

Proceseisen

Behorend bij de Raamovereenkomst 3B

1 oktober 2026

Kenmerk <ROK Proceseisen v1.0 01-10-2026 definitief>

Versie 1.0

Definitief

bronversie Format A-302 v20260115



Gemeente Utrecht

Utrecht.nl

1	Inleiding	3
1.1	Algemene bepalingen	3
1.2	Audits	3
1.3	Communicatie	4
1.4	Documentatie	5
1.5	Facturatie	5
1.6	Garantie	6
1.7	Intellectueel eigendom	6
1.8	Issueregister	6
1.9	Medewerkers	6
1.10	Project Management Plan	7
1.11	Projectorganisatie	8
1.12	Projectoverleg	9
1.13	Rapportages	10
1.14	Risicomanagement	10
1.15	Tussenevaluaties	11
1.16	Veiligheid en Gezondheid	11
1.17	Voorstel tot Wijziging (VtW)	12
1.18	Cybersecurity en informatiebeveiliging (ICO)	13

1 Inleiding

In dit document zijn de proceseisen opgenomen waar in de uitvoering van de Raamovereenkomst 3B aan dient te worden voldaan. Door het indienen van uw inschrijving voor deze opdracht verklaart u onvoorwaardelijk akkoord te gaan met ALLE eisen aan de opdracht.

De eisen zijn thematisch gegroepeerd in paragrafen. De volgorde van de paragrafen is alfabetisch.

1.1 Algemene bepalingen

1.	Opdrachtnemer richt zijn werkzaamheden zodanig in dat deze beheerst binnen de kaders van de ROK en de betreffende NOK verlopen.
2.	Opdrachtnemer voldoet gedurende de contractduur aan alle voor de opdracht relevante normen, beleidskaders en contractvoorwaarden die in de aanbestedingsstukken van toepassing worden verklaard alsmede aan alle van toepassing zijnde wet- en regelgeving.
3.	Opdrachtnemer dient binnen de in de aanvraag genoemde termijn na ontvangst van een aanvraag voor een NOK een voorstel in te dienen. Dit voorstel bevat minimaal scope, uitgangspunten, aanpak, planning, raakvlakken, risico's, benodigde inzet, prijsopbouw en acceptatiepunten.
4.	De offerteprijs voor een NOK dient transparant te zijn opgebouwd en gebaseerd te zijn op de tarieven en eenheidsprijzen zoals afgegeven in het prijsinvulformulier bij inschrijving.
5.	Opdrachtnemer mag werkzaamheden onder een NOK pas starten nadat deze NOK door Opdrachtgever is getekend.
6.	Indien Opdrachtnemer onvoldoende capaciteit levert, structureel afspraken niet nakomt of prestaties achterblijven, dient Opdrachtnemer op verzoek van Opdrachtgever binnen twee weken een herstelplan op te stellen met maatregelen, planning, verantwoordelijken en rapportagemomenten.
7.	Opdrachtnemer blijft te allen tijde volledig verantwoordelijk voor ontwerp, verificatie, validatie, testresultaten, kwaliteit en conformiteit van de op te leveren systemen, tooling en documentatie. Toetsing, review, opmerkingen, audits, deelname aan testen of acceptatie door Opdrachtgever verminderen of verplaatsen deze verantwoordelijkheid niet.

1.2 Audits

8.	Opdrachtgever heeft het recht om een audit of inblikmoment uit te voeren op locatie van opdrachtnemer, in de OTAP-omgeving of op andere relevante uitvoeringslocaties.
9.	Opdrachtnemer verleent volledige en tijdige medewerking aan audits, inspecties, controles en verbeteracties die uit dergelijke inblikmomenten voortkomen.
10.	De kosten gemaakt door Opdrachtnemer voor de audit zijn voor Opdrachtnemer.
11.	Tijdens een audit kunnen, niet limitatief, onderstaande onderwerpen gecontroleerd worden: a. Technische ontwerpen b. Naleving richtlijnen Opdrachtgever en OEM zowel ten aanzien van software en hardware c. De organisatie van Opdrachtnemer d. Naleving ontwerpprocessen e. Naleving beheerprocessen f. Naleving kwaliteitssysteem

	g. Kennisborging h. Productontwikkeling i. Informatiebeveiliging
12.	Uiterlijk drie weken na de audit zal Opdrachtgever aan Opdrachtnemer het auditrapport verstrekken. Dit rapport bestaat uit: a. Het auditresultaat per gecontroleerd onderwerp. b. Per gecontroleerd onderwerp eventuele acties.
13.	De opvolging van deze acties kunnen tijdens een aparte audit door Opdrachtgever gecontroleerd worden.
14.	Opdrachtgever is gerechtigd de audit (mede) te laten uitvoeren door een externe partij waaronder in ieder geval ook de OEM wordt verstaan.

1.3 Communicatie

15.	Gedurende de gehele duur van de Raamovereenkomst en daarop gebaseerde Nadere overeenkomsten vindt alle mondelinge en schriftelijke communicatie, inclusief storingsmeldingen, rapportages, ontwerpen en overdrachtsdocumenten, plaats in het Nederlands.
16.	Schriftelijke communicatie tussen Opdrachtnemer en Opdrachtgever dient plaats te vinden per e-mail. Mondelinge afspraken dienen schriftelijk te worden bevestigd door Opdrachtnemer binnen 2 Werkdagen.
17.	Opdrachtnemer dient er rekening mee te houden ten aanzien van al zijn werkzaamheden dat: - de werkdagen van Opdrachtgever maandag t/m donderdag zijn. - de werktijden van Opdrachtgever 08:30 tot 17:00 zijn. Afwijkingen op bovengenoemde werkdagen en tijden zijn in onderlinge afstemming mogelijk zowel op initiatief van Opdrachtgever als Opdrachtnemer.

1.4 Documentatie

18.	Alle door Opdrachtnemer opgebouwde beheergegevens, configuraties, documentatie, bronbestanden en registraties worden zodanig ingericht dat eenvoudige digitale overdracht aan Opdrachtgever of derde partij mogelijk is. Opdrachtnemer dient voor documentatie, configuraties en uitwisselbestanden gangbare formaten te gebruiken zodat hiervoor geen exclusieve tooling noodzakelijk is.
19.	Uitwisseling en opslag van digitale documenten dient plaats te vinden middels de online omgeving van Opdrachtnemer. Hiervoor krijgen door Opdrachtgever aangewezen personen toegangsrechten.
20.	Na afsluiting van een NOK verwijdt Opdrachtnemer bedrijfsvertrouwelijke informatie van Opdrachtgever van eigen systemen, voor zover bewaarplichten of schriftelijke afspraken tussen Opdrachtgever en Opdrachtnemer zich daar niet tegen verzetten.
21.	Ter bevordering van de efficiënte inzet van Opdrachtgever dient Opdrachtnemer kwaliteitsmanagement te borgen dat documenten die ter review aan Opdrachtgever worden aangeboden maximaal in twee reviewrondes geaccepteerd kunnen worden. De eerste ronde is het aanleveren van reviewcommentaar, de tweede ronde is het beschouwen van de wijzigingen naar aanleiding van de review. Als een derde ronde noodzakelijk is, dient de Opdrachtnemer dit binnen de planning op te lossen en aantoonbaar te verbeteren zodat dit niet nogmaals optreedt.
22.	Opdrachtnemer past aantoonbaar versiebeheer toe op documentatie, software, configuraties, inclusief historie van wijzigingen en vrijgaven. Definitieve documenten hebben versies x.0, versies ter review x.n.
23.	Opdrachtnemer stelt per NOK een overzicht op van de te leveren documentatie en biedt dit ter acceptatie aan aan Opdrachtgever.
24.	Opdrachtnemer zal documentatie met betrekking tot haar leveringen steeds actueel houden. Zodra blijkt dat de documentatie niet of niet langer juist of volledig is, zal Opdrachtnemer de documentatie zo spoedig mogelijk en uiterlijk binnen 20 werkdagen actualiseren.

1.5 Facturatie

25.	Facturatie kan alleen plaatsvinden op basis van prestatieverklaringen van Opdrachtgever aan Opdrachtnemer.
26.	Prestatieverklaringen kunnen uitsluitend worden aangevraagd op werkpakketten en leveringen zoals gespecificeerd in (a) het tussen Opdrachtgever en Opdrachtnemer overeen te komen Project Management Plan (PMP) voor de betreffende NOK of (b) overeengekomen Voorstellen tot Wijziging.
27.	Facturen dienen transparant te zijn opgebouwd zodanig dat zij zijn te relateren aan de eenheidsprijzen en tarieven zoals bij inschrijving zijn opgegeven in het prijsinvulformulier.
28.	Factuurbedragen die niet te relateren zijn aan een overeengekomen werkpakket of levering worden door Opdrachtgever afgewezen.
29.	Factuurbedragen die niet te relateren zijn aan de afgegeven prijzen en tarieven zoals bij inschrijving zijn opgegeven in het prijsinvulformulier worden door Opdrachtgever afgewezen.
30.	Het verzoek tot afgifte van een prestatieverklaring dient: 1) schriftelijk te geschieden; 2) vergezeld te gaan van een overzicht van de binnen de betaalpost uitgevoerde werkzaamheden en/of geleverde systemen, en indien van toepassing door de Opdrachtgever geaccepteerde V&V rapportages waaruit blijkt dat leveringen voldoen aan de eisen in het PVE.

31.	De prijs van een Werkpakket en de prijzen van daarin benoemde Werkzaamheden dienen in overeenstemming te zijn met werkelijk uit te voeren Werkzaamheden en de daarbij behorende prijzen en tarieven zoals bij inschrijving zijn opgegeven in het prijsinvulformulier.
32.	De bedragen voor alle indirecte kosten, eventuele opbrengsten en winst en risico dienen te zijn inbegrepen in de bedragen van de verschillende werkpakketten en dus niet als apart werkpakket te zijn opgenomen.

1.6 Garantie

33.	Opdrachtnemer dient een garantieverklaring af te geven met betrekking tot alle in het kader van een NOK, vallend onder de ROK, geleverde systemen, tooling en documentatie.
34.	Voorname garantieverklaring dient te gelden tot minimaal 12 maanden na acceptatie door Opdrachtgever van het betreffende systeem, tooling of documentatie.
35.	Binnen de afgegeven garantieperiode dient Opdrachtgever op eerste aanzegging van Opdrachtgever het item waar de garantie op wordt afgeroepen zo spoedig mogelijk te herstellen respectievelijk geheel of gedeeltelijk te vervangen.

1.7 Intellectueel eigendom

36.	Alle systeemdocumentatie, ontwikkelde tooling en systemen welke gedurende de Raamovereenkomst door Opdrachtnemer wordt ontwikkeld in het kader van een Nadere Overeenkomst, dient te worden gekwalificeerd als Maatwerk(programmatuur) en is conform artikel 21.4 van de Algemene Voorwaarden, vanaf datum oplevering eigendom van Opdrachtgever.
37.	Voor zover systemen, tooling en documentatie niet in het kader van een Nadere Overeenkomst zijn ontwikkeld maar wel nodig zijn voor gebruik en beheer verleent Opdrachtnemer aan Opdrachtgever hiertoe voor onbepaalde tijd de volledige gebruiksrechten. Onder gebruik en beheer wordt ook verstaan: onderhoud, wijziging, herstel, doorontwikkeling en overdracht aan een derde partij, inclusief eventuele wachtwoorden en andere toegangsbeveiligingsmiddelen.

1.8 Issueregister

38.	Opdrachtnemer beheert een issueregister voor issues met betrekking tot de Raamovereenkomst en de daaronder vallende Nadere Overeenkomsten. Het issueregister heeft ten doel om alle issues (gebreken, storingen, incidenten, wijzigingen, wensen, etc) te registreren en opvolgbaar te maken.
39.	Het risico- en issueregister dient geplaatst te worden binnen de digitale omgeving van de raamovereenkomst zodat deze continue inzichtelijk en beschikbaar is voor Opdrachtgever.

1.9 Medewerkers

40.	Medewerkers met toegang tot OT/PA-systemen beschikken aantoonbaar over de voor hun rol vereiste deskundigheid m.b.t. OT, betreffende OEM-systeemplatform, nautische objecten
-----	--

	en brug-bediening en -besturing (middels ervaring en referenties) en volgen relevante veiligheids- en cybersecurity-instructies.
41.	Opdrachtnemer dient ten behoeve van project- en contractmanagement uitsluitend personeel in te zetten dat hier voldoende kennis en ervaring mee heeft. Onder voldoende ervaring wordt verstaan: - Minimaal HBO werk- en denkniveau - Aantoonbare affiniteit met OT/PA
42.	Al het personeel dat werkzaamheden verricht nabij de elektrische energievoorziening of -sturing van objecten van Opdrachtgever dient ten minste over een aanwijzing Voldoende Onderricht Persoon (VOP) of, indien deze elektrotechnische werkzaamheden verricht, Vakbekwaam Persoon (VP) conform de NEN3140 te beschikken. Deze aanwijzing dient minimaal 2 weken voor aanvang van de werkzaamheden aan Opdrachtgever overhandigt te worden waarna Opdrachtgever voor de duur van de werkzaamheden een schriftelijke aanwijzing verstrekt aan de desbetreffende persoon van Opdrachtnemer.
43.	Opdrachtnemer stelt een lijst op van al het personeel dat voldoet aan bovenstaande kwalificaties en dat wordt ingezet voor werkzaamheden bij Opdrachtgever. Deze lijst dient beheerd te worden door Opdrachtnemer en gedeeld te worden met Opdrachtgever.
44.	Opdrachtnemer dient personeelwijzigingen in het kader van de Raamovereenkomst of één van de Nadere Overeenkomsten tenminste een maand vooraf, kenbaar te maken.
45.	Vervanging van sleutelrollen vindt uitsluitend plaats met minimaal gelijkwaardige kandidaten en wordt vooraf afgestemd met Opdrachtgever. Opdrachtgever bepaalt daarbij wat sleutelrollen zijn.
46.	Vervanging van personeel mag niet leiden tot capaciteits -en/of kennisverlies waardoor gecontracteerde werkzaamheden worden vertraagd.
47.	Opdrachtgever is gerechtigd om Opdrachtnemer te verzoeken personeel te vervangen waar Opdrachtnemer gehoor aan dient te geven. Hiertoe kan worden overgegaan indien één of meer van onderstaande situaties aantoonbaar van toepassing is: 1) Personeel blijkt ongeschikt om werkzaamheden uit te voeren (bijvoorbeeld bij herhaling fouten maken die leiden tot gebreken of vertragingen bij het oplossen van gebreken). 2) Personeel heeft zich op enigerlei gedragen in strijd met de gedragscode van Opdrachtgever.

1.10 Project Management Plan

48.	Een door Opdrachtgever geaccepteerd PMP is een voorwaarde om te starten met de werkzaamheden.
49.	Elke wijziging op het PMP dient ter beoordeling en acceptatie te worden voorgelegd aan Opdrachtgever.
50.	Opdrachtnemer actualiseert het PMP minimaal elke 3 maanden gedurende de duur van de betreffende NOK. Hiermee bewerkstelligt Opdrachtnemer dat het PMP bij voortduring geschikt, passend en doeltreffend blijft.
51.	Opdrachtnemer doet voor wat betreft haar PMP (en overige documenten die met Opdrachtgever worden gedeeld) aan versiebeheer. Elke nieuwe versie geeft in een overzicht aan wat er is veranderd t.o.v. de vorige versie.
52.	Opdrachtgever geeft binnen uiterlijk 10 werkdagen commentaar op een concept PMP dat ter beoordeling door Opdrachtnemer wordt ingediend.
53.	Opdrachtnemer verwerkt binnen uiterlijk 10 werkdagen het commentaar van Opdrachtgever in een nieuwe versie van het PMP welke binnen diezelfde termijn aan Opdrachtgever wordt opgeleverd.
54.	Het PMP dient een nadere invulling te zijn van het beknopte Plan van Aanpak zoals ingediend bij de inschrijving.

55.	Opdrachtnemer dient in het PMP te beschrijven met welke onderaannemers (indien van toepassing) zij in het kader van NOK1 samenwerkt en hoe deze samenwerking vorm wordt gegeven. Op de inzet van onderaannemers geldt het gestelde in de Algemene Voorwaarden.
56.	Het PMP dient een facturatieschema te bevatten op basis van de werkpakketten zoals gedefinieerd in de Work Breakdown Structure (WBS) in het PMP. Zie ook de eisen die zijn gesteld aan PMP en facturatie in de "ROK Proceseisen"
57.	Het PMP dient in separate deelplannen en/of hoofdstukken in te gaan op de hieronder afzonderlijk gespecificeerde onderwerpen: - Projectplanning > work breakdown structure in termen van werkpakketten > planning - Projectorganisatie - Onderaanneming - Projectoverleggen - Voortgangsrapportages - Ontwerp en Engineering: > eisenmanagement > raakvlakmanagement > veiligheidsfuncties > risicobeoordelingen > verificatie en validatie - Stakeholdermanagement - Documentatie - Implementatieplan - Escalatieproces Voor deze onderwerpen kunnen in de Programma's van Eisen (PvE's) van de Nadere Overeenkomsten nadere eisen zijn gespecificeerd waaraan in de uitwerking dient te worden voldaan.
58.	Daar waar de onderwerpen die uitgewerkt dienen te worden in het PMP reeds zijn uitgewerkt in een gecertificeerd KwaliteitsManagementSysteem (KMS) van Opdrachtnemer, dient in het PMP daarnaar te worden verwezen. Opdrachtgever dient inzage te krijgen in het betreffende KMS.
59.	De projectplanning dient een heldere fasering van werkzaamheden te bevatten in termen van werkpakketten op basis waarvan prestatieverklaringen kunnen worden afgegeven ten behoeve van de facturatie.
60.	De projectplanning dient het kritieke pad te tonen.
61.	De projectplanning dient te voorzien in buffers (in de tijd). Deze dienen gerelateerd te zijn aan geïdentificeerde risico's uit het risicodossier.

1.11 Projectorganisatie

62.	Ten behoeve van stakeholdermanagement dient Opdrachtnemer een RASCI-tabel op te zetten waarin naast de functionarissen van Opdrachtnemer ook de functionarissen van Opdrachtgever zijn opgenomen. Deze RASCI-tabel dient door Opdrachtnemer in gezamenlijkheid met Opdrachtgever te worden opgesteld. Dit geldt voor zowel de Raamovereenkomst alsmede voor de daaronder vallende individuele Nadere Overeenkomsten. Hierbij streeft Opdrachtgever naar een directe aanspreekpartner voor de volgende rollen in zijn team: Project Manager, Technisch Manager, Contract Manager en Manager Projectbeheersing. De RASCI tabellen voor de Nadere Overeenkomsten dienen te
-----	---

	worden opgenomen in de Project Management Plannen (PMP) voor de betreffende Nadere Overeenkomsten.
63.	Opdrachtgever dient na opdracht voor een NOK een kick-off vergadering te organiseren waaraan alle betrokken functionarissen van de Opdrachtnemer dienen deel te nemen.
64.	Opdrachtgever en Opdrachtnemer bereiden dit kick-off overleg gezamenlijk voor.
65.	Het kick-off overleg wordt genotuleerd door de Opdrachtnemer. Tot het verslag behoort een actie- en besluitenlijst.
66.	Het verslag van het kick-off overleg wordt ter review en acceptatie aangeboden aan Opdrachtgever en op het eerstvolgende projectoverleg vastgesteld.
67.	Opdrachtnemer dient uiterlijk 10 werkdagen voorafgaande aan het kick-off overleg een concept Project Management Plan (PMP) voor de betreffende Nadere Overeenkomst (NOK) in bij Opdrachtgever.
68.	Opdrachtnemer dient op basis van de uitkomst van het kick-off overleg het concept PMP aan te passen en uiterlijk 10 werkdagen na het kick-off overleg in te dienen bij Opdrachtgever.
69.	Opdrachtnemer wijst uiterlijk bij contractstart één vaste accountmanager en één plaatsvervanger aan als aanspreekpunt voor de uitvoering van de ROK.
70.	Opdrachtnemer wijst uiterlijk bij contractstart één vaste project- en technisch manager aan als aanspreekpunt voor de uitvoering van de ROK.
71.	Indien Opdrachtnemer werkzaamheden uitbesteedt aan onderaannemers levert Opdrachtnemer technische regie, toetsing en afstemming zodat de integraliteit van de werkzaamheden wordt geborgd.
72.	Voor werkzaamheden welke niet tot de scope van de Raamovereenkomst of van één van de Nadere Overeenkomsten behoren, maar wel noodzakelijk zijn voor de werking en oplevering van de op te leveren scope, heeft de Opdrachtnemer coördinatie verplichting over de door Opdrachtgever ingeschakelde derden. Dit betreft bijvoorbeeld de aannemer die in het kader van NOK1 de bouwkundige aanpassingen aan de bediencentrale uitvoert, of de provider van het fiber-netwerk tussen de bediencentrale en de bruggen.
73.	Opdrachtnemer dient te beschikken over een organisatie die in staat is de projectwerkzaamheden uit dit PvE te realiseren conform aantoonbare kwaliteitsprocessen zodat: a. de geëiste kwaliteit gerealiseerd wordt; b. de planning nageleefd wordt; c. proactief gehandeld wordt bij Issues.
74.	Opdrachtnemer beschikt gedurende de looptijd van de Raamovereenkomst over aantoonbare expertise en voldoende capaciteit voor OT/PA-engineering, beheer, cybersecurity, test/release, documentatiebeheer en storingsdienst en domeinkennis t.a.v. nautische objecten, brugbediening en -besturing en evt. andere activiteiten welke nodig zijn in het kader van deze ROK met de daaronder overeengekomen NOK's.
75.	Opdrachtnemer dient te beschikken over een organisatie die: a. haar, voor deze Raamovereenkomst noodzakelijke, kennis aantoonbaar borgt. b. werkt op basis van een ISO 9001 (of vergelijkbare norm) gecertificeerd kwaliteitssysteem.

1.12 Projectoverleg

76.	Opdrachtnemer organiseert ieder kwartaal een raamovereenkomstoverleg waarin haar raamovereenkomstrapportage wordt besproken. Opdrachtnemer levert daarvan binnen twee werkdagen een verslag met acties en eigenaren.
77.	Projectoverleggen in het kader van de Raamovereenkomst en de daaronder vallende Nadere Overeenkomsten worden op een locatie van Opdrachtgever gehouden. Vergaderruimte worden via Opdrachtgever gereserveerd. In overleg en als noodzakelijk kunnen incidenteel bijeenkomsten bij Opdrachtnemer gehouden worden.

78.	Projectoverleggen in het kader van de Raamovereenkomst en de daaronder vallende Nadere Overeenkomsten dienen minimaal 10 werkdagen van te voren door Opdrachtnemer in overleg met Opdrachtgever te worden vastgesteld.
79.	Voor alle momenten waarop informatie en/of een bijdrage van Opdrachtgever is gewenst neemt Opdrachtnemer initiatief om dit tijdig te plannen.

1.13 Rapportages

80.	Opdrachtnemer levert elke kwartaal een raamovereenkomstrapportage op met de status van lopende NOK's, afwijkingen, Voorstellen tot Wijziging (VTW's), risico's, issues, capaciteit, besluiten, afhankelijkheden en openstaande acties.
81.	Opdrachtnemer dient voor de afzonderlijke NOK's vierwekelijks een voortgangsrapportage op te stellen en deze uiterlijk één week voor het eerstvolgende overleg met Opdrachtgever digitaal te verstrekken aan de Opdrachtgever.
82.	In de voortgangsrapportage dienen tenminste de volgende onderdelen te worden opgenomen: a. Voortgang op hoofdlijnen: - beschrijving van de voortgang per product of activiteit sinds de vorige rapportage; - (mogelijke) knelpunten in de voortgang; - actuele projectplanning en afwijkingen ten opzichte van de baseline projectplanning ; b. Risico's: - top 5 risico's uit het risicodossier en de beheersmaatregelen; - wijzingen of aanvullingen op het risicodossier. c. Overzicht van Issues waarbij het volgende onderscheid wordt gemaakt: - nieuw geïdentificeerde Issues met beschrijving mogelijk gevolg in geld, tijd en kwaliteit - Onder handen issues - Afgehandelde Issues d. Raakvlakken - Nieuwe raakvlakken - Gewijzigde raakvlakken e. Facturatie f. Cybersecurity en Informatieveiligheid g. Veiligheid en Gezondheid (V&G)

1.14 Risicomanagement

83.	Opdrachtnemer bereidt voor de afzonderlijke NOK's risicobedoelingen voor en faciliteert deze met de door Opdrachtgever aangewezen disciplines. Indien Opdrachtgever een risicomethodiek of format beschikbaar stelt, past Opdrachtnemer deze toe. Uitgangspunten, voorgestelde beheersmaatregelen, veiligheidsfuncties en restrisico's worden ter acceptatie aan Opdrachtgever voorgelegd en pas na acceptatie als ontwerp- of wijzigingsuitgangspunt gehanteerd.
84.	Risicobedoelingen worden opgenomen in de projectplanningen van de afzonderlijke NOK's
85.	Opdrachtnemer beheert een risicoregister voor risico's met betrekking tot de Raamovereenkomst en de daaronder vallende Nadere Overeenkomsten. Risico's betreffen kwaliteit, tijd, geld.

1.15 Tussenevaluaties

86.	Middels een tussenevaluatie kunnen Opdrachtgever en Opdrachtnemer reflecteren op activiteiten en gebeurtenissen met als doel hiervan te leren en het geleerde toe te passen bij de verdere invulling van de Overeenkomst. Aspecten die hierbij aan bod komen zijn bijvoorbeeld: a. Kwaliteit geleverde diensten en producten b. Samenwerking c. Communicatie d. Prestaties e. Opvolging van plannen en (verbeter-)acties
87.	Tussenevaluaties staan los van andere in dit PvE genoemde overleggen.
88.	Opdrachtgever en Opdrachtnemer mogen beide het initiatief nemen tot een tussenevaluatie en zijn beide verplicht hieraan deel te nemen.
89.	De aanwezigen bij de tussenevaluatie zijn afkomstig uit het project- en beheerteams van beide partijen.
90.	De tussenevaluatie wordt in onderling overleg gepland. De eerste dient bij voorkeur binnen een maand na initiatie van de overeenkomst gehouden te worden.
91.	Er is geen beperking op het aantal en de duur van een tussenevaluatie, wel dient er rekening gehouden te worden met twee tussenevaluaties per jaar.

1.16 Veiligheid en Gezondheid

92.	Voor zover een NOK ontwerp- en/of uitvoeringsfasen bevat dient Opdrachtnemer voor deze fasen afzonderlijke Veiligheids- en Gezondheidsplannen (V&G-plannen) op te stellen. Gedurende de contractperiode van de betreffende NOK dienen deze V&G-plannen gehanteerd en geactualiseerd te worden. Een V&G-plan dient uiterlijk twee maanden voordat de fase waarop het V&G-plan betrekking heeft ter acceptatie voorgelegd te worden aan Opdrachtgever.
93.	De V&G-plannen dienen ten minste te voldoen aan artikel 2.28 van het Arbeidsomstandighedenbesluit en omvatten minimaal de volgende onderdelen: a. een beschrijving van de organisatie ten aanzien van V&G met overzicht van alle bij het werk betrokken partijen; b. een projectspecifieke inventarisatie en evaluatie van de: - projectrisico's, - samenlooprisico's, - specifieke risico's die samenhangen met doorgaande exploitatie. c. de te nemen maatregelen; d. de gemaakte afspraken die zijn vastgelegd over de uitvoering van deze maatregelen en het toezicht op de naleving ervan; e. de bouwkundige, technische en organisatorische (BTO) keuzes die in de ontwerpfase zijn gemaakt met betrekking tot veiligheid en gezondheid.
94.	Opdrachtgever stelt Opdrachtnemer aan als Veiligheid en Gezondheid (V&G) coördinator ontwerpfase, conform artikel 2.29 van het Arbeidsomstandighedenbesluit. Opdrachtnemer geeft uitvoering aan de coördinatietaken genoemd in artikel 2.30 van het Arbeidsomstandighedenbesluit. Opdrachtnemer zal één of meer coördinatoren voor de uitvoeringsfase en het eventuele Meerjarig Onderhoud (V& G- coördinatoren) aanstellen, indien hij daartoe op grond van artikel 2.29 van het Arbeidsomstandighedenbesluit verplicht is. De aangestelde coördinatoren geven uitvoering aan de coördinatietaken genoemd in artikel 2.31 van het Arbeidsomstandigheden besluit.

95.	In de uitvoeringsfase (waarin fysieke werkzaamheden worden uitgevoerd aan de objecten) dient de uitvoerende partij alle medewerkers en derden voor te lichten over de inhoud van het V&G-plan voor de betreffende uitvoeringsfase en overige relevante informatie vanuit bijvoorbeeld een BLVC-plan (toolbox). Dit dient te gebeuren bij de start van de werkzaamheden en dient herhaald te worden ieder keer wanneer iemand de bouwplaats bezoekt of voor het eerst werkzaamheden uit gaat voeren. Opdrachtnemer dient bij de eerste V&G instructies een vertegenwoordiger van Opdrachtgever uit te nodigen om zich te vergewissen dat de instructies en regels omtrent veilig werken volledig en juist zijn. Op initiatief van deze vertegenwoordiger kan besloten worden de aanwezigheid bij volgende instructies af te bouwen. Opdrachtgever dient minimaal 2 weken vooraf geïnformeerd te worden over het moment en de locatie van de toolbox.
96.	Naast V&G-plannen voor bepaalde projectfasen dient Opdrachtnemer per Nadere Overeenkomst een V&G-dossier op te stellen en actueel te houden gedurende de duur van de betreffende Nadere Overeenkomst. Het V&G-dossier beschrijft de specifieke risico's van de geleverde systemen welke samenhangen met gebruik en onderhoud van deze systemen.
97.	Het V&G-dossier voldoet ten minste aan de verplichtingen voortvloeiende uit artikel 2.30 sub c Arbeidsomstandighedenbesluit en omvat ten minste de informatie met betrekking tot integrale veiligheidsaspecten dan wel verwijzingen daarnaar ten aanzien van: a. Vastgestelde risico's; b. Beheersmaatregelen; c. Ontwerpkeuzes; d. As-built gegevens; e. Overblijvende integrale veiligheidsrisico's voor beheer en onderhoud en sloop; f. Overige relevante informatie.
98.	Opdrachtnemer dient de beschrijving van de processen met betrekking tot calamiteiten, waarmee Opdrachtnemer bewerkstelligt dat de gevolgen van een eventuele calamiteit tot een minimum beperkt worden, ter toetsing in te dienen bij Opdrachtgever voor de start van de werkzaamheden, middels een calamiteitenplan.
99.	In het calamiteitenplan dient te worden beschreven: a. geïdentificeerde mogelijke calamiteiten (scenario's); b. het tijdig signaleren van calamiteiten; c. instructies over hoe te handelen bij calamiteiten; d. coördinatie van Werkzaamheden tijdens calamiteiten, inclusief aangewezen hulpverleners en coördinatoren; e. eventuele acties ter voorkoming van escalatie en het beperken van vervolgschade; f. de bereikbaarheid voor hulpverleningsdiensten; g. de wijze van hulpverlening; h. de Beschikbaarheid van materiaal en materieel; i. communicatie met Opdrachtgever en (vaar)wegbeheerders; j. door de Opdrachtnemer te nemen maatregelen in geval van calamiteiten; k. communicatie van het calamiteitenplan aan alle betrokkenen; l. training van coördinatoren en hulpverleners; m. geplande oefeningen en toolboxmeetings.

1.17 Voorstel tot Wijziging (VtW)

100.	Zowel Opdrachtnemer als Opdrachtgever kunnen een initiatief nemen tot een Voorstel tot Wijziging (VtW) op een actieve NOK met onderliggende documenten.
101.	Opdrachtnemer dient een VtW uit te werken en schriftelijk in te dienen waarbij de volgende informatie minimaal verstrekt moet worden: a. Uniek nummer van de VtW

	b. Datum indienen c. Beknopte omschrijving van de wijziging, inclusief oorzaak en noodzaak d. Kostenonderbouwing e. Planning van de uitvoering f. Eventuele relatie met andere wijzigingen g. Relatie en impact op technische standaard en reeds opgeleverde objecten i. Tekenvelden voor akkoord / niet-akkoord Opdrachtgever
102.	Prijzen en tarieven in de Kostenonderbouwing van de VtW dienen overeen te komen met het bij inschrijving geleverde prijsinvulformulier. Bij posten waar offertes van onderaannemers of leveranciers aan ten grondslag liggen worden deze op eerste aanvraag van Opdrachtgever door Opdrachtnemer verstrekt, en wordt het gecontracteerde percentage AKWR, daar waar dat van toepassing is, apart vermeld.
103.	VtW's dienen alleen uitgevoerd te worden na vooraf gegeven schriftelijke toestemming van Opdrachtgever. Opdrachtgever heeft het recht VtW's niet goed te keuren. VtW's worden getoetst aan de betreffende Nadere overeenkomst en de Aanbestedingswet.
104.	Relatief kleine wijzigingen mogen gebundeld in één VtW worden ingediend bij Opdrachtgever.
105.	Wat wel en niet een kleine wijziging betreft wordt samen door Opdrachtgever en Opdrachtnemer vastgesteld. De administratieve last en financiële impact zijn hierbij medebepalend.
106.	VtW's, die zijn geaccordeerd door Opdrachtgever, dienen volgens de overeengekomen planning door Opdrachtnemer te worden uitgevoerd.
107.	Elke VtW wordt als issue behandeld en opgenomen in een centraal issueregister.

1.18 Cybersecurity en informatiebeveiliging (ICO)

108.	De Opdrachtnemer dient de Werkzaamheden met betrekking tot cybersecurity zodanig te verrichten dat het gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.	VSP/VSE-eisen CSIR3.103
109.	De Opdrachtnemer dient zijn procesbeschrijving (cybersecurity plan), waarmee invulling wordt gegeven aan de bovenliggende topeis en ten minste aan alle daaraan onderliggende eisen, ter kennis te brengen van de Opdrachtgever.	VSP/VSE-eisen CSIR3.104
110.	De Opdrachtnemer dient de maandelijkse rapportage van security incidenten aan te leveren conform de bijlage CSR 21 "Uniform aanleveren van incidentrapportages".	VSP/VSE-eisen CSIR3.105
111.	De Opdrachtnemer dient als onderdeel van zijn Ontwerpwerkzaamheden ten aanzien van cybersecurity een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken en ter kennis te brengen van de Opdrachtgever. In de exploitatiefase dient de Opdrachtnemer ten aanzien van cybersecurity ten minste jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken.	VSP/VSE-eisen CSIR3.106
112.	De Opdrachtnemer dient een sleutelfunctionaris aan te stellen die verantwoordelijk is voor de Werkzaamheden met betrekking tot cybersecurity.	VSP/VSE-eisen CSIR3.107
113.	De opdrachtgever dient een proces in te richten voor het ontvangen van meldingen van kwetsbaarheden van buitenaf conform de "Leidraad Coordinated Vulnerability Disclosure" van het Nationaal Cyber Security Centrum.	VSP/VSE-eisen CSIR3.108
114.	De Opdrachtnemer dient de eisen ten aanzien van cybersecurity onverkort aan te houden bij de inrichting en onderhoud van een test- en ontwikkelomgeving.	VSP/VSE-eisen CSIR3.109

115.	De Opdrachtnemer dient voor alle beheerobjecten de van toepassing verklaarde maatregelen uit de Cybersecurity Implementatierichtlijn Objecten uit te voeren die behoren bij cybersecurity weerstandsniveau 1 tenzij er voor een beheerobject een ander cybersecurity weerstandsniveau is aangegeven. Beheerobject "Bediencentrale" – cybersecurity weerstandsniveau 2 (twee) Beheerobject "Brug" - cybersecurity weerstandsniveau 1 (één)	VSP/VSE-eisen CSIR3.110
116.	Indien bijlage V "Cybersecurity Implementatierichtlijn Objecten" niet voorziet in cybersecuritymaatregelen voor de invulling van de cybersecurity eisen, dan dient de Opdrachtnemer de NEN-ISO/IEC 27002 (Code voor Informatiebeveiliging) en/of delen van de IEC 62443 standaards (Industrial Automation and Control Systems (IACS) Security) te volgen.	VSP/VSE-eisen CSIR3.111
117.	De Opdrachtnemer dient met betrekking tot het beheren en onderhouden van cybersecuritymaatregelen te handelen conform paragraaf 2.9 "Maatregelen beheer en onderhoud" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.112
118.	Indien de Opdrachtnemer tijdelijk niet aan cybersecurityeisen dreigt te voldoen, dan dient de Opdrachtnemer dit te behandelen als een afwijking in het kader van zijn kwaliteitsmanagementsysteem en dient de Opdrachtnemer deze afwijkingenrapportage ter kennis te brengen van de Opdrachtgever en op te nemen in het cybersecurity dossier.	VSP/VSE-eisen CSIR3.113
119.	De Opdrachtnemer dient ten minste één keer per jaar een audit uit te voeren naar de opzet, het bestaan en de werking van de getroffen cybersecuritymaatregelen en dient de auditrapportage ter kennis te brengen van de Opdrachtgever.	VSP/VSE-eisen CSIR3.114
120.	De Opdrachtnemer dient met betrekking tot opvolging van cybersecurity inbreuken en/of verhoogde dreiging te handelen conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 13 "Handelswijze bij SOC incident melding en verhoogde dreiging" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.115
121.	De Opdrachtnemer dient een proces met betrekking tot "incident response" te beschrijven (Incident Response Plan), conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 14 "Incident Response" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" een Incident Response Plan op te stellen.	VSP/VSE-eisen CSIR3.116
122.	De Opdrachtnemer dient de opgetreden cybersecurity incidenten te analyseren en maatregelen te treffen om herhaling te voorkomen. De Opdrachtnemer dient jaarlijks alle cybersecurity incidenten te analyseren en deze rapportage op te nemen in het cybersecurity dossier.	VSP/VSE-eisen CSIR3.117
123.	De Opdrachtnemer dient een proces inzake 'probleembeheer' te beschrijven zodanig dat security incidenten, waarvoor nog geen oplossing beschikbaar is, worden beheerst en zodanig dat op proactieve wijze nieuwe incidenten kunnen worden voorkomen en/of de gevolgen daarvan worden beperkt.	VSP/VSE-eisen CSIR3.118
124.	De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen aan het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.	VSP/VSE-eisen CSIR3.119
125.	De Opdrachtnemer dient in het kader van de Algemene verordening gegevensbescherming (AVG) Verwerkersovereenkomst (die bij aanbestedingsstukken zit en wordt getekend tegelijk met de ROK en NOK1) de persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, rechtmatig te behandelen.	VSP/VSE-eisen CSIR3.120
126.	Indien de Opdrachtnemer persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, opslaat en/of verwerkt, dan dient de Opdrachtnemer deze te behandelen in	VSP/VSE-eisen CSIR3.121

	overeenstemming met de Verwerkersovereenkomst die bij aanbestedingsstukken zit en wordt getekend tegelijk met de ROK en NOK1 een verwerkersovereenkomst af te sluiten met de Opdrachtgever conform het sjabloon "verwerkersovereenkomst" dat de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt.	
127.	Indien de Opdrachtnemer camera's inzet en/of camerabeelden opslaat, verwerkt of distribueert, dan dient de Opdrachtnemer de bijlage CSR 20 "Camera's en omgang met camerabeelden van de verkeersregistratiesystemen" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" te volgen.	VSP/VSE-eisen CSIR3.122
128.	De Opdrachtnemer dient voor de beveiliging van informatie van de Opdrachtgever en van Documenten, de door de Opdrachtgever aangegeven document-classificatie en bijbehorende beveiligingsmaatregelen aan te houden, conform de bijlage CSR 1 "Omgaan met vertrouwelijke informatie en documenten" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.123
129.	De Opdrachtnemer dient alle opdracht-gerelateerde informatie, zowel door de opdrachtgever verstrekte documenten als zelf geproduceerde informatie, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.	VSP/VSE-eisen CSIR3.124
130.	De Opdrachtnemer dient op basis van risicoanalyse maatregelen tegen spionage te nemen zodanig dat de Documenten met betrekking tot ICT en IA, waaronder documentatie, offertes, contracten, IP-tabellen, netwerkschema's, modellen, tekeningen en berekeningen, zijn beveiligd tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging.	VSP/VSE-eisen CSIR3.125
131.	De Opdrachtnemer dient uiterlijk bij beëindiging van de Overeenkomst alle Documenten en door de Opdrachtgever ter beschikking gestelde informatie die kwetsbaarheden kunnen veroorzaken voor de Opdrachtgever over te dragen aan de Opdrachtgever. Alle informatie dient te worden vernietigd in de informatievoorziening van de Opdrachtnemer. Deze eis is ook van toepassing op een eventuele tussentijdse beëindiging van de Overeenkomst.	VSP/VSE-eisen CSIR3.126
132.	Indien de Opdrachtnemer ICT- en IA-componenten en/of de daarop aanwezige informatie verwijdt, hergebruikt en/of vernietigt, dan dient hij te handelen conform de bijlage CSR 23 "Verwijdering en vernietiging van informatie en apparatuur" van bijlage V "Cybersecurity Implementatierichtlijn objecten".	VSP/VSE-eisen CSIR3.127
133.	De Opdrachtnemer dient met betrekking tot bewustwording en training van (zelfstandige) hulppersonen, voor zover relevant voor hun functie, cybersecuritymaatregelen te treffen conform paragraaf 2.7 "Maatregelen Bewustwording en Training" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.128
134.	De Opdrachtnemer dient Werkzaamheden aan het ontwerp, beheer en onderhoud evenals de gevoelige informatie en documentatie van de beheerobjecten en de hieraan gerelateerde ICT en IA door (zelfstandige) hulppersonen te laten verrichten die een geheimhoudingsverklaring hebben ondertekend en over een Verklaring Omtrent het Gedrag (VOG) beschikken die gerelateerd is aan de beoogde Werkzaamheden. In afwachting van het resultaat van de aanvraag van een VOG kan gedurende een periode van maximaal zes weken na start van de betreffende Werkzaamheden, welke termijn niet kan worden verlengd, worden volstaan met een eigen verklaring van de (zelfstandige) hulppersoon.	VSP/VSE-eisen CSIR3.129

135.	De Opdrachtnemer dient voor de toegang tot beheerobjecten de bijlage CSR 2 "Personele Toegang" van bijlage V "Cybersecurity Implementatierichtlijn objecten" te volgen.	VSP/VSE-eisen CSIR3.130
136.	De Opdrachtnemer draagt er zorg voor dat zijn (zelfstandige) hulppersonen de huis- en gedragsregels zoals vastgelegd in de bijlage CSR 17 "Beveiligingshuisregels" van bijlage V "Cybersecurity Implementatierichtlijn Objecten", kennen en naleven.	VSP/VSE-eisen CSIR3.131
137.	Indien de Opdrachtnemer toegang tot ICT en IA op afstand (remote access) wenst, dan dient de Opdrachtnemer deze toegang via de centrale, beveiligde en gemonitorde voorzieningen van de Opdrachtgever te laten verlopen.	VSP/VSE-eisen CSIR3.132
138.	Indien de Opdrachtnemer toegang tot ICT en IA op afstand (remote access) wenst, dan dient de Opdrachtnemer een aanvraag in te dienen conform de procedure beschreven in "Aanvraagformulier Netwerktogang voor Derden", die de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt.	VSP/VSE-eisen CSIR3.133
139.	De Opdrachtnemer dient te zorgen voor een procedure en actuele registratie van: 1. de door de Opdrachtnemer aan de (zelfstandige) hulppersonen verstrekte logische toegang tot ICT en IA door middel van accounts, autorisaties en bijbehorende middelen; 2. de fysieke toegang van de (zelfstandige) hulppersonen tot ICT en IA gerelateerde ruimten.	VSP/VSE-eisen CSIR3.134
140.	De (beheer)processen voor de fysieke beveiliging van het terrein en gebouwen hierbinnen dienen conform paragraaf 2.1.2 "Fysieke beveiliging terrein en gebouwen" en CSR 24 "Fysieke beveiligingsmaatregelen" ingevuld te worden.	VSP/VSE-eisen CSIR3.135
141.	De Opdrachtnemer dient met betrekking tot fysieke toegangsbeveiliging van de ICT en IA gerelateerde ruimten (waaronder bedien- en technische ruimten) binnen beheerobjecten cybersecuritymaatregelen te treffen conform paragraaf 2.1.1 "Maatregelen fysieke toegangsbeveiliging IA-gerelateerde ruimten" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.136
142.	De Opdrachtnemer dient met betrekking tot de logische toegang tot ICT en IA en de fysieke toegang tot ICT en IA gerelateerde ruimten conform paragraaf 2.2 "Maatregelen Logische Toegang" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen.	VSP/VSE-eisen CSIR3.137
143.	De Opdrachtnemer dient voor een zorgvuldige omgang met de aan hem toevertrouwde accounts en bijbehorende wachtwoorden te handelen conform de bijlage CSR 7 "Wachtwoorden" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.138
144.	De Opdrachtnemer dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot beheerobjecten, data, ICT en IA) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.	VSP/VSE-eisen CSIR3.139
145.	De Opdrachtnemer dient alle door de Opdrachtgever ter beschikking gestelde bedrijfsmiddelen nadat ze niet meer van dienst zijn geworden doch uiterlijk bij beëindiging van de Overeenkomst terug te geven.	VSP/VSE-eisen CSIR3.140
146.	De Opdrachtnemer dient met betrekking tot het datanetwerk te handelen conform paragraaf 2.4.1 "Netwerkkoppelingen" en conform de bijlage CSR 3 "Architectuur objectnetwerk" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.141

147.	De Opdrachtnemer dient met betrekking tot datanetwerkkoppelingen cybersecuritymaatregelen te treffen conform paragraaf 2.4.1 "Netwerkkoppelingen" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.142
148.	Indien de Opdrachtnemer cryptografie inzet ter bescherming van vertrouwelijkheid, authenticiteit en/of integriteit van Documenten en informatie, dan dient hij cybersecuritymaatregelen te treffen conform paragraaf 2.4.2 "Cryptografie" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.143
149.	De Opdrachtnemer dient bij koppeling van randapparatuur aan de ICT en IA van de Opdrachtgever de bijlage CSR 4 "Het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" aan te houden voor bescherming tegen malware.	VSP/VSE-eisen CSIR3.144
150.	De Opdrachtnemer dient maximale hardening toe te passen voor zijn (rand)apparatuur en (delen van) zijn eigen datanetwerkinfrastructuur die ten behoeve van de Werkzaamheden gekoppeld zijn aan de datanetwerkinfrastructuur van de Opdrachtgever.	VSP/VSE-eisen CSIR3.145
151.	De Opdrachtnemer dient met betrekking tot het kunnen koppelen aan het SOC van de Opdrachtgever, cybersecuritymaatregelen te treffen conform paragraaf 2.6 "Maatregelen logging en monitoring" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.146
152.	Indien er sprake is van een koppeling van (delen van) het datanetwerk van de Opdrachtnemer aan het datanetwerk van de Opdrachtgever, dan dient de Opdrachtnemer zijn medewerking te verlenen aan het risicogestuurd (laten) (pen)testen van (delen van) zijn datanetwerk.	VSP/VSE-eisen CSIR3.147
153.	Indien er sprake is van een koppeling van (delen van) het datanetwerk van de Opdrachtnemer aan het datanetwerk van de Opdrachtgever, dan dient de Opdrachtnemer zijn medewerking te verlenen aan het risicogestuurd (laten) monitoren van (delen van) zijn datanetwerk.	VSP/VSE-eisen CSIR3.148
154.	De Opdrachtnemer dient voor het ontwikkelen en/of het onderhouden van software de gangbare principes en de voorgeschreven maatregelen uit het document "Grip op Secure Software Development (SSD) Beveiligingseisen voor (web)applicaties" van het Centrum Informatiebeveiliging en Privacybescherming (CIP) te volgen.	VSP/VSE-eisen CSIR3.149
155.	De Opdrachtnemer dient voor het intellectueel eigendomsrecht, gebruiksrecht en Escrow van software voor ICT en IA de bijlage CSR 19 "Intellectueel Eigendom" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te volgen. Opdrachtgever bepaalt op basis van een risico afweging tot inzet van Escrow.	VSP/VSE-eisen CSIR3.150
156.	De Opdrachtnemer dient met betrekking tot het doorvoeren van Wijzigingen aan bestaande ICT en IA cybersecuritymaatregelen te treffen conform paragraaf 2.8 "Maatregelen gecontroleerd wijzigen" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.151
157.	De Opdrachtnemer dient zijn medewerking te verlenen aan het (laten) pentesten en (laten) uitvoeren van (geautomatiseerde) kwetsbaarheidsscans van de ICT en IA door de Opdrachtgever.	VSP/VSE-eisen CSIR3.152
158.	De Opdrachtnemer dient met betrekking tot het patchen van de ICT en IA te handelen conform paragraaf 2.5.3 "Maatregelen bescherming tegen kwetsbaarheden" en conform de bijlage CSR 8 "Patch management" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.153
159.	Indien de Opdrachtnemer meent geen gebruik te maken van de mogelijkheid om te patchen, dan dient hij een gemotiveerd voorstel ter kennis te brengen van de Opdrachtgever.	VSP/VSE-eisen CSIR3.154

160.	Indien de Opdrachtgever melding maakt van een patch dan dient de Opdrachtnemer daarvoor een implementatieadvies ter kennis te brengen van de Opdrachtgever. Daarbij gelden de volgende doorlooptijden: 1. voor een kritieke patch: maximaal 48 uur na melding door de Opdrachtgever, gerekend vanaf de eerstvolgende werkdag; 2. voor een niet kritieke patch: maximaal twee maanden na melding door de Opdrachtgever. De Opdrachtnemer dient de patch, na Acceptatie door de Opdrachtgever van het implementatieadvies, conform het advies te implementeren.	VSP/VSE-eisen CSIR3.155
161.	Indien ICT en IA niet beschermd worden door antimalware oplossingen, dan dient de Opdrachtnemer ten minste jaarlijks te scannen op malware en aangetroffen malware te verwijderen, conform de bijlage CSR 11 "Malware scanning en opschoning middels een usb" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.156
162.	De Opdrachtnemer dient het door de Opdrachtgever ter beschikking gestelde template cybersecurity beveiligingsplan of dossier op te bouwen en actueel te houden en op verzoek te leveren aan de Opdrachtgever.	VSP/VSE-eisen CSIR3.157
163.	De Opdrachtnemer dient alle configurations items (CI's) van de ICT en IA te registreren in een door de Opdrachtgever beschikbaar gesteld Excel format en te leveren aan de Opdrachtgever, conform de bijlage CSR 16 "Registratie assets in een configuratiemanagement database (CMDB)" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.158
164.	De Opdrachtnemer dient conform bijlage CSR 15 "Recoveryplan" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" aan de Opdrachtgever een recoveryplan ter beschikking te stellen, waarmee tevens een succesvolle cyberaanval op de ICT en IA (assume breach) wordt afgedekt.	VSP/VSE-eisen CSIR3.159
165.	De Opdrachtnemer dient een protocol voor back-up en recovery ter beschikking te stellen aan de Opdrachtgever, conform paragraaf 2.10 "Maatregelen Back-ups" en conform de bijlage CSR 18 "Back-up en Recovery" van de bijlage V "Cybersecurity Implementatierichtlijn Objecten".	VSP/VSE-eisen CSIR3.160
166.	De Opdrachtnemer dient een continuïteitsplan te ontwikkelen en te onderhouden om voorbereid te zijn op de gevolgen van onderbreking van nutsvoorzieningen (stroomuitval) voor de ICT en IA conform de bijlage CSR 12 "Continuïteitsplan voor energievoorziening".	VSP/VSE-eisen CSIR3.161
167.	De Opdrachtnemer dient minimaal jaarlijks de ontwikkelde continuïteitsplannen uit te voeren om te bewerkstelligen dat ze actueel en doeltreffend blijven.	VSP/VSE-eisen CSIR3.162
168.	Indien de Opdrachtnemer Werkzaamheden door zelfstandige hulppersonen wil laten verrichten, dan dient de Opdrachtnemer een quickscan uit te voeren conform de handleiding "Quickscan nationale veiligheid bij inkoop en aanbesteden" en het resultaat ter kennis te brengen van de Opdrachtgever.	VSP/VSE-eisen CSIR3.163
169.	De Opdrachtnemer dient in zijn projectmanagementplan specifiek voor de opdracht de projectorganisatie te beschrijven, waarin ten minste de leidinggevende functies en sleutelfuncties zijn weergegeven met hun taken, verantwoordelijkheden en bevoegdheden.	VSP/VSE-eisen CSIR3.164
170.	De Opdrachtnemer dient in zijn projectmanagementplan specifiek voor de opdracht de processen te beschrijven, gebruikmakende van procesbeschrijvingen conform het(de) gecertificeerde kwaliteitsmanagementsysteem(en), waarbij ten minste invulling wordt gegeven aan de in de Overeenkomst gestelde proceseisen en waarmee de Opdrachtnemer aantoont dat deze processen het vermogen hebben om het beoogde resultaat te bereiken;	VSP/VSE-eisen CSIR3.165

171.	De Opdrachtnemer vereist dat zijn (zelfstandige) hulppersonen de cybersecurity eisen en maatregelen toepassen in overeenstemming met de vastgestelde beleidsregels en procedures.	VSP/VSE-eisen CSIR3.166
172.	De Opdrachtnemer dient de cybersecurity eisen integraal onderdeel te maken van het projectmanagementsysteem en/of Information Security Management Systeem (ISMS).	VSP/VSE-eisen CSIR3.167
173.	De Opdrachtnemer dient het projectmanagementsysteem met geplande tussenpozen te beoordelen, om te bewerkstelligen dat dit bij voortduring geschikt, passend en doeltreffend is.	VSP/VSE-eisen CSIR3.168
174.	De Opdrachtnemer dient te meten, te analyseren en te verbeteren zodanig dat het projectmanagementsysteem doeltreffend functioneert.	VSP/VSE-eisen CSIR3.169
175.	De Opdrachtnemer dient negatieve bevindingen en tekortkomingen die door de Opdrachtgever zijn geconstateerd en gemeld aan de Opdrachtnemer, af te handelen op gelijke wijze als afwijkingen die door de Opdrachtnemer zijn geconstateerd.	VSP/VSE-eisen CSIR3.170
176.	De Opdrachtnemer dient de zelfstandige hulppersonen te managen, zodanig dat wordt gewaarborgd dat de door zelfstandige hulppersonen verrichte Werkzaamheden en de resultaten daarvan voldoen aan de eisen voortvloeiende uit de Overeenkomst.	VSP/VSE-eisen CSIR3.171