gevraagde Prestatie/Dienst altijd gegarandeerd wordt. Het uitsluitend voldoen aan de in de Overeenkomst genoemde eisen ontslaat de Opdrachtnemer nimmer van de verplichting altijd te voldoen aan de eisen van een professioneel Opdrachtnemer en de verplichting mogelijke hiaten als vanzelf aan te vullen en te verbeteren.

Contractgemachtigde(n)

Eis (2) : *Mandaat vertegenwoordiger(s) van de Opdrachtnemer*

De contractgemachtigde(n) van de Opdrachtnemer heeft (hebben) in het overleg voldoende mandaat voor alle te voeren besprekingen en te nemen besluiten binnen de kaders van de Overeenkomst. Dit om snelle besluitvorming te faciliteren binnen de gestelde kaders van de Overeenkomst(en).

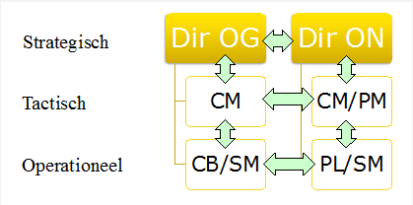
Escalatie Procedure

Eis (3) : *Escalatieproces*

1. Indien op het operationele niveau op een bepaald moment ten aanzien van de te leveren Prestatie/Dienst volgens de Opdrachtgever en/of Opdrachtnemer niet wordt voldaan aan de gestelde eisen en of afspraken en er hierdoor een geschil ontstaat, mogen zowel Opdrachtgever als Opdrachtnemer, na kennisgeving, dit geschil voorleggen/escaleren naar het tactische niveau.

2. Indien het geschil uit het vorige lid ook op tactisch niveau niet (tijdig) opgelost kan worden, mogen zowel Opdrachtgever als Opdrachtnemer, na kennisgeving, dit geschil voorleggen/escaleren naar het strategisch niveau.

3. De onderstaande contract en escalatielijnen dient te worden gehanteerd door Partijen, waarbij de directie van de Opdrachtgever vertegenwoordig kan worden door het verantwoordelijke afdelingshoofd.



Eis (4) : *Opdrachtnemer sluit aan bij het escalatieproces van de Opdrachtgever*

Opdrachtnemer dient te voorzien in identieke escalatieniveaus als de Opdrachtgever en dient deze niveaus te voorzien van het juiste mandaat, zodat de voortgang en kwaliteit geborgd blijven kunnen worden.

Toelichting : De mogelijkheid tot escalatie laat onverlet het recht tot aansprakelijkheidstelling (als bedoeld in artikel **21** ARVODI-2018) dan wel tot ontbinding en opzegging (als bedoeld in artikel **22** ARVODI-2018).

Organisatie van Opdrachtnemer

Eis (5) : *Inrichten organisatie*

Opdrachtnemer zal een organisatie inrichten waarmee hij de uitgevraagde Dienst aan de Opdrachtgever levert en waarmee hij in staat is om:

- De noodzakelijke kennis op te bouwen en vast te houden (kennisborging) met betrekking tot de uit te voeren werkzaamheden, waarbij het beroep op de Opdrachtgever of andere Opdrachtnemers van Rijkswaterstaat zoveel mogelijk beperkt wordt (zelfwerkzaamheid);
- Te allen tijde aan te tonen dat de geleverde Dienst(en) voldoet (n) aan de gestelde eisen:
- Te allen tijde aan te tonen dat zijn apparatuur voldoet aan de eisen waarvoor zij wordt gebruikt;
- Alle communicatie met de contactpersonen van de Opdrachtgever in het Nederlands plaats te laten vinden, tenzij dit anders in de Overeenkomst wordt vastgelegd;
- Wijzigingen in zijn organisatie tijdig en volledig schriftelijk kenbaar te maken aan Opdrachtgever en mondeling in het daartoe bestemde overleg.

Documentatie

Eis (6) : *Voertaal documentatie*

Alle documentatie die door Opdrachtnemer wordt opgesteld en uitgewisseld met Opdrachtgever geschiedt in de Nederlandse taal, tenzij anders overeengekomen.

Eis (7) : *Versiebeheer*

Het proces versiebeheer dient door Opdrachtnemer beschreven te zijn en voor alle documenten eenduidig gehanteerd te worden en op verzoek van Opdrachtgever beschikbaar te zijn.

Eis (8) : *Formaat van de documentatie*

1. Alle documentatie dient zonder verlies van informatie of opmaak leesbaar te zijn met de bij Opdrachtgever in gebruik zijnde versies van MS-office (Word, PowerPoint, Excel etc.)

2. Indien een ander formaat dan MS-office wordt gebruikt, dient dit zonder extra hulpmiddel geopend en zonder verlies van informatie

of opmaak ingelezen te kunnen worden in de bij Opdrachtgever in gebruik zijnde versie van MS-office.

Planning in documenten

Eis (9) : *Planning opgenomen in enig document zoals bijvoorbeeld in plannen, plannen van aanpak, voortgangsrapportages of offertes*

Voor alle planningen van werkzaamheden die de Opdrachtnemer in het kader van zijn werkzaamheden oplevert, geldt dat:

- Gedefinieerde hoofd- en sub-fasen en raakvlakken duidelijk herkenbaar moeten zijn;
- (een groep van) activiteiten duidelijk herkenbaar moet(en) zijn en altijd gekoppeld aan door Opdrachtgever controleerbare (deel)(Op)levering(en);
- (deel)(Op)levering(en) individueel herkenbaar moeten zijn;
- Beoordeling- en Acceptatiemomenten in de planning herkenbaar moeten zijn opgenomen en gekoppeld kunnen worden aan mijlpalen.

Proces Meerwerk en Minderwerk en Verzoek tot Wijziging (VTW)

Gedurende de looptijd van de Overeenkomst kan er sprake zijn van Vergoeding, Meerwerk en Minderwerk overeenkomstig artikel **16** ARVODI-2018. Aanvullend op artikel **16** ARVODI-2018 zijn de onderstaande 2 eisen van toepassing.

Eis (10) : *Te volgen werkwijze bij Meerwerk of Minderwerk Opdrachtnemer*

1. Opdrachtnemer maakt, met inbegrip van de urgentie, schriftelijk/mondeling melding van Meer-/Minderwerk aan de Contractgemachtigde Opdrachtgever;
2. Binnen 5 werkdagen na de onder 1. genoemde melding doet Opdrachtgever aan Opdrachtnemer het verzoek tot het indienen van een offerte middels het formulier Voorstel tot Wijziging (VTW) (zie bijlage 1);
3. In de offerte dient in minimaal 2 scenario's te zijn vastgelegd welke risico's (in relatie tot tijd, geld, kwaliteit en allocatie) er zijn
    a. als geen Meer-/Minderwerk e/o VTW plaatsvindt;
    b. als Meer-/Minderwerk e/o VTW wordt doorgevoerd.
4. De Opdrachtgever bevestigt de schriftelijke ontvangst van de offerte binnen 5 Werkdagen.
5. De Opdrachtgever beoordeelt de offerte binnen 10 Werkdagen na de onder 4. bedoelde bevestiging (tenzij voorafgaand aan indiening van de offerte anderszins is afgestemd met Opdrachtnemer) en zal, eventueel na overleg met de Opdrachtnemer, al dan niet instemmen;
6. Voor de aanvaarding van de opdracht van Meer-/Minderwerk dienen, indien van toepassing, Opdrachtnemer en Opdrachtgever overeenstemming te hebben over de kwaliteit, nieuwe planning, nieuwe risico's en het bedrag;

7. Indien Opdrachtgever de offerte schriftelijk aanvaart middels een wijziging op de overeenkomst, dient Opdrachtnemer de werkzaamheden binnen 10 Werkdagen na aanvaarding aan te vangen, tenzij in het onder 2. gedane verzoek een afwijkende aanvangsdatum van de werkzaamheden is aangegeven.

Eis (11) : *(Proces)Eisen aan offertes*

Voor alle uit te brengen offertes ten aanzien van Meer-/Minderwerk geldt dat:

1. Deze voorzien moeten zijn van goed en helder te beoordelen op te leveren (uitgevraagde) (deel)(Op)leveringen/werkzaamheden (Meerwerk) dan wel goed en helder te beoordelen niet meer op te leveren (uitgevraagde) (deel)(Op)leveringen/werkzaamheden (Minderwerk);
2. In de offerte kenbaar moet worden gemaakt waarom de opdracht voor Meerwerk noodzakelijk is en worden aangegeven waar de Overeenkomst tekortschiet dan wel tegenstrijdig is;
3. De offerte voorzien moet zijn van een vaste (fixed) prijs, en indien dit niet mogelijk is van een passende onderbouwde bandbreedte van maximaal 5 %;
4. Deze voorzien moet zijn van een transparante gespecificeerde kostencalculatie;
5. Een risico-analyse (zie ook Eis 10 onderdeel 3) is opgenomen en de verwerking hiervan is opgenomen in de risicobeheersing, zoals verwoord bij risicomanagement;
6. Een aanpassing op de planning is opgenomen, dan wel wordt aangegeven dat het geen invloed heeft op de geldende planning en deze aan de algemene eisen voor een planning moet voldoen;
7. De offerte een geldigheidsduur heeft van 3 maanden na formele indiening van de offerte bij contractgemachtigde;
8. Aan het opstellen van een offerte geen extra kosten voor Opdrachtgever verbonden zijn;
9. Afwijking van punt 1 tot en met 8 alleen mogelijk is na overleg en goedkeuring van de Contractgemachtigde van de Opdrachtgever.

Projectmatig werken

Projectbeheersing

Eis (12) : *Opdrachtnemer onderhoudt de planning*

1. De Opdrachtnemer zal tijdens de projectuitvoering alle maatregelen nemen om ervoor zorg te dragen dat de werkzaamheden worden uitgevoerd volgens de overeengekomen planning, waarvoor geldt dat Opdrachtnemer de afgesproken

planning onderhoudt waarbij ten minste per vastgestelde periode (afspraak in PSU vastleggen):

- De planning wordt bijgewerkt;
- In de planning de actuele standlijn wordt aangegeven;
- De bijgewerkte planning als onderdeel van de voortgangsrapportage zal worden verstrekt.

Eis (13) : *Planningsmanagement*

1. Opdrachtnemer bewaakt dat de werkzaamheden uitgevoerd worden conform de eisen van de Overeenkomst.

2. Opdrachtnemer zal, indien de planning meer dan **2** weken zal wijzigen ten opzichte van de laatste versie die bij Opdrachtgever bekend is, Opdrachtgever hier onverwijld van in kennis stellen.

3. Indien een situatie als onder 2 zich voordoet dient Opdrachtnemer bij het eerst volgende voortgangsoverleg aan te geven wat de oorzaak is en welke beheersmaatregelen Opdrachtnemer genomen heeft om aan de Overeenkomst te blijven voldoen.

Bijzondere VSP situaties

Bijzondere VSP situaties

Eis (14) : *Aan eisen gesteld in bijlage 2 "Informatiebeveiliging Vraagspecificatie-Processen voor IV-contracten" dient voor zover deze van toepassing zijn op de Diensten te worden voldaan.*

Kwaliteitsmanagement

Kwaliteitsmanagement

De verantwoordelijkheid voor het voldoen aan eisen van de Overeenkomst ligt bij de opdrachtnemer**.** De opdrachtnemer beheerst zijn Prestatie/Dienst en kan het voldoen aan de eisen van (deel)producten aantonen met de registraties die zijn opgenomen in zijn verificatie- en keuringsplan(nen) en de daaruit afkomstige rapporten. Het belangrijkste element van het kwaliteitsmanagement van de opdrachtnemer is dat hij zelf zijn processen beschrijft, risico's beheerst, tijdig afwijkingen signaleert, tijdig passende (correctieve, corrigerende en/of preventieve) maatregelen neemt en dit hele proces regelmatig evalueert. De opdrachtnemer moet kunnen aantonen dat de cirkel van Deming (plan-do-check-act) werkt op zijn project.

Eis (15) : *Proces Kwaliteitsmanagement*

1 De Opdrachtnemer is middels kwaliteitsbeheersing verantwoordelijk voor de te leveren Prestatie/Dienst.

2 De Opdrachtnemer stelt op basis van zijn Kwaliteitsmanagement-systeem (KMS), voor de Overeenkomst een Project Management Plan (PMP) op waarin alle van belang zijnde processen die van toepassing zijn voor een goede uitvoering en beheersing van de Overeenkomst en de DVO worden beschreven.

   a. De Opdrachtnemer verstrekt het Project Management Plan ter Beoordeling aan Opdrachtgever samen met de inschrijfdocumenten. De relevante bijlagen waarnaar in het PMP wordt verwezen, worden eveneens aan de Opdrachtgever verstrekt.

3 De Opdrachtnemer dient een Auditplan op te stellen voor de te leveren Prestatie/Dienst, audits uit te voeren en een Auditregister op te stellen.

4 De Opdrachtnemer dient:
- Afwijkingen te identificeren, te registreren, te communiceren, te beoordelen, te corrigeren, te evalueren en de gewenste verbeteringen door te voeren, en
- een wijzigingsvoorstel in te dienen, indien hij meent dat afwijking van blijvende aard is, en
- een Afwijkingenregister bij te houden.

5 De Opdrachtnemer rapporteert aan de Opdrachtgever in de daartoe geëigende overleggen over het Auditplan, de resultaten uit de gevoerde audits, de geregistreerde afwijkingen alsmede de door te voeren verbeteringen en de voortgang daarvan.

Eis (16) : *Product Project Management Plan (PMP)*

1. In het Project Management Plan dienen processen uit het KMS van Opdrachtnemer en proceseisen uit deze bijlage helder en transparant te worden beschreven alsmede een
    a. beschrijving van het doel en de relatie met het Kwaliteitsmanagementsysteem (KMS):
        - een beschrijving van, of een verwijzing naar, de van toepassing zijnde procedures en werkinstructies die deel uitmaken van het Kwaliteitsmanagementsysteem,
        - beschrijving van de wijze waarop invulling wordt gegeven aan de implementatie en de evaluatie van de doeltreffendheid van het Kwaliteitsmanagementsysteem en
        - een beschrijving van de rollen, taken en verantwoordelijkheden
    b. De navolgende processen uit het KMS van Opdrachtnemer, , alsmede de onderlinge relaties van deze processen dienen helder en transparant beschreven te worden;
        - Leiderschap
        - eventuele Ondersteuning
        - Omgang met offertes en opdrachten
            - Offerte procedure (zie eis 11)
            - Uitvoering (Hfd 8; ISO 9001:2015)
            - Beheersing van extern geleverde processen, producten en diensten (Hfd 8.4 ISO 9001:2015)
        - Procesbeheersing
            - Bewaken scope (procedure wijzigingen) / Beheersing van wijzigingen (Hfd 8.5.6 ISO 9001:2015)
            - Verbetering (Hfd 10 ISO 9001:2015) Verificatieplan, -nota en –rapport
            - Auditplan, registratie en afwijkingenregister
        - Procedure Risicomanagement
            - Processen in relatie tot de eisen **34** en **35** van dit document
            - Risicoregister (zie eis 35)
        - Continue verbetering (Hfd10.3 ISO 9001;2015)Wijze van informatieoverdracht richting de Opdrachtgever en andere externe betrokkenen, inclusief overlegafspraken

2. In het PMP dienen minimaal de volgende onderwerpen, conform de processen, specifiek voor de Diensten, volledig te zijn uitgewerkt:

a. Beschrijving van de invulling van kwaliteitsborging door de Opdrachtnemer op de werkprocessen;
b. Beschrijving van de relatie tussen de op te stellen plannen;
c. Beschrijving van de invulling van de interne kwaliteitsborging door de Opdrachtnemer door middel van audits en afwijkingsregistraties;

d. Wijze van informatieoverdracht richting de Opdrachtgever en andere externe betrokkenen, inclusief overlegafspraken.

Eis (17) : *Product Auditplan*

Het door de Opdrachtnemer op te stellen Auditplan dient minimaal een inhoudelijke beschrijving en een planning van de uit te voeren audits te bevatten.

Eis (18) : *Product Auditregister*

Het door de Opdrachtnemer op te stellen en te hanteren Auditregister dient minimaal de volgende zaken te bevatten:

- Soort Dienst waar de audit betrekking op heeft;
- Datum uitgevoerde audit;
- Auditor;
- Resultaten audit;
- Vervolgactie audit.

Eis (19) : *Product Afwijkingenregister*

Het door de Opdrachtnemer op te stellen en te hanteren Afwijkingenregister dient per afwijking minimaal de volgende zaken te bevatten:

- Uniek volgnummer van de afwijking;
- Omschrijving van de afwijking;
- Datum constatering;
- Verantwoordelijke actor;
- Status van de correctie;
- Datum wanneer corrigerende maatregel(en) uitgevoerd zullen zijn;
- Datum sluiting van het afwijkingsrapport.

Beoordelen

Eis (20) : *Proces Beoordelen*

1. Als de Opdrachtnemer een item ter Beoordeling voorlegt, bevestigt de Opdrachtgever de ontvangst binnen ***5*** Werkdagen.

2. De Opdrachtgever deelt binnen ***10*** Werkdagen na voorleggen mee of hij al dan niet bezwaar heeft, tenzij in de beoordelingslijst een andere termijn wordt genoemd.
    a. Als de Opdrachtgever niet in staat is binnen de hiertoe genoemde termijn van Beoordeling aan de Opdrachtnemer mee te delen of hij al dan niet bezwaar heeft, meldt hij dat voor afloop van die termijn aan de Opdrachtnemer onder vermelding van de aanvullende termijn waarbinnen hij alsnog aan de Opdrachtnemer zal meedelen of hij wel of geen bezwaar heeft.

b. Ingeval voornoemde (aanvullende) termijn voor Beoordeling is verstreken en de Opdrachtgever heeft geen schriftelijke verklaring van (al dan niet) bezwaar overlegd, treden partijen onverwijld in overleg over de consequenties daarvan.

3. Indien de Opdrachtgever een verklaring van bezwaar afgeeft dient de Opdrachtgever aan te geven aan welke criteria niet is voldaan.

4. De Opdrachtnemer dient in dat geval binnen ***5*** Werkdagen het item opnieuw ter Beoordeling voor te leggen en daarbij voor eigen rekening de redenen, die aan de verklaring van bezwaar ten grondslag liggen, te hebben weggenomen.

Accepteren

Eis (21) : *Proces Accepteren*

1. Acceptatie kan plaatsvinden wanneer aangetoond is dat:
   - De (set van) (op)levering(en) voldoet aan gestelde eisen, compleet is - waarbij verificatierapportage onderdeel uitmaakt van de (set van) (op)levering(en) - en consistent is, en
   - de verificatiemethode conform het kwaliteitssysteem van Opdrachtnemer heeft plaatsgevonden.

2. De Opdrachtgever dient, binnen **10** Werkdagen, schriftelijk aan de Opdrachtnemer mee te delen of hij al dan niet overgaat tot Acceptatie van (het onderdeel van) de Prestatie/Dienst. Indien de Opdrachtgever niet overgaat tot Acceptatie van (het onderdeel van) de Prestatie/Dienst zal de Opdrachtgever daarbij kenbaar maken aan welke eis(en) niet is voldaan. De Opdrachtgever zal (het onderdeel van) de Prestatie/Dienst dan als niet geleverd beschouwen.

Overleggen

Eis (22) : *Proces Overleggen*

1. De Opdrachtgever en de Opdrachtnemer organiseren dat er binnen **10** Werkdagen na ingang van het contract een Project Start Up (PSU) zal plaatsvinden.

2. De Opdrachtgever en de Opdrachtnemer dienen in de voorbereiding af te stemmen met betrekking tot welke onderwerpen na de PSU een verdere verdieping/uitwerking plaats zal vinden (project follow up's/voortgangsoverleggen) en in welke van de daartoe geëigende overleggen.

a. Voortgangsoverleggen op operationeel/tactisch niveau vinden in beginsel **1x per half jaar** plaats; Indien nodig kan de frequentie worden aangepast.

3. De Opdrachtnemer en de Opdrachtgever dienen regelmatig Risico-overleg te voeren teneinde risico's af te stemmen (cyclische risicobeheersing).

Eis (23) : *Product Project Start Up (PSU)*

1. In de voorbereiding op de PSU vindt onderlinge afstemming plaats over de onderwerpen die in de PSU aan bod zullen komen alsmede de diepgang.

Op hoofdlijnen zijn deze onderwerpen als volgt:
- Omgang tussen Opdrachtgever en Opdrachtnemer;
- Organisatie;
- Informatie / communicatie/ overleg structuur;
- De Overeenkomst;
- Risico-inventarisatie en beheersing;
- Kwaliteitsborging;
- Tijd;
- Geld.

Eis (24) : *Product Managementstatement*

Partijen dienen het beoogde resultaat van de samenwerking vast te leggen in een Managementstatement waarin wederzijds de intenties en afspraken worden benadrukt.

Eis (25) : *Product Risico-overleg*

Opdrachtnemer en Opdrachtgever stemmen samen, in daartoe geëigende overleggen, risico's, beheersmaatregelen alsmede de status en het resultaat van de beheersmaatregelen af, met daarbij aandacht voor het treffen van beheersmaatregelen in relatie tot elkaars risico's.

In onderling overleg verdelen Partijen de contract risico's op basis van degene die de beste beheersing kan verzorgen, waarbij het mogelijk is dat risico's een gezamenlijke verantwoordelijk zijn.

Eis (26) : *Locatie(s) overleg*

Tijdens de PSU bepalen Opdrachtgever en Opdrachtnemer gezamenlijk welk soort overleg, met welke frequentie op welke locatie(s) gehouden gaan worden gedurende de duur van deze overeenkomst.

Eis (27) : *Deelnemers overleg*

1. Voor de overleggen worden door zowel Opdrachtgever als Opdrachtnemer minimaal **2** personen afgevaardigd.

2. De deelnemers aan het overleg zijn namens Opdrachtgever en Opdrachtnemer in ieder geval de Contractgemachtigden voor die Overeenkomst.

3. Opdrachtgever levert altijd de voorzitter.

Eis (28) : *Taken overleg*

Opdrachtnemer verzorgt de volgende taken met betrekking tot het organiseren van de overleggen met uitzondering van de PSU:

- De uitnodigingen, agenda, verslaglegging, notulen en actielijst;
- Stelt minimaal **10** Werkdagen voor de geplande datum in samenwerking met Opdrachtgever de agenda op;
- Eventueel te bespreken memo's, notities van zowel Opdrachtgever als Opdrachtnemer etc. worden minimaal **5** Werkdagen voor de geplande datum verspreid;
- De notulen worden binnen **5** Werkdagen na het overleg in concept ter Beoordeling aan Opdrachtgever aangeboden;
- Opdrachtgever reageert uiterlijk binnen **5** Werkdagen na ontvangst van de notulen.

Toetsen

Eis (29) : *Proces Toetsen*

1. De Opdrachtgever is bevoegd te Toetsen of de kwaliteitsborging van de Prestatie/Dienst plaatsvindt overeenkomstig het Kwaliteitsmanagementsysteem (KMS) van de Opdrachtnemer. Om tot dit oordeel te kunnen komen maakt de Opdrachtgever gebruik van een mix van systeem-, proces- en product-Toetsen.
    a. De Opdrachtnemer dient de Opdrachtgever te allen tijde kosteloos medewerking te verlenen om een systeem-, proces- of product-Toets te (laten) verrichten en de hiervoor benodigde documenten en informatie te leveren.
    b. De Opdrachtgever heeft de bevoegdheid om te allen tijde alle percelen van de Opdrachtnemer, onderaannemers en leveranciers te betreden waar werkzaamheden ten behoeve van de Overeenkomst worden verricht en zich daarbij te doen vergezellen door derden of deskundigen.
    c. De Opdrachtgever dient bij het uitoefenen van zijn toetsingsbevoegdheid de Diensten zo weinig mogelijk te verstoren.
    d. Opdrachtgever geeft minimaal **10** Werkdagen van te voren schriftelijk aan dat er bij Opdrachtnemer getoetst zal worden.

2. De Toetsen worden op basis van risico's ingepland. De Opdrachtgever hanteert hiertoe zijn eigen risicolog. De Opdrachtgever is gerechtigd de inschatting van deze risico's door de Opdrachtnemer al dan niet over te nemen.

3. Het staat de Opdrachtgever vrij zijn toetsingsbevoegdheid naar eigen inzicht uit te oefenen.

4. De Opdrachtgever dient resultaten en conclusies van door de Opdrachtgever uitgevoerde Toetsen helder, objectief en eenduidig te formuleren in (positieve dan wel negatieve) Bevindingen.

5. De Opdrachtgever dient negatieve Bevindingen binnen ***5*** Werkdagen schriftelijk ter beschikking te stellen aan de Opdrachtnemer.

6. De Opdrachtgever is gerechtigd een negatieve Bevinding te classificeren als Tekortkoming.

Risicomanagement

Eis (30) : *Proces Risicomanagement*

1. De Opdrachtnemer dient risicomanagement (risicoanalyse en risicobeheersing) uit te voeren gedurende alle fasen van de uitvoering van de Prestatie/Dienst.
    a. De Opdrachtnemer dient voor iedere discipline de risico's te inventariseren en te analyseren die verbonden zijn aan de uitvoering van de Prestatie/Dienst.
    b. De Opdrachtnemer dient de door de Opdrachtgever geïdentificeerde risico's over te nemen in zijn risico-inventarisatie.
    c. De Opdrachtnemer dient elk geïnventariseerd en geanalyseerd risico te kwantificeren en voor elk geïnventariseerd en geanalyseerd risico beheersmaatregelen vast te stellen en aan te kunnen tonen dat de beheersmaatregelen genomen zijn.

2. De Opdrachtnemer dient op basis van de geïdentificeerde risico's en de tijdsduur van de betreffende werkzaamheden waarop de risico's betrekking hebben de effecten van de getroffen corrigerende en preventieve maatregelen te beoordelen en indien nodig maatregelen te treffen om de gewenste verbeteringen door te voeren.

3. De Opdrachtnemer dient een Risicoregister aan te leggen en actueel te houden.

Eis (31) : *Product Risicoregister*

Het Risicoregister dient minimaal de actuele risico's en inmiddels beheerste risico's te bevatten, met per risico ten minste:

- Beschrijving van het risico (de ongewenste gebeurtenis);
- Beschrijving van de oorzaak;
- Beschrijving van het gevolg;
- Inschatting in kans en gevolgklassen van het initieel risico en restrisico;
- Beschrijving van de beheersmaatregel(en);
- Status van de beheersmaatregel(en).

Verifiëren

Eis (32) : *Proces Verifiëren*

1. De Opdrachtnemer dient door middel van Verificatie aan te tonen dat de Prestatie/Dienst voldoen aan de daaraan gestelde eisen in de Proces-Eisen en Eisen zoals gespecificeerd in de Overeenkomst.

2. De Opdrachtnemer dient (eventueel per onderdeel van de Prestatie/Dienst) een Verificatieplan op te stellen.

3. De Opdrachtnemer dient in Verificatierapporten vast te leggen dat wordt voldaan aan de betreffende eis(en).

4. De Opdrachtnemer dient een Verificatienota op te stellen waarin traceerbaar wordt gemaakt dat in alle fasen voor alle onderdelen van de Prestatie/Dienst wordt voldaan aan alle eisen.

Eis (33) : *Product Verificatieplan*

1. Een Verificatieplan dient per eis aan te geven hoe zal worden aangetoond, dat wordt voldaan aan de betreffende eis.

    a. In een Verificatieplan dient per eis ten minste het volgende te zijn vastgelegd:
        - Omschrijving van de eis (met eisnummer);
        - Van toepassing zijnde uitgangspunten uit bindende, informatieve en overige documenten;
        - Beschrijving van de toe te passen verificatiemethode;
        - De criteria op basis waarvan wordt aangetoond dat is voldaan aan de eis;
        - Wie de Verificatie uitvoert.

    b. Voor elke verificatiemethode dient de geldigheid te worden vastgesteld, tenzij:
        - Een gestandaardiseerde verificatiemethode wordt toegepast die door de Opdrachtgever wordt erkend of
        - een binnen de Overeenkomst van toepassing verklaard document wordt toegepast of
        - een verificatiemethode zich in de praktijk heeft bewezen en de referentie door de Opdrachtgever wordt aanvaard.

Eis (34) : *Product Verificatierapport*

1. Een Verificatierapport dient aan te geven dat wordt voldaan aan de betreffende (set van) eis(en) en hoe dit is vastgesteld.

    a. In een Verificatierapport dient ten minste het volgende te zijn vastgelegd:
        - De betreffende (set van) eis(en) (met eisnummer(s));
        - Van toepassing zijnde bindende, informatieve en overige documenten;
        - Hoe de eis is geverifieerd en met welke verificatiemethode;
        - Wat de criteria zijn op basis waarvan wordt aangetoond dat is voldaan aan de eis;
        - Wie de Verificatie heeft uitgevoerd;
        - Dat is aangetoond dat is voldaan aan de eis;
        - Bewijsdocument(en), of verwijzing naar bewijsdocument(en), waarin is aangetoond dat wordt voldaan aan de gestelde eis;
        - Wie de Verificatie heeft beoordeeld en geautoriseerd.

Eis (35) : *Product Verificatienota*

1. De Verificatienota dient de relatie vast te leggen tussen enerzijds de Prestatie/Dienst en de eisen en anderzijds de Verificaties.

    a. De Verificatienota dient de volgende informatie te bevatten:

- Overzicht van alle eisen (nummer en beschrijving van de eis) ten aanzien van de Prestatie/Dienst uit de Proces-Eisen;
- Per eis een verwijzing naar de registraties (Verificatieplan, Verificatierapport(en)) waaruit blijkt hoe is aangetoond en traceerbaar is dat aan deze eisen wordt voldaan.

Eis (36) : *Proces Factureren en Betalen*

1. Voor alle factureringen en betalingen geldt dat zij altijd vallen onder het proces Beoordelen en Accepteren van deze VSP.

    a. De pro forma facturen, inclusief de onderbouwing van het betalingsverzoek van Opdrachtnemer worden ter Beoordeling aan Opdrachtgever aangeboden.
    b. Na een positieve Beoordeling van de pro forma factuur door Opdrachtgever geeft Opdrachtgever het overeengekomen bedrag voor betaling vrij (prestatie verklaren (PV)) en krijgt Opdrachtnemer bericht dat een factuur voor het overeengekomen bedrag ten laste van Opdrachtgever kan worden verzonden.
        i. Het adres en bestelnummer worden schriftelijk aan Opdrachtnemer kenbaar gemaakt.

Handelingen na oplevering van Diensten

Evaluatie

Eis (37) : *Projectevaluatie*

Partijen houden na afloop/beëindiging van de Overeenkomst een gezamenlijke evaluatie, tenzij beide partijen aangeven dit niet noodzakelijk te vinden.

- De evaluatie wordt binnen **20** Werkdagen na beëindigen/afsluiten van het contract door Opdrachtnemer gepland en gezamenlijk gehouden;
- Opdrachtnemer en Opdrachtgever stellen samen de agenda op, doel is de efficiency en doelmatigheid van beide partijen te evalueren;
- De bevindingen worden schriftelijk vastgelegd en door Opdrachtgever en Opdrachtnemer ondertekend;
- Opdrachtnemer verzorgt de administratie en vastlegging.

Opslag en archivering (Op)leveringen

Eis (38) : *Opslag en archivering (Op)leveringen*

1. De Opdrachtnemer dient alle relevante concepten en/of documenten/(Op)leveringen die (positief) Beoordeeld of Geaccepteerd zijn zonder vertraging (digitaal) op te slaan en te archiveren en op verzoek gedurende minimaal **2** jaar nadat het contract is beëindigd beschikbaar te maken/houden voor de Opdrachtgever.

Bijlage

Bijlage 1: Formulier VTW

In te vullen door initiator		
Initiatie		
☐ **Opdrachtnemer: WIJZIGINGSVOORSTEL** **(VSP- Proces Eisen – eis 12)**		
☐ **Opdrachtgever: VOORNEMEN TOT OPDRAGEN VAN EEN WIJZIGING** **(VSP -Proces Eisen – eis 11)**		
Identificatie		
Opdrachtgever Rijkswaterstaat – Centrale Informatievoorziening (CIV)		
Opdrachtnemer :		
Overeenkomstnummer :	Ref.nr.: <…>	Datum / versie:
Aanleiding van de Wijziging		
Korte beschrijving van het verzoek tot Wijziging.		
Wijziging betreft		
Document:	Tekst Wijziging:	
☐ Overeenkomst	(a)	
☐ Proces Eisen	<…>	
☐	<…>	
☐	<…>	
☐	<…>	

In te vullen door opdrachtnemer		
Consequenties en risico's voor Tijd, Geld, Kwaliteit en Allocatie (indien van toepassing)		
☐ Tijd	<…> Werkpakket(ten) nr. <…> Zie planning: bijlage <…> datum / versie <datum> / <versie>	
☐ Geld	<…> ☐ Meerkosten m.b.t. Betaalpost(ten) nr. <…> à € <bedrag>, exclusief BTW ☐ Minderkosten m.b.t. Betaalpost(en) nr. <…> à € <bedrag>, exclusief BTW	
☐ Kwaliteit	☐ welke risico's zijn er als er geen (contract)wijziging plaats vind ☐ welke risico's zijn er als de (contract)wijziging wordt doorgevoerd Minimaal 2 scenario's met onderbouwing: ☐ Scenario 1 ☐ Scenario 2	
☐ Allocatie	Indien van toepassing	
Ondertekening		
Naam Opdrachtnemer:	Handtekening:	Plaats / Datum:
Naam Opdrachtgever:	Handtekening:	Plaats / Datum:
NB. De Wijziging van de Overeenkomst komt tot stand na schriftelijke Acceptatie door de Opdrachtgever		

Bijlage 2 Informatiebeveiliging VSP

Informatiebeveiliging Vraagspecificatie-Processen voor IV-contracten

Datum	12 augustus 2019
Status	definitief

Colofon

Uitgegeven door	Security Centre, Rijkswaterstaat
Informatie	Marco Rijkschroeff / Turabi Yildirim/ Sahar Habib
Telefoon	
Fax	
Uitgevoerd door	Security Centre, Rijkswaterstaat
Opmaak	
Datum	12 augustus 2019
Status	definitief
Versienummer	1.6

Inhoud

1 Proceseisen informatiebeveiliging in IV-inkoopcontracten

OPMERKING: Dit document is een bijlage met de proceseisen vermeld in het vastgestelde moederdocument "Informatiebeveiliging in standaard RWS IV-Contracteisen".

Verwijzingen naar externe documenten zijn vermeld als {n} of IBR-m en zijn terug te vinden in Appendix A. Termen die beginnen met een hoofdletter zijn eigennamen en verwijzen naar specifieke betekenissen in de ARBIT en ARVODI contractteksten. Overige termen komen overeen met de definities genoemd in Nederlandstalige versie van NEN/IEC ISO 27000. Voor alle andere termen wordt verwezen naar de generieke betekenis, terug te vinden in het Van Dale Groot woordenboek van de Nederlandse taal. Achtergrondinformatie bij de gehanteerde nummering van eisen is terug te vinden in Appendix B.

1.1 Informatiebeveiligingsbeleid

5.1.1 Opdrachtnemer is aantoonbaar voor de overeengekomen Prestatie gecertificeerd conform de meest recente versie van de NEN-ISO/IEC 27001 norm of gelijkwaardig, en blijft dit voor ten minste de duur van de Overeenkomst.

5.1.SC-01a Opdrachtnemer dient het deel van zijn informatievoorziening dat benodigd is voor de door de Opdrachtgever gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de Opdrachtgever geclassificeerde informatie en documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.

5.1.SC-01b Opdrachtnemer dient, daar waar Opdrachtgever niet verwijst naar specifieke beveiligingsrichtlijnen bij de te treffen maatregelen, de richtlijnen uit de meest recente versie van de NEN-ISO/IEC 27002 norm aan te houden.

1.1 Organiseren van informatiebeveiliging

6.1.1 Opdrachtnemer dient voor ten minste alle processen genoemd in de Overeenkomst aantoonbaar de verantwoordelijkheden, taken en bevoegdheden op de daartoe geëigende plaatsen binnen de (project)organisatie te beleggen.

6.1.2 Opdrachtnemer dient beleid te hebben voor functiescheiding (mits redelijkerwijs mogelijk) bij het beleggen van uitvoerende, controlerende, en beheertaken betrokken bij de Prestatie, en dient dit aantoonbaar operationeel geborgd te hebben in processen, waarmee ook ongeautoriseerde toegang tot bedrijfsmiddelen wordt waargenomen of voorkomen.

6.1.5 Opdrachtnemer dient te beschikken over een operationeel geborgd projectbeheerproces voor de Prestatie waarin informatiebeveiliging aantoonbaar geïntegreerd is.

6.2.1 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het beveiligen en versleutelen van gegevens op mobiele apparatuur betrokken bij de Prestatie waarbij rekening wordt gehouden met de richtlijn IBR-1 *Beleid voor gegevensclassificatie* {10}, actualiteit van de veiligheid van de gebruikte versleutelingsmethoden {1} en de Handreiking: BIO Mobile Device Management {9}.

6.2.2 Toegang op afstand van alle informatiesystemen betrokken bij de Prestatie in het netwerk van Opdrachtgever is uitsluitend toegestaan via een speciaal hiervoor ingerichte Toegang Derden dienst {2} van Opdrachtgever.

1.2 Veilig personeel

7.1.1 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor de screening van het Personeel dat werkzaamheden verricht:

1. op het gebied van ontwikkelen of herzien van ontwerptekeningen en/of -documenten;
2. ten behoeve van het ontwikkelen, testen, beheren, installeren, configureren en/of bedienen van programmatuur of apparatuur;
3. in bedienings- of technische ruimtes;
4. aan kabels en leidingen;
5. aan beveiligings- en veiligheidsdocumentatie en -instructies,

betrokken bij de Prestatie middels ten minste een relevante Verklaring Omtrent Gedrag (VOG), waarbij gedurende de contractperiode een screening nooit ouder mag zijn dan 5 jaar. Hangende de aanvraag van een screening kan worden volstaan met een eigen verklaring van betreffende persoon gedurende een periode van maximaal zes weken gerekend vanaf de startdatum van deze persoon bij de Prestatie, welke niet verlengd kan worden.

7.2.2a Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat Personeel een opleiding en -training op het gebied van beveiligingsbewustzijn heeft ontvangen passend bij de aard van de uit te voeren werkzaamheden, alsmede jaarlijkse bijscholing krijgt, waarin ten minste ook persoonlijke verantwoordelijkheid en specifieke beveiligingskaders van Opdrachtgever ter sprake komen.

7.2.2b Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat Personeel verantwoordelijk voor het testen van informatiesystemen betrokken bij de Prestatie, beschikken over actuele en gespecialiseerde kennis, ervaring en opleiding met betrekking tot het testen van de beveiliging hiervan.

7.3.1 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het definiëren van verantwoordelijkheden en taken met betrekking tot informatiebeveiliging voor de Prestatie en dient naar het Personeel te communiceren dat:

1. deze van kracht blijven na beëindiging of wijziging van het dienstverband;
2. deze ten uitvoer moeten worden gebracht.

1.3 Beheer van bedrijfsmiddelen

8.1.1a Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat van alle informatiesystemen betrokken bij de Prestatie een inventaris is opgesteld in een Configuration Management Database (CMDB), zodanig dat deze effectief kan worden gebruikt voor een effectief Configuration Management (CM) ITIL proces en dat deze CMDB actueel wordt gehouden.

8.1.1b Opdrachtnemer dient op verzoek van Opdrachtgever de gegevens vermeld in de Configuration Management Database (CMDB), van alle informatiesystemen betrokken bij de Prestatie, over te dragen.

8.1.SC-12 De Opdrachtnemer dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot objecten, data, informatiesystemen en Industriële Automatisering) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.

8.2.1 Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat alle informatie betrokken bij de Prestatie is geclassificeerd conform IBR-1: *Beleid voor gegevensclassificatie* {10} en dat de hierbij behorende beveiligingsmaatregelen worden nageleefd.

8.3.x Opdrachtnemer dient over operationeel geborgde processen te beschikken voor het veilig verwijderen van media, transport van media, het beheer van verwijderbare media en het onherstelbaar verwijderen van onnodige inhoud van herbruikbare media betrokken bij de Prestatie, conform de richtlijn IBR-1: *Beleid voor gegevensclassificatie* {10} en conform Handreiking BIO: Handreiking Veilige afvoer van ICT-middelen {8}.

1.4 Toegangsbeveiliging

9.1.1 Opdrachtnemer dient te zorgen voor een operationeel geborgde procedure voor het verschaffen van fysieke dan wel logische toegang tot informatieverwerkende faciliteiten, inclusief de uitgifte en inname van accounts en autorisaties, en een actuele registratie hiervan.

9.1.SC-02 Indien Opdrachtgever of derde partij verantwoordelijk is voor het verschaffen van de fysieke of logische toegang tot informatieverwerkende faciliteiten, dan dient Opdrachtnemer zich te houden aan de door Opdrachtgever of derde partij gehanteerde toegangsprocedure.

9.2.x Opdrachtnemer dient minimaal om het halve jaar zowel de fysieke als logische toegangsrechten tot informatieverwerkende faciliteiten van het Personeel te beoordelen en te actualiseren via een operationeel geborgd en formeel proces en zijn medewerking te verlenen voor de periodieke controle en schoning van de eindgebruikers accounts en rechten van Opdrachtgever.

9.3.1 Opdrachtnemer dient van het Personeel te eisen dat het zich houdt aan de richtlijn IBR-3 *Beleid voor wachtwoordgebruik* {10} bij het gebruiken van authenticatiegegevens gerelateerd aan de Prestatie.

9.4.4 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het controleren van het gebruik van systeemhulpmiddelen, die in staat zijn om beheersmaatregelen te omzeilen voor informatiesystemen betrokken bij de Prestatie. Het gebruik ervan dient gelogd te worden.

9.4.5 Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat uitsluitend Personeel die daartoe specifiek bevoegd is, toegang heeft tot de Broncode van informatiesystemen betrokken bij de Prestatie.

1.5 Cryptografie

10.1.x Indien Opdrachtnemer contractueel of wettelijk verplicht is tot de inzet van cryptografie ter bescherming van informatie betrokken bij de Prestatie, dient Opdrachtnemer voor het gebruik van deze cryptografische beheersmaatregelen over beleid en operationeel geborgde processen te beschikken, inclusief het gebruik, de bescherming en de levensduur van de daarbij behorende cryptografische sleutels, tijdens hun gehele levenscyclus conform passende standaarden (bv PKI-Overheid of ISO 11770).

1.6 Fysieke beveiliging en beveiliging van de omgeving

11.1.1 Opdrachtnemer dient fysieke beveiligingszones te hebben gedefinieerd en in gebruik te hebben om gebieden te beschermen, die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten, met betrekking tot de Prestatie.

11.1.5 Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor het werken in beveiligde gebieden, zoals bedoeld in eis VSP 11.1.1.

11.2.7 Opdrachtnemer dient aantoonbaar te beschikken over een operationeel geborgd proces voor het vernietigen van data op media bij afvoeren of vervangen van (delen van) informatiesystemen die deze media bevatten en betrokken zijn bij de Prestatie, conform Handreiking BIO: Handreiking Veilige afvoer van ICT-middelen {8}.

11.2.8 Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor de bescherming van onbeheerde informatiesystemen die betrokken zijn bij de Prestatie.

1.7 Beveiliging bedrijfsvoering

12.1.1 Opdrachtnemer dient aantoonbaar operationeel geborgde bedieningsprocedures te hebben en beschikbaar te stellen aan het Personeel en, indien van toepassing de medewerkers van Opdrachtgever, dat ze nodig heeft voor de Prestatie.

12.2.1 Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor bescherming tegen malware op informatiesystemen betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan preventie, detectie, communicatie en herstel.

12.2.SC-17 De Opdrachtnemer dient bij onderhoudswerkzaamheden en koppeling van randapparatuur aan de ICT van de Opdrachtgever de richtlijn IBR-8 *Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT systemen van RWS* {10} en Handreiking: BIO Mobile Device Management {9} aan te houden voor bescherming tegen malware.

12.3.1a Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het minimaal dagelijks maken van back-ups van alle informatie en programmatuur in gebruik voor de Prestatie.

12.3.1b Opdrachtnemer dient het recovery proces dat deel uitmaakt van het back-upproces van alle informatie en programmatuur in gebruik voor de Prestatie, minimaal jaarlijks te testen en naar Opdrachtgever te communiceren over de uitkomst hiervan.

12.4.1 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het voldoende periodiek beoordelen van logbestanden van informatiesystemen betrokken bij de Prestatie, waarbij het interval tussen twee beoordelingen nooit meer mag bedragen dan één maand.

12.4.3 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het maandelijks beoordelen van activiteiten van systeembeheerders en -operators op informatiesystemen betrokken bij de Prestatie, welke zijn vastgelegd in logbestanden.

12.4.CC-21 Opdrachtnemer dient logbestanden van informatiesystemen betrokken bij de Prestatie minimaal drie maanden (en bij een vermoed incident minimaal 3 jaar) beschikbaar te houden tenzij met Opdrachtgever een andere bewaartermijn is overeengekomen, en op verzoek deze logbestanden ter inzage te overhandigen aan Opdrachtgever.

12.6.1 Opdrachtnemer dient voor informatiebeveiliging minimaal jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC 27005 of gelijkwaardig te maken en passende maatregelen te treffen.

12.6.SC-16 Opdrachtnemer dient de informatiesystemen betrokken bij de Prestatie te controleren op kwetsbaarheden middels gangbare testmethodieken en conform de BIO Handreiking: Penetratietesten {12} en in afstemming en na goedkeuring door Opdrachtgever de informatiesystemen te patchen.

1.8 Communicatiebeveiliging

13.1.1 Opdrachtnemer dient, om informatie in informatiesystemen te beschermen, aantoonbaar operationeel geborgde processen te hebben voor beheer en beheersing van netwerken betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan onderstaande aspecten:
- Management of network security
- Technical vulnerability management
- Identification and authentication
- Network audit logging and monitoring

- Intrusion detection and prevention
- Protection against malicious code
- Cryptographic based services
- Business continuity management.

13.1.SC-15 Opdrachtnemer dient zorg te dragen dat het aantal data netwerkkoppelingen beperkt blijft tot alleen de functioneel noodzakelijke, waarbij de koppeling een passende vorm van beveiliging kent en geen onacceptabele risico's oplevert. Voor elke koppeling is een risicoanalyse en afweging gemaakt.

13.1.2 Opdrachtnemer dient beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle diensten betrokken bij de Prestatie opgenomen te hebben in een Service Level Agreement (SLA) met Opdrachtgever met ten minste aandacht voor de beveiligingsaspecten beschikbaarheid, melden van incidenten, doorvoeren van wijzigingen en escalatie.

13.1.SC-18 Opdrachtnemer dient op verzoek van Opdrachtgever een actueel overzicht aan te leveren waarin alle datanetwerkkoppelingen worden weergegeven met bijbehorende security maatregelen.

13.2.1 Opdrachtnemer dient aantoonbaar operationeel geborgde beleidsregels, procedures en beheersmaatregelen te hebben ter bescherming van het informatietransport betrokken bij de Prestatie, dat via alle soorten communicatiefaciliteiten verloopt.

1.9 Acquisitie, ontwikkeling en onderhoud van apparatuur en programmatuur

14.1.1 Opdrachtnemer dient gedurende de hele levenscyclus beveiliging integraal onderdeel te maken van het proces voor ontwikkeling en onderhoud van informatiesystemen. Dit dient op basis van een expliciete risicoafweging worden uitgevoerd ten behoeven van het vaststellen van de beveiligingseisen conform de BIO Handreiking: Risicoanalysemethode {11} en de Handreiking: Risicomanagement ISO-27005 {13}. In het geval van programmatuur dienen hiertoe minimaal de maatregelen geïmplementeerd te worden genoemd in het CIP document Grip op SSD - Beveiligingseisen voor (web)applicaties {3}.

14.1.SC-24 Opdrachtnemer dient gedurende de hele levenscyclus beveiliging integraal onderdeel te maken van het proces voor ontwikkeling en onderhoud van mobiele applicaties, hiertoe dienen minimaal de maatregelen geïmplementeerd te worden genoemd in het document "Handreiking Mobiele App Ontwikkeling en Beheer voor de Rijksoverheid {4}.

14.2.x Opdrachtnemer dient informatiebeveiliging aantoonbaar operationeel geborgd te hebben in de processen die deel uitmaken van de ontwikkelingslevenscyclus van informatiesystemen betrokken bij de Prestatie, waarbij ten minste de proceseisen worden geïmplementeerd uit de Richtlijn IBR-4 *Richtlijnen voor beveiligen bij ontwikkelen* {10}. In het geval van software dienen hiertoe minimaal de proceseisen worden geïmplementeerd uit het CIP document Grip op SSD - Beveiligingseisen voor (web)applicaties {3}.

14.2.SC-05 Opdrachtnemer garandeert de werking van informatiesystemen (ten minste tot de door de Leverancier aangeduide End of Life (EOL) hiervan) die onderdeel uitmaken van de Prestatie, op/met producten of programmatuur die níet EOL zijn en met een up-to-date patchniveau, óf biedt een kosteloze upgrade aan om dit alsnog mogelijk te maken.

14.2.SC-06a Opdrachtnemer dient voor informatiesystemen betrokken bij de Prestatie binnen 60 dagen na kennisneming van kwetsbaarheden in het geval van programmatuur en binnen 6 maanden in het geval van apparatuur, kosteloos aanpassingen of patches vrij te geven (ten minste tot de door de Leverancier aangeduide End of Life (EOL) van dit informatiesysteem) met als doel deze kwetsbaarheden te verhelpen.

14.2.SC-06b Opdrachtnemer dient te beschikken over een operationeel geborgd proces voor het periodiek doorvoeren van security patches of software updates om de informatiesystemen up te date te houden

14.3.1 Opdrachtnemer dient testgegevens betrokken bij de Prestatie, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik.

1.10 Leveranciersrelaties

15.1.3 De Opdrachtnemer dient te borgen dat, in het geval dat voor de levering van de Prestatie gebruik wordt gemaakt van onderaannemers, bij de inkoop van diensten of producten van bedrijven de beveiligingseisen van Opdrachtgever door betrokkenen worden aangehouden.

15.1.SC-25 De Opdrachtnemer dient, in het geval dat voor de levering van de Prestatie gebruik wordt gemaakt van onderaannemers, waarbij bij inkoop van diensten of producten vendorlock-in van een onderaannemer kan ontstaan en/of de nationale veiligheid in het geding kan worden gebracht, dit eerst voor te leggen aan Opdrachtgever.

15.2.1 Opdrachtgever heeft het recht om audit(s) uit te voeren waarin de eisen uit het contract tussen Opdrachtgever en Opdrachtnemer worden getoetst op opzet, bestaan, en/of werking. Aan deze audit dient Opdrachtnemer vrijwillig medewerking te verlenen.

1.11 Beheer van informatiebeveiligingsincidenten

16.1.x Opdrachtnemer dient over een operationeel geborgd proces te beschikken voor de registratie, rapportage en afhandeling van informatiebeveiligingsincidenten die aansluit op het incidentmanagementproces van Opdrachtgever waarbij ten minste de eisen worden geïmplementeerd uit de richtlijn IBR-5 *Richtlijn voor informatiebeveiligingsincidenten* {10}. Ten minste maandelijks dient over deze informatiebeveiligingsincidenten gerapporteerd te worden richting Opdrachtgever.

16.1.SC-19 De Opdrachtnemer dient over een operationeel geborgd proces te beschikken voor de registratie en de response op security incident en/of event meldingen van het Security Operations Centre van Opdrachtgever.

1.12 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

17.1.2 Opdrachtnemer dient aantoonbaar te beschikken over een continuïteitsplan voor het handhaven van de Prestatie in ongunstige situaties conform de BIO Algemene handreiking continuïteitsbeheer {14}, waarin ook de continuïteit van de informatiebeveiliging is gewaarborgd.

17.1.3 Opdrachtnemer dient het continuïteitsplan voor de Prestatie minimaal jaarlijks aantoonbaar te verifiëren en bij te werken om te waarborgen dat deze deugdelijk en doeltreffend blijft. Voor het continuïteitsplan kan uitgegaan worden van de BIO Algemene handreiking continuïteitsbeheer {14}.

1.13 Naleving

18.1.3 Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor het beschermen tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave, van registraties op informatiesystemen betrokken bij de Prestatie, in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen.

18.1.SC-20 De Opdrachtnemer dient maatregelen te treffen om documenten, zoals offertes, contracten, netwerkschema's, risicoanalyse uitwerkingen, kwetsbaarheidscans, penetratie testrapporten en accounts en wachtwoorden te beveiligen tegen spionage in de breedste zin des woords.

18.1.CC-09 Gegevens of programmatuur van Opdrachtgever, of door deze gegenereerde metadata, welke zich bevinden op informatiesystemen van Opdrachtnemer, is en blijft ten allen tijde eigendom van Opdrachtgever. Indien gegevens door Opdrachtgever aan Opdrachtnemer zijn verstrekt, mag Personeel dit alleen gebruiken voor het doel waarvoor dit is gebeurd.

18.1.CC-10 Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor het vernietigen van gegevens of programmatuur van Opdrachtgever op apparatuur en alle back-up media van Opdrachtnemer, na contractbeëindiging tussen beide partijen.

18.1.CC-12 Wanneer gegevens van Opdrachtgever zich bevinden op informatiesystemen van Opdrachtnemer, dient bij contractbeëindiging tussen deze beide partijen, de Opdrachtnemer assistentie te leveren bij de overdracht van deze informatie naar de nieuwe leverancier of terug naar Opdrachtgever.

18.1.CC-14 Wanneer gegevens of programmatuur van Opdrachtgever zich bevinden op informatiesystemen van Opdrachtnemer, dient Opdrachtnemer aan te geven waar deze informatiesystemen zich bevinden. Indien deze zich buiten de EU bevinden, mag dit uitsluitend in landen waar een passend niveau van gegevensbescherming wordt geboden; welke landen dit zijn, is bepaald door de Europese Commissie[1].

18.1.SC-23 De Opdrachtnemer dient bij inzet van certificaten voor publieke webdiensten van RWS of het authentiseren van servers met samenwerkingspartners gebruik te maken van PKI Overheid certificaten die aangevraagd moeten worden bij Opdrachtgever. In overige gevallen dienen de passende standaarden te worden gehanteerd conform de NCSC richtlijn ICT-beveiligingsrichtlijnen voor Transport Layer Security {1}.

18.2.1 Opdrachtnemer dient tenminste jaarlijks een audit uit te voeren naar de opzet, bestaan en werking van de maatregelen op het gebied van de informatiebeveiliging gemeld in het contract met Opdrachtgever, en deze Opdrachtgever te rapporteren (als onderdeel van het Informatiebeveiliging Beveiligingsplan IV) over de bevindingen en voorgenomen verbetermaatregelen.

18.2.2 Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor het periodiek beoordelen van de naleving van beleidsregels, normen en andere eisen betreffende beveiliging, bij Personeel betrokken bij de Prestatie.

18.2.3 Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor het periodiek beoordelen van de naleving van technische beleidsregels, normen en andere eisen betreffende beveiliging bij informatiesystemen betrokken bij de Prestatie. Naleving kan aangetoond worden met (geautomatiseerde) kwetsbaarheidsanalyses of pentesten, zie daarvoor de BIO Handreiking: Penetratietesten {12}.

18.2.SC-09 Opdrachtnemer dient een Informatiebeveiliging Beveiligingsplan uit te werken waarin de getroffen beheersmaatregelen zijn uitgewerkt en het Informatiebeveiliging Beveiligingsplan jaarlijks actualiseren naar aanleiding van de periodieke beoordelingen van opzet, bestaan en werking van de

[1] Momenteel zijn dit: Noorwegen, IJsland, bepaalde Kanaaleilanden, Argentinië, Canada, Zwitserland en de VS (met beperkingen).

beheersmaatregelen. De template voor het Informatiebeveiliging Beveiligingsplan IV {15} wordt door de opdrachtgever beschikbaar gesteld.

18.2.SC-10 Opdrachtnemer dient in afstemming met Opdrachtgever het Informatiebeveiliging Beveiligingsplan op te stellen.

18.2.SC-21 Opdrachtnemer dient met Opdrachtgever specifiek af te stemmen voor afwijkingen op de security eisen voor processen en informatiesystemen betrokken bij de Prestatie. Opdrachtnemer dient deze afwijkingen vast te leggen als een explain in het Informatiebeveiliging Beveiligingsplan IV en het eventuele restrisico eveneens te beschrijven.

18.2.SC-22 De Opdrachtnemer dient conform de gemaakte afspraken met Opdrachtgever inzake eventuele explains invulling te geven aan het verbeterplan voor de explains en periodiek hierover de status te rapporteren aan Opdrachtgever.

18.2.SC-08 Opdrachtnemer dient zich te houden aan de afspraken en procedures op het gebied van informatiebeveiliging waarin doel, wijze, en frequentie van contact over de informatiebeveiliging beschreven staat op strategisch, tactisch en operationeel niveau.

Appendix A: Bronnen in contractteksten

In de contractteksten staan bronnen vermeld; het gaat hier om de volgende bronnen.

Nummer	Bron
{1}	Nationaal Cyber Security Center (NCSC), "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)", URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
{2}	Rijkswaterstaat IRN, "Afspraken en Procedures Netwerkdienstverlening: Netwerktoegang voor Derden".
{3}	Centrum Informatiebeveiliging en Privacy (CIP), "Grip op SSD - Beveiligingseisen voor (web)applicaties", URL: SSD normen V3.0 (cip-overheid.nl) / https://www.cip-overheid.nl/category/producten/secure-software/
{4}	Rijksoverheid: Handreiking Mobiele App Ontwikkeling en Beheer voor de RIjksoverheid: https://www.noraonline.nl/wiki/Mobility / Handreiking_Mobiele_App_3.0.pdf (noraonline.nl)
{5}	Rijkswaterstaat IRN, "RWS IV Aansluitvoorwaarden/RIVA", URL: Classificatie RWS Informatie: https://www.rijkswaterstaat.nl/zakelijk/zakendoen-met-rijkswaterstaat/werkwijzen/werkwijze-in-iv/index.aspx
{6}	Rijkswaterstaat IRN, "Aansluitvoorwaarden NNV Rijkswaterstaat"
{7}	Open Web Application Security Project (OWASP), "OWASP Top 10" https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
{8}	BIO Handreiking Veilige afvoer van ICT-middelen https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/04/201902-Handreiking-Veilige-afvoer-van-ICT-middelen-v2.0.pdf ☐
{9}	BIO Handreiking Mobile Device Management https://www.informatiebeveiligingsdienst.nl/product/mobile-device-management/
{10}	Richtlijnen informatiebeveiliging bij RWS IV-contracteisen v1.0
{11}	BIO Handreiking Risicoanalysemethode https://www.informatiebeveiligingsdienst.nl/product/handreiking-diepgaande-risicoanalyse-methode-gemeenten/
{12}	BIO Handreiking Penetratietesten https://www.informatiebeveiligingsdienst.nl/product/handreiking-penetratietesten-v1-0/
{13}	Handreiking Risicomanagement ISO-27005
{14}	BIO Algemene handreiking continuïteitsbeheer https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/07/201903-Model-Continu%C3%AFteitsplan_v2.0.docx
{15}	Template Informatiebeveiliging Beveiligingsplan IV
IBR-1	Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Beleid voor gegevensclassificatie"
IBR-2	Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Beleid voor logische toegangsbeveiliging"
IBR-3	Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Beleid voor wachtwoordgebruik"

IBR-4	Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor beveiligen bij ontwikkelen"
IBR-5	Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor informatiebeveiligingsincidenten"
IBR-6	Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor fysieke beveiliging"
IBR-7	Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor logging"
IBR-8	Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT systemen van RWS"

VERBORGEN tekst in de alinea hieronder, deze alinea is bestemd voor OG
Indien de contractteksten worden gebruikt door andere diensten dan RWS kan ervoor gekozen worden om deze bronnen aan te passen naar eigen organisatie-specifieke bronnen. De bronnen die daadwerkelijk worden genoemd in een definitieve contracttekst dienen uiteraard als bijlage te worden meegestuurd met het contract (dat is niet noodzakelijk als de link publiekelijk toegankelijk is)!

Appendix B: Nummering van contracteisen

De nummering van de contracteisen verwijst naar de overeenkomstige driepuntsnormen in het NEN document "ISO/IEC 27002:2013: IT Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging" en dient primair voor intern RWS gebruik. Omdat dit praktisch bleek is echter in sommige gevallen van deze nummering afgeweken. Het gaat hier om de onderstaande afwijkingen:

1. In sommige gevallen is een eis in tweeën gesplitst; in dat geval zijn er een "a" een "b" achter de driepuntsnorm geplaatst om het onderscheid te kunnen maken.
2. In sommige gevallen zijn de driepuntsnormen onder één tweepuntsnorm samengevoegd tot één contracteis waarbij het derde cijfer in de driepuntsnorm-notatie is vervangen door een "x".

Eisen uit het CIP document "Cloud computing - Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)" waarvoor geen overeenkomstige eis bestaat binnen ISO/IEC 27002, zijn toegevoegd bij een corresponderende tweepuntsnorm, met als derde "cijfer" in de driepuntsnotatie "CC-n", waarbij "n" overeenk